Arrêté n° 2043 CM du 18 octobre 2018 relatif à la dématérialisation des actes des autorités administratives et aux téléservices

(NOR : ADN1822077AC-1)
Paru in extenso au journal officiel n°76 NS du 08/11/2018 à la page 5718 dans la partie ARRETES DU CONSEIL DES MINISTRES

Version en vigueur au 08/11/2018

Le Président de la Polynésie française,
Sur le rapport du ministre de la modernisation de l'administration, en charge de l'énergie et du numérique,
Vu la loi organique n° 2004-192 du 27 février 2004 modifiée portant statut d'autonomie de la Polynésie française, ensemble la loi n° 2004-193 du 27 février 2004 complétant le statut d'autonomie de la Polynésie française ;
Vu l'arrêté n° 650 PR du 23 mai 2018 portant nomination du vice-président et des ministres du gouvernement de la Polynésie française, et déterminant leurs fonctions ;
Vu l'arrêté n° 1167 CM du 23 août 2013 modifié relatif à la création, l'organisation et le fonctionnement de la direction générale de l'économie numérique (DGEN) ;
Vu la loi du pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices ;
Le conseil des ministres en ayant délibéré dans sa séance du 17 octobre 2018,

Arrête :

SECTION I - DES ECHANGES DE DONNEES ELECTRONIQUES ENTRE UNE AUTORITE ADMINISTRATIVE ET SES USAGERS DANS LE CADRE D'UN TELESERVICE

Article 1er

Tout envoi à une autorité administrative par voie électronique dans le cadre d'un téléservice fait l'objet d'un accusé de réception électronique tel que prévu à l'article LP. 14 de la loi du pays susvisée. Ce dernier comporte notamment les mentions suivantes :

- la date de réception de l'envoi électronique effectué par l'usager ;

- la désignation, l'adresse postale, et le cas échéant électronique, ainsi que le numéro de téléphone du service de l'autorité administrative chargé du dossier ;

- la possibilité offerte au demandeur de se voir délivrer une attestation ;

- dans le cas où la demande de l'usager est susceptible de donner lieu à une décision implicite de rejet ou d'acceptation, la date à laquelle, à défaut d'une décision expresse, celle-ci sera considérée comme acceptée ou rejetée ;

- dans le cas où la demande de l'usager est susceptible de donner lieu à une décision implicite de rejet, les délais et les voies de recours à l'encontre de la décision.

Art. 2

Lorsqu'une saisine par le biais d'un téléservice est incomplète, l'accusé de réception doit indiquer les pièces et informations manquantes exigées par les textes législatifs et règlementaires en vigueur, ainsi que le délai fixé pour la réception de celles-ci.

Le délai au terme duquel, à défaut de décision expresse, une demande est réputée acceptée ne court qu'à compter de la réception des pièces et des informations manquantes requises.

Le délai au terme duquel, à défaut de décision expresse, une demande est réputée rejetée est suspendu pendant le délai imparti pour produire les pièces et informations manquantes requises. Toutefois, la production de ces pièces et informations avant l'expiration du délai fixé met fin à cette suspension.

Le service d'une autorité administrative mentionne également à l'intéressé le délai prévu, selon les cas, au deuxième ou au troisième alinéa du présent article.

Art. 3

Si la délivrance de l'accusé de réception électronique n'est pas instantanée, un accusé d'enregistrement électronique, qui indique le jour et l'heure de réception, est adressé à l'usager dans le délai d'un (1) jour ouvré. L'accusé de réception

électronique est ensuite envoyé, par le service d'une autorité administrative compétente, dans un délai de sept (7) jours ouvrés à compter de l'enregistrement de l'envoi.

Art. 4

L'accusé d'enregistrement électronique et l'accusé de réception électronique sont adressés à l'intéressé à l'adresse électronique qu'il a utilisé pour effectuer son envoi. L'intéressé déclare que l'adresse électronique communiquée est fiable et utilisée par ses soins.

SECTION II - DE LA SECURITE DES ECHANGES ELECTRONIQUES ENTRE LES AUTORITES ADMINISTRATIVES ET ENTRE UNE AUTORITE ADMINISTRATIVE ET SES USAGERS

Art. 5

Le référentiel général de sécurité prévu à l'article LP. 20 de la loi du pays susvisée est approuvé. Le référentiel figure à l'annexe I du présent arrêté.

Il est tenu à jour par la direction générale de l'économie numérique et est rendu disponible en ligne sur le site internet officiel : www.lexpol.pf.

Art. 6

Dans les conditions fixées par le référentiel général de sécurité susmentionné, l'autorité administrative visée à l'article LP. 1er doit, afin de protéger son système d'information, conformément à l'état de l'art en matière de sécurité de l'information :

1° Identifier l'ensemble des risques pesant sur la sécurité du système et des informations qu'il traite, eu égard notamment aux conditions d'emploi du système ;

2° Fixer les objectifs de sécurité, notamment en matière de disponibilité et d'intégrité du système, de confidentialité et d'intégrité des informations ainsi que d'identification des utilisateurs du système, pour répondre de manière proportionnée au besoin de protection du système et des informations face aux risques identifiés ;

3° Et en déduire les fonctions de sécurité et leur niveau qui permettent d'atteindre ces objectifs et respecter les règles correspondantes du référentiel général de sécurité.

Dans les conditions fixées par le référentiel susmentionné, l'autorité administrative réexamine la sécurité du système et des informations en cas de besoin ou en fonction de l'évolution des risques.

Art. 7

Suite à l'analyse des risques prévue à l'article précédent, le service de l'autorité administrative peut être amené à devoir recourir à des produits de sécurité et à des prestataires de services de confiance qualifiés figurant à l'annexe III du présent arrêté.

Dans les cas où le service de l'autorité administrative ne recourt pas à des produits de sécurité ou des prestataires de service de confiance qualifiés malgré les conclusions de l'analyse des risques, il remplit le formulaire qui figure en annexe II du présent arrêté, afin de motiver son choix, et verse ce document au dossier d'homologation lors de la procédure d'homologation visée aux articles 8 à 11 du présent arrêté.

Art. 8

Dans le cadre de l'article LP. 21 de la loi du pays susvisée, le service de l'autorité administrative procède à l'homologation de son système d'information en se référant au guide annexé au référentiel général de sécurité.

Art. 9

La décision d'homologation est prononcée par l'autorité d'homologation.

Pour les services administratifs de la Polynésie française, l'autorité d'homologation est le Président de la Polynésie française. Ce dernier peut déléguer cette compétence au vice-président et aux ministres du gouvernement de la Polynésie française.

Pour les autres autorités administratives, telles que les établissements publics du pays, les autorités administratives indépendantes, les organismes de protection sociale et les autres organismes et personnes de droit public et de droit privé chargés d'une mission de service public administratif, la compétence se situe au niveau du responsable hiérarchique de la structure qui peut la déléguer. L'homologation de sécurité ne demeure valide que tant que le système d'information est exploité dans le contexte décrit dans le dossier d'homologation. Les changements prévus dans le guide d'homologation impliquent un réexamen du dossier, pouvant conduire à une nouvelle décision d'homologation ou à un retrait de la décision.

Art. 10

L'autorité d'homologation est assistée par une commission d'homologation. Celle-ci est chargée de préparer la décision d'homologation.

Le nombre de membres, la composition et la gouvernance de cette commission sont adaptés à la nature du système d'information et sont proportionnés à ses enjeux.

Dans le cadre de l'instruction relative à l'homologation et de son suivi, la commission d'homologation est notamment chargée du suivi des plannings et de l'analyse de l'ensemble des documents versés au dossier d'homologation.

La composition et le fonctionnement de la commission d'homologation figurent à l'annexe D du référentiel général de

sécurité.

Art. 11

Le service de l'autorité administrative rend accessible l'attestation d'homologation de son système d'information et/ou de son téléservice, selon les mêmes modalités que celles prévues à l'article LP. 12 de la loi du pays susvisée.

Art. 12

La liste de référence des produits de sécurité et des prestataires de services de confiance qualifiés mentionnée à l'article LP. 22 de la loi du pays susvisée est approuvée.

La liste figure à l'annexe III du présent arrêté.

Elle est tenue à jour par la direction générale de l'économie numérique et est rendue disponible en ligne sur le site internet officiel : www.lexpol.pf.

SECTION III - EFFETS JURIDIQUES

PARAGRAPHE I - DES PRESTATAIRES ET DES SERVICES DE CONFIANCES

Art. 13

Les informations visées à l'article LP. 35 de la loi du pays susvisée sont vérifiées par le prestataire de services de confiance qualifié :

1° Par la présence en personne de la personne physique ou du représentant dûment désigné de la personne morale ;

2° Ou au moyen d'un certificat de signature électronique qualifié ou d'un cachet électronique qualifié délivré conformément au point 1°.

Art. 14

La liste des prestataires de services de confiance qualifiés mentionnée à l'article LP. 40 de la loi du pays susvisée est approuvée.

La liste figure à l'annexe IV du présent arrêté.

Elles sont tenues à jour par la direction générale de l'économie numérique et disponibles en ligne sur le site internet officiel : www.lexpol.pf.

Art. 15

Le référentiel d'exigences des services de confiance qualifiés prévu à l'article LP. 41 de la loi du pays susvisée est approuvé.

Le référentiel figure à l'annexe V du présent arrêté.

Il est tenu à jour par la direction générale de l'économie numérique et est rendu disponible en ligne sur le site internet officiel : www.lexpol.pf.

PARAGRAPHE II - DE LA COPIE NUMÉRIQUE

Art. 16

Est présumée fiable et opposable à des fins probatoires et conservatoires, au sens du deuxième alinéa de l'article LP. 43 de la loi du pays susvisée, la copie numérique résultant :

- soit d'un procédé de reproduction qui entraîne une modification irréversible du support de la copie ;

- soit, en cas de reproduction par voie électronique, d'un procédé électronique qui répond aux conditions prévues aux articles 17 à 21 du présent arrêté.

Art. 17

Le procédé de reproduction par voie électronique doit produire des informations liées à la copie et destinées à l'identification de celle-ci. Elles précisent le contexte de la numérisation, en particulier la date et l'heure de création de la copie.

La qualité du procédé doit être établie par des tests sur des documents similaires à ceux reproduits et vérifiée par des contrôles.

Art. 18

L'intégrité de la copie résultant d'un procédé de reproduction par voie électronique est attestée par une empreinte électronique qui garantit que toute modification ultérieure de la copie à laquelle elle est attachée est détectable.

Cette condition est présumée remplie par l'usage d'un horodatage qualifié, d'un cachet électronique qualifié ou d'une signature électronique qualifiée, au sens de la loi du pays susvisée.

Art. 19

La copie électronique est conservée, archivée dans des conditions propres à éviter toute altération, toute modification et

atteinte à l'intégrité de sa forme ou de son contenu.

Les opérations requises pour assurer la lisibilité de la copie électronique dans le temps ne constituent pas une altération de son contenu ou de sa forme dès lors qu'elles sont tracées et donnent lieu à la génération d'une nouvelle empreinte électronique de la copie, dans les mêmes conditions de sécurité que l'empreinte réalisée initialement.

Art. 20

Les empreintes et les traces générées en application des articles 18 et 19 du présent arrêté sont conservées aussi longtemps que la copie électronique produite et dans des conditions ne permettant pas leur modification.

Art. 21

L'accès aux dispositifs de reproduction et de conservation décrit aux articles 17 à 20 du présent arrêté fait l'objet de mesures de sécurité appropriées et qui sont conformes à l'état de l'art.

Art. 22

Les dispositifs et mesures prévues aux articles 17 à 21 du présent arrêté sont décrits dans une documentation conservée aussi longtemps que la copie électronique produite.

SECTION IV - REFERENTIEL GENERAL D'ACCESSIBILITE

Art. 23

Le référentiel général d'accessibilité prévu à l'article LP. 45 de la loi du pays susvisée est approuvé.

Le référentiel figure à l'annexe VI du présent arrêté.

Il est tenu à jour par la direction générale de l'économie numérique et est rendu disponible en ligne sur le site internet officiel : www.lexpol.pf.

SECTION V - REFERENTIEL GENERAL D'INTEROPERABILITE

Art. 24

Le référentiel général d'interopérabilité prévu à l'article LP. 46 de la loi du pays susvisée est approuvé.

Le référentiel figure à l'annexe VII du présent arrêté.

Il est tenu à jour par la direction générale de l'économie numérique et est rendu disponible en ligne sur le site internet officiel : www.lexpol.pf.

Art. 25

Le ministre de la modernisation de l'administration, en charge de l'énergie et du numérique, est chargé de l'exécution du présent arrêté qui sera publié au Journal officiel de la Polynésie française.

Fait à Papeete, le 18 octobre 2018.

Par le Président de la Polynésie française :
Edouard FRITCH.

Le ministre de la modernisation
de l'administration,
Priscille Tea FROGIER.

Liste des annexes relatif à la dématérialisation des actes des autorités administratives et aux téléservices

Liste des annexes de l’arrêté CM relatif à la dématérialisation des actes des autorités administratives et aux téléservices

ANNEXE I: **Référentiel Général de Sécurité** (RGS) accompagné du guide d'homologation et l'annexe au guide d'homologation ;

Documents applicables concernant l'utilisation de certificats électroniques

Annexe A 1 - Règles relatives à la mise en œuvre des fonctions de sécurité basées sur l'emploi de certificats électroniques

Annexe A 2 - Politique de Certification Type "certificats électroniques de personne"

Annexe A 3 - Politique de Certification Type "certificats électroniques de services applicatifs"

Annexe A 4 - Profils de Certificats / LCR / OCSP et Algorithmes Cryptographiques

Annexe A 5 - Politique d'Horodatage Type

Documents applicables concernant l'utilisation de mécanismes cryptographiques

Annexe B 1 - Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques

Annexe B 2 - Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques

Annexe B 3 - Règles et recommandations concernant les mécanismes d'authentification

Référentiel d'exigences applicables aux prestataires d'audit de la SSI

Annexe C - Référentiel d'exigences applicables aux prestataires d'audit de la SSI

Guide d'homologation

Annexe D - Guide d'homologation

ANNEXE II : Formulaire de motivation de non-recours à des produits de sécurité ou des prestataires de services de confiance qualifiés

ANNEXE III: Liste de référence des prestataires de services de confiance qualifiés et des produits de sécurité

ANNEXE IV: Liste nationale des prestataires de services de confiance qualifiés e-IDAS

ANNEXE V: Référentiel d'exigences

Annexe A 1 – Références documentaires

Annexe A 2 – Liste des spécifications techniques recommandées relatives aux signatures et cachets électroniques avancés

Annexe A 3 – Profils de certificats recommandés

ANNEXE VI: Référentiel général d'accessibilité pour les administrations de la Polynésie française (RGAA PF) - Introduction

Annexe VI Bis – RGAA PF - Guide d'accompagnement

Annexe VI Ter – RGAA PF - Référentiel technique

Annexe VI Quater – RGAA PF – Glossaire

ANNEXE VII: Référentiel général d'interopérabilité (RGI PF)

ANNEXE 1

Référentiel général de sécurité

Historique des versions		
Date	**Version**	**Évolution du document**
	1.0	Publication de la première version du référentiel général de sécurité

Avant-propos

Le présent référentiel est pris en application de l'article LP 20 de la loi de pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices, et de son arrêté d'application.

Le présent document et ses annexes sont une copie adaptée du référentiel général de sécurité en vigueur en métropole, version 2.0 du 13 juin 2014 et du guide d'homologation de sécurité en neuf étapes de l'Agence nationale de la sécurité des systèmes d'information[1] (ANSSI).

Le texte fait des renvois à des documents publiés par l'ANSSI ou encore disponibles sur son site internet www.ssi.gouv.fr, en ce qu'ils reflètent l'état de l'art en matière de sécurité de l'information.

Le référentiel et ses annexes sont disponibles en ligne sur le site internet www.lexpol.pf et leur mise à jour est assurée par la Direction générale de l'économie numérique.

Le présent document propose :

- D'une part une méthodologie orientée autour de la responsabilisation des autorités vis-à-vis de leurs systèmes d'information (ci-après SI) à travers la démarche d'homologation ;
- D'autre part des règles et bonnes pratiques que doivent mettre en œuvre les administrations lorsqu'elles recourent à des prestations et produits spécifiques : certification et horodatage électroniques, audit de sécurité, produits de sécurité.

Il comprend les règles permettant aux autorités administratives de garantir aux usagers et aux autres administrations un niveau de sécurité de leurs systèmes d'information adapté aux enjeux et risques liés à la cybersécurité.

Il intègre ainsi les principes et règles liés à :

- La description des étapes de la mise en conformité ;
- La cryptologie et à la protection des échanges électroniques ;
- La gestion des accusés d'enregistrement et des accusés de réception.

La notion de Système d'information ou SI désigne l'ensemble des composants d'un système informatique, de ses composants réseaux et télécoms, qu'il soit interne ou externe à l'autorité administrative et offrant des services

- Aux agents d'une autorité administrative dans le cadre d'échange avec d'autres agents d'une autre autorité administrative
- Aux usagers des services de l'autorité administrative quand ses derniers sont dématérialisés

[1] L'ANSSI est un service à compétence nationale rattaché au Secrétaire général de la défense et de la sécurité nationale, l'autorité chargée d'assister le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale. Parmi ses nombreux objectifs, l'un deux consiste à promouvoir un espace de confiance pour les services en ligne. Elle y participe en ce sens notamment au travers de la règlementation (référentiels) et ses labels (certification des produits de sécurité et qualification des produits de sécurité et des prestataires de service de confiance).

Sommaire

Chapitre 1. Mise en conformité avec les exigences de la loi du pays relative à la dématérialisation des actes des autorités administratives et aux téléservices

Le référentiel général de sécurité (RGS) vise à renforcer la confiance des usagers dans les téléservices proposés par les autorités administratives, notamment lorsque ceux-ci traitent des données personnelles. Il s'applique aux systèmes d'information mis en œuvre par les autorités administratives dans leurs relations entre elles et avec les usagers. Il peut aussi être considéré comme un recueil de bonnes pratiques pour tous les autres organismes.

Afin de mettre leur système d'information en conformité avec le RGS, les autorités administratives doivent adopter une démarche en cinq étapes, prévue par les articles 6 et 8 de l'arrêté relatif à la dématérialisation des actes des autorités administratives et aux téléservices :

1. réalisation d'une analyse des risques ;
2. définition des objectifs de sécurité ;
3. choix et mise en œuvre des mesures appropriées de protection et de défense du SI ;
4. homologation de sécurité du système d'information ;
5. suivi opérationnel de la sécurité du SI.

Dans l'éventualité où le système d'information serait déjà en service sans avoir fait l'objet de cette démarche, ou bien a été modifié, la procédure simplifiée suivante peut être mise en œuvre :

1. réalisation d'un audit de la sécurité du système d'information en interne ou externalisé auprès d'un prestataire ;
2. réalisation d'une analyse des risques simplifiée ;
3. mise en œuvre des mesures correctives fixées dans le rapport d'audit ;
4. homologation de sécurité du système d'information ;
5. suivi opérationnel de la sécurité du SI.

Au-delà des mesures techniques et organisationnelles, les autorités administratives doivent veiller :

- aux clauses relatives à la sécurité des contrats qu'elles passent avec des prestataires chargés de les assister dans leur démarche de sécurisation de leurs systèmes d'information. Ces services peuvent être de nature intellectuelle (audit de la sécurité du système d'information, traitement d'incident de sécurité, notamment) ou technique (mécanisme de détection, externalisation, infogérance, mise dans le nuage (cloud) de tout ou partie du système d'information, tierce maintenance applicative, etc.) ;
- au facteur humain : la sensibilisation du personnel aux questions de sécurité est primordiale, ainsi que la formation de ceux qui interviennent plus spécifiquement dans la mise en œuvre et le suivi opérationnel de la sécurité du système d'information (surveillance, détection, prévention).

D'une manière générale, il est recommandé de s'appuyer sur les guides et la documentation produits par l'ANSSI, en ce que ces références reflètent l'état de l'art et les bonnes pratiques en la matière.

Chapitre 2. Description des étapes de la mise en conformité

2.1 Analyse des risques

L'analyse de risques précise les besoins de sécurité du système d'information en fonction des menaces et des enjeux.

La démarche d'analyse de risques consiste à identifier les évènements qui peuvent affecter la sécurité du système, d'en estimer les conséquences et les impacts potentiels puis de décider des actions à réaliser afin de réduire le risque à un niveau acceptable.

Les menaces[2] à prendre en compte sont celles qui pèsent réellement sur le système et sur les informations qu'il traite, transmet et stocke, dans l'environnement dans lequel il se situe.

Lorsque le système d'information intègre des certificats électroniques ou de l'horodatage électronique, l'analyse des risques doit permettre de décider des usages (signature, authentification, confidentialité, etc.) et des niveaux de sécurité (*, ** ou ***) qui seront mis en œuvre.

Il est recommandé de s'appuyer sur la norme ISO 27005, qui fixe un cadre théorique de la gestion des risques. Sa mise en œuvre pratique peut être facilitée par les explications et les outils, notamment logiciels, proposés par la méthode Expression des besoins et indentification des objectifs de sécurité (EBIOS).

2.2 Définition des objectifs de sécurité

Une fois les risques appréciés, l'autorité administrative doit énoncer les objectifs de sécurité à satisfaire. Aux trois grands domaines traditionnels (disponibilité et intégrité des données et du système, confidentialité des données et des éléments critiques du système d'information) peuvent s'ajouter deux domaines complémentaires :

- l'authentification, afin de garantir que la personne identifiée est effectivement celle qu'elle prétend être ;
- la traçabilité, afin de pouvoir associer les actions sur les données et les processus aux personnes effectivement connectées au système et ainsi permettre de déceler toute action ou tentative d'action illégitime.

Les objectifs de sécurité doivent être exprimés aussi bien en termes de protection que de défense des systèmes d'information. Les autorités administratives peuvent s'appuyer sur le guide méthodologique EBIOS, afin de formuler précisément ces objectifs de sécurité qui définissent les buts à atteindre pour amener un risque identifié à un niveau acceptable, en agissant sur l'attractivité, la faisabilité, la vulnérabilité ou les impacts.

2.3 Choix et mise en œuvre des mesures de sécurité adaptées

L'expression des objectifs de sécurité permet d'apprécier les fonctions de sécurité qui peuvent être mises en œuvre pour les atteindre (art. 6 de l'arrêté relatif à la dématérialisation des actes des autorités administratives et aux téléservices). Ces fonctions de sécurité sont matérialisées par le choix de moyens et de mesures de nature :

- Technique : produits de sécurité (matériels ou logiciels), prestations de services de confiance informatiques ou autres dispositifs de sécurité (blindage, détecteur d'intrusion...) ;
- Organisationnelle : organisation des responsabilités (habilitation du personnel, contrôle des accès, protection physique des éléments sensibles...), gestion des ressources humaines (affectation d'agents responsables de la gestion du système d'information, formation du personnel spécialisé, sensibilisation des utilisateurs).

Ces mesures de sécurité peuvent être sélectionnées au sein des référentiels et normes existants. Elles peuvent également en être adaptées ou bien être créées ex nihilo.

2.4 Homologation de sécurité du système d'information

Les systèmes d'information qui entrent dans le champ de la loi du pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices doivent faire l'objet, avant leur mise en service opérationnelle, d'une décision d'homologation de sécurité (article LP 21 de la loi du pays susvisée).

Elle est prononcée par une autorité d'homologation, désignée par la ou les autorités administratives chargées du système d'information. La durée de validité de l'homologation ne peut excéder 5 ans.

La décision d'homologation atteste, au nom de l'autorité administrative, que le système d'information est protégé conformément aux objectifs de sécurité fixés et que les risques résiduels sont acceptés. La décision d'homologation s'appuie sur un dossier d'homologation. Lorsqu'elle concerne un téléservice, cette décision est rendue accessible aux usagers.

Conformément à cette logique de responsabilisation et en application de l'article 7 de l'arrêté relatif à la dématérialisation des actes des autorités administratives et aux téléservices, les autorités administratives sont tenues de justifier le non recours à des produits de sécurité ou des prestataires de services de confiance qualifiés. Dans ce cadre, elles sont tenues de verser au dossier d'homologation le formulaire de motivation de non-recours à des produits de sécurité ou des prestataires de services de confiance qualifiés figurant à l'annexe II de l'arrêté relatif à la dématérialisation des actes des autorités administratives et aux téléservices.

Il est recommandé que les systèmes d'information homologués fassent l'objet d'une revue périodique.

Afin d'homologuer leurs systèmes d'information, les autorités administratives recourent, conformément à l'article 8 de l'arrêté relatif à la dématérialisation des actes des autorités administratives et aux téléservices, au guide d'homologation annexé au présent document [RGS_D].

2.5 Suivi opérationnel de la sécurité du système d'information

Les mesures de protection d'un système d'information doivent être accompagnées d'un suivi opérationnel quotidien ainsi que de mesures de surveillance et de détection, afin de réagir au plus tôt aux incidents de sécurité et de les traiter au mieux.

Le suivi opérationnel consiste à collecter et à analyser les journaux d'évènements et les alarmes des composants techniques des SI, à mener des audits réguliers, à appliquer des mesures correctives après un audit ou un incident de sécurité, à mettre en œuvre une chaîne d'alerte en cas d'intrusion supposée ou avérée sur le système d'information, à gérer les droits d'accès des utilisateurs, à maitriser les comptes à privilèges, à assurer une veille sur les menaces et les vulnérabilités, à entretenir des plans de continuité et de reprise d'activité, à sensibiliser le personnel et à gérer les crises lorsqu'elles surviennent.

Chapitre 3. Règles relatives à la cryptographie et à la protection des échanges électroniques

Les règles techniques imposées par le RGS portent uniquement sur la sécurisation des infrastructures utilisées pour procéder aux échanges électroniques entre les autorités administratives et les usagers ainsi qu'entre les autorités administratives elles-mêmes.

Le RGS n'impose aucune technologie particulière et laisse aux autorités administratives le choix des mesures à mettre en œuvre. Il fixe cependant des exigences relatives à certaines fonctions de sécurité, notamment la certification, l'horodatage et l'audit.

En fonction de leur besoin de sécurité, issu de l'analyse de risques, il appartient aux autorités administratives de déterminer les fonctions de sécurité ainsi que les niveaux de sécurité associés, en s'appuyant sur les méthodes, les outils et les bonnes pratiques proposés aux chapitres 2 à 6.

Lorsqu'elles choisissent de mettre en œuvre des fonctions de sécurité traitées dans le présent chapitre, les autorités administratives choisissent le niveau de sécurité adapté à leur besoin et appliquent les règles correspondantes décrites dans ce référentiel. Dans tous les cas, il est recommandé l'usage de produits qualifiés quand ils existent et lorsqu'ils sont disponibles en Polynésie française.

3.1 Règles relatives à la cryptographie

Lorsqu'elles mettent en place des mesures de sécurité comprenant des mécanismes cryptographiques, les autorités administratives doivent respecter les règles, et si possible les recommandations, indiquées dans les annexes [RGS_B1] et [RGS_B2], communs à tous les mécanismes cryptographiques, ainsi que l'annexe [RGS_B3], dédié aux mécanismes d'authentification.

3.2 Règles relatives à la protection des échanges électroniques

Les règles de sécurité à respecter pour les fonctions de sécurité d'authentification, de signature électronique, de confidentialité et d'horodatage, reposent sur l'emploi de contremarques de temps dans le cas de l'horodatage électronique et de certificats électroniques pour toutes les autres fonctions.

a. Règles relatives aux certificats électroniques

Les exigences concernant le composant « *certificat électronique* » sont décrites dans deux annexes du RGS appelées respectivement « *Politique de certification type - Personne physique* » ([RGS_A2]) et « *Politique de certification type - Services applicatifs* » ([RGS_A3]). Elles portent sur le contenu des certificats et sur les conditions dans lesquelles il est émis par un prestataire de services de certification électronique (PSCE), ainsi que sur le dispositif de stockage de la clé privée.

Le RGS offre la possibilité de disposer :

- des certificats mono-usage à usage d'authentification de personne physique ou de serveur, de signature, de cachet et de confidentialité pour des niveaux une étoile (*), deux étoiles (**) et trois étoiles (***) (cf. [RGS_A2] et [RGS_A3]) ;
- d'un certificat électronique unique, dit « à double usage », pour les fonctions d'authentification de personne physique et de signature électronique. Ce certificat ne peut être prévu qu'aux niveaux (*) et (**) (cf. [RGS_A2]).

a.1 L'authentification d'une entité par certificat électronique

L'authentification[2] a pour but de vérifier l'identité dont se réclame une personne ou une machine.

[2] S'identifier consiste à communiquer une identité préalablement enregistrée, s'authentifiée consiste à apporter la preuve de cette identité. L'authentification est généralement précédée d'une identification.

La mise en œuvre par une autorité administrative des fonctions de sécurité « *Authentification* » ou « *Authentification serveur* » peut se faire selon trois niveaux de sécurité aux exigences croissantes : (*), (**) et (***).

Ces exigences, décrites dans les annexes [RGS_A1], couvrent, pour les trois niveaux de sécurité, l'ensemble des composants nécessaires à la mise en œuvre de cette fonction de sécurité, à savoir :

- la bi-clé et le certificat électronique dont l'usage est l'authentification ;
- le dispositif d'authentification ;
- le module de vérification d'authentification ;
- l'application d'authentification.

a.2 La signature et le cachet électroniques

La signature électronique d'une personne permet de garantir l'identité du signataire, l'intégrité du document signé et le lien entre le document signé et la signature. Elle traduit ainsi la manifestation du consentement du signataire quant au contenu des informations signées.

Dans le cas des échanges dématérialisés faisant intervenir des services applicatifs, la fonction de « *cachet* » permet de garantir l'intégrité des informations échangées et l'identification du service ayant « cacheté » ces informations. Cette fonction de « *cachet* » est, pour une machine, l'équivalent de la fonction signature pour une personne.

La mise en œuvre par une autorité administrative des fonctions de sécurité « Signature électronique » ou « cachet » peut se faire selon trois niveaux de sécurité aux exigences croissantes : (*), (**) et (***). Ces exigences, décrites dans l'annexe [RGS_A1], couvrent, pour les trois niveaux de sécurité, l'ensemble des composants nécessaires à la mise en œuvre de cette fonction de sécurité, à savoir :

- la bi-clé et le certificat électronique dont l'usage est la signature électronique ou le cachet ;
- le dispositif de création de signature électronique ou de cachet ;
- l'application de création de signature électronique ou de cachet ;
- le module de vérification de signature électronique ou de cachet.

Cas particulier de la signature des décisions des autorités administratives au sens de la loi du pays susvisée :

Conformément à l'article LP 4 de la loi du pays susvisée, les autorités administratives doivent respecter les exigences du RGS lorsqu'elles mettent en œuvre, pour la signature de leurs décisions, des systèmes d'information utilisant des fonctions de sécurité décrites dans le RGS (certificats électroniques, audit, etc.).

L'autorité administrative détermine le niveau de sécurité, de une étoile (*) à trois étoiles (***), requis pour l'usage de la signature électronique des actes administratives qu'elle émet. Elle doit respecter les règles définies au présent chapitre.

Néanmoins, par dérogation à l'article LP 4 de la loi du pays susvisée, sont dispensés de la signature de leur auteur les décisions émanant des autorités administratives qui sont notifiées aux usagers par l'intermédiaire d'un téléservice ainsi que les actes préparatoires à ces actes ou à ces décisions ; dès lors qu'ils comportent les prénom, nom, qualité de leur auteur, ainsi que la mention du service auquel il appartient (article LP 19 de la loi du pays susvisée).

a.3 La confidentialité

Le chiffrement constitue le mécanisme essentiel de protection de la confidentialité. Cependant, la confidentialité des informations peut aussi être protégée par des mesures complémentaires de gestion des droits d'accès de chacun (en lecture, en écriture ou en modification) aux données contenues dans le système d'information. À cet effet, il est recommandé de mettre en place des mécanismes techniques afin de

s’assurer que seules les personnes autorisées puissent accéder aux données en fonction de leur besoin d’en connaître. Ces mécanismes doivent être robustes et implémentés au plus près du lieu de stockage des données.

La mise en œuvre par une autorité administrative de la fonction de sécurité « Confidentialité » peut se faire selon trois niveaux de sécurité aux exigences croissantes : (*), (**) et (***).

Ces exigences, décrites dans l’annexe [RGS_A1], couvrent, pour les trois niveaux de sécurité, l’ensemble des composants nécessaires à la mise en œuvre de cette fonction de sécurité, à savoir :

- la bi-clé et le certificat électronique dont l’usage est le chiffrement ;
- le dispositif de chiffrement ;
- le module de chiffrement ;
- le module de déchiffrement.

b. Règles relatives à l’horodatage électronique

Les exigences concernant le composant « *contremarque de temps* » sont décrites dans l’annexe du RGS« *Politique d’horodatage type* » ([RGS_A5]). Elles portent sur le contenu des contremarques de temps et sur les conditions dans lesquelles il est émis par un prestataire de services d’horodatage électronique (PSHE).

Une fonction d’horodatage permet d’attester qu’une donnée sous forme électronique existe à un instant donné. Cette fonction met en œuvre une contremarque de temps générée à l’aide d’un mécanisme cryptographique respectant les règles et, si possible, les recommandations contenues dans les référentiels [RGS_B1] et [RGS_B2].

Cette contremarque, délivrée par un *prestataire de services d’horodatage électronique* (PSHE), doit respecter les exigences de l’annexe [RGS_A5], appelée « *Politique d’horodatage type* ». Cette annexe ne distingue qu’un niveau unique de sécurité, auquel les autorités administratives doivent se conformer dès lors qu’elles souhaitent mettre en œuvre la fonction d’horodatage électronique au sein de leur système d’information.

Chapitre 4. Règles relatives aux accusés d'enregistrement et aux accusés de réception

L'article LP 14 de la loi du pays susvisée prévoit que les accusés d'enregistrement et les accusés de réception sont émis selon un procédé conforme au RGS. Ces accusés ne constituent pas en eux-mêmes des fonctions de sécurité. En revanche, ils peuvent s'appuyer sur des fonctions de sécurité telles que la signature, le cachet et l'horodatage.

Les accusés d'enregistrement et de réception sont générés et émis par les autorités administratives à destination des usagers. Les autorités administratives doivent déterminer les fonctions de sécurité nécessaires à la protection de ces accusés ainsi que leur niveau de sécurité.

Dans le cas général, il est recommandé que les accusés d'enregistrement et de réception émis en application des dispositions prévues à l'article LP 14 de la loi du pays susvisée :

- soient horodatés avec des contremarques de temps conformes aux exigences du document [RGS_A_5] pour le niveau de sécurité unique prévu par ce document ;
- soient signés par un agent d'une autorité administrative (ou cachetés par une machine d'une autorité administrative), conformément aux exigences des documents [RGS_A_2] et [RGS_A_3] pour le niveau de sécurité choisi par l'autorité administrative parmi les niveaux (*), (**) et (***) ;
- utilisent des mécanismes cryptographiques conformes aux référentiels [RGS_B_1] et [RGS_B_2].

S'agissant de la gestion des accusés, la sauvegarde des accusés d'enregistrement et de réception doit être assurée dans tous les cas, tant que peuvent survenir d'éventuelles réclamations de la part des usagers.

Chapitre 5. Qualification des produits de sécurité et des prestataires de services de confiance

Les autorités administratives recourent à des produits de sécurité et à des prestataires de services de confiance qualifiés ou à tout autre produit ou prestataire non qualifiés pour autant qu'elles estiment que ces derniers répondent à leurs besoins de sécurité.

Dans le premier cas, les autorités administratives se réfèrent à la liste de référence des produits et prestataires de services de confiance qualifiés approuvée par l'article 12 de l'arrêté relatif à la dématérialisation des actes des autorités administratives et aux téléservices.

Dans le second cas, les autorités administratives sont tenues de verser au dossier d'homologation le formulaire de motivation de non recours à des produits de sécurité ou des prestataires de services de confiance qualifiés figurant à l'annexe II de l'arrêté relatif à la dématérialisation des actes des autorités administratives et aux téléservices.

Conformément à l'article LP 22 de la loi du pays susvisée, cette qualification correspond à la qualification délivrée par les autorités de métropole en application de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

De ce fait, pour être qualifié en Polynésie française, un produit de sécurité ou un prestataire de services de confiance doit au préalable avoir obtenu la qualification délivrée sur la base de l'ordonnance n° 2005-1516 du 8 décembre 2005 susvisée.

Dès lors, un produit de sécurité ou un prestataire de services de confiance qualifiés en Polynésie française conformément à l'article LP 22 de la loi du pays susvisée respecte les exigences prévues par les annexes du présent document.

5.1 Qualification des produits de sécurité

Pour mémoire, la qualification délivrée par les autorités de métropole relative aux produits de sécurité prévoit trois niveaux de qualification :

- Qualification élémentaire ;
- Qualification standard ;
- Qualification renforcée.

5.2 Qualification des prestataires de services de confiance (PSCO)

Pour mémoire, la qualification délivrée par les autorités de métropole relative aux PSCO peut concerner différentes catégories distinctes :

- Les prestataires de services de certification électronique (PSCE) ;
- Les prestataires de services d'horodatage électronique (PSHE) ;
- Les prestataires d'audit de la sécurité des systèmes d'information (PASSI).

Chapitre 6. Recommandations relatives à l'application du référentiel

Au-delà de l'analyse de risques et de l'homologation, il est recommandé d'adopter de bonnes pratiques relatives à la méthodologie, aux procédures et à l'organisation.

6.1 Organiser la sécurité des systèmes d'information

a. Organiser les responsabilités liées à la sécurité des systèmes d'information

Les autorités administratives doivent mettre en œuvre une organisation qui endosse les responsabilités liées à la sécurité des systèmes d'information.

De préférence dirigée par un représentant de l'autorité administrative, cette organisation doit disposer des moyens matériels nécessaires à la réalisation de ses missions et de la capacité à gérer les risques, les crises ou les incidents qui pourraient en résulter. Le cas échant, elle s'appuie sur une chaîne fonctionnelle SSI chargée de l'assister dans le pilotage, la gestion et le suivi des moyens SSI : le responsable de la sécurité des systèmes d'information (RSSI), le correspondant SSI, etc.

Éventuellement à l'aide de la chaîne fonctionnelle SSI, l'organisation mise en place par l'autorité administrative peut assurer les missions suivantes :

- Coordination des actions permettant l'intégration des clauses liées à la SSI dans les contrats ou les conventions impliquant un accès par des tiers à des informations ou à des ressources informatiques ;
- Formalisation de la répartition des responsabilités liées à la SSI (définition des périmètres de responsabilité, des délégations de compétences, etc.) ;
- Établissement des relations nécessaires avec les autorités externes de défense des systèmes d'information, notamment pour la gestion des intrusions et des attaques sur les systèmes.

b. Mettre en place un système de management de la sécurité des systèmes d'information

Il est recommandé de mettre en œuvre des processus permettant de rechercher une amélioration constante de la SSI. Par exemple, la mise en place d'un système de management de la sécurité de l'information (SMSI), tel que défini dans la norme ISO 27001, permet non seulement de planifier et de mettre en œuvre les mesures de protection du système d'information, mais également d'en vérifier la pertinence et la conformité par rapport aux objectifs établis.

c. Élaborer une politique de sécurité des systèmes d'information

Il est recommandé d'élaborer et de formaliser une politique de sécurité des systèmes d'information (PSSI). Elle peut être générale ou déclinée en fonction des besoins spécifiques de chaque domaine de chaque système d'information. Le guide « *Politique SSI* » de l'ANSSI fournit une aide pour son élaboration ainsi que le « *Guide d'hygiène informatique* » de l'ANSSI.

6.2 Impliquer les instances décisionnelles

Les instances décisionnelles des autorités administratives doivent être impliquées dans la sécurisation des systèmes d'information dont elles ont *in fine* la responsabilité, afin de donner les orientations adéquates, notamment en termes d'investissement humain et financier, et de valider les objectifs de sécurité et les orientations stratégiques. La norme ISO 27001 fournit, à titre indicatif, une liste de sujets susceptibles d'être traités au niveau de la direction d'une autorité administrative.

6.3 Adapter l'effort de protection des systèmes d'information aux enjeux de sécurité et prendre en compte la SSI dans les projets

La sécurité d'un système d'information doit être adaptée aux enjeux du système lui-même et aux besoins de sécurité de l'autorité administrative, afin d'y consacrer les moyens financiers et humains nécessaires et suffisants. Dans ce but, il est recommandé d'utiliser les guides de l'ANSSI « Maturité SSI » et « Gestion et *intégration de la SSI dans les projets* » (GISSIP) et « *Intégrer la sécurité numérique en démarche Agile* ».

Ils permettent, dans le cadre du développement d'un projet de système d'information, de déterminer les enjeux relatifs à la sécurité et d'identifier l'ensemble des livrables relatifs à la SSI.

6.4 Adopter une démarche globale

L'ensemble de la démarche de sécurisation des systèmes d'information doit procéder d'une volonté cohérente et globale, afin d'éviter la dispersion des efforts des équipes en charge de la SSI ou la mise en œuvre de mesures de sécurité parcellaires. Chaque décision doit être prise au juste niveau hiérarchique. Il est ainsi recommandé :

- de prendre en considération tous les aspects qui peuvent affecter la SSI, qu'ils soient techniques (matériels, logiciels, réseaux) ou non (organisations, infrastructure, personnel) ;
- d'envisager tous les risques et menaces, quelle que soit leur origine ;
- de prendre en compte la SSI à tous les niveaux hiérarchiques. La SSI repose sur une vision stratégique et nécessite des choix d'autorité (enjeux, moyens humains et financiers, risques résiduels acceptés) ainsi qu'un contrôle des actions et de leur légitimité ;
- de responsabiliser tous les acteurs (décideurs, maîtrise d'ouvrage et d'œuvre, utilisateurs) ;
- d'intégrer la SSI tout au long du cycle de vie des systèmes d'information (depuis l'étude d'opportunité jusqu'à la fin de vie du système).

D'une manière similaire, la sécurité doit être prise en compte dès la phase de définition des objectifs fonctionnels des systèmes d'information, afin de :

- Limiter les surcoûts inhérents à l'application tardive de mesures de sécurité ;
- Garantir l'efficacité des mesures mises en œuvre ;
- Favoriser l'appropriation de la sécurité par les équipes en charge du SI.

6.5 Informer et sensibiliser le personnel

L'ensemble des agents d'une autorité administrative, et le cas échant les contractants et les utilisateurs tiers, doivent suivre une formation adaptée sur la sensibilisation et recevoir régulièrement les mises à jour des politiques et des procédures qui concernent leurs missions. Cette formation doit permettre de réduire les risques liés à la méconnaissance des principes de base et des règles élémentaires de bonne utilisation de l'outil informatique.

La sensibilisation du personnel doit être régulière. À cet effet, il est recommandé de suivre les bonnes pratiques publiées par l'ANSSI pour l'application de principes de base en matière de sécurité des systèmes d'information : www.ssi.gouv.fr/fr/bonnes-pratiques/principes-generaux.

6.6 Prendre en compte la sécurité dans les contrats et les achats

Les exigences de sécurité relatives aux produits ou aux prestations acquis doivent faire l'objet d'une étude et doivent être clairement formalisées et intégrées dans les dossiers d'appels d'offres, au même titre que les exigences fonctionnelles, réglementaires, de performance ou de qualité.

Ces exigences peuvent concerner le système qui fait l'objet de la consultation, mais aussi la gestion du projet lui-même (formation ou habilitation des personnels), en incluant les phases opérationnelles et de maintenance. Il convient notamment de :

- Veiller à intégrer aux règlements de consultation ou aux cahiers des charges les référentiels de l'ANSSI applicables (produits certifiés, qualifiés, agréés…) ;
- Demander à ce que les produits de sécurité soient fournis avec l'ensemble des éléments permettant d'en apprécier le niveau de sécurité ;
- Préciser les clauses relatives à la maintenance des produits acquis dans les contrats ainsi que les délais d'intervention avec des pénalités ;
- Préciser les clauses concernant les conditions de l'intervention et de l'accès physique et logique des sous-traitants ainsi que des garanties de confidentialité et de sécurité concernant les sous-traitants (clauses dites de porte-fort) avec leurs localisations :

- Préciser les clauses garantissant la qualité et la sécurité des prestations et produits fournis ;
- Préciser les conditions de propriété des codes sources et/ou les éventuels droits d'accès auxdits codes sources ;
- Prévoir, le cas échéant, la réversibilité des prestations et la portabilité des données générées pendant celles-ci en s'assurant en particulier que les bases de données sont extractibles, que celle-ci peut être distinguée du système lui-même et que les formats utilisés sont ouverts ;
- Préciser la nature et les modalités de réalisation des indicateurs pertinents, des tableaux de bord et mécanismes de suivi des prestations de sécurité ;
- Prévoir les modalités de réaction aux crises et aux incidents susceptibles d'affecter le système ;
- Prévoir des points de contact compétents à même de répondre aux besoins des autorités administratives ;
- Vérifier, dans les réponses à appel d'offres, la couverture des exigences sécurité inscrites dans la consultation.
- Avoir une politique concernant la gestion des habilitations (sécurité des accès, etc.), la protection des données à caractère personnel
- Les garanties doivent être en adéquation avec le projet et la responsabilité conforme au droit commun.
- Prévoir une possibilité de continuité de service en cas d'arrêt du produit.

Une attention particulière devra être portée aux mécanismes de validation et de recette des composants mettant en œuvre les exigences de sécurité.

6.7 Prendre en compte la sécurité dans les projets d'externalisation et d'informatique en nuage

Le recours à l'externalisation ou à « l'informatique en nuage » présente des risques spécifiques qu'il convient d'évaluer avant d'aborder une telle démarche. Ces risques peuvent être liés au contexte même de l'opération d'externalisation ou à des spécifications contractuelles déficientes ou incomplètes. Dans cette hypothèse, il est recommandé d'appliquer les prescriptions décrites dans le guide de l'ANSSI « *Maîtriser les risques de l'infogérance – Externalisation des systèmes d'information* ». Ce guide fournit :

- une démarche cohérente de prise en compte des aspects SSI lors de la rédaction du cahier des charges d'une opération d'externalisation ;
- un ensemble de clauses types ainsi qu'une base d'exigences de sécurité, à adapter et à personnaliser en fonction du contexte particulier de chaque projet d'externalisation.

6.8 Mettre en place des mécanismes de défense des systèmes d'information

En complément des mécanismes de protection des systèmes d'information, et en fonction de leurs enjeux de sécurité, les autorités administratives doivent adopter des mesures complémentaires relatives à la défense des systèmes d'information. Ces mesures consistent, en particulier, à assurer :

- la connaissance des systèmes exploités par l'autorité administrative, ou en relation avec elle (cartographie des SI, répertoire des interconnexions, etc.) ;
- la détection des malveillances, des erreurs et des imprudences, en périphérie ou à l'intérieur des systèmes d'informations des autorités administratives ;
- la traçabilité des actions et des accès réalisés sur les systèmes d'information (journalisation, notamment) ;
- la pérennisation des savoir-faire et des compétences, notamment en termes d'exploitation des SI ;
- la conservation de la preuve des infractions découvertes.

6.9 Utiliser les produits et prestataires labellisés pour leur sécurité

La qualification permet d'attester de la conformité des produits de sécurité et des prestataires de services de confiance à un niveau de sécurité du référentiel RGS. En Polynésie française, cette qualification correspondant à la qualification délivrée par les autorités de métropole en application de l'ordonnance n°

2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

Ainsi, il est recommandé aux autorités administratives :

- d'utiliser chaque fois que possible des produits de sécurité et des PSCO qualifiés selon les dispositions du chapitre 5 ;
- de prendre en considération, pour le choix des prestataires, en plus de leur qualification, leur éventuelle certification selon la norme ISO 27001 ou d'autres normes équivalentes ;
- de prendre en considération, pour le choix de prestataires, la certification de leurs personnels lorsque des compétences particulières sont requises pour une fonction.

6.10 Élaborer des plans de traitement d'incidents ainsi que de continuité et de reprise d'activité

Les autorités doivent se préparer à faire face à des incidents de sécurité pour lesquels toutes les mesures préventives auraient échoué. A ce titre, elles doivent mettre en œuvre un plan de continuité d'activité et un plan de reprise d'activité qui identifient les moyens et les procédures nécessaires pour revenir à une situation nominale le plus rapidement possible, en cas d'incident grave. Ces documents doivent être régulièrement mis à jour. Les plans et les procédures qui en découlent doivent faire l'objet de tests réguliers.

6.11 Procéder à des audits réguliers de la sécurité du système d'information

Les autorités administratives doivent réaliser ou faire réaliser des audits réguliers de leurs SI. À cet effet, le référentiel d'exigences relatif aux prestataires d'audit de la sécurité des systèmes d'information (annexe C du RGS) fixe les règles que doivent respecter les prestataires tiers qui réalisent des audits de la sécurité des systèmes d'information des autorités administratives. Cette annexe décrit également des recommandations à l'intention des commanditaires d'audits, dans le cadre de la passation de marchés publics ou d'un accord contractuel, ainsi qu'aux prestataires d'audit dans le cadre de leur devoir de conseil, d'information et de mise en garde.

Afin de s'assurer qu'elles recourent à des prestataires qui respectent ces exigences, les autorités administratives doivent, autant que possible, faire appel à des prestataires ayant obtenu une qualification, selon les dispositions du chapitre 5.

6.12 Réaliser une veille sur les menaces et les vulnérabilités

Se tenir informé sur l'évolution des menaces et des vulnérabilités, en identifiant les incidents qu'elles favorisent ainsi que leurs impacts potentiels, constitue une mesure fondamentale de défense. Les sites institutionnels, comme celui du CERT-FR (www.cert.ssi.gouv.fr), ou ceux des éditeurs de logiciels et de matériels constituent des sources d'information essentielles sur les vulnérabilités identifiées, ainsi que sur les contre-mesures et les correctifs éventuels. Les mises à jour des logiciels et d'autres équipements, les correctifs des systèmes d'exploitation et des applications font l'objet d'alertes et d'avis qu'il est indispensable de suivre.

6.13 Favoriser l'interopérabilité

L'administration électronique ne saurait évoluer sans une prise en compte des règles relatives à l'interopérabilité et à la mise en cohérence des différents systèmes d'information des autorités administratives et de leurs partenaires (usagers, acteurs industriels, etc.). L'interopérabilité est en particulier traitée à travers le Référentiel général d'interopérabilité.

6.14 Appliquer des mesures respectueuses de la protection des données à caractère personnel

Les mesures de sécurité choisies pour répondre aux objectifs de sécurité doivent impérativement répondre aux exigences du respect de la vie privée des agents d'une autorité administrative et des usagers. La mise en œuvre d'un système de surveillance d'un système d'information d'un téléservice comme la collecte des données de connexion ou d'usages d'un système d'information d'un téléservice doivent s'inscrire dans les

mesures et dispositions de la réglementation en vigueur, notamment les exigences de la réglementation relatives aux données à caractère personnel.

Chapitre 7. Liste des annexes du RGS

Ces documents sont consultables à l'adresse www.lexpol.pf.

7.1 Documents applicables concernant l'utilisation de certificats électroniques

[RGS_A1] Règles relatives à la mise en œuvre des fonctions de sécurité basées sur l'emploi de certificats électroniques, version 1.0

[RGS_A2] Politique de Certification Type « certificats électroniques de personne », version 1.0

[RGS_A3] Politique de Certification Type « services applicatifs », version 1.0

[RGS_A4] Profils de certificats, CRL, OCSP et algorithmes cryptographiques, version 1.0

[RGS_A5] Politique d'Horodatage Type, version 1.0

7.2 Documents applicables concernant l'utilisation de mécanismes cryptographiques

[RGS_B1] Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.0

[RGS_B2] Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 1.0

[RGS_B3] Règles et recommandations concernant les mécanismes d'authentification, version 1.0

7.3 Référentiel d'exigences applicables aux prestataires d'audit de la SSI

[RGS_C] Référentiel d'exigences applicables aux prestataires d'audit de la SSI, version 1.0

7.4 Guide d'homologation

[RGS_D] Guide d'homologation, version 1.0

Chapitre 8. Références techniques

[ISO27001] ISO/CEI 27001 :2013, Technologies de l'information – Systèmes de management de la sécurité de l'information – Exigences.

[ISO27002] ISO/CEI 27002:2013, Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour le management de la sécurité de l'information.

[ISO27005] ISO/CEI 27005:2011, Technologies de l'information – Techniques de sécurité – Gestion des risques liés à la sécurité de l'information.

[ISO27035] ISO/CEI 27035:2011, Technologies de l'information – Techniques de sécurité – Gestion des incidents de sécurité de l'information.

[PCI-DSS] PCI (Payment Card Industry) Data Security Standard – Conditions et procédures d'évaluation de sécurité, version 3.0 d'octobre 2013.

[PSSI] Guide « Politique SSI » de l'ANSSI. Disponible en ligne : www.ssi.gouv.fr/fr/bonnes-pratiques/outils-methodologiques/pssi-guide-d-elaboration-de-politiques-de-securite-des-systemes-d-information.html

[Maturité SSI] Guide « maturité SSI » de l'ANSSI. Disponible en ligne :

www.ssi.gouv.fr/fr/bonnes-pratiques/outils-methodologiques/guide-relatif-a-la-maturite-ssi.html

[EBIOS 2010] Méthode d'analyse de risque de l'ANSSI. Disponible en ligne :

www.ssi.gouv.fr/fr/bonnes-pratiques/outils-methodologiques/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite.html

[GISSIP] Guide « Gestion et Intégration de la SSI dans les Projets » de l'ANSSI :

www.ssi.gouv.fr/fr/bonnes-pratiques/outils-methodologiques/gissip-guide-d-integration-de-la-securite-des-systemes-d-information-dans-les.html

[Guide Maîtriser les risques de l'infogérance – Externalisation des systèmes Externalisation] d'information. Disponible en ligne :

www.ssi.gouv.fr/IMG/pdf/2010-12-03_Guide_externalisation.pdf

[GHI] Guide d'hygiène informatique. Janvier 2017. Disponible sur :

www.ssi.gouv.fr/IMG/pdf/guide_hygiene_informatique_anssi.pdf

[CC] Common Criteria for Information Technology Security Evaluation.

Annexe A 1

Règles relatives à la mise en œuvre des fonctions de sécurité basées sur l'emploi de certificats électroniques

Historique des versions		
Date	**Version**	**Évolution du document**
	1.0	Publication de la première version de l'annexe A1 du référentiel général de sécurité

Avant-propos

Le présent référentiel est pris en application de l'article LP 20 de la loi du pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices, et de son arrêté d'application.

Le présent document et ses annexes sont une copie adaptée du RGS_A1 – Règles relatives à la mise en œuvre des fonctions de sécurité basées sur l'emploi de certificats électroniques, en vigueur en métropole, version 3.0 du 27 février 2014.

Le texte fait des renvois à des documents publiés par l'Agence nationale de la sécurité des systèmes d'information1 (ANSSI) ou encore disponibles sur son site internet www.ssi.gouv.fr, en ce qu'ils reflètent l'état de l'art en matière de sécurité informatique.

Le référentiel et ses annexes sont disponibles en ligne sur le site internet www.dgen.pf, et leur mise à jour est assurée par la Direction générale de l'économie numérique.

[1] L'ANSSI est un service à compétence nationale rattaché au Secrétaire général de la défense et de la sécurité nationale, l'autorité chargée d'assister le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale. Parmi ses nombreux objectifs, l'un d'eux consiste à promouvoir un espace de confiance pour les services en ligne. Elle y participe en ce sens notamment au travers de la règlementation (référentiels) et ses labels (certification des produits de sécurité et qualification des produits de sécurité et des prestataires de service de confiance).

I. Objet et contenu du document

Le présent document fait partie des documents constitutifs du Référentiel Général de Sécurité [RGS]. Il en constitue l'annexe A1].

Il fixe les règles de sécurité applicables aux différents « composants » nécessaires à la mise en œuvre des fonctions de sécurité basées sur l'emploi des certificats électroniques et décrites dans le [RGS].

Ces fonctions de sécurité sont les suivantes :

- signature électronique ;
- authentification de personne ;
- double usage signature électronique et authentification ;
- confidentialité ;
- cachet ;
- authentification de serveur.

Ces composants sont les suivants :

- les bi-clés et certificats électroniques délivrés par des prestataires de service de certification électronique pour les usages listés ci-dessus ;
- le dispositif de protection des éléments secrets ;
- les applications qui assurent l'interface avec les usagers (ou les machines), les dispositifs de protection et les éléments secrets.

Il s'adresse aux autorités administratives (AA) qui ont décidé, après analyse des risques, de mettre en œuvre, pour un niveau de sécurité donné parmi *, ** et ***, l'une ou plusieurs des fonctions de sécurité du [RGS] précisées ci-dessus.

Les règles spécifiques à une fonction de sécurité donnée seront précédées du nom de la fonction de sécurité entre « [] » (exemple [Signature électronique]). De la même manière, les règles applicables aux certificats électroniques délivrés à des personnes seront précédées par [Personne] et celles applicables aux services applicatifs par [Service applicatif].

II. Présentation des fonctions de sécurité

II.1. Fonction de sécurité « signature électronique »

La signature électronique est l'une des fonctions de sécurité apportant de la confiance dans les échanges dématérialisés entre usagers et autorités administratives ou entre autorités administratives.

Dans le cadre du [RGS] et de son utilisation dans l'administration, les types de relations couverts par le service de signature sont notamment les suivants :

- signature électronique par un usager, puis vérification de cette signature par un téléservice d'une autorité administrative accessible par voie électronique ;
- signature électronique par un usager, puis vérification de cette signature par un agent d'une autorité administrative ;
- signature électronique par un agent d'une autorité administrative, puis vérification de cette signature par un usager ;
- signature électronique par un agent d'un acte administratif puis vérification de cette signature par un autre agent.

La signature électronique peut être requise et mise en œuvre lorsque l'usager est en relation avec une application d'échange dématérialisé depuis un outil informatique.

Le recours à la signature électronique est nécessaire tant à l'expression du consentement qu'à la validité des actes administratifs établis sous forme électronique.

Le principe de fonctionnement et d'interaction des composants entre eux est le suivant : l'application de création de signature, déployée sur une machine (PC, borne publique, serveur...) peut réaliser les premières itérations de calcul d'un condensat, à l'aide d'une fonction de hachage, à partir des informations à signer ;

- elle transmet les informations nécessaires à la réalisation de la signature (informations à signer complètes ou partielles, condensat partiel le cas échéant) au dispositif de création de signature (exemples : carte à puce, clé USB) également connecté à la machine.
- le dispositif de création de signature réalise les itérations restantes (a minima la dernière itération) du calcul du condensat, à l'aide d'une fonction de hachage, à partir des informations transmises par l'application de création de signature ; le dispositif de signature réalise un calcul cryptographique de signature du condensat en utilisant la clé privée de signature de l'agent ou de l'usager, activée le cas échéant par un code d'activation (code PIN par exemple) ;
- ce condensat signé, dit signature électronique, est retourné à l'application ;
- la vérification de la signature s'effectue à l'aide d'un module de vérification de signature et du certificat électronique délivré par PSCE qui lie l'identité de l'agent ou de l'usager avec sa clé publique : un calcul cryptographique est effectué à l'aide de la clé publique sur la signature électronique et comparé au condensat obtenu par hachage des informations à signer.

Dans le cadre du [RGS], l'utilisation de la clé privée de signature du porteur et du certificat mono-usage

associé est strictement limitée à la signature électronique[2]. Étant précisé que cette clé privée est personnelle au porteur qu'il soit usager ou qu'il soit un agent.

II.2. Fonction de sécurité « confidentialité »

La confidentialité est l'une des fonctions de sécurité apportant de la confiance dans les échanges dématérialisés entre usagers et autorités administratives ou entre autorités administratives.

Dans le cadre du [RGS] et de son utilisation dans l'administration, les types de relations couverts par la fonction de sécurité « Confidentialité » sont notamment les suivants :

- chiffrement de données électroniques, par un service d'une autorité administrative, à destination d'un usager ou d'un agent d'une autorité administrative ;
- chiffrement de données électroniques, par un service, à destination d'un agent d'une autorité
- administrative ;
- chiffrement de données électroniques, par un usager ou un agent, à destination d'un agent d'une autorité administrative.

Le chiffrement permet d'assurer que les données échangées ne seront accessibles, lors de l'échange ou de leur stockage, que par le ou les destinataires de ces données.

Un tel chiffrement peut être requis et mis en œuvre lorsque, par exemple, l'usager est en relation avec une application d'échange dématérialisé depuis un outil informatique et que les informations échangées nécessitent d'être protégées en confidentialité en raison de leur sensibilité.

Le principe de fonctionnement typique d'interaction des composants entre eux pour mettre en œuvre la fonction de sécurité « Confidentialité » est le suivant :

- le chiffrement des données échangées entre un émetteur et un destinataire est effectué in fine à l'aide d'une clé symétrique dite « clé de session « ;
- elle est elle-même échangée de façon confidentielle entre l'émetteur et le destinataire, en ayant recours soit à un mécanisme cryptographique asymétrique soit à un mécanisme de type Diffie-Hellman. Le module de chiffrement de l'utilisateur utilise la clé publique du destinataire pour réaliser un calcul cryptographique. Cette clé publique est trouvée dans le certificat électronique du destinataire délivré par un PSCE. Le résultat est transmis au destinataire ;
- le destinataire déchiffre ce résultat à l'aide de sa clé privée confinée dans un dispositif de stockage par l'intermédiaire d'un module de déchiffrement.

Il est également possible de ne pas recourir à une clé de session symétrique pour effectuer le chiffrement de données : les données peuvent être chiffrées directement avec la clé publique du destinataire et déchiffrées par lui à l'aide de sa clé privée.

Dans le cadre du [RGS], l'utilisation de la clé privée de déchiffrement du porteur et du certificat mono-usage associé est strictement limitée au service de confidentialité.

[2] L'utilisation de certificats électroniques dits « double usage » (authentification et signature) tels que décrits dans le document [RGS_A2] est également tolérée.

II.3. Fonction de sécurité « authentification »

L'authentification est l'une des fonctions de sécurité apportant de la confiance dans les échanges dématérialisés entre usagers et autorités administratives ou entre autorités administratives.

Dans le cadre du [RGS] et de son utilisation dans l'administration, les types de relations couverts par le service d'authentification sont notamment les suivants :

- authentification d'un usager vis-à-vis d'un service de l'administration accessible par voie électronique,
- authentification d'un usager vis-à-vis d'un agent d'une autorité administrative,
- authentification d'un agent d'une autorité administrative vis-à-vis d'un usager.

Cette fonction de sécurité permet à un usager ou à un agent de s'authentifier dans le cadre des types de relations mentionnés ci-dessus. Ce document ne traite que de l'authentification basée sur des mécanismes cryptographiques asymétriques.

Le principe de fonctionnement et d'interaction des composants entre eux est le suivant :

- l'application de création de cachet, déployée sur une ou plusieurs machines calcule un condensat, à l'aide d'une fonction de hachage, à partir des informations à signer ;
- elle transmet ce condensat au dispositif de création de cachet ;
- le dispositif de création de cachet réalise un calcul cryptographique de signature du condensat en utilisant la clé privée de signature du service de création de cachet, activée le cas échéant par un code d'activation (code PIN par exemple) par le responsable du certificat de cachet ;
- ce condensat signé, dit cachet, est retourné à l'application ;
- la vérification du cachet s'effectue à l'aide d'un module de vérification de cachet et du certificat électronique délivré par PSCE qui lie l'identité du service de création de cachet avec sa clé publique : un calcul cryptographique est effectué à l'aide de la clé publique sur la signature électronique et comparé au condensat obtenu par hachage des informations à signer.

Dans le cadre du [RGS], l'utilisation de la clé privée d'authentification du porteur et du certificat mono-usage associé est strictement limitée à l'authentification[3].

II.4. Fonction de sécurité « cachet »

Le cachet, apposé par un service de création de cachet, est l'une des fonctions de sécurité apportant de la confiance dans les échanges dématérialisés entre usagers et autorités administratives ou entre autorités administratives. Le terme « cachet » est utilisé par un service applicatif, se différenciant ainsi de la « signature électronique « qui est un terme consacré réservé à une personne physique.

Dans le cadre du [RGS] et de son utilisation dans l'administration, les types de relations couverts par la fonction de sécurité « Cachet » sont notamment les suivants :

- apposition d'un cachet sur des données par un service applicatif d'une autorité administrative

[3] L'utilisation de certificats électronique dits « double usage » (à des fins d'authentification et de signature) tels que décrits dans le document [RGS_A2] est également tolérée.

et vérification de ce cachet par un usager ;

- apposition d'un cachet sur des données par un service applicatif et vérification de ce cachet par un agent d'une autorité administrative ;
- apposition d'un cachet sur des données par un service applicatif et vérification de ce cachet par un autre service applicatif.

Le principe de fonctionnement et d'interaction des composants entre eux est le suivant :

- l'application de création de cachet, déployée sur une machine (PC, borne publique, serveur...) peut réaliser les premières itérations de calcul d'un condensat, à l'aide d'une fonction de hachage, à partir des informations à signer ;
- Elle transmet les informations nécessaires à la réalisation du cachet (informations à signer complètes ou partielles, condensat partiel le cas échéant) au dispositif de création de cachet (exemples : carte à puce, clé USB) également connecté à la machine ;
- «le dispositif de création de cachet réalise les itérations restantes (a minima la dernière itération) du calcul du condensat, à l'aide d'une fonction de hachage, à partir des informations transmises par l'application de création de cachet ; ce condensat signé, dit cachet, est retourné à l'application ;
- la vérification du cachet s'effectue à l'aide d'un module de vérification de cachet et du certificat électronique délivré par PSCE qui lie l'identité du service de création de cachet avec sa clé publique : un calcul cryptographique est effectué à l'aide de la clé publique sur la signature électronique et comparé au condensat obtenu par hachage des informations à signer.

Dans le cadre du [RGS], l'utilisation de la clé privée du service de création de cachet et du certificat mono-usage associé est strictement limitée au service de cachet.

II.5. Fonction de sécurité « authentification serveur »

L'authentification d'un serveur est l'une des fonctions de sécurité apportant de la confiance dans les échanges dématérialisés entre usagers et autorités administratives ou entre autorités administratives.

Dans le cadre du [RGS] et de son utilisation dans l'administration, les types de relations couverts par le service d'authentification serveur sont notamment les suivants :

- établissement d'une session sécurisée entre un serveur d'une autorité administrative et un usager,
- établissement d'une session sécurisée entre un serveur et un agent d'une autorité administrative,
- établissement d'une session sécurisée entre deux serveurs.

Cette fonction de sécurité permet à un serveur de s'authentifier et d'établir des sessions sécurisées dans le cadre des types de relations mentionnés ci-dessus.

Le principe de fonctionnement et d'interaction des composants entre eux est le suivant :

- l'application d'authentification transmet une requête d'authentification (un « challenge ») au dispositif d'authentification dans lequel la clé privée d'authentification du serveur est confinée et protégée notamment en confidentialité ;
- le dispositif d'authentification réalise un calcul cryptographique de signature du « challenge » en utilisant la clé privée, une fois celle-ci activée par le responsable du serveur, le cas échéant à l'aide d'un code d'activation (code PIN par exemple) ;
- ce challenge signé est retourné à l'application ;

- la vérification de l'authentification s'effectue à l'aide d'un module de vérification et du certificat électronique délivré par PSCE qui lie l'identité du serveur avec sa clé publique : un calcul cryptographique « inverse » est effectué à l'aide de la clé publique sur le challenge signé et comparé au challenge initial.

Dans le cadre du [RGS], l'utilisation de la clé privée d'authentification du serveur et du certificat mono-usage associé est strictement limitée au service d'authentification et d'établissement de session sécurisée.

III. Exigences relatives à la mise en œuvre des fonctions de sécurité

Ce paragraphe regroupe toutes les exigences de sécurité, d'interopérabilité ainsi que les bonnes pratiques pour les composants participant aux fonctions de sécurité.

III.1. Les certificats délivrés par les PSCE

Les exigences que doit respecter un PSCE, délivrant des certificats électroniques sont définies dans les politiques de certification type (PC Type) « Personne » et « Service applicatif » [RGS_A2] et [RGS_A3]. Ces deux PC Types distingue les exigences spécifiques à chacune des fonctions de sécurité ainsi que trois niveaux de sécurité aux exigences croissantes *, ** et *** (à l'exception de l'usage combiné « Authentification et Signature » qui n'en compte que deux : * et **).

En l'occurrence, la PC Type « Personne » traite des fonctions de sécurité « signature électronique » , « authentification « et « confidentialité ». La PC Type « Service applicatif « traite des fonctions de sécurité » cachet « et « authentification serveur ». Ces deux PC Types distinguent également les règles spécifiques au porteur ou au secteur pour lesquels le certificat électronique est délivré : particulier, agent d'une autorité administrative de la Polynésie française, employé de société, secteur public, secteur privé.

Il est autorisé d'utiliser au sein d'un système d'information un certificat électronique de niveau de sécurité supérieur à celui de la fonction de sécurité sous réserve que le niveau du dispositif de protection de la clé privée et le niveau du certificat soient cohérents. Par exemple, un certificat électronique conforme aux exigences du niveau (***) pourra être employé dans des téléservices de niveaux inférieurs, sous réserve de son interopérabilité.

Ces PC Type s'appuient sur l'annexe [RGS_A4] du [RGS] qui définit les règles et recommandations sur les profils des certificats, les listes de certificats révoqués et le protocole OCSP ainsi que des exigences sur les algorithmes cryptographiques mis en œuvre.

Un PSCE peut faire qualifier à un niveau de sécurité donné l'offre de certificats électroniques selon les modalités prévues par l'article LP 22 de la loi du pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices. Dans ce cas, il doit intégrer dans sa PC l'ensemble des exigences de la PC Type correspondant à l'usage et au niveau visé et respecter ensuite l'ensemble des engagements pris.

III.2. Les dispositifs de protection des éléments secrets

Le dispositif de protection des éléments secrets est un logiciel ou le matériel (carte à puce par exemple) qui stocke la clé privée dédiée à une fonction de sécurité donnée, les éléments permettant de la déverrouiller (code PIN par exemple), qui permet sa mise en œuvre et, le cas échéant, leur génération.

III.2.1. Dispositifs de protection des éléments secrets d'une personne physique

III.2.1.1. Exigences de sécurité

Les exigences sont décrites dans l'annexe 3 des PC Type [RGS_A2].

Quel que soit le niveau visé, le dispositif de protection des éléments secrets de la personne doit répondre aux exigences de sécurité suivantes :

- si la bi-clé est générée par le dispositif, garantir que cette génération est réalisée exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique de la bi-clé générée ;
- détecter les défauts lors des phases d'initialisation, de personnalisation et d'opération ;

- garantir la confidentialité et l'intégrité de la clé privée ;
- assurer la correspondance entre la clé privée et la clé publique ;
- permettre de garantir l'authenticité et l'intégrité de la clé publique lors de son export hors du dispositif.
- [Tous usages sauf Confidentialité]
- disposer de techniques sûres de destruction de la clé privée en cas de régénération de la clé privée ou de destruction des clés privées qui ne sont plus utilisées ;
- [Confidentialité]
- permettre de garantir la confidentialité, l'authenticité et l'intégrité de la clé symétrique lors de son export hors du dispositif à destination de l'application de déchiffrement des données.

III.2.1.2. Exigences sur la qualification

Le respect des règles suivantes n'est exigé que lorsque le PSCE souhaite faire qualifier son offre de certificats électroniques au(x) niveau(x) de sécurité considéré(s) selon les modalités prévues par l'article LP 22 de la loi du pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices et déclinées au chapitre 5 du corps de texte du [RGS] et délivre au porteur final ou au responsable du certificat électronique du service applicatif le dispositif de protection des éléments secrets. Dans tous les autres cas, leur respect est recommandé.

Au niveau *** :

Le dispositif de protection des éléments secrets doit être qualifié au niveau renforcé[4], selon le processus décrit dans le [RGS], et être conforme aux exigences du chapitre ci-dessus.

Au niveau ** :

Le dispositif de protection des éléments doit être qualifié au minimum au niveau standard[5], selon le processus décrit dans le [RGS], et être conforme aux exigences du chapitre ci-dessus.

Il est toutefois recommandé d'utiliser un dispositif de protection éléments secrets qualifié au niveau renforcé.

Au niveau * :

Le dispositif de protection des éléments secrets doit être qualifié au minimum au niveau élémentaire[6], selon le processus décrit dans le [RGS], et être conforme aux exigences du chapitre ci-dessus.

Il est toutefois recommandé d'utiliser un dispositif de protection des éléments secrets qualifié au niveau standard.

[4] [5] et [6] Sous réserve qu'il existe au moins une telle référence sur la liste de référence des produits de sécurité et des prestataires de services de confiance qualifiés visée à l'article LP 22 de la loi du pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices. Dans le cas contraire, le PSCE souhaitant faire qualifier son offre de certificats électroniques doit obtenir une dérogation de l'ANSSI.

III.2.2. Dispositifs de protection des éléments secrets d'un service applicatif

III.2.2.1. Exigences de sécurité

Les exigences sont décrites dans l'annexe 3 des PC Type [RGS_A3].

Quel que soit le niveau visé, le dispositif de protection des éléments secrets du service applicatif doit répondre aux exigences de sécurité suivantes :

- si la bi-clé est générée par le dispositif, garantir que cette génération est réalisée exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique de la bi-clé générée ;
- assurer la correspondance entre la clé privée et la clé publique.

Par ailleurs, des mesures de sécurité organisationnelles, procédurales ou techniques doivent être mises en place afin de :

- détecter les défauts lors des phases d'initialisation, et d'opération et disposer de techniques sûres de destruction de la clé privée en cas de re -génération de la clé privée ;
- garantir la confidentialité et l'intégrité de la clé privée ;
- permettre de garantir l'authenticité et l'intégrité de la clé publique lors de son export hors du dispositif.

Cachet
➢ assurer pour le serveur légitime uniquement la fonction de génération des cachets électroniques et protéger la clé privée contre toute utilisation par des tiers.

Authentification Serveur
➢ assurer pour le serveur légitime uniquement, d'une part, la fonction d'authentification et, d'autre part, la fonction de déchiffrement de clés symétriques de session, et protéger la clé privée contre toute utilisation par des tiers ; ➢ permettre de garantir l'authenticité et l'intégrité de la clé symétrique de session, une fois déchiffrée, lors de son export hors du dispositif à destination de l'application de déchiffrement des données.

Nota : Les dispositifs matériels, de types cartes à puces ou modules cryptographiques qualifiés figurant sur la liste de référence visée à l'article LP 22 de la loi du pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices, respectent ces exigences. Toutefois, des solutions logicielles sont susceptibles de respecter ces exigences pourvues que des mesures de sécurité additionnelles propres à l'environnement dans lequel est déployée la clé privée soient mises en place.

III.2.2.2. Exigences en terme d'évaluation et d'audit

Les composantes de l'IGC qui mettent en œuvre la clé privée doit faire l'objet d'un audit de sécurité.

Pour les niveaux ** et ***, l'audit technique de la sécurité doit être effectué au minimum tous les deux ans. Cet audit doit comprendre :

- un audit de l'architecture réseau (liaison entre les différentes zones et entités, filtrage),
- un audit de configuration (équipements réseau et de sécurité, serveurs d'infrastructure)
- un audit organisationnel.

Au-delà des strictes composantes de l'IGC, l'environnement dans lequel est déployée la clé privée peut faire

l'objet d'un audit de sécurité.

III.3. Les Applications

III.3.1. Exigences de sécurité

[Signature] Il est recommandé d'utiliser une application de création de signature conforme au profil de protection [PPAppli]. De la même manière, il est recommandé d'utiliser un module de vérification de signature conforme au profil de protection [PPVérif].

[Confidentialité] Les opérations cryptographiques de chiffrement sont mises en œuvre dans un module de chiffrement qui va procéder au chiffrement. Quel que soit le niveau, un module de chiffrement doit répondre aux exigences de sécurité suivantes :

- garantir la robustesse cryptographique de la clé symétrique de message ou de fichier qui est générée ;
- détecter les défauts lors des phases d'initialisation, de personnalisation et d'opération et disposer de techniques sûres de destruction des clés qui ne sont plus utilisées ;
- garantir la confidentialité et l'intégrité de la clé symétrique de fichier ou de message et des données à chiffrer ;
- assurer l'accès à la clé symétrique de message ou de fichier exclusivement par les utilisateurs autorisés et protéger cette clé contre toute utilisation par des tiers.

[Confidentialité] Les opérations cryptographiques de déchiffrement sont mises en œuvre dans un module de déchiffrement qui va procéder au déchiffrement. Quel que soit le niveau, un module de déchiffrement doit répondre aux exigences de sécurité suivantes :

- détecter les défauts lors des phases d'initialisation, de personnalisation et d'opération et disposer de techniques sûres de destruction des clés qui ne sont plus utilisées ;
- garantir la confidentialité et l'intégrité de la clé symétrique de fichier ou de message et des données à chiffrer ;
- assurer l'accès à la clé symétrique de message ou de fichier exclusivement par les utilisateurs autorisés et protéger cette clé contre toute utilisation par des tiers.

III.3.2. Exigences sur la qualification

Aux niveaux *** et **, il est recommandé d'utiliser des applications qualifiées au niveau standard. Au niveau *, il est recommandé d'utiliser des applications qualifiées au niveau élémentaire.

III.3.3. Bonnes pratiques

Avant de se fier à un certificat électronique, il faut notamment vérifier que celui-ci :

- contient une indication d'usage conforme à ce qui est attendu ;
- est valide et n'est pas révoqué ;
- à une chaîne de certification qui est correcte à tous les niveaux ;
- correspond au niveau de sécurité cohérent avec l'usage pour lequel il est destiné.

Il est recommandé pour ce faire d'élaborer une politique de vérification des certificats électroniques.

III.4. Environnement d'utilisation

Les fonctions de sécurité « Signature », « Authentification » et « Confidentialité » sont notamment mises en œuvre sur une borne publique ou un ordinateur dans un cadre privé ou professionnel pour un usage par une personne physique.

Les fonctions de sécurité « Cachet » et « Authentification Serveur » sont notamment mises en œuvre sur un ou plusieurs serveurs hébergeant un service applicatif, pour un usage relevant d'une personne morale et sous le contrôle d'une personne physique.

Il est recommandé de prendre en compte les mesures de sécurité suivantes :

- protection contre les virus, avec mises à jour régulière ;
- contrôle et limitation des échanges entre la machine hôte et d'autres machines dans un réseau ouvert ;
- restriction, lorsque cela est possible, de l'accès aux fonctions d'administration de la machine aux seuls administrateurs de celles-ci (différenciation compte utilisateur/administrateur) ;
- installation et mise à jour de logiciels et de composants sur la machine sous le contrôle de l'administrateur ;
- refus par le système d'exploitation de l'ordinateur ou de la borne d'exécuter des applications téléchargées ne provenant pas de sources sûres ;
- mise à jour des composants logiciels et systèmes lors de la mise à disposition de mises à jour de sécurité de ceux-ci.

[Personne] Dans le cas de l'utilisation d'une carte à puce comme dispositif de protection des éléments secrets, il est recommandé, et tout particulièrement au niveau ***, d'utiliser un lecteur de carte à puce avec PIN/PAD intégré qualifié permettant de saisir le code de déverrouillage et de le vérifier sans que celui-ci ne transite via l'ordinateur ou la borne d'accès publique, ou le serveur utilisés.

[Confidentialité] Les opérations de chiffrement et de déchiffrement doivent permettre, à tout moment, de garantir la confidentialité des données à chiffrer / déchiffrer. Il est donc recommandé, au niveau ***, de procéder aux opérations de chiffrement et de déchiffrement de telle façon que les informations à protéger ne soient jamais présentes en clair sur une machine reliée au réseau sur lequel transitent les données chiffrées à protéger.

IV. Documents de référence

IV.1. Réglementation

Renvoi	**Document**
[LOIDUPAYS]	Loi du pays relative à la dématérialisation des actes des autorités administratives et aux téléservices

IV.2. Documents techniques

Renvoi	**Document**
[PP_Appli]	Profil de protection application de création de signature électronique Version 1.6 d'août 2008

[PPVérif]	Profil de protection module de vérification de signature électronique Version 1.6 d'août 2008
[RGS]	Référentiel Général de Sécurité - Version 1.0
[RGS_A2]	Politique de Certification Type « Personne « - Version 1.0
[RGS_A3]	Politique de Certification Type « Service applicatif « - Version 1.0
[RGS_A4]	Profils de certificats, de LCR et OCSP et algorithmes cryptographiques – Version 1.0

Annexe A2

Politique de Certification Type
« Certificats électroniques de personne »

Historique des versions		
Date	**Version**	**Évolution du document**
xxx	1.0	Publication de la première version de l'annexe A2 du référentiel général de sécurité

Avant propos

Le présent document fait partie du référentiel général de sécurité (RGS), pris en application de l'article LP 20 de la loi du pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices, et de son arrêté d'application.

Le présent document et ses annexes sont une copie adaptée du RGS A2 – Politique de Certification Type « certificats électroniques de personne », en vigueur en métropole, version 3.0 du 27 février 2014.

Le texte fait des renvois à des documents publiés par l'Agence nationale de la sécurité des systèmes d'information[7] (ANSSI) ou encore disponibles sur son site internet www.ssi.gouv.fr, en ce qu'ils reflètent l'état de l'art en matière de sécurité informatique.

Le référentiel et ses annexes sont disponibles en ligne sur le site internet www.dgen.pf, et leur mise à jour est assurée par la Direction générale de l'économie numérique.

[7] L'ANSSI est un service à compétence nationale rattaché au Secrétaire général de la défense et de la sécurité nationale, l'autorité chargée d'assister le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale. Parmi ses nombreux objectifs, l'un d'eux consiste à promouvoir un espace de confiance pour les services en ligne. Elle y participe en ce sens notamment au travers de la règlementation (référentiels) et ses labels (certification des produits de sécurité et qualification des produits de sécurité et des prestataires de service de confiance).

I. Introduction

I.1. Présentation générale

I.1.1. Objet du document

Le présent document « Politique de Certification Type, certificats électroniques de personne » (PC Type Personne) fait partie du Référentiel Général de Sécurité [RGS]. Il en constitue l'annexe [RGS_A2].

Ce référentiel technique liste les règles que les prestataires de services de certification électronique (PSCE), délivrant des certificats électroniques à des personnes doivent respecter. Les PSCE délivrant des certificats électroniques à des services applicatifs se reporteront à l'annexe [RGS_A3].

Ce document distingue trois niveaux de sécurité aux exigences croissantes : *, ** et ***. Il distingue par ailleurs quatre usages de certificats électroniques : signature électronique, authentification, confidentialité, signature électronique + authentification. Enfin, il distingue trois types de porteur du certificat électronique délivré : particulier, agent d'une autorité administrative, employé d'une entreprise privée.

Conformément à la loi du pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices, il est du ressort de l'autorité administrative (AA) de déterminer le niveau de sécurité ainsi que les fonctions de sécurité qu'elle souhaite mettre en place au sein de son SI.

Elle peut, par conséquent, décider de recourir à la fonction de sécurité « Signature «, « Authentification », « Confidentialité » ou « Authentification et Signature [8] » basée sur des mécanismes cryptographiques asymétriques nécessitant l'usage de certificats électroniques. Le cas échéant, une fois le niveau de sécurité déterminé parmi *, ** et ***, l'AA doit recourir à des certificats électroniques délivrés par des PSCE conformes à la présente PC Type au dit niveau.

Un PSCE peut obtenir une qualification de son offre de services conformément à l'article LP 22 de la loi du pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices. Cette qualification permet d'attester de la conformité de l'offre du PSCE aux exigences du présent document, pour un ou plusieurs niveaux de sécurité, un ou plusieurs usages et types de porteur de certificats électroniques.

Les exigences, communes à tous les niveaux et particulières à un niveau donné, spécifiées dans la présente PC Type doivent être respectées intégralement par les PSCE moyennant l'exception suivante : dans la présente PC Type, un certain nombre de recommandations sont formulées. Les PSCE sont incités à les respecter également dès maintenant car ces recommandations, qui ne sont pas d'application obligatoire dans la présente version de ce document, devraient le devenir dans une version ultérieure.

Cette PC Type n'est pas une PC à part entière : elle ne peut pas être utilisée telle quelle par un PSCE en tant que PC pour être mentionnée dans ses certificats et sa DPC. Un PSCE souhaitant être qualifié par rapport à un des niveaux de sécurité de la présente PC Type doit en reprendre, dans sa propre PC, l'ensemble des exigences correspondant au niveau visé.

Afin de favoriser l'interopérabilité, dans le cadre de la sécurisation des échanges électroniques entre AA et usagers et entre AA, des règles et recommandations sur les formats de certificats et de listes de révocations, compatibles avec la norme [X.509] sont formulées dans le document [RGS_A4].

[8] Dans le cas précis des certificats électroniques à double usage « authentification + signature électronique », seuls les deux premiers niveaux de sécurité (*) et (**) sont disponibles. De tels certificats électroniques ne peuvent donc pas prétendre au niveau (***).

I.1.2. Conventions de rédaction

De manière à mettre en exergue les règles spécifiques à un niveau de sécurité, à un type d'usage ou à un type de porteur, celles-ci seront présentées dans un encadré, le titre du cadre précisant son périmètre d'application (usage du certificat électronique, niveau de sécurité et type de porteur du certificat électronique). La forme est la suivante :

[Usage]	**[Niveau de sécurité]**	**[Type de porteur]**
Intitulé de la règle		

Les exigences qui ne sont pas encadrées s'appliquent de manière identique aux trois niveaux.

I.2. Identification du document

La présente PC Type est dénommée «RGS - Politique de Certification Type - certificats électroniques de personne». Elle peut être identifiée par son nom, son numéro de version et sa date de mise à jour.

I.3. Définitions et acronymes

I.3.1. Acronymes

Les acronymes utilisés dans la présente PC Type sont les suivants :

AA	Autorité Administrative
AC	Autorité de Certification
AE	Autorité d'Enregistrement
AED	Autorité d'Enregistrement Déléguée
AH	Autorité d'Horodatage
ANSSI	Agence nationale de la sécurité des systèmes d'information
CEN	Comité Européen de Normalisation
DGME	Direction Générale de la Modernisation de l'État
DN	Distinguished Name
DPC	Déclaration des Pratiques de Certification
ETSI	European Telecommunications Standards Institute
IGC	Infrastructure de Gestion de Clés
LAR	Liste des certificats d'AC Révoqués
LCR	Liste des Certificats Révoqués
MC	Mandataire de Certification
OC	Opérateur de Certification
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PC	Politique de Certification
PP	Profil de Protection
PSCE	Prestataire de Services de Certification Électronique

RSA	Rivest Shamir Adelman
SP	Service de Publication
SSI	Sécurité des Systèmes d'Information
URL	Uniform Resource Locator

I.3.2. Définitions

Les termes utilisés dans la présente PC Type sont les suivants :

Agent - Personne physique agissant pour le compte d'une autorité administrative.

Applications utilisatrices - Services applicatifs exploitant les certificats émis par l'Autorité de Certification pour des besoins d'authentification, de chiffrement ou de signature du porteur du certificat ou des besoin d'authentification ou de cachet du serveur auquel le certificat est rattaché.

Autorités administratives - Ce terme générique, défini à l'article LP 1 de la loi du pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices, désigne la Polynésie française, ses établissements publics, les autorités administratives indépendantes, les organismes de protection sociale et les autres organismes et personnes de droit public et de droit privé chargés d'une mission de service public administratif ;

Autorité d'horodatage - Autorité responsable de la gestion d'un service d'horodatage (cf. politique d'horodatage type du [RGS]).

Autorité de certification (AC) - Au sein d'un PSCE, une Autorité de Certification a en charge, au nom et sous la responsabilité de ce PSCE, l'application d'au moins une politique de certification et est identifiée comme telle, en tant qu'émetteur (champ «issuer» du certificat), dans les certificats émis au titre de cette politique de certification. Dans le cadre de la présente PC Type, le terme de PSCE n'est pas utilisé en dehors du présent chapitre et du chapitre I.1 et le terme d'AC est le seul utilisé. Il désigne l'AC chargée de l'application de la politique de certification, répondant aux exigences de la présente PC Type, au sein du PSCE souhaitant faire qualifier la famille de certificats correspondante.

Certificat électronique - Document sous forme électronique attestant du lien entre une clé publique et l'identité de son propriétaire. Cette attestation prend la forme d'une signature électronique réalisée par un prestataire de service de certification électronique (PSCE). Il est délivré par une Autorité de Certification. Le certificat est valide pendant une durée donnée précisée dans celui-ci. Les usages des certificats électroniques régis par le présent document sont la signature électronique, l'authentification, la confidentialité ainsi que le double usage signature électronique + authentification.

Composante - Plate-forme opérée par une entité et constituée d'au moins un poste informatique, une application et, le cas échéant, un moyen de cryptologie et jouant un rôle déterminé dans la mise en œuvre opérationnelle d'au moins une fonction de l'IGC. L'entité peut être le PSCE lui-même ou une entité externe liée au PSCE par voie contractuelle, réglementaire ou hiérarchique.

Déclaration des pratiques de certification (DPC) - Une DPC identifie les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que l'AC applique dans le cadre de la fourniture de ses services de certification électronique aux usagers et en conformité avec la ou les politiques de certification qu'elle s'est engagée à respecter.

Dispositif de protection des éléments secrets - Un dispositif de protection des éléments secrets désigne un dispositif de stockage des éléments secrets remis au porteur (exemples : clé privée, code PIN, etc). Il peut prendre la forme d'une carte à puce, d'une clé USB à capacités cryptographique ou se présenter au format logiciel (exemple fichier PKCS#12).

Entité - Désigne une autorité administrative ou une entreprise au sens le plus large, c'est-à-dire également

les personnes morales de droit privé de type associations.

Infrastructure de gestion de clés (IGC) - Ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs certificats utilisés par des services de confiance. Une IGC peut être composée d'une autorité de certification, d'un opérateur de certification, d'une autorité d'enregistrement centralisée et/ou locale, de mandataires de certification, d'une entité d'archivage, d'une entité de publication, etc.

Politique de certification (PC) - Ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une AC se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes. Une PC peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les porteurs et les utilisateurs de certificats.

Porteur de certificat - Personne physique identifiée dans le certificat et qui est le détenteur de la clé privée correspondant à la clé publique.

Prestataire de services de certification électronique (PSCE) - Un PSCE est un type de prestataire de services de confiance (PSCO) particulier. Un PSCE se définit comme toute personne ou entité qui est responsable de la gestion de certificats électroniques tout au long de leur cycle de vie, vis-à-vis des porteurs et utilisateurs de ces certificats. Un PSCE peut fournir des certificats électroniques pour différents usages, niveaux de sécurité et pour différents types de porteur. Un PSCE comporte au moins une AC mais peut en comporter plusieurs en fonction de son organisation. Les différentes AC d'un PSCE peuvent être indépendantes les unes des autres et/ou liées par des liens hiérarchiques ou autres (AC Racines / AC Filles). Un PSCE est identifié dans un certificat dont il a la responsabilité au travers de son AC ayant émis ce certificat et qui est elle-même directement identifiée dans le champ «issuer» du certificat.

Produit de sécurité - Un dispositif matériel ou logiciel, ou les composants correspondants du dispositif matériel ou logiciel, qui sont destinés à être utilisés pour la fourniture de services de confiance et nécessaires à la sécurisation d'une information ou d'un système.

Promoteur d'application - Un responsable d'un service de la sphère publique accessible par voie électronique.

Qualification d'un prestataire de services de certification électronique - La qualification d'un PSCE permet d'attester de la conformité de l'offre de certification électronique d'un PSCE à un niveau de sécurité du [RGS]. Conformément à l'article LP 22 de la loi du pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices, cette qualification correspond à la qualification délivrée par les autorités de métropole en application de l'ordonnance n° 2005-1516 du 8 décembre 2015 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

Qualification d'un produit de sécurité – La qualification d'un produit de sécurité permet d'attester de la conformité d'un produit à un niveau de sécurité du [RGS]. Conformément à l'article LP 22 de la loi du pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices, cette qualification correspond à la qualification délivrée par les autorités de métropole en application de l'ordonnance n° 2005-1516 du 8 décembre 2015 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

Système d'information – Tout ensemble de moyens destinés à élaborer, traiter, stocker ou transmettre des informations faisant l'objet d'échanges par voie électronique entre autorités administratives et usagers ainsi qu'entre autorités administratives.

Usager - Toute personne physique ou toute personne morale de droit privé, à l'exception de celles qui sont chargées d'une mission de service public lorsqu'est en cause l'exercice de cette mission. Selon le contexte,

un usager peut être un porteur ou un utilisateur de certificats.

Utilisateur de certificat - Entité ou personne physique qui utilise un certificat et qui s'y fie pour vérifier une signature électronique ou une valeur d'authentification provenant d'un porteur de certificat ou chiffrer des données à destination d'un porteur de certificat.

I.4.Entités intervenant dans l'IGC

I.4.1. Autorités de certification

L'AC a en charge la fourniture des prestations de gestion des certificats tout au long de leur cycle de vie (génération, diffusion, renouvellement, révocation...) et s'appuie pour cela sur une infrastructure technique : une infrastructure de gestion de clés (IGC).

Les prestations de l'AC sont le résultat de différentes fonctions qui correspondent aux différentes étapes du cycle de vie des bi-clés et des certificats.

Afin de clarifier et faciliter l'identification des exigences, et en cohérence avec les documents de l'ETSI dans le domaine (cf. les normes ETSI_QCP et ETSI_NQCP), la décomposition fonctionnelle d'une IGC qui est retenue dans la présente PC Type est la suivante[9] :

- **Autorité d'enregistrement (AE)** [10] - Cette fonction vérifie et valide les informations d'identification du futur porteur d'un certificat, ainsi qu'éventuellement d'autres attributs spécifiques, avant de transmettre la demande correspondante à la fonction adéquate de l'IGC, en fonction des services rendus et de l'organisation de l'IGC. L'AE a également en charge, lorsque cela est nécessaire, la re-vérification des informations du porteur lors du renouvellement du certificat de celui-ci.
- **Fonction de génération des certificats** - Cette fonction génère (création du format, signature électronique avec la clé privée de l'AC) les certificats à partir des informations transmises par l'autorité d'enregistrement et de la clé publique du porteur provenant soit du porteur, soit de la fonction de génération des éléments secrets du porteur, si c'est cette dernière qui génère la bi-clé du porteur.
- **Fonction de génération des éléments secrets du porteur** - Cette fonction génère les éléments secrets à destination du porteur, si l'AC a en charge une telle génération, et les prépare en vue de leur remise au porteur (par exemple, personnalisation de la carte à puce destinée au porteur, courrier sécurisé avec le code d'activation, etc.). De tels éléments secrets peuvent être, par exemple, directement la bi-clé du porteur, les codes (activation / déblocage) liés au dispositif de stockage de la clé privée du porteur ou encore des codes ou clés temporaires permettant au porteur de mener à distance le processus de génération / récupération de son certificat.
- **Fonction de remise au porteur** - Cette fonction remet au porteur au minimum son certificat ainsi que, le cas échéant, les autres éléments fournis par l'AC (dispositif du porteur, clé privée du porteur,

[9] Cette décomposition est donnée à titre d'illustration pour les besoins de la présente PC Type et n'impose aucune restriction sur la décomposition d'une implémentation effective d'une IGC.

[10] Les documents de l'ETSI, notamment les normes ETSI_QCP et ETSI_NQCP, utilisent le terme Service d'Enregistrement. Le [RFC3647], utilise le terme Autorité d'Enregistrement. En cohérence avec ce dernier document, il est conservé l'utilisation du terme Autorité d'Enregistrement, mais qui doit être compris, dans la présente PC Type, en tant que fonction et non pas en tant que composante technique de l'IGC.

codes d'activation…).

- **Fonction de publication** - Cette fonction met à disposition des différentes parties concernées, les conditions générales, politiques et pratiques publiées par l'AC, les certificats d'AC et toute autre information pertinente destinée aux porteurs et/ou aux utilisateurs de certificats, hors informations d'état des certificats. Elle peut également mettre à disposition, en fonction de la politique de l'AC, les certificats valides de ses porteurs.
- **Fonction de gestion des révocations -** Cette fonction traite les demandes de révocation (notamment identification et authentification du demandeur) et détermine les actions à mener. Les résultats des traitements sont diffusés via la fonction d'information sur l'état des certificats.
- **Fonction d'information sur l'état des certificats** - Cette fonction fournit aux utilisateurs de certificats des informations sur l'état des certificats (révoqués, suspendus, etc.). Cette fonction peut être mise en œuvre selon un mode de publication d'informations mises à jour à intervalles réguliers (LCR, LAR) ou selon un mode requête / réponse temps réel (OCSP).

[Confidentialité]		

Une IGC gérant des certificats de confidentialité doit assurer au surplus les fonctions suivantes :

- **Fonction de gestion des recouvrements** - Cette fonction traite les demandes de recouvrement de clés privées des porteurs (notamment identification et authentification du demandeur) et détermine les actions à mener. Dans le cas d'une décision positive, le recouvrement est réalisé par la fonction de séquestre et recouvrement.
- **Fonction de séquestre et recouvrement** - Cette fonction fournit la capacité de séquestrer de manière sécurisée les clés privées de confidentialité des porteurs, puis de les recouvrer en cas de besoin, sur la base de demandes authentifiées et traitées par la fonction de gestion des recouvrements (cf. chapitre IV.12).

Les fonctions ci-dessus, à l'exception des fonctions de génération des éléments secrets, de séquestre et de recouvrement, sont les fonctions minimales que doit obligatoirement mettre en œuvre une IGC gérant des certificats électroniques.

Un certain nombre d'entités / personnes physiques externes à l'IGC interagissent avec cette dernière. Il s'agit notamment :

- **Porteur** - La personne physique identifiée dans le certificat et qui est le détenteur de la clé privée correspondant à la clé publique qui est dans ce certificat.
- **Utilisateur de certificat** - L'entité ou la personne physique qui reçoit un certificat et qui s'y fie pour vérifier une signature électronique ou une valeur d'authentification provenant du porteur du certificat ou chiffrer des données à destination du porteur du certificat.
- **Personne autorisée** - Il s'agit d'une personne autre que le porteur et le mandataire de certification et qui est autorisée par la politique de certification de l'AC ou par contrat avec l'AC à mener certaines actions pour le compte du porteur (demande de révocation, de renouvellement, …). Typiquement, dans une entreprise ou une administration, il peut s'agir d'un responsable hiérarchique du porteur ou d'un responsable des ressources humaines.

		| [Entreprise] [Administration]

- Mandataire de certification (MC) - Le mandataire de certification est désigné par et placé sous la responsabilité de l'entité cliente. Il est en relation directe avec l'AE. Il assure pour elle un certain nombre de vérifications concernant l'identité et, éventuellement, les attributs des porteurs de cette entité (il assure notamment le face-à-face pour l'identification des porteurs lorsque celui-ci est requis).

L'organisation et l'ordonnancement des différentes fonctions de l'IGC les unes par rapport aux autres dépendent du modèle adopté par l'AC. La présente PC Type n'impose aucun modèle particulier, dans la limite où l'AC respecte les exigences qui y sont définies.

Cependant, les parties de l'AC concernées par la génération de certificats et la gestion des révocations doivent être indépendantes d'autres organisations en ce qui concerne leurs décisions concernant la mise en place, la fourniture, le maintien et la suspension des services ; en particulier, leurs cadres dirigeants, leur personnel d'encadrement et leur personnel ayant des rôles de confiance, doivent être libres de toute pression d'ordre commercial, financier ou autre, qui pourraient influer négativement sur la confiance dans les services fournis par l'AC. Les parties de l'AC concernées par la génération de certificat et de la gestion des révocations doivent avoir une structure documentée qui préserve l'impartialité des opérations.

L'organisation adoptée dépend notamment des prestations fournies par l'AC : génération ou non de la bi-clé du porteur, fourniture ou non du dispositif de protection des éléments secrets au porteur et, si oui, fourniture avant ou après génération de la bi-clé du porteur, etc.

L'AC doit préciser dans sa PC les prestations effectivement fournies et son organisation fonctionnelle correspondante.

Dans la pratique, la mise en œuvre opérationnelle de ces fonctions peut être effectuée par une ou plusieurs composantes(s) de l'IGC (opérateurs techniques et/ou autorités tel que OC, AE, SP, AH,…), qui peuvent être internes à l'AC et/ou opérées par des entités externes.

La Déclaration des Pratiques de Certification (DPC) de l'AC doit décrire l'organisation opérationnelle de son IGC et la répartition des rôles entre les différentes composantes en fonction de l'organisation fonctionnelle et de la définition des rôles décrites dans sa PC.

Quelle que soit l'organisation opérationnelle mise en œuvre, l'AC reste in fine responsable vis-à-vis de toute partie externe à l'IGC (utilisateurs, autorités publiques, etc.) des prestations fournies et doit garantir le respect des engagements pris dans sa PC et sa DPC, relatifs à son activité de certification. En particulier, les politiques et les procédures, en fonction desquelles l'AC fonctionne, doivent être non-discriminatoires.

Le cadre contractuel entre l'AC et ses différentes composantes opérées par des entités externes doit être clairement documenté.

Une AC qualifiée pour son offre de certificats électroniques (niveau de sécurité, types d'usage et de porteur) conformément à l'article LP 22 de la loi du pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices respecte les exigences décrites dans la présente PC Type et s'engage à ce que les composantes de l'IGC, internes et externes à l'AC, respectent aussi les exigences qui les concernent.

Dans le cadre de ses fonctions opérationnelles, qu'elle assume directement ou qu'elle sous-traite à des entités externes, les exigences qui incombent à l'AC en tant que responsable de l'ensemble de l'IGC sont les suivantes :

- Être une entité légale au sens de la règlementation.
- Rendre accessible l'ensemble des prestations déclarées dans sa PC aux promoteurs d'application d'échanges dématérialisés de l'administration, aux porteurs, aux utilisateurs de certificats, ceux qui mettent en œuvre ses certificats.

- S’assurer que les exigences de la PC et les procédures de la DPC sont appliquées par chacune des composantes de l’IGC et sont adéquates et conformes aux normes en vigueur.
- Mettre en œuvre les différentes fonctions identifiées dans sa PC, correspondant au minimum aux fonctions obligatoires de la présente PC Type, notamment en matière de génération des certificats, de remise au porteur, de gestion des révocations et d’information sur l’état des certificats.
- Élaborer, mettre en œuvre, contrôler et maintenir de façon itérative les mesures de sécurité et les procédures opérationnelles, concernant ses installations, ses systèmes et ses biens informationnels.

	Niveau (***)	
➢ L’AC doit mener une analyse de risque permettant de déterminer les objectifs de sécurité propres à couvrir les risques métiers de l’ensemble de l’IGC et les mesures de sécurité techniques et non techniques correspondantes à mettre en œuvre. Elle élabore sa DPC en fonction de cette analyse.		

	Niveaux (*) et (**)	
➢ Il est recommandé que l’AC mène une analyse de risque.		

- Mettre en œuvre tout ce qui est nécessaire pour respecter les engagements définis dans sa PC, et correspondant au minimum aux exigences de la présente PC Type, notamment en termes de fiabilité, de qualité et de sécurité. À ce titre, elle doit posséder un ou des systèmes de gestion de la qualité et de la sécurité de l’information adaptés aux services de certification qu’elle assure.
- Générer, et renouveler lorsque nécessaire, ses bi-clés et les certificats correspondants (signature de certificats, de LCR et de réponses OCSP), ou faire renouveler ses certificats si l’AC est rattachée à une AC hiérarchiquement supérieure. Diffuser ses certificats d’AC aux porteurs et utilisateurs de certificats.
- Suivre les demandes en capacité et réaliser des projections concernant les futurs besoins en capacité afin de garantir la disponibilité du service, notamment en matière de capacité de traitement et de stockage.

		[Entreprise] [Administration]
➢ Être en relation par voie contractuelle / hiérarchique / réglementaire avec l’entité pour laquelle elle a en charge la gestion des certificats des porteurs de cette entité. LAC peut aussi, le cas échéant, être en relation contractuelle / hiérarchique / réglementaire avec le ou les mandataires de certification choisis par l’entité.		

		[Particulier]
➢ Être en relation par voie contractuelle / hiérarchique / réglementaire avec le porteur pour la gestion de ses certificats.		

I.4.2. Autorité d’enregistrement

L’AE a pour rôle de vérifier l’identité du futur porteur de certificat. Pour cela, l’AE assure les tâches suivantes :

- l’établissement et la transmission de la demande de certificat à la fonction adéquate de l’IGC suivant l’organisation de cette dernière et les prestations offertes ;
- l’archivage des pièces du dossier d’enregistrement (ou l’envoi vers la composante chargée de

l'archivage) ;

- la conservation et la protection en confidentialité et en intégrité des données personnelles d'authentification du porteur ou, le cas échéant, du MC, y compris lors des échanges de ces données avec les autres fonctions de l'IGC (notamment, elle respecte la législation relative à la protection des données personnelles).

		[Entreprise] [Administration]
➢ la prise en compte et la vérification des informations du futur porteur et de son entité de rattachement et la constitution du dossier d'enregistrement correspondant ; ➢ le cas échéant, la prise en compte et la vérification des informations du futur MC (cf. dernier paragraphe du I.4.2) et de son entité de rattachement et la constitution du dossier d'enregistrement correspondant ; ➢ L'AE peut s'appuyer sur un MC désigné et placé sous la responsabilité de l'entité cliente pour effectuer tout ou partie des opérations de vérification des informations (cf. chapitre I.4.5.2 ci-dessous). Dans ce cas, l'AE doit s'assurer que les demandes sont complètes et exactes et effectuées par un MC dûment autorisé. Dans tous les cas, l'archivage des pièces du dossier d'enregistrement (sous forme électronique et/ou papier) est de la responsabilité de l'AE (cf. chapitre V.5).		

		[Particulier]
➢ la prise en compte et la vérification des informations du futur porteur et la constitution du dossier d'enregistrement correspondant ;		

Il est à noter que l'AE peut déléguer tout ou partie de ses fonctions à des unités de proximité désignées sous le nom d'autorités d'enregistrement déléguées (AED).

1.4.3. Porteurs de certificats

Dans le contexte du présent référentiel, un porteur de certificats ne peut être qu'une personne physique qui utilise sa clé privée et le certificat électronique associé :

- pour son propre compte, dans le cas des particuliers ;
- pour ses activités en lien avec l'entité, identifiée dans le certificat électronique, avec laquelle il a une relation contractuelle, hiérarchique ou réglementaire, dans le cas agents d'AA ou d'employés d'entreprises privées.

Le porteur respecte les conditions qui lui incombent définies dans la PC de l'AC, qui doit reprendre les conditions définies dans la présente PC Type.

1.4.4. Utilisateurs de certificats

➢ **[Confidentialité]**		
Un utilisateur (ou accepteur) de certificats électroniques de confidentialité peut être notamment : ➢ Un service en ligne qui utilise un dispositif de chiffrement pour chiffrer des données ou un message à destination du porteur du certificat ; ➢ Une personne qui émet un message chiffré à l'intention du porteur du certificat électronique.		

[Authentification]		
Un utilisateur (ou accepteur) de certificats électroniques d'authentification peut être notamment : ➢ Un service en ligne qui utilise un certificat et un dispositif de vérification d'authentification soit pour valider une demande d'accès faite par le porteur du certificat dans le cadre d'un contrôle d'accès, soit pour authentifier l'origine d'un message ou de données transmises par le porteur du certificat ; ➢ Un usager destinataire d'un message ou de données et qui utilise un certificat et un dispositif de vérification d'authentification afin d'en authentifier l'origine.		

[Signature]		
Un utilisateur (ou accepteur) de certificats de signature électronique peut être notamment : ➢ Un service en ligne qui utilise un dispositif de vérification de signature pour vérifier la signature électronique apposée sur des données ou un message par le porteur du certificat ; ➢ Un usager qui signe électroniquement un document ou un message ; ➢ Un usager destinataire d'un message ou de données et qui utilise un certificat et un dispositif de vérification de signature afin de vérifier la signature électronique apposée par le porteur du certificat sur ce message ou sur ces données.		

[Authentification et Signature]		
Un utilisateur (ou accepteur) de certificats double usage signature électronique + authentification peut être notamment l'un de ceux identifiés ci-dessus pour les usages séparés de signature électronique et d'authentification.		

Les utilisateurs de certificats doivent prendre toutes autres précautions prescrites dans les éventuels accords ou tout autre document, notamment ceux précisés aux chapitres IX.6.3 et IX.6.4. En particulier, l'AC doit respecter ses responsabilités envers les utilisateurs qui ont « raisonnablement « confiance dans un certificat

I.4.5. Autres participants

I.4.5.1. Composantes de l'IGC

La décomposition en fonctions de l'IGC est présentée au chapitre I.4.1 ci-dessus. Les composantes de l'IGC mettant en œuvre ces fonctions devront être présentées dans la DPC de l'AC.

I.4.5.2. Mandataire de certification

		[Entreprise] [Administration]
Le recours à un mandataire de certification (MC) n'est pas obligatoire pour une entité. Une même entité peut s'appuyer sur un ou plusieurs MC. Dans le cas où elle y a recours, le MC doit être formellement désigné par un représentant légal de l'entité concernée. Le MC est en relation directe avec l'AE de l'IGC. Les engagements du MC à l'égard de l'AC doivent être précisés dans un contrat écrit avec l'entité responsable du MC. Ce contrat stipule notamment que le MC doit : ➢ effectuer correctement et de façon indépendante les contrôles d'identité des futurs porteurs de l'entité pour laquelle il est MC,		

- respecter les parties de la PC et de la DPC de l'AC qui lui incombent.

L'entité doit signaler à l'AC, si possible préalablement mais au moins sans délai, le départ du MC de ses fonctions et, éventuellement, lui désigner un successeur.

Le MC ne doit en aucun cas avoir accès aux moyens qui lui permettraient d'activer et d'utiliser la clé privée associée à la clé publique contenue dans le certificat délivré au porteur.

I.5. Usage des certificats

I.5.1. Domaines d'utilisation applicables

I.5.1.1. Bi-clés et certificats des porteurs

Usages des certificats électroniques des porteurs :

[Confidentialité]		

Lorsque le certificat électronique délivré par le PSCE est un certificat de confidentialité, les usages sont :

- Déchiffrement : à l'aide de sa clé privée, un porteur déchiffre les données qui lui ont été transmises dans le cadre d'échanges dématérialisés, chiffrées à partir de sa clé publique ;
- Chiffrement : à l'aide de la publique du destinataire, une personne chiffre des données.

Cela couvre notamment le cas de chiffrement par une clé symétrique de fichiers ou de messages, clé elle-même protégée par un mécanisme cryptographique asymétrique, de type RSA (chiffrement de la clé symétrique par la clé publique du porteur et déchiffrement par sa clé privée) ou de type Diffie-Hellman (obtention de la clé symétrique, par l'émetteur d'un message, via un algorithme combinant la clé privée de l'émetteur et la clé publique du destinataire, et inversement pour l'obtention de cette clé symétrique par le destinataire du message).

[Authentification]		

Lorsque le certificat électronique délivré par le PSCE est un certificat d'authentification, les usages sont l'authentification des porteurs auprès de serveurs distants ou auprès d'autres personnes.

Il peut s'agir d'authentification dans le cadre d'un contrôle d'accès à un serveur ou une application, ou de l'authentification de l'origine de données dans le cadre de la messagerie électronique.

[Signature]		

Lorsque le certificat électronique délivré par le PSCE est un certificat de signature électronique, les usages sont la signature électronique de données.

Une telle signature électronique apporte, outre l'authenticité et l'intégrité des données ainsi signées, la manifestation du consentement du signataire quant au contenu de ces données.

[Authentification et Signature]		

Lorsque le certificat électronique délivré par le PSCE est un certificat double usage signature électronique + authentification, les usages sont l'ensemble de ceux identifiés ci-dessus pour les usages séparés d'authentification et de signature.

Certaines applications d'échanges dématérialisés de la sphère publique peuvent nécessiter des certificats à

des fins de tests ou de recette. De tels certificats doivent pouvoir être distingués des certificats «de production» fournis et gérés par l'AC. Dans certains cas, une AC spécifique «de test» pourra être mise en place.

[Signature]		
Nota - S'agissant de signatures électroniques devant pouvoir être vérifiées potentiellement longtemps (plusieurs années) après la fin de validité des certificats correspondants, il est recommandé que les applications s'appuient sur des politiques de signatures formalisées déterminant, notamment, les informations à conserver (certificats, statuts de ces certificats,…) et le recours éventuel à des services d'horodatage et d'archivage sécurisé.		

Niveaux de sécurité :

	Niveau (***)	
Les certificats électronique objets de la présente PC Type sont utilisés par des applications pour lesquelles les besoins de sécurité sont très forts eu égard aux risques très élevés qui les menacent (usurpation d'identité, …).		

	Niveau (**)	
Les certificats électronique objets de la présente PC Type sont utilisés par des applications pour lesquelles les besoins de sécurité sont forts eu égard aux risques élevés qui les menacent (usurpation d'identité, …).		

	Niveau (*)	
Les certificats électronique objets de la présente PC Type sont utilisés par des applications pour lesquelles les besoins de sécurité sont moyens eu égard aux risques qui les menacent.		

I.5.1.2. Bi-clés et certificats d'AC et de composantes

Cette PC Type comporte également des exigences concernant les bi-clés et certificats de l'AC (signature des certificats des porteurs, des LCR / LAR ou des réponses OCSP) ainsi que des clés, bi-clés et certificats des composantes de l'IGC (sécurisation des échanges entre composantes, authentification des opérateurs, etc.).

L'AC génère et signe différents types d'objets : certificats, LCR / LAR ou réponses OCSP. Pour signer ces objets, l'AC dispose d'au moins une bi-clé, mais il est recommandé qu'elle mette en œuvre des bi-clés séparées en particulier pour les réponses OCSP.

Les certificats des clés publiques de ces bi-clés peuvent être générés par différentes AC. Les cas les plus courants sont les suivants :

1) L'AC dispose d'une seule bi-clé et le certificat correspondant est rattaché à une AC de niveau supérieur (hiérarchie d'AC).
2) L'AC dispose d'une seule bi-clé et le certificat correspondant est un certificat racine (certificat autosigné non rattaché à une AC de niveau supérieur). Elle émet des certificats d'utilisateurs finaux.
3) L'AC dispose de bi-clés distinctes, le certificat correspondant à la bi-clé de signature de certificats est un certificat racine (certificat autosigné non rattaché à une AC de niveau supérieur) et les certificats des autres bi-clés sont signés par cette bi-clé de signature de certificats de l'AC. Les certificats d'utilisateurs finaux sont signés par ces autres bi-clés.
4) L'AC dispose de bi-clés distinctes, le certificat correspondant à la bi-clé de signature de certificats

est rattaché à une AC de niveau supérieur (hiérarchie d'AC) et les certificats correspondant aux autres bi-clés sont signés par cette bi-clé de signature de certificats de l'AC.

5) L'AC dispose de bi-clés distinctes, les certificats correspondant à ces bi-clés sont rattachés à une AC de niveau supérieur (hiérarchie d'AC).

Le cas n°2 est interdit.

La présente PC Type recommande la mise en œuvre du cas n°5, qui permet notamment à l'AC de niveau supérieur de générer et diffuser de manière plus simple des LAR en cas de révocations des certificats d'AC de niveau inférieur.

Quelle que soit l'approche retenue par l'AC (bi-clés séparées ou non), les bi-clés et certificats de l'AC pour la signature de certificats, de LCR / LAR ou de réponses OCSP ne doivent être utilisés qu'à cette fin. Ils ne doivent notamment être utilisés ni à des fins de confidentialité, ni à des fins d'authentification.

Conformément au [CWA14167-1], les différentes clés internes à l'IGC peuvent être décomposées suivant les catégories suivantes :

- la (ou les) clé(s) de signature d'AC, utilisée(s) pour signer les certificats générés par l'AC
- ainsi que les informations sur l'état des certificats (LCR / LAR ou réponses OCSP) ;
- les clés d'infrastructure, utilisées par les systèmes intervenant dans l'IGC à des fins d'authentification, de signature des journaux d'évènements, de chiffrement des données échangées ou stockées au sein de l'IGC, etc. ;
- les clés de contrôle, assignées au personnel de l'IGC afin de s'authentifier vis-à-vis des différents systèmes, de signer et/ou de chiffrer des messages ou des données échangés, etc.

Les deux derniers types de clés peuvent être des clés asymétriques et/ou symétriques.

Ces différents types de clés, et éventuellement les certificats correspondants, doivent être couverts par leurs propres engagements, complets et à part entière. Ces engagements doivent faire partie directement de la propre PC de l'AC, couvrant les certificats de porteurs (cf. chapitre I.1), ou bien faire l'objet de PC séparées (par exemple, PC d'une AC Racine couvrant les certificats d'AC).

La PC de l'AC répondant à la présente PC Type doit au minimum reprendre les exigences de cette dernière sur les certificats d'AC et de composantes. En cas de traitement de ces certificats dans des PC séparées, ces PC doivent être cohérentes avec les exigences de la PC de l'AC et de la présente PC Type.

I.5.2. Domaines d'utilisation interdits

Les restrictions d'utilisation des bi-clés et des certificats sont définies au chapitre IV.5 ci-dessous, en fonction du niveau de sécurité. L'AC doit respecter ces restrictions et imposer leur respect par ses porteurs et ses utilisateurs de certificats.

À cette fin, elle doit communiquer à tous les porteurs, MC et utilisateurs potentiels les termes et conditions relatives à l'utilisation du certificat.

I.6. Gestion de la PC

I.6.1. Entité gérant la PC

La direction de l'AC est responsable de la validation et de la gestion de la PC répondant aux exigences de la présente PC Type.

I.6.2. Point de contact

À préciser dans la PC de l'AC.

I.6.3. Entité déterminant la conformité d'une DPC avec cette PC

L'AC doit être pourvu d'une direction ayant autorité et une responsabilité finale pour déterminer la conformité de la DPC avec la PC.

I.6.4. Procédures d'approbation de la conformité de la DPC

L'AC doit mettre en place un processus d'approbation de la conformité de la DPC avec la PC.

L'AC est responsable de la gestion (mise à jour, révisions) de la DPC. Toute demande de mise à jour de la DPC doit suivre le processus d'approbation mis en place. Toute nouvelle version de la DPC doit être publiée, conformément aux exigences du paragraphe II.2 sans délai.

II. Responsabilités concernant la mise à disposition des informations devant être publiées

II.1. Entités chargées de la mise à disposition des informations

Pour la mise à disposition des informations devant être publiées à destination des porteurs et des utilisateurs de certificats, l'AC doit mettre en œuvre au sein de son IGC une fonction de publication et une fonction d'information sur l'état des certificats (cf. chapitre I.4.1 ci-dessus).

La PC de l'AC doit préciser les méthodes de mise à disposition et les URL correspondantes (annuaire accessible par le protocole LDAP et/ou HTTP, serveur Web, serveur OCSP, etc.).

II.2. Informations devant être publiées

L'AC a pour obligation de publier au minimum les informations suivantes à destination des porteurs et utilisateurs de certificats :

- sa politique de certification, couvrant l'ensemble des rubriques du [RFC3647][11] et conforme à la présente PC Type, ainsi que les éventuels documents complémentaires (par exemple, profils des certificats s'ils sont définis dans un document séparé) ;
- la liste des certificats révoqués (porteurs et AC) ;
- les certificats de l'AC, en cours de validité ;
- si l'AC est rattachée à une hiérarchie d'AC, les certificats en cours de validité des AC de cette hiérarchie, les différentes politiques de certification correspondantes et les éventuels documents complémentaires, ceci jusqu'à l'AC Racine ;
- pour les certificats d'AC autosignés (AC Racine), les informations permettant aux utilisateurs de certificats de s'assurer de l'origine de ces certificats (cf. chapitre VI.1.4) et de leur état (cf. chapitre IV.10).

L'AC a l'obligation de publier, à destination des porteurs et utilisateurs de certificats, sa déclaration des pratiques de certification ainsi que toute autre documentation pertinente pour rendre possible l'évaluation de la conformité avec sa politique de certification. Cependant, elle n'est en général pas tenue de rendre publics tous les détails relatifs à ses pratiques.

L'AC a également pour obligation de publier, à destination des porteurs de certificats, les différents formulaires nécessaires pour la gestion des certificats (demande d'enregistrement, demande de révocation, demande de renouvellement, etc.).

De plus, compte tenu de la complexité de lecture d'une PC pour des porteurs ou des utilisateurs de certificats non spécialistes du domaine, il est obligatoire que l'AC publie également des conditions générales d'utilisation correspondant aux «PKI Disclosure Statement» (PDS) définis dans les normes [ETSI_NQCP] et [RFC3647].

Il est recommandé que ces conditions générales aient une structure conforme à celle décrite en annexe B de [ETSI_NQCP] et reprennent ainsi, à destination des porteurs et des utilisateurs de certificats, les informations pertinentes de la PC de l'AC :

- les conditions d'usages des certificats et leurs limites,

[11] Si sa PC n'est pas strictement conforme au plan du [RFC3647], l'AC devra y joindre un tableau de correspondance démontrant la complétude de sa PC par rapport au [RFC3647].

- l'identifiant : OID de la PC applicable,
- les obligations et responsabilités des différentes parties, notamment les exigences relatives à la vérification du statut de révocation d'un certificat pour les utilisateurs,
- les garanties et limites de garanties de l'AC,
- les informations sur comment vérifier un certificat,
- la durée de conservation des dossiers d'enregistrement et des journaux d'évènements,
- les procédures pour la résolution des réclamations et des litiges,
- le système légal applicable,
- si l'AC a été déclarée conforme à la politique identifiée et dans ce cas au travers de quel schéma.

Ces conditions générales font notamment partie intégrante du dossier d'enregistrement.

Le moyen utilisé pour la publication de ces informations, sauf pour les LCR / LAR (cf. chapitre IV.10), est libre mais doit être précisé dans la PC de l'AC. Il doit garantir l'intégrité, la lisibilité, la compréhensibilité et la clarté des informations publiées.

II.3. Délais et fréquences de publication

Les informations liées à l'IGC (nouvelle version de la PC, formulaires, etc.) doivent être publiées dès que nécessaire afin que soit assurée à tout moment la cohérence entre les informations publiées et les engagements, moyens et procédures effectifs de l'AC. En particulier, toute nouvelle version doit être communiquée au porteur ou MC lors d'une demande de renouvellement de clé et doit faire l'objet d'un nouvel accord. Les systèmes publiant ces informations doivent au moins être disponibles les jours ouvrés.

Les certificats d'AC doivent être diffusés préalablement à toute diffusion de certificats de porteurs et/ou de LCR correspondants et les systèmes les publiant doivent avoir une disponibilité de 24h/24 et 7j/7[12].

Les délais et fréquences de publication des informations d'état des certificats ainsi que les exigences de disponibilité des systèmes les publiant sont décrites aux chapitres IV.9 et IV.10.

Il est à noter qu'une perte d'intégrité d'une information mise à disposition (présence de l'information et intégrité de son contenu) est considérée comme une indisponibilité de cette information.

II.4. Contrôle d'accès aux informations publiées

L'ensemble des informations publiées à destination des utilisateurs de certificats doit être libre d'accès en lecture.

	Niveau (***)	
L'accès en modification aux systèmes de publication (ajout, suppression, modification des informations publiées) doit être strictement limité aux fonctions internes habilitées de l'IGC, au travers d'un contrôle d'accès fort (basé sur une authentification au moins à deux facteurs).		

	Niveau (**)	

[12] Le PSCE décrira dans sa PC/DPC les moyens mis en œuvre pour respecter cet engagement.

L’accès en modification aux systèmes de publication des informations d’état des certificats (ajout, suppression, modification des informations publiées) doit être strictement limité aux fonctions internes habilitées de l’IGC, au travers d’un contrôle d’accès fort (basé sur une authentification au moins à deux facteurs).

	Niveau (**)	
L’accès en modification aux systèmes de publication des autres informations doit être strictement limité aux fonctions internes habilitées de l’IGC, au moins au travers d’un contrôle d’accès de type mots de passe basé sur une politique de gestion stricte des mots de passe.		

	Niveau (*)	
L’accès en modification aux systèmes de publication (ajout, suppression, modification des informations publiées) doit être strictement limité aux fonctions internes habilitées de l’IGC, au moins au travers d’un contrôle d’accès de type mots de passe basé sur une politique de gestion stricte des mots de passe.		

III. Identification et authentification

III.1. Nommage

III.1.1 Types de noms

Les noms utilisés doivent être conformes aux spécifications de la norme [X.500].

Dans chaque certificat conforme à la norme [X.509], l'AC émettrice (issuer) et le porteur (subject) sont identifiés par un «Distinguished Name» (DN) répondant aux exigences de la norme [X.501].

Des règles sur la construction du DN de ces champs sont précisées dans le document [RGS_A_4].

III.1.2. Nécessité d'utilisation de noms explicites

Les noms choisis pour désigner les porteurs de certificats doivent être explicites.

Lorsqu'un pseudonyme est utilisé, il doit être explicitement identifié comme tel dans le DN.

Dans le cas contraire, le DN du porteur est construit à partir des nom et prénom de son état civil tel que porté sur les documents d'identité présentés lors de son enregistrement auprès de l'AE ou, le cas échéant, du MC.

III.1.3. Pseudonymisation des porteurs

L'AC doit pouvoir à tout moment être en mesure de fournir, moyennant le respect de ses obligations en matière de protection des données personnelles (cf. chapitre IX.4), l'identité réelle du porteur en conservant les caractéristiques et références des documents présentés par le porteur pour justifier de son identité.

L'identifiant d'un porteur dans son certificat peut être un pseudonyme à condition d'être identifié comme tel (cf. [RGS_A4]).

III.1.4. Règles d'interprétation des différentes formes de nom

Le document [RGS_A4] fournit des règles à ce sujet. Le cas échéant des précisions seront fournies par l'AC dans sa PC.

III.1.5. Unicité des noms

Le DN du champ «subject» de chaque certificat de porteur doit permettre d'identifier de façon unique le porteur correspondant au sein du domaine de l'AC.

Ce DN doit pour cela respecter les règles correspondantes définies dans le document [RGS_A4], notamment pour le traitement des cas d'homonymie au sein du domaine de l'AC.

Durant toute la durée de vie de l'AC, un DN attribué à un porteur de certificats ne peut être attribué à un autre porteur. L'AC précisera dans sa PC et sa DPC comment elle répond à cette exigence.

Il est à noter que l'unicité d'un certificat est basée sur l'unicité de son numéro de série à l'intérieur du domaine de l'AC, mais que ce numéro est propre au certificat et non pas au porteur et ne permet donc pas d'assurer une continuité de l'identification dans les certificats successifs d'un porteur donné.

III.1.6. Identification, authentification et rôle des marques déposées

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

L'AC est responsable de l'unicité des noms de ses porteurs et de la résolution des litiges portant sur la revendication d'utilisation d'un nom.

Des précisions seront fournies dans la PC de l'AC.

III.2. Validation initiale de l'identité

L'enregistrement d'un porteur peut se faire soit directement auprès de l'AE, soit via un mandataire de certification de l'entité dans le cas des certificats délivrés à des agents d'AA ou des employés d'entreprises. Dans ce dernier cas, le MC doit être préalablement enregistré par l'AE.

La vérification et la validation initiales de l'identité d'une entité, d'une personne physique et éventuellement de son rattachement à une entité, est ainsi réalisée dans les cas suivants :

		[Entreprise] [Administration]
➢ Enregistrement d'un porteur sans MC : validation par l'AE de l'identité «personne morale» de l'entité de rattachement du porteur, de l'identité «personne physique» du futur porteur et du rattachement du futur porteur à l'entité. ➢ Enregistrement d'un MC : validation de l'identité «personne morale» de l'entité pour laquelle le MC interviendra, de l'identité «personne physique» du futur MC et du rattachement du futur MC à l'entité. ➢ Enregistrement d'un porteur via un MC : validation par le MC de l'identité «personne physique» du futur porteur et de son rattachement à l'entité pour laquelle le MC intervient.		

		[Particulier]
Enregistrement d'un porteur [PARTICULIER] : validation par l'AE de l'identité «personne physique» du futur porteur.		

Pour des raisons de simplicité de présentation, ces différents cas sont regroupés dans le chapitre III.2.3.

III.2.1. Méthode pour prouver la possession de la clé privée

Lorsque c'est le porteur qui génère sa bi-clé, il doit alors fournir à l'AC, via le MC le cas échéant, une preuve de possession de sa clé privée correspondant à la clé publique contenue dans la demande de certificat.

III.2.2. Validation de l'identité d'un organisme

Cf. chapitre III.2.3

III.2.3. Validation de l'identité d'un individu

III.2.3.1. Enregistrement d'un porteur [Particulier]

Dossier d'enregistrement :

Le dossier d'enregistrement, déposé auprès de l'AE, doit au moins comprendre :

- une demande de certificat écrite signée, et datée de moins de 3 mois, par le futur porteur,
- un document officiel d'identité en cours de validité du futur porteur comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour), qui est présenté à l'AE qui en conserve une copie,
- l'adresse postale et / ou l'adresse mail permettant à l'AC de contacter le porteur,
- les conditions générales d'utilisation signées.

[Signature]	**Niveau (***)**	

➢ L'engagement relatif à l'utilisation d'un dispositif sécurisé de création de signature conforme aux exigences de l'annexe 3, dans le cas où le PSCE ne le délivre pas.

Nota 1 – Certaines pièces constitutives du dossier d'enregistrement, ou leur signature par le porteur, peuvent être fournies ou réalisées lors de la remise du certificat par l'AC.

Nota 2 - Le porteur doit être informé que les informations personnelles d'identité pourront être utilisées comme éléments d'authentification lors de la demande de révocation, dans le cas où l'AC s'appuie sur un tel mécanisme. En complément, ou à la place, de l'utilisation de ces informations personnelles, il pourra être convenu avec l'AC d'un jeu de questions/réponses ou équivalent.

Nota 3 - Lorsque le porteur est un mineur ou un incapable majeur, la demande de certificat écrite est signée par son représentant (tuteur ou administration légale). Ce dernier joint également à la demande un document officiel de sa propre identité et un document justifiant son statut de représentant du mineur ou de l'incapable majeur.

Procédure de vérification de l'identité du porteur :

	Niveau (***)	
La vérification de l'identité du porteur par l'AE est réalisée lors d'un face-à-face physique[13].		

	Niveau (**)	
L'authentification du porteur par l'AE est réalisée lors d'un face-à-face physique[14] ou sous forme dématérialisée à condition que la demande soit signée par le porteur à l'aide d'un procédé de signature électronique conforme au minimum aux exigences du niveau (**)[15] décrites dans le document [RGS_A1] et que la signature soit vérifiée et valide au moment de l'enregistrement.		

	Niveau (*)	
L'authentification du porteur peut notamment se faire : ➢ Soit par l'envoi du dossier papier à l'AE accompagné d'une photocopie du document d'identité d futur porteur certifiée conforme par lui-même (date, de moins de 3 mois, et signature du futur porteu sur la photocopie de ses papiers d'identité, précédées de la mention «copie certifiée conforme l'original»). ➢ Soit via une demande d'enregistrement dématérialisée signée électroniquement par le futur porteur à l'aide d'un procédé de signature électronique conforme aux exigences du niveau (*) décrites dans le document [RGS_A_3] et que la signature soit vérifiée et valide au moment de l'enregistrement.		

[13] Ce face-à-face physique peut être réalisé lors de la remise par l'AC au porteur du certificat ainsi que du dispositif de stockage de la bi-clé si et seulement si cette dernière est générée par l'AC. Si tel est le cas, l'AC décrira dans sa PC la façon dont elle s'assure de la fiabilité des informations contenues dans le dossier d'enregistrement du futur porteur. Il est toutefois recommandé de procéder au face-à-face physique dès la phase d'enregistrement.

[14] Cf. note de bas de page n°13.

[15] Il est recommandé que le procédé de signature électronique soit conforme aux exigences du niveau (***) afin que la signature soit présumée fiable.

➢ Soit par la communication d'un élément propre au futur porteur permettant de l'identifier au sein d'une base de données administrative pré-établie.

III.2.3.2. Enregistrement d'un porteur [Entreprise] / [Administration] sans MC

L'enregistrement du futur porteur représentant une entité nécessite, l'identification de cette entité, l'identification de la personne physique et la preuve du rattachement de la personne physique à l'entité.

Dossier d'enregistrement :

Le dossier d'enregistrement, déposé directement auprès de l'AE, doit au moins comprendre :

- un mandat signé, et daté de moins de 3 mois, par un représentant légal de l'entité désignant le futur porteur auquel le certificat doit être délivré. Ce mandat doit être signé pour acceptation par le futur porteur bénéficiaire,
- [Entreprise] toute pièce, valide lors de la demande de certificat (extrait Kbis ou situation au Répertoire Territoriale des Entreprises, ...), attestant de l'existence de l'entreprise et portant le numéro TAHITI de celle-ci, ou, à défaut, une autre pièce attestant l'identification unique de l'entreprise qui figurera dans le certificat,
- [Entreprise] tout document attestant de la qualité du signataire de la demande de certificat,
- [Administration] une pièce, valide au moment de l'enregistrement, portant délégation de l'autorité responsable de la structure administrative,
- un document officiel d'identité en cours de validité du futur porteur ou une carte professionnelle délivrée par une autorité administrative[16], comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour) ou une référence au dossier administratif de l'agent. Ces documents sont transmis à l'AE qui en conserve une copie ou les traces,
- l'adresse postale et / ou l'adresse mail permettant à l'AC de contacter le porteur,
- les conditions générales d'utilisation signées.

[Signature]	**Niveau (***)**	
➢ l'engagement relatif à l'utilisation d'un dispositif sécurisé de création de signature conforme aux exigences de l'annexe 3, dans le cas où le PSCE ne le délivre pas.		

Nota 1 - Le porteur doit être informé que les informations personnelles d'identité pourront être utilisées comme élément d'authentification lors de la demande de révocation, dans le cas où l'AC s'appuie sur un tel mécanisme. En complément, ou à la place, de l'utilisation de ces informations personnelles, il pourra être convenu avec l'AC d'un jeu de questions/réponses ou équivalent.

Nota 2 – Ce dossier d'enregistrement peut être complété, si non complet à l'issue de la phase d'enregistrement, lors de la remise du certificat (et éventuellement de la bi-clé).

Procédure d'enregistrement du porteur :

[16] L'autorité administrative doit, dans ce cas, maintenir un registre des identités garantissant le lien entre l'agent et la carte professionnelle.

	Niveau (***)	
L'authentification du porteur par l'AE est réalisée lors d'un face-à-face physique[17].		

	Niveau (**)	
L'authentification du porteur par l'AE est réalisée lors d'un face-à-face physique[18] ou sous forme dématérialisée à condition que la demande soit signée par le porteur à l'aide d'un procédé de signature électronique conforme au minimum aux exigences du niveau (**)[19] décrites dans le document [RGS_A1] et que la signature soit vérifiée et valide au moment de l'enregistrement.		

	Niveau (*)	
L'authentification du porteur peut notamment se faire : ➢ Soit par l'envoi du dossier papier à l'AE accompagné d'une photocopie du document d'identité du futur porteur certifiée conforme par lui-même (date, de moins de 3 mois, et signature du futur porteur sur la photocopie de ses papiers d'identité, précédées de la mention «copie certifiée conforme à l'original»). ➢ Soit via une demande d'enregistrement dématérialisée signée électroniquement par le futur porteur à l'aide d'un procédé de signature électronique conforme aux exigences du niveau (*) décrites dans le document [RGS_A_3] et que la signature soit vérifiée et valide au moment de l'enregistrement. ➢ Soit par la communication d'un élément propre au futur porteur permettant de l'identifier au sein d'une base de données administrative pré-établie.		

III.2.3.3. Enregistrement d'un Mandataire de Certification

L'ensemble de ce chapitre ne concerne que les certificats [ENTREPRISE] / [ADMINISTRATION].

Une AE est amenée à constituer un dossier d'enregistrement pour un Mandataire de Certification pour répondre aux besoins suivants :

- Utilisation du dossier du MC comme référence pour les données d'identification de l'entité de tous les porteurs présentés par le MC.
- Éventuellement, fourniture de certificats électronique au MC pour qu'il puisse signer les dossiers d'enregistrement de porteurs de l'entité qu'il représente, s'authentifier auprès du service d'AC et transmettre les dossiers de façon sécurisée.

[17] Le face-à-face physique peut être réalisé lors de la remise par l'AC au porteur du certificat ainsi que du dispositif de stockage de la bi-clé si et seulement si cette dernière est générée par l'AC. Si tel est le cas, l'AC décrira dans sa PC la façon dont elle s'assure de la fiabilité des informations contenues dans le dossier d'enregistrement du futur porteur. Il est toutefois recommandé de procéder au face-à-face physique dès la phase d'enregistrement.

[18] Le face-à-face physique peut être réalisé lors de la remise par l'AC au porteur du certificat ainsi que du dispositif de stockage de la bi-clé si et seulement si cette dernière est générée par l'AC. Si tel est le cas, l'AC décrira dans sa PC la façon dont elle s'assure de la fiabilité des informations contenues dans le dossier d'enregistrement du futur porteur. Il est toutefois recommandé de procéder au face-à-face physique dès la phase d'enregistrement.

[19] Il est recommandé que le procédé de signature électronique soit conforme aux exigences du niveau (***) afin que la signature soit présumée fiable.

Dossier d'enregistrement :

Le dossier d'enregistrement d'un MC doit au moins comprendre :

- un mandat signé, et daté de moins de 3 mois, par un représentant légal de l'entité désignant le MC. Ce mandat doit être signé par le MC pour acceptation,
- un engagement signé, et daté de moins de 3 mois, du MC, auprès de l'AC, à effectuer correctement et de façon indépendante les contrôles des dossiers des demandeurs,
- un engagement signé, et daté de moins de 3 mois, du MC à signaler à l'AE son départ de l'entité,
- [Entreprise] toute pièce, valide lors de la demande de certificat (extrait Kbis ou situation au Répertoire Territoriale des Entreprises, ...), attestant de l'existence de l'entreprise et portant le numéro TAHITI de celle-ci, ou, à défaut, une autre pièce attestant l'identification unique de l'entreprise qui figurera dans le certificat,
- [Administration] une pièce, valide au moment de l'enregistrement, portant délégation de l'autorité responsable de la structure administrative,
- Un document officiel d'identité en cours de validité du MC ou une carte professionnelle délivrée par une autorité administrative[20], comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour) ou une référence au dossier administratif du MC. Ces documents sont transmis à l'AE qui en conserve une copie ou les traces,

Nota - Le MC doit être informé que les informations personnelles d'identité pourront être utilisées comme éléments d'authentification lors de la demande de révocation, dans le cas où l'AC s'appuie sur un tel mécanisme. En complément, ou à la place, de l'utilisation de ces informations personnelles, il pourra être convenu avec l'AC d'un jeu de questions/réponses ou équivalent.

Procédure d'enregistrement :

	Niveau (***)	
L'authentification du MC par l'AE est réalisée lors d'un face-à-face physique[21].		

	Niveau (**)	
L'authentification du MC par l'AE est réalisée lors d'un face-à-face physique[22] ou sous forme dématérialisée à condition que le dossier de demande soit signé par le MC à l'aide d'un procédé de signature électronique conforme au minimum aux exigences du niveau (**)[23] décrites dans le document [RGS_A1] et que la signature soit vérifiée et valide au moment de l'enregistrement.		

[20] L'autorité administrative doit, dans ce cas, maintenir un registre des identités garantissant le lien entre l'agent et la carte professionnelle.

[21] Le face-à-face physique peut être réalisé lors de la remise par l'AC au porteur du certificat ainsi que du dispositif de stockage de la bi-clé si et seulement si cette dernière est générée par l'AC. Si tel est le cas, l'AC décrira dans sa PC la façon dont elle s'assure de la fiabilité des informations contenues dans le dossier d'enregistrement du futur porteur. Il est toutefois recommandé de procéder au face-à-face physique dès la phase d'enregistrement.

[22] Cf. note de bas de page précédente.

[23] Il est recommandé que le procédé de signature électronique soit conforme aux exigences du niveau (***) afin que la signature soit présumée fiable.

	Niveau (*)	
L'authentification du MC par l'AE peut se faire par l'envoi du dossier papier par courrier accompagné d'une photocopie des documents d'identité de chacun des signataires des pièces du dossier (représentant légal, MC) certifiée conforme par le signataire concerné (date, de moins de 3 mois, et signature de la personne concernée sur la photocopie de ces papiers d'identité, précédées de la mention « copie certifiée conforme à l'original »). Cette authentification peut également se faire sous forme dématérialisée à condition que les différentes pièces justificatives du dossier soient signées à l'aide d'un procédé de signature électronique conforme aux exigences du niveau (*) décrites dans le document [RGS_A_3] et que la signature soit vérifiée et valide au moment de l'enregistrement.		

III.2.3.4. Enregistrement d'un porteur [Entreprise] / [Administration] via un MC

Dossier d'enregistrement :

Le dossier d'enregistrement, déposé auprès d'un MC, doit au moins comprendre :

- une demande de certificat, datée de moins de 3 mois, indiquant l'identité du porteur, co-signé par le porteur et le MC,
- un document officiel d'identité en cours de validité du futur porteur ou une carte professionnelle délivrée par une autorité administrative[24], comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour) ou une référence au dossier administratif de l'agent. Ces documents sont transmis à l'AE qui en conserve une copie ou les traces,
- l'adresse postale et / ou l'adresse mail permettant à l'AC de contacter le porteur,
- les conditions générales d'utilisation signées.

[Signature]	**Niveau (***)**	
➢ l'engagement relatif à l'utilisation d'un dispositif sécurisé de création de signature conforme aux exigences de l'annexe 3, dans le cas ou le PSCE ne le délivre pas.		

Nota 1 – Le porteur doit être informé que les informations personnelles d'identité pourront être utilisées comme éléments d'authentification lors de la demande de révocation, dans le cas où l'AC s'appuie sur un tel mécanisme. En complément, ou à la place, de l'utilisation de ces informations personnelles, il pourra être convenu avec l'AC d'un jeu de questions/réponses ou équivalent.

Nota 2 – Ce dossier d'enregistrement peut être complété, si non complet à l'issue de la phase d'enregistrement, lors de la remise du certificat (et éventuellement de la bi-clé).

Procédure d'enregistrement :

	Niveau (***)	
L'authentification du porteur par le MC est réalisée lors d'un face-à-face physique[25].		

[24] L'autorité administrative doit, dans ce cas, maintenir un registre des identités garantissant le lien entre l'agent et la carte professionnelle.

[25] Le face-à-face physique permettant au MC de vérifier l'identité du porteur peut être réalisé lors de la remise par l'AC au porteur du certificat ainsi que du dispositif de stockage de la bi-clé si et seulement si cette dernière est générée par l'AC. Si tel est

	Niveau (**)	
L'authentification du porteur par le MC est réalisée lors d'un face-à-face physique[26] ou sous forme dématérialisée à condition que le dossier de demande soit signé par le porteur à l'aide d'un procédé de signature électronique conforme au minimum aux exigences du niveau (**)[27] décrites dans le document [RGS_A_3] et que la signature soit vérifiée et valide au moment de l'enregistrement.		

	Niveau (*)	
L'authentification du porteur par le MC peut se faire par l'envoi du dossier papier par courrier accompagné d'une photocopie des documents d'identité de chacun des signataires des pièces du dossier (représentant légal, [porteur/MC]) certifiée conforme par le signataire concerné (date, de moins de 3 mois, et signature de la personne concernée sur la photocopie de ses papiers d'identité précédées de la mention «copie certifiée conforme à l'original»). Cette authentification peut également se faire sous forme dématérialisée à condition que les différentes pièces justificatives du dossier soient signées à l'aide d'un procédé de signature électronique conforme aux exigences du niveau (*) décrites dans le document [RGS_A1] et que la signature soit vérifiée et valide au moment de l'enregistrement.		

Lors de la transmission des dossiers de porteurs par le MC, celui-ci doit s'authentifier auprès de l'AE :

- soit à l'aide d'un certificat électronique remis par l'AC,
- soit au cours d'un face-à-face et/ou par le paraphe du MC apposé sur les différentes pages du dossier de demande, complété par sa signature sur les principales pages.

III.2.4. Informations non vérifiées du porteur

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

III.2.5. Validation de l'autorité du demandeur

		[Entreprise] / [Administration]
Cette étape est effectuée en même temps que la validation de l'identité de la personne physique (directement par l'AE ou par le MC).		

III.2.6. Critères d'interopérabilité

L'AC gère et documente les demandes d'accords et les accords de reconnaissance avec des AC extérieures au domaine de sécurité auquel l'AC appartient.

III.3. Identification et validation d'une demande de renouvellement des clés

Le renouvellement de la bi-clé d'un porteur entraîne automatiquement la génération et la fourniture d'un

---

le cas, l'AC décrira dans sa PC la façon dont elle s'assure de la fiabilité des informations contenues dans le dossier d'enregistrement du futur porteur. Il est toutefois recommandé de procéder au face-à-face physique dès la phase d'enregistrement.

[26] Cf. note de bas de page précédente.

[27] Il est recommandé que le procédé de signature électronique soit conforme aux exigences du niveau (***) afin que la signature soit présumée fiable.

nouveau certificat. De plus, un nouveau certificat ne peut pas être fourni au porteur sans renouvellement de la bi-clé correspondante (cf. chapitre IV.6).

Ce chapitre concerne aussi bien le cas où la bi-clé est générée par le porteur que le cas où elle est générée par l'AC.

III.3.1. Identification et validation pour un renouvellement courant

	Niveau (**) et (***)	
Lors du premier renouvellement, l'AC doit au minimum s'assurer que les informations du dossier d'enregistrement initial sont toujours valides et que le certificat à renouveler existe, et est toujours valide.		

	Niveau (*)	
Lors du premier renouvellement, la vérification de l'identité du porteur est optionnelle. Elle est laissée à l'appréciation de l'AC qui engage sa responsabilité quant à la validité des informations contenues dans le certificat renouvelé.		

Lors du renouvellement suivant, l'AE, saisie de la demande, identifiera le porteur selon la même procédure que pour l'enregistrement initial ou une procédure offrant un niveau de garantie équivalent.

III.3.2. Identification et validation pour un renouvellement après révocation

Suite à la révocation définitive d'un certificat, quelle qu'en soit la cause, la procédure d'identification et de validation de la demande de renouvellement doit être identique à la procédure d'enregistrement initial ou doit être une procédure offrant un niveau de garantie équivalent.

III.4. Identification et validation d'une demande de révocation

	Niveau (***)	
Si la demande de révocation est faite via un service téléphonique ou via un service en ligne (serveur web), le demandeur doit être formellement authentifié : vérification de l'identité du demandeur et de son autorité par rapport au certificat à révoquer. Par exemple : série d'au moins 4 ou 5 questions / réponses sur des informations propres au demandeur, dont au moins une réponse ne peut réellement être connue que du demandeur (question d'identification personnelle liée au demandeur et/ou dont la réponse a été choisie au moment de l'enregistrement ou lors du retrait du certificat (cf. chapitre III.2.3), utilisation d'un identifiant / mot de passe envoyé préalablement au demandeur de façon sécurisée).		

	Niveau (**)	
Si la demande de révocation est faite via un service téléphonique ou via un service en ligne (serveur web), le demandeur doit être formellement authentifié : vérification de l'identité du demandeur et de son autorité par rapport au certificat à révoquer. Par exemple : série d'au moins 3 ou 4 questions / réponses sur des informations propres au demandeur, dont au moins une réponse ne peut réellement être connue que du demandeur (question d'identification personnelle liée au demandeur et/ou dont la réponse a été choisie au moment de l'enregistrement ou lors du retrait du certificat, utilisation d'un identifiant / mot de passe envoyé préalablement au demandeur de façon sécurisée).		

	Niveau (*)	
Si la demande de révocation est faite via un service téléphonique ou via un service en ligne (serveur web), elle doit faire l'objet d'un minimum d'authentification : vérification d'une ou deux informations de base du demandeur (adresse, n° de téléphone, etc.) et de son autorité par rapport au certificat à révoquer.		

Une demande de révocation peut également être faite par courrier ou par télécopie. Elle doit alors être signée par le demandeur et le service de gestion des révocations doit s'assurer de l'identité du demandeur (vérification de la signature manuscrite par rapport à une signature préalablement enregistrée) et de son autorité par rapport au certificat à révoquer.

IV. Exigences opérationnelles sur le cycle de vie des certificats

IV.1. Demande de certificat

IV.1.1. Origine d'une demande de certificat

		[Entreprise] / [Administration]
Un certificat peut être demandé par un représentant légal de l'entité ou un MC dûment mandaté pour cette entité, après consentement préalable du futur porteur ou, si les raisons du service l'exigent, pour une administration, après vérification que le futur porteur a été informé de ses responsabilités et les a accepté au sein d'une attestation personnelle de responsabilité.		

		[Particulier]
Un certificat ne peut être demandé que par le futur porteur ou par le représentant d'un incapable majeur ou d'un mineur[28].		

IV.1.2. Processus et responsabilités pour l'établissement d'une demande de certificat

Les informations suivantes doivent au moins faire partie de la demande de certificat (cf. chapitre III.2 ci-dessus) :

- Le nom du porteur à utiliser dans le certificat ;
- Les données personnelles d'identification du porteur[29] ;

		[Entreprise] / [Administration]
➢ les données d'identification de l'entité (sauf si l'enregistrement est effectué par l'intermédiaire d'un MC).		

[Confidentialité]		
➢ Le cas échéant, la demande de certificat (cf. chapitre III.2 ci-dessus) doit intégrer les informations concernant la demande de séquestre de la clé privée du porteur correspondant au certificat sur lequel porte la demande et la durée souhaitée de conservation de la clé privée séquestrée.		

		[Entreprise] / [Administration]
Le dossier de demande est établi soit directement par le futur porteur à partir des éléments fournis par son entité, soit par son entité et signé par le futur porteur. Si l'entreprise n'a pas mis en place de MC, le dossier est transmis directement à l'AE. Si l'entreprise a mis en place un MC, le dossier lui est remis.		

[28] Le représentant d'un mineur peut être un administrateur légal (parents du mineur) ou un tuteur désigné par le juge des tutelles tel que défini dans le code civil. Le représentant d'un incapable majeur peut être un curateur ou un tuteur désigné par le juge des tutelles tel que défini dans le code civil.

[29] Afin de pouvoir traiter les cas d'homonymie, le nom et le prénom doivent être complétés par une donnée complémentaire qui permet d'assurer l'unicité des DN durant toute la durée de vie de l'AC.

		[Particulier]
Le dossier de demande est établi par le futur porteur et transmis à l'AE.		

Par ailleurs, l'AE doit s'assurer de disposer d'une information permettant de contacter le MC ou le futur porteur du certificat.

IV.2. Traitement d'une demande de certificat

IV.2.1. Exécution des processus d'identification et de validation de la demande

Les identités « personne physique » et, le cas échéant, «personne morale» sont vérifiées conformément aux exigences du chapitre III.2.

L'AE, ou le MC le cas échéant, doit effectuer les opérations suivantes :

- Valider l'identité du futur porteur ;
- Vérifier la cohérence des justificatifs présentés ;
- Vérifier que le futur porteur a pris connaissance des modalités applicables pour l'utilisation du certificat. (Voir les conditions générales d'utilisation), à moins que cette vérification ne soit effectuée lors de la remise de la carte.

		[Entreprise] / [Administration]
Dans le cas d'une demande via un MC, celui-ci retransmet le dossier à l'AE après avoir effectué les opérations ci-dessus. L'AE doit alors s'assurer que la demande correspond bien au mandat du MC.		

Une fois ces opérations effectuées, l'AE émet la demande de génération du certificat et, le cas échéant, de la bi-clé vers la fonction adéquate de l'IGC (cf. chapitre I.4.1).

L'AE conserve ensuite une trace des justificatifs d'identité présentés :

- Si le dossier est au format papier, sous la forme d'une photocopie signée à la fois par le futur porteur et par l'AE, ou le MC le cas échéant, les signatures étant précédées de la mention « copie certifiée conforme à l'original » ;
- Si le dossier est au format électronique, les différents justificatifs ou les informations de traçabilité (sous une forme électronique ayant valeur légale).

IV.2.2. Acceptation ou rejet de la demande

En cas de rejet de la demande, l'AE en informe le porteur, ou le MC le cas échéant, en justifiant le rejet.

IV.2.3. Durée d'établissement du certificat

La présente PC Type ne formule pas d'exigence spécifique sur le sujet. À préciser par l'AC dans sa PC, en visant une durée d'établissement la plus courte possible.

IV.3. Délivrance du certificat

IV.3.1. Actions de l'AC concernant la délivrance du certificat

Suite à l'authentification de l'origine et à la vérification de l'intégrité de la demande provenant de l'AE, l'AC déclenche les processus de génération et de préparation des différents éléments destinés au porteur : au

minimum, le certificat[30], et, selon les cas, la bi-clé du porteur, son dispositif de protection des éléments secrets, les codes d'activation, etc. (cf. chapitre I.4.1).

Si l'AC génère la bi-clé du porteur, le processus de génération du certificat doit être lié de manière sécurisée au processus de génération de la bi-clé : l'ordonnancement des opérations doit être assuré ainsi que, le cas échéant en fonction de l'architecture de l'IGC, l'intégrité et l'authentification des échanges entres les composantes. Par ailleurs, la clé privée doit être transmise de façon sécurisée au porteur, en en garantissant l'intégrité et la confidentialité.

Les conditions de génération des clés et des certificats et les mesures de sécurité à respecter sont précisées aux chapitres V et VI ci-dessous, notamment la séparation des rôles de confiance (cf. chapitre V.2).

IV.3.2. Notification par l'AC de la délivrance du certificat au porteur

	Niveau (**) et (***)	
La remise du certificat doit se faire en mains propres (face-à-face) au minimum dans le cas où l'authentification du porteur se fait via un face-à-face et que ce face-à-face n'a pas eu lieu au moment de l'enregistrement (cf. chapitre III.2). Si la remise du certificat ne se fait pas en mains propres, l'AC précisera dans sa PC comment elle s'assure que le certificat est bien remis au bon porteur ou à une personne dûment autorisée (par exemple, envoi sur carte à puce ou sur disquette en courrier recommandé, téléchargement grâce à un code d'accès préalablement fourni au porteur, ...).		

	Niveau (***)	
De plus, si l'AC n'a pas généré elle-même la bi-clé du porteur, elle doit s'assurer que le certificat est bien associé, dans l'environnement du porteur, à la clé privée correspondante (par exemple, mise à disposition d'une application en ligne permettant de réaliser une authentification de test). Il s'agit notamment du cas où le certificat est associé à une clé privée stockée sur une carte à puce non fournie par l'AC : le certificat doit alors être téléchargé sur la bonne carte à puce.		

	Niveau (*)	
Le certificat peut-être transmis par message électronique à une adresse fournie par le porteur, ou bien l'URL permettant de télécharger le certificat peut être envoyée à une telle adresse.		

Le certificat complet et exact doit être mis à la disposition du MC ou de son porteur.

Nota – Si la remise du certificat doit se faire en mains propres auprès de l'AE, le porteur ou MC sera également tributaire des modalités d'accueil de l'AE.

IV.4. Acceptation du certificat

IV.4.1. Démarche d'acceptation du certificat

	Niveau (***)	

[30] Si la bi-clé est générée par le porteur, la clé publique doit être transmise à l'AC (cf. chapitre VI.1.3).

L'AC doit obtenir confirmation de l'acceptation explicite du certificat par le porteur sous la forme d'un accord signé (papier ou électronique) ou de l'attestation personnelle de responsabilité (cf. IV.1.1). L'AC doit garder une trace de l'acceptation du certificat par le porteur.

	Niveau (**)	
L'AC doit obtenir confirmation de l'acceptation du certificat par le porteur, si possible de façon explicite sous la forme d'un accord signé (papier ou électronique), ou de l'attestation personnelle de responsabilité (cf. IV.1.1). Si la remise du certificat au porteur, ou le cas échéant à son MC, peut faire l'objet d'une date connue avec un degré suffisant de certitude, l'AC peut s'appuyer sur un mécanisme d'acceptation tacite du certificat moyennant un délai maximum laissé au porteur, à compter de la date de réception de son certificat, pour signaler sa non-acceptation du certificat. La première utilisation du certificat peut également valoir acceptation tacite. Dans le cas d'une acceptation tacite, les obligations du porteur et le délai correspondant doivent être clairement mentionnés dans la PC de l'AC ainsi que dans les conditions générales d'utilisation (cf. chapitre II.2) et/ou le contrat porteur. L'AC doit garder une trace de l'acceptation du certificat par le porteur si celle-ci est explicite.		

	Niveau (*)	
L'acceptation peut être tacite à compter de la date d'envoi du certificat (ou des informations de téléchargement) au porteur. Le processus d'acceptation du certificat et les obligations correspondantes du porteur doivent être clairement mentionnés dans la PC de l'AC ainsi que dans les conditions générales d'utilisation (cf. chapitre II.2) et/ou le contrat porteur.		

IV.4.2. Publication du certificat

Si le certificat fait l'objet d'une publication par l'AC, les conditions d'une telle publication doivent être précisées par l'AC dans sa PC. Notamment, cette publication ne peut avoir lieu sans l'accord du porteur du certificat et qu'après acceptation du contenu du certificat par celui-ci.

IV.4.3. Notification par l'AC aux autres entités de la délivrance du certificat

L'AC informe l'AE de la délivrance du certificat, qui se charge d'en informer le MC le cas échéant.

IV.5. Usages de la bi-clé et du certificat

IV.5.1. Utilisation de la clé privée et du certificat par le porteur

L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée à la fonction de sécurité concernée (cf. chapitre I.5.1.1). Les porteurs doivent respecter strictement les usages autorisés des bi-clés et des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.

L'usage autorisé de la bi-clé du porteur et du certificat associé doit par ailleurs être indiqué dans le certificat lui-même, via les extensions concernant les usages des clés (cf. [RGS_A4]). Cet usage doit également être clairement explicité dans la PC de l'AC, ainsi que dans les conditions générales d'utilisation et/ou le contrat porteur. Faisant partie du dossier d'enregistrement, les conditions générales sont portées à la connaissance du porteur ou du MC par l'AC avant d'entrer en relation contractuelle.

IV.5.2. Utilisation de la clé publique et du certificat par l'utilisateur du certificat

Cf. chapitre précédent et chapitre I.5.

Les utilisateurs de certificats doivent respecter strictement les usages autorisés des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.

IV.6. Renouvellement d'un certificat

Conformément au [RFC3647], la notion de «renouvellement de certificat» correspond à la délivrance d'un nouveau certificat pour lequel seules les dates de validité sont modifiées, toutes les autres informations sont identiques au certificat précédent (y compris la clé publique du porteur).

Dans le cadre de la présente PC Type, il ne peut pas y avoir de renouvellement de certificat sans renouvellement de la bi-clé correspondante. Aussi, si c'est l'AC qui génère les bi-clés des porteurs, elle doit garantir qu'un certificat correspondant à une bi-clé existante ne peut pas être renouvelé au sens du [RFC3647]. Dans le cas contraire, elle doit s'en assurer auprès du porteur, au minimum au travers d'un engagement contractuel clair et explicite du porteur vis-à-vis de l'AC.

IV.7. Délivrance d'un nouveau certificat suite à changement de la bi-clé

Conformément au [RFC3647], ce chapitre traite de la délivrance d'un nouveau certificat au porteur liée à la génération d'une nouvelle bi-clé.

IV.7.1. Causes possibles de changement d'une bi-clé

Les bi-clés doivent être périodiquement renouvelées afin de minimiser les possibilités d'attaques cryptographiques. Ainsi, les bi-clés des porteurs, et les certificats correspondants, seront renouvelés au minimum à une fréquence conforme au tableau suivant :

Description	**Niveau ***	**Niveau ****	**Niveau*****
Durée de vie maximale d'une bi-clé et d'un certificat porteur :			
• Particulier	5 ans	5 ans	5 ans
• Agent	3 ans	3 ans	3 ans
• Entreprise	3 ans	3 ans	3 ans

Par ailleurs, une bi-clé et un certificat peuvent être renouvelés par anticipation, suite à la révocation du certificat du porteur (cf. Chapitre IV.9, notamment le chapitre IV.9.1.1 pour les différentes causes possibles de révocation).

Nota - Dans la suite du présent chapitre, le terme utilisé est « fourniture d'un nouveau certificat ». Ce terme recouvre également, dans le cas où elle est générée par l'AC, la fourniture de la nouvelle bi-clé du porteur.

IV.7.2. Origine d'une demande d'un nouveau certificat

Le déclenchement de la fourniture d'un nouveau certificat du porteur peut être automatique ou bien à l'initiative du porteur.

[ENTREPRISE] [ADMINISTRATION] L'entité, via son MC le cas échéant, peut également être à l'initiative d'une demande de fourniture d'un nouveau certificat pour un porteur qui lui est rattaché.

IV.7.3. Procédure de traitement d'une demande d'un nouveau certificat

L'identification et la validation d'une demande de fourniture d'un nouveau certificat sont précisées au chapitre III.3 ci-dessus.

Pour les actions de l'AC, cf. chapitre IV.3.1.

IV.7.4. Notification au porteur de l'établissement du nouveau certificat

Cf. chapitre IV.3.2.

IV.7.5. Démarche d'acceptation du nouveau certificat

Cf. chapitre IV.4.1.

IV.7.6. Publication du nouveau certificat

Cf. chapitre IV.4.2.

IV.7.7. Notification par l'AC aux autres entités de la délivrance du nouveau certificat

Cf. chapitre IV.4.3.

IV.8. Modification du certificat

Conformément au [RFC3647], la modification d'un certificat correspond à des modifications d'informations sans changement de la clé publique (cf. chapitre IV.7) et autres qu'uniquement la modification des dates de validité (cf. chapitre IV.6).

La modification de certificat n'est pas recommandée dans la présente PC Type. Toutefois, si elle est mise en œuvre, elle doit modifier le numéro de série du certificat, révoquer le certificat initial et ne concerner que les certificats d'utilisateurs finaux.

IV.9. Révocation et suspension des certificats

IV.9.1. Causes possibles d'une révocation

IV 9.1.1. Certificats de porteurs

Les circonstances suivantes peuvent être à l'origine de la révocation du certificat d'un porteur :

- Les informations du porteur figurant dans son certificat ne sont plus en conformité avec l'identité ou l'utilisation prévue dans le certificat (par exemple changement du nom de famille suite à un mariage), ceci avant l'expiration normale du certificat ;
- Le porteur n'a pas respecté les modalités applicables d'utilisation du certificat ;
- Le porteur et/ou, le cas échéant, le MC / l'entité n'ont pas respecté leurs obligations découlant de la PC de l'AC ;
- Une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement du porteur ;
- La clé privée du porteur est suspectée de compromission, est compromise, est perdue ou est volée (éventuellement les données d'activation associées) ;
- Le porteur ou une entité autorisée (représentant légal de l'entité ou MC par exemple) demande la révocation du certificat (notamment dans le cas d'une destruction ou altération de la clé privée du porteur et/ou de son support) ;
- Le décès du porteur ou la cessation d'activité de l'entité du porteur.

Lorsqu'une des circonstances ci-dessus se réalise et que l'AC en a connaissance (elle en est informée ou elle obtient l'information au cours d'une de ses vérifications, lors de la délivrance d'un nouveau certificat notamment), le certificat concerné doit être révoqué.

IV 9.1.2. Certificats d'une composante de l'IGC

Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat d'une composante de

l'IGC (y compris un certificat d'AC pour la génération de certificats, de LCR et/ou de réponses OCSP) :

- Suspicion de compromission, compromission, perte ou vol de la clé privée de la composante ;
- Décision de changement de composante de l'IGC suite à la détection d'une non-conformité des procédures appliquées au sein de la composante avec celles annoncées dans la DPC (par exemple, suite à un audit de qualification ou de conformité négatif) ;
- Cessation d'activité de l'entité opérant la composante.

IV.9.2. Origine d'une demande de révocation

IV.9.2.1. Certificats de porteurs

Les personnes / entités qui peuvent demander la révocation d'un certificat de porteur sont les suivantes :

- Le porteur au nom duquel le certificat a été émis ;
- L'AC émettrice du certificat ou l'une de ses composantes (AE) ;

		[Entreprise] / [Administration]
➢ Le MC ; ➢ un représentant légal de l'entité.		

Nota : Le porteur doit être informé des personnes / entités susceptibles d'effectuer une demande de révocation pour son certificat.

IV.9.2.2. Certificats d'une composante de l'IGC

La révocation d'un certificat d'AC ne peut être décidée que par l'entité responsable de l'AC, ou par les autorités judiciaires via une décision de justice.

La révocation des autres certificats de composantes est décidée par l'entité opérant la composante concernée qui doit en informer l'AC sans délai.

IV.9.3. Procédure de traitement d'une demande de révocation

IV.9.3.1. Révocation d'un certificat de porteur

Les exigences d'identification et de validation d'une demande de révocation, effectuée hors ligne ou en ligne par la fonction de gestion des révocations, sont décrites au chapitre III.4.

L'AC doit préciser dans sa PC comment la fonction de gestion des révocations est organisée et quels sont les points d'accès à cette fonction pour les demandeurs de révocation.

Les informations suivantes doivent au moins figurer dans la demande de révocation de certificat :

- L'identité du porteur du certificat utilisée dans le certificat (nom, prénom, ...) ;
- Le nom du demandeur de la révocation ;
- Toute information permettant de retrouver rapidement et sans erreur le certificat à révoquer (n° de série,...) ;
- Éventuellement, la cause de révocation.

Une fois la demande authentifiée et contrôlée, la fonction de gestion des révocations révoque le certificat correspondant en changeant son statut, puis communique ce nouveau statut à la fonction d'information sur l'état des certificats.

L'information de révocation doit être diffusée au minimum selon l'une des solutions suivantes :

- Via une LCR signée par l'AC elle-même soit par une entité désignée par l'AC ;
- Via un service OCSP dont la réponse est soit signée par le certificat de l'AC ayant émis le certificat à révoquer ou par un certificat de répondeur OCSP lui-même signé par l'AC ayant émis le certificat à révoquer (cf. chapitre IV.9.9).

Le demandeur de la révocation doit être informé du bon déroulement de l'opération et de la révocation effective du certificat. De plus, si le porteur du certificat n'est pas le demandeur, il doit également être informé de la révocation effective de son certificat.

L'opération est enregistrée dans les journaux d'évènements avec, le cas échéant, suffisamment d'informations sur les causes initiales ayant entraîné la révocation du certificat.

IV 9.3.2. Révocation d'un certificat d'une composante de l'IGC

L'AC précisera dans sa DPC les procédures à mettre en œuvre en cas de révocation d'un certificat d'une composante de l'IGC.

En cas de révocation d'un des certificats de la chaîne de certification, l'AC doit informer dans les plus brefs délais et par tout moyen (et si possible par anticipation) l'ensemble des porteurs concernés que leurs certificats ne sont plus valides. Pour cela, l'IGC pourra par exemple envoyer des récépissés aux AE et aux MC. Ces derniers devront informer les porteurs de certificats en leur indiquant explicitement que leurs certificats ne sont plus valides car un des certificats de la chaîne de certification n'est plus valide.

Afin de faciliter la révocation du certificat de l'AC, il est obligatoire que le certificat associé à la clé de l'AC signant les certificats porteurs soit signé par une autre AC et ne soit pas autosigné (cf. chapitre I.4.1.2).

IV.9.4. Délai accordé au porteur pour formuler la demande de révocation

Dès que le porteur (ou une personne autorisée) a connaissance qu'une des causes possibles de révocation, de son ressort, est effective, il doit formuler sa demande de révocation sans délai.

IV.9.5. Délai de traitement par l'AC d'une demande de révocation

IV 9.5.1. Révocation d'un certificat de porteur

Par nature, une demande de révocation doit être traitée en urgence.

IV.9.5.2. Disponibilité du système de traitement des demandes de révocation

La fonction de gestion des révocations doit être disponible aux heures ouvrées au niveau * et 24h/24 et 7j/7 aux niveaux ** et ***. Cette fonction doit avoir une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) conforme au tableau suivant :

Description	**Niveau ***	**Niveau ****	**Niveau *****
Durée maximale d'indisponibilité par interruption (panne ou maintenance) de la fonction de gestion des révocations	2h (jours ouvrées)	2h	1h

Cette fonction doit avoir une durée maximale totale d'indisponibilité par mois conforme au tableau suivant :

Description	**Niveau ***	**Niveau ****	**Niveau *****
Durée maximale totale d'indisponibilité par mois de la fonction de gestion des révocations	16h (jours ouvrées)	8h	4h

Toute demande de révocation d'un certificat porteur doit être traitée dans un délai inférieur à 72h pour un niveau * et inférieur à 24h pour les niveaux ** et ***. Ce délai s'entend entre la réception de la demande de révocation authentifiée et la mise à disposition de l'information de révocation auprès des utilisateurs.

IV.9.5.3. Révocation d'un certificat d'une composante de l'IGC

La révocation d'un certificat d'une composante de l'IGC doit être effectuée dès la détection d'un évènement décrit dans les causes de révocation possibles pour ce type de certificat. La révocation du certificat est effective lorsque le numéro de série du certificat est introduit dans la liste de révocation de l'AC qui a émis le certificat, et que cette liste est accessible au téléchargement.

La révocation d'un certificat de signature de l'AC (signature de certificats, de LCR / LAR ou de réponses OCSP) doit être effectuée immédiatement, particulièrement dans le cas de la compromission de la clé.

IV.9.6. Exigences de vérification de la révocation par les utilisateurs de certificats

L'utilisateur d'un certificat de porteur est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante. La méthode utilisée (LCR, Delta LCR, OCSP…) est à l'appréciation de l'utilisateur selon leur disponibilité et les contraintes liées à leur emploi.

IV.9.7. Fréquence d'établissement et durée de validité des LCR

Lorsque l'information sur l'état de la révocation d'un certificat est assurée au travers de la mise en place d'un service de LCR et, le cas échéant, de Delta LCR, la fréquence minimale de leur publication doit être de 72h pour le niveau * et 24h pour les niveaux ** et ***.

Afin d'assurer une continuité du service dans le cas où un incident sur la publication des LCR survienne, il est recommandé que la durée de validité des LCR (et dLCR) soit le double de leur fréquence de publication. En aucun cas elle ne pourra excéder 6 jours.

Une liste de certificats d'autorités révoqués (LAR) est une LCR qui ne contient que des numéros de certificats d'AC. Les LAR émises par une AC racine doivent avoir une durée dictée par l'analyse de risque (s'il y en a une). Sa durée doit être au maximum d'un an ; il est recommandé, dans la plupart des cas, qu'elle soit mensuelle.

La fréquence de publication de nouvelles LAR doit être cohérente avec la durée de ces LAR (si la durée de validité d'une LAR est de 1 mois, l'émission d'une nouvelle LAR toutes les trois semaines est une fréquence adaptée).

IV.9.8. Délai maximum de publication d'une LCR

Lorsque l'information sur l'état de la révocation d'un certificat est assurée au travers de la mise en place d'un service de publication de LCR et, le cas échéant, de Delta LCR, celles-ci doivent être publiées et disponibles pour le téléchargement au maximum dans les 30 minutes suivant leur génération[31].

Le délai de publication des LAR devra être précisé dans la PC de l'AC racine.

IV.9.9. Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats

Lorsque l'information sur l'état de la révocation d'un certificat est assurée au travers de la mise en place d'un service OCSP, celui-ci doit respecter les exigences d'intégrité, de disponibilité et de délai de publication

[31] Recommandation d'immédiateté.

décrites dans cette PC Type.

IV.9.10. Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats

Cf. chapitre IV.9.6 ci-dessus.

IV.9.11. Autres moyens disponibles d'information sur les révocations

Ces autres moyens d'information sur les révocations peuvent être mis en place à condition qu'ils respectent les exigences d'intégrité, de disponibilité et de délai de publication décrite dans la présente PC Type.

À préciser par l'AC dans sa PC.

IV.9.12. Exigences spécifiques en cas de compromission de la clé privée

Pour les certificats de porteur, les entités autorisées à effectuer une demande de révocation sont tenues de le faire sans délais après avoir eu connaissance de la compromission de la clé privée.

Pour les certificats d'AC, outre les exigences du chapitre IV.9.3.2 ci-dessus, la révocation suite à une compromission de la clé privée doit faire l'objet d'une information clairement diffusée au moins sur le site Internet de l'AC et éventuellement relayée par d'autres moyens (autres sites Internet institutionnels, journaux, etc.).

[Authentification]/[Signature]	**Niveau (***)**	
L'AC doit imposer au porteur ou au MC qu'en cas de compromission de la clé privée du porteur ou de connaissance de la compromission de la clé privée de l'AC ayant émis son certificat, le porteur s'oblige à interrompre immédiatement et définitivement l'usage de sa clé privée et de son certificat associé.		

[Confidentialité]	**Niveau (***)**	
L'AC doit imposer au porteur ou au MC qu'en cas de compromission de la clé privée du porteur, le porteur s'oblige à interrompre immédiatement et définitivement l'usage de son certificat de confidentialité à des fins de chiffrement. Le porteur s'engage, dans la mesure des moyens disponibles, à déchiffrer les données précédemment chiffrées au moyen de son certificat de confidentialité. Le porteur s'oblige à protéger ces données par tout autre moyen apte à répondre au besoin de confidentialité identifié pour le niveau de sécurité considéré.		

IV.9.13. Causes possibles d'une suspension

La suspension de certificats n'est pas autorisée dans la présente PC Type.

IV.9.14. Origine d'une demande de suspension

Sans objet.

IV.9.15. Procédure de traitement d'une demande de suspension

Sans objet.

IV.9.16. Limites de la période de suspension d'un certificat

Sans objet.

IV.10. Fonction d'information sur l'état des certificats

IV.10.1. Caractéristiques opérationnelles

L'AC doit fournir aux utilisateurs de certificats les informations leur permettant de vérifier et de valider, préalablement à son utilisation, le statut d'un certificat et de l'ensemble de la chaîne de certification correspondante (jusqu'à et y compris l'AC Racine), c'est-à-dire de vérifier également les signatures des certificats de la chaîne, les signatures garantissant l'origine et l'intégrité des LCR / LAR ou des jetons OCSP et l'état du certificat de l'AC Racine.

La fonction d'information sur l'état des certificats doit au moins mettre à la disposition des utilisateurs de certificats une solution : LCR ou OCSP.

Lorsqu'un service de LCR / LAR est proposé, alors celles-ci doivent être au format V2.

IV.10.2. Disponibilité de la fonction d'information sur l'état des certificats

La fonction d'information sur l'état des certificats doit être disponible 24h/24 7j/7.

Cette fonction doit avoir une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) conforme au tableau suivant :

Description	**Niveau ***	**Niveau ****	**Niveau*****
Durée maximale d'indisponibilité par interruption (panne ou maintenance) de la fonction d'information sur l'état des certificats	4h (jours ouvrés)	4h	2h[32]

Cette fonction doit avoir une durée maximale totale d'indisponibilité par mois conforme au tableau suivant :

Description	**Niveau ***	**Niveau ****	**Niveau*****
Durée maximale totale d'indisponibilité par mois de la fonction d'information sur l'état des certificats	32h (jours ouvrés)	16h	8h

Lorsque la fonction de vérification en ligne du statut d'un certificat (OCSP) est mise en œuvre, le temps de réponse du serveur à la requête reçue[33] doit être au maximum de 10 secondes.

IV.10.3. Dispositifs optionnels

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

[32] Il est recommandé que cette durée soit de 1h lorsque le PSCE délivre des certificats d'authentification (personne ou machine), chiffrement et de cachet à des fins de signature de contremarques de temps.

[33] Durée mesurée au niveau du serveur (requête reçue par le serveur et réponse au départ du serveur)

IV.11. Fin de la relation entre le porteur et l'AC

En cas de fin de relation contractuelle / hiérarchique / réglementaire entre l'AC et le porteur avant la fin de validité du certificat, pour une raison ou pour une autre, ce dernier doit être révoqué.

IV.12. Séquestre de clé et recouvrement

Seules les clés privées associées aux certificats électroniques dont l'usage est la confidentialité (chiffrement) peuvent être séquestrées à des fins de recouvrement. Les clés privées d'AC et les clés privées associées aux certificats électroniques des autres usages ne doivent en aucun cas être séquestrées.

[Confidentialité]		
Afin de mettre en œuvre un mécanisme permettant de déchiffrer des informations, préalablement chiffrées, en l'absence de la clé privée d'origine du porteur concerné (absence du porteur, perte de sa clé privée par le porteur, panne de son dispositif de protection de clés privées, …), plusieurs solutions sont envisageables : 1) Chiffrer systématiquement les clés symétriques de fichiers ou de messages en utilisant, en plus des clés publiques des porteurs concernés, la clé publique d'un agent de recouvrement qui pourra, en cas de besoin, utiliser sa clé privée pour effectuer le déchiffrement ; 2) Séquestrer les clés privées des porteurs, et les recouvrer, au cas par cas, lorsque nécessaire. Il est hors du cadre du présent document de traiter des avantages et inconvénients des solutions permettant de déchiffrer un fichier ou un message en l'absence de la clé privée d'origine du porteur. De plus, la présente PC Type ne traite que du recouvrement de données chiffrées suite à séquestre des clés privées de déchiffrement des porteurs. Le recouvrement de données chiffrées via la clé privée d'un agent de recouvrement est du ressort de l'application et de sa politique de sécurité et est hors du cadre de la présente PC Type. Le séquestre des clés privées de déchiffrement du porteur par l'AC n'est pas imposé par des obligations légales. Il est cependant fortement conseillé aux AC d'offrir ce service de séquestre à leurs clients pour des raisons de disponibilité et d'accès aux données chiffrées. En effet, en cas de perte de sa clé privée, le porteur sera ainsi en mesure de déchiffrer la clé symétrique de fichier ou de message et de déchiffrer les données qu'il avait protégées en confidentialité. Enfin, cette PC Type ne traite que du séquestre et du recouvrement de clés privées correspondant à des certificats émis par l'AC elle-même en conformité avec cette même PC Type. Un service de séquestre et de recouvrement autonome est hors du cadre de la présente PC Type.		

IV.12.1. Politique et pratiques de recouvrement par séquestre des clés

Les différentes étapes de séquestre et de recouvrement de clés privées associées aux certificats électroniques dont l'usage est la confidentialité (chiffrement) doivent respecter les exigences des chapitres qui suivent.

IV.12.1.1 Demande de séquestre

[Confidentialité]		
Une demande de séquestre de clé privée est effectuée, auprès de l'AE, en même temps que la demande du certificat correspondant et par la même personne. Cette demande doit comporter la durée souhaitée de conservation de la clé privée séquestrée, en fonction de la durée maximale pouvant être offerte par l'AC qui doit être au moins égale à la durée de validité du certificat correspondant.		

[Confidentialité]		**[Entreprise] / [Administration]**

Si le demandeur n'est pas le futur porteur, ce dernier doit en être informé et donner son consentement préalable.

IV.12.1.2 Traitement d'une demande de séquestre

[Confidentialité]		
Une demande de séquestre d'une clé privée étant formulée en même temps et par la même personne que la demande de certificat correspondant, le processus d'identification et de validation d'une telle demande correspond à celui d'une demande de certificat (cf. chapitre IV.2.1). L'AE transmet ensuite la demande de séquestre à la fonction adéquate de l'IGC (cf. chapitre I.4.1). Les demandes de séquestre sont à archiver par l'AE au même titre que les dossiers d'enregistrement correspondants (cf. chapitre I.4.2). Si l'AC génère la bi-clé du porteur, la fonction de génération des éléments secrets du porteur, suite à génération de la clé privée à séquestrer, la transmet à la fonction de séquestre et recouvrement suivant un processus qui doit en assurer, de bout en bout, la confidentialité, l'intégrité et l'authentification d'origine. Si la clé privée n'est pas générée par l'AC mais par le porteur, elle doit être remise à la fonction de séquestre et recouvrement de l'AC suivant un processus qui permet d'en assurer, de bout en bout, la confidentialité, l'intégrité et l'authentification d'origine. L'intégrité et la confidentialité des clés privées séquestrées doivent être assurées en permanence, y compris lors d'éventuels échanges internes à l'IGC. La conservation de ces clés doit se faire soit dans un module cryptographique, soit sous forme chiffrée, suivant les mêmes conditions que celles définies au chapitre VI.2.4 pour la conservation des copies de secours des clés d'AC. Les mécanismes assurant la sécurité des clés séquestrées doivent être adaptés à la durée de conservation de ces clés. L'AC devra préciser dans sa PC quelles sont les informations permettant d'identifier de manière unique et non ambiguë chaque clé privée séquestrée (en s'appuyant, par exemple, sur le DN du porteur, le n° de série du certificat correspondant et/ou un n° de série propre à la clé privée). Un porteur pouvant disposer de plusieurs clés privées, à un instant donné ainsi que suite aux renouvellements successifs de ses bi-clés, une identification reposant uniquement sur l'identification du porteur est a priori insuffisante. Au plus tard au moment du séquestre effectif de la clé privée concernée, l'AC doit transmettre à toute personne autorisée à demander ultérieurement le recouvrement de cette clé (cf. chapitre suivant)[34], et dont il a connaissance à ce moment-là, ces informations d'identification de la clé privée séquestrée et qui devront être mentionnées dans toute demande de recouvrement.		

IV.12.1.3 Origine d'une demande de recouvrement

[Confidentialité]		**[Particulier]**
Outre le porteur lui-même et les entités autorisées par la loi à accéder aux clés privées séquestrées par une AC, seules les personnes explicitement désignée à l'AC par le porteur, éventuellement sous conditions (par exemple, en cas de décès du porteur), peuvent demander le recouvrement d'une clé privée d'un porteur donné.		

[34] En dehors des entités autorisées par la loi

[Confidentialité]		**[Entreprise] / [Administration]**
Outre le porteur lui-même et les entités autorisées par la loi à accéder aux clés privées séquestrées par une AC, seules le représentant légal de l'entité ou toute personne explicitement désignée par un représentant légal de l'entité, cette personne pouvant être désignée nominativement ou par sa fonction, peuvent demander le recouvrement d'une clé privée d'un porteur donné.		

IV.12.1.4 Identification et validation d'une demande de recouvrement

[Confidentialité]		
L'identité du demandeur d'un recouvrement d'une clé séquestrée doit être validée, sauf cas particulier des entités autorisées par la loi, par la fonction de gestion des recouvrements suivant les mêmes exigences que la validation initiale de l'identité d'un demandeur d'un certificat définies au chapitre III.2. La demande de recouvrement doit comporter au minimum les informations suivantes : le motif du recouvrement de la clé privée ainsi que les informations permettant d'identifier la clé privée à recouvrer (cf. chapitre IV.12.1.2). Une fois l'identité du demandeur validée et la clé à recouvrer identifiée, la fonction de gestion des recouvrements s'assure que le demandeur est bien l'une des personnes autorisées à demander le recouvrement de la clé concernée.		

IV.12.1.5 Traitement d'une demande de recouvrement

[Confidentialité]		
Suite à identification et validation de la demande de recouvrement (cf. chapitre précédent), la fonction de gestion des recouvrements émet la demande pour effectuer le recouvrement de la clé privée concernée vers la fonction de séquestre et recouvrement de l'IGC, en protégeant cette demande en intégrité et en confidentialité. La fonction de séquestre et recouvrement authentifie la demande de recouvrement puis saisit les personnes nécessaires pour le recouvrement de la clé privée du porteur. La fonction de séquestre et recouvrement authentifie ces personnes préalablement à l'opération de recouvrement.		

[Confidentialité]	**Niveaux (**) et (***)**	
L'opération de recouvrement doit nécessiter l'authentification d'au moins deux personnes dans des rôles de confiance (par exemple, responsable sécurité et opérateur).		

[Confidentialité]	**Niveau (*)**	
L'opération de recouvrement doit nécessiter l'authentification d'au moins une personne dans un rôle de confiance.		

[Confidentialité]		
L'opération de recouvrement doit garantir qu'aucune autre information, que la clé privée sur laquelle porte le recouvrement, ne peut être divulguée. La fonction de séquestre et recouvrement remet ensuite de manière sécurisée la clé privée recouvrée au demandeur du recouvrement. Cette remise s'effectue avec une sécurité équivalente à la remise de la clé privée lors de la génération du certificat du porteur (cf. chapitres VI.1.2 et VI.4).		

La fonction de gestion des recouvrements a la responsabilité de l'archivage des pièces du dossier de demande de recouvrement (ou de l'envoi vers la composante chargée de l'archivage), l'archivage des informations liées à l'opération de recouvrement étant du ressort de la fonction de séquestre et recouvrement au titre de l'archivage des journaux d'évènements correspondants (cf. chapitres V.4 et V.5).

IV.12.1.6 Destruction des clés séquestrées

[Confidentialité]		
Dès la fin de la période de conservation d'une clé séquestrée, tout exemplaire de cette clé détenue par l'AC doit être détruit de manière fiable afin de ne pouvoir ni recouvrer ni reconstituer la clé.		

IV.12.1.7 Disponibilité des fonctions liées au séquestre et au recouvrement

[Confidentialité]		
La présente PC Type ne formule pas d'exigence spécifique sur le sujet. L'AC doit préciser dans sa PC ses engagements quant à la disponibilité de sa fonction de gestion des recouvrements et de sa fonction de séquestre et recouvrement. Elle doit également préciser ses engagements en matière de délai de traitement maximal d'une demande de recouvrement, entre la réception d'une demande de recouvrement authentifiée et la remise de la clé privée recouvrée au demandeur.		

IV.12.2. Politique et pratiques de recouvrement par encapsulation des clés de session

Sans objet.

V. Mesures de sécurité non techniques

Les exigences définies dans la suite du présent chapitre sont les exigences minimales que l'AC doit respecter. Elles doivent être complétées et déclinées en mesures de sécurité en fonction de l'environnement réel de l'IGC.

V.1. Mesures de sécurité physique

V.1.1. Situation géographique et construction des sites

La présente PC Type ne formule pas d'exigence spécifique concernant la localisation géographique de l'IGC et de ses composantes.

La construction des sites doit respecter les règlements et normes en vigueur ainsi qu'éventuellement des exigences spécifiques face à des risques de type tremblement de terre ou explosion (proximité d'une zone d'usines ou d'entrepôts de produits chimiques, ...).

V.1.2. Accès physique

Afin d'éviter toute perte, dommage et compromission des ressources de l'IGC et l'interruption des services de l'AC, les accès aux locaux des différentes composantes de l'IGC doivent être contrôlés.

En outre, toute personne entrant dans ces zones physiquement sécurisées ne doit pas être laissée, pendant une période de temps significative, sans la surveillance d'une personne autorisée.

	Niveau (***)	
Pour les fonctions de génération des certificats, de génération des éléments secrets du porteur et de gestion des révocations et, le cas échéant, pour les fonctions de gestion des recouvrements et de séquestre et recouvrement : L'accès doit être strictement limité aux seules personnes nominativement autorisées à pénétrer dans les locaux et la traçabilité des accès doit être assurée. En dehors des heures ouvrables, la sécurité doit être renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logique. Afin d'assurer la disponibilité des systèmes, l'accès aux machines doit être limité aux seules personnes autorisées à effectuer des opérations nécessitant l'accès physique aux machines. Pour cela, les composantes concernées de l'IGC doivent définir un périmètre de sécurité physique où sont installées ces machines. La mise en œuvre de ce périmètre doit permettre de respecter la séparation des rôles de confiance telle que prévue dans la PC de l'AC, en conformité avec la présente PC Type. Notamment, il est recommandé que tout local utilisé en commun avec d'autres fonctions que les fonctions rendues par la composante concernée soit en dehors de ce périmètre de sécurité.		

	Niveau (**)	
Pour les fonctions de génération des certificats, de génération des éléments secrets du porteur et de gestion des révocations et, le cas échéant, pour les fonctions de gestion des recouvrements et de séquestre et recouvrement : L'accès doit être strictement limité aux seules personnes autorisées à pénétrer dans les locaux et la traçabilité des accès doit être assurée. En dehors des heures ouvrables, la sécurité doit être renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logique Afin d'assurer la disponibilité des systèmes, il est recommandé que l'accès aux machines soit limité aux seules personnes autorisées à effectuer des opérations nécessitant l'accès physique aux machines.		

Nota - On entend par machines l'ensemble des serveurs, boîtiers cryptographiques, stations et éléments actifs

du réseau utilisés pour la mise en œuvre de ces fonctions.

V.1.3. Alimentation électrique et climatisation

Les caractéristiques des équipements d'alimentation électrique et de climatisation doivent permettre de respecter les conditions d'usage des équipements de l'IGC telles que fixées par leurs fournisseurs.

Elles doivent également permettre de respecter les exigences de la présente PC Type, ainsi que les engagements pris par l'AC dans sa PC, en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

V.1.4. Vulnérabilité aux dégâts des eaux

Les moyens de protection contre les dégâts des eaux doivent permettre de respecter les exigences de la présente PC Type, ainsi que les engagements pris par l'AC dans sa PC, en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

V.1.5. Prévention et protection incendie

Les moyens de prévention et de lutte contre les incendies doivent permettre de respecter les exigences de la présente PC Type, ainsi que les engagements pris par l'AC dans sa PC, en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

V.1.6. Conservation des supports

Les différentes informations intervenant dans les activités de l'IGC doivent être identifiées et leurs besoins de sécurité définis (en confidentialité, intégrité et disponibilité). L'AC doit maintenir un inventaire de ces informations. L'AC doit mettre en place des mesures pour éviter la compromission et le vol de ces informations.

Les supports (papier, disque dur, disquette, CD, etc.) correspondant à ces informations doivent être gérés selon des procédures conformes à ces besoins de sécurité. En particulier, ils doivent être manipulés de manière sécurisée afin de protéger les supports contre les dommages, le vol et les accès non autorisés.

Des procédures de gestion doivent protéger ces supports contre l'obsolescence et la détérioration pendant la période de temps durant laquelle l'AC s'engage à conserver les informations qu'ils contiennent.

V.1.7. Mise hors service des supports

En fin de vie, les supports devront être, soit détruits, soit réinitialisés en vue d'une réutilisation, en fonction du niveau de confidentialité des informations correspondantes.

Les procédures et moyens de destruction et de réinitialisation doivent être conformes à ce niveau de confidentialité (voir notamment le guide [972-1]).

V.1.8. Sauvegardes hors site

En complément de sauvegardes sur sites, il est recommandé que les composantes de l'IGC mettent en œuvre des sauvegardes hors sites de leurs applications et de leurs informations. Ces sauvegardes doivent être organisées de façon à assurer une reprise des fonctions de l'IGC après incident le plus rapidement possible, et conforme aux exigences de la présente PC Type et aux engagements de l'AC dans sa PC en matière de disponibilité, en particulier pour les fonctions de gestion des révocations et d'information sur l'état des certificats (cf. chapitres IV.9.5.1 et IV.10.2).

Les informations sauvegardées hors site doivent respecter les exigences de la présente PC Type en matière de protection en confidentialité et en intégrité de ces informations.

	Niveaux (**) et (***)	
Les composantes de l'IGC en charge des fonctions de gestion des révocations et d'information sur l'état des certificats, au moins, doivent obligatoirement mettre en œuvre des sauvegardes hors site permettant une reprise rapide de ces fonctions suite à la survenance d'un sinistre ou d'un évènement affectant gravement et de manière durable la réalisation de ces prestations (destruction du site, etc.). Les fonctions de sauvegarde et de restauration doivent être effectuées par les rôles de confiance appropriés et conformément aux mesures de sécurité procédurales.		

V.2. Mesures de sécurité procédurales

V.2.1. Rôles de confiance

Chaque composante de l'IGC doit distinguer au moins les cinq rôles fonctionnels[35] de confiance suivants

- **Responsable de sécurité** - Le responsable de sécurité est chargé de la mise en œuvre et du contrôle de la politique de sécurité d'une ou plusieurs composantes de l'IGC. Il gère les contrôles d'accès physiques aux équipements des systèmes de la composante. Il est habilité à prendre connaissance des archives et des journaux d'évènements. Il est responsable des opérations de génération et de révocation des certificats.
- **Responsable d'application** - Le responsable d'application est chargé, au sein de la composante à laquelle il est rattaché, de la mise en œuvre de la politique de certification et de la déclaration des pratiques de certification de l'IGC au niveau de l'application dont il est responsable. Sa responsabilité couvre l'ensemble des fonctions rendues par cette application et des performances correspondantes.
- **Ingénieur système** - Il est chargé de la mise en route, de la configuration et de la maintenance technique des équipements informatiques de la composante. Il assure l'administration technique des systèmes et des réseaux de la composante.
- **Opérateur** - Un opérateur au sein d'une composante de l'IGC réalise, dans le cadre de ses attributions, l'exploitation au quotidien des applications pour les fonctions mises en œuvre par la composante.
- **Contrôleur** - Personne autorisée à accéder et en charge de l'analyse régulière des archives et de l'analyse des journaux d'évènements afin de détecter tout incident, anomalie, tentative de compromission, etc.

En plus de ces rôles de confiance au sein de chaque composante de l'IGC, et en fonction de l'organisation de l'IGC et des outils mis en œuvre, l'AC peut être amenée à distinguer également en tant que rôle de confiance, les rôles de porteur de parts de secrets d'IGC : cf. chapitres VI.1 et VI.2.

Ces porteurs de parts de secrets ont la responsabilité d'assurer la confidentialité, l'intégrité et la disponibilité des parts qui leur sont confiés.

De manière générale, des procédures doivent être établies et appliquées pour tous les rôles administratifs et

[35] En fonction de la taille de l'entité concernée, de la charge de travail correspondant au rôle, etc., ainsi qu'en fonction des exigences de sécurité et de continuité d'activité, un même rôle fonctionnel peut / doit être tenu par différentes personnes.

les rôles de confiance ayant trait à la fourniture de services de certification.

Ces rôles doivent être décrits et définis dans la description des postes propre à chaque entité opérant une des composantes de l'IGC sur les principes de séparation des responsabilités et du moindre privilège. Ces rôles doivent déterminer la sensibilité du poste, en fonction des responsabilités et des niveaux d'accès, des vérifications des antécédents et de la formation et de la sensibilisation des employés.

Lorsqu'appropriées, ces descriptions doivent différencier entre les fonctions générales et les fonctions spécifiques à l'AC. L'AC doit implémenter techniquement ce principe de moindre privilège via les mécanismes de contrôle d'accès qu'elle met en œuvre.

De plus, les opérations de sécurité de l'AC doivent être séparées des opérations normales. Les responsabilités des opérations de sécurité incluent :

- Les procédures et responsabilités opérationnelles ;
- La planification et la validation des systèmes sécurisés ;
- La protection contre les logiciels malicieux ;
- L'entretien ;
- La gestion de réseaux ;
- La surveillance active des journaux d'audit, l'analyse des évènements et les suites ;
- La manipulation et la sécurité des supports ;
- L'échange de données et de logiciels.

Ces responsabilités sont gérées par les opérations de sécurité de l'AC, mais peuvent être effectivement réalisées par du personnel opérationnel non spécialiste (en étant supervisé), tel que défini dans la politique de sécurité appropriée et les documents relatifs aux rôles et responsabilités.

Des mesures doivent être mises en place pour empêcher que des équipements, des informations, des supports et des logiciels ayant trait aux services de l'AC soient sortis du site sans autorisation.

V.2.2. Nombre de personnes requises par tâches

Selon le type d'opération effectuée, le nombre et la qualité des personnes devant nécessairement être présentes, en tant qu'acteurs ou témoins, peuvent être différents.

Pour des raisons de sécurité, il est demandé de répartir les fonctions sensibles sur plusieurs personnes. La présente PC Type définit un certain nombre d'exigences concernant cette répartition, notamment pour les opérations liées aux modules cryptographiques de l'IGC (cf. chapitre VI).

La DPC de l'AC devra préciser quelles sont les opérations nécessitant l'intervention de plusieurs personnes et quelles sont les contraintes que ces personnes doivent respecter (positions dans l'organisation, liens hiérarchiques, etc.).

V.2.3. Identification et authentification pour chaque rôle

Chaque entité opérant une composante de l'IGC doit faire vérifier l'identité et les autorisations de tout membre de son personnel amené à travailler au sein de la composante avant de lui attribuer un rôle et les droits correspondants, notamment :

- Que son nom soit ajouté aux listes de contrôle d'accès aux locaux de l'entité hébergeant la composante concernée par le rôle ;
- Que son nom soit ajouté à la liste des personnes autorisées à accéder physiquement à ces systèmes ;

- Le cas échéant et en fonction du rôle, qu'un compte soit ouvert à son nom dans ces systèmes ;
- éventuellement, que des clés cryptographiques et/ou un certificat lui soient délivrés pour accomplir le rôle qui lui est dévolu dans l'IGC.

Ces contrôles doivent être décrits dans la DPC de l'AC et doivent être conformes à la politique de sécurité de la composante.

Chaque attribution d'un rôle à un membre du personnel de l'IGC doit être notifiée par écrit. Ce rôle doit être clairement mentionné et décrit dans sa fiche de poste.

V.2.4. Rôles exigeant une séparation des attributions

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre. Pour les rôles de confiance, il est néanmoins recommandé qu'une même personne ne détienne pas plusieurs rôles et, au minimum, les exigences ci-dessous de non cumul doivent être respectées.

Les attributions associées à chaque rôle doivent être décrites dans la DPC de l'AC et être conformes à la politique de sécurité de la composante concernée.

	Niveaux (**) et (***)	
Concernant les rôles de confiance, les cumuls suivants sont interdits : ➢ Responsable de sécurité et ingénieur système / opérateur / contrôleur ; ➢ Ingénieur système, opérateur et contrôleur.		

	Niveau (*)	
Concernant les rôles de confiance, le cumul suivant est interdit : ➢ responsable de sécurité et ingénieur système.		

V.3. Mesures de sécurité vis-à-vis du personnel

V.3.1. Qualifications, compétences et habilitations requises

Tous les personnels amenés à travailler au sein de composantes de l'IGC doivent être soumis à une clause de confidentialité vis-à-vis de leur employeur. Dans le cas des agents, ceux-ci sont soumis à leur devoir de réserve.

Chaque entité opérant une composante de l'IGC doit s'assurer que les attributions de ses personnels, amenés à travailler au sein de la composante, correspondent à leurs compétences professionnelles.

Le personnel d'encadrement doit posséder l'expertise appropriée à son rôle et être familier des procédures de sécurité en vigueur au sein de l'IGC.

L'AC doit informer toute personne intervenant dans des rôles de confiance de l'IGC :

- De ses responsabilités relatives aux services de l'IGC,
- Des procédures liées à la sécurité du système et au contrôle du personnel, auxquelles elle doit se conformer.

En particulier, les personnes intervenant dans des rôles de confiance doivent y être formellement affectées par l'encadrement supérieur chargé de la sécurité.

V.3.2. Procédures de vérification des antécédents

Chaque entité opérant une composante de l'IGC doit mettre en œuvre tous les moyens légaux dont elle peut disposer pour s'assurer de l'honnêteté de ses personnels amenés à travailler au sein de la composante. Ces personnels ne doivent notamment pas avoir de condamnation de justice en contradiction avec leurs attributions.

À ce titre, l'employeur peut demander à ces personnels la communication d'une copie du bulletin n° 3 de leur casier judiciaire.

L'employeur peut décider en cas de refus de communiquer cette copie ou en cas de présence de condamnation de justice incompatible avec les attributions de la personne, de lui retirer ces attributions.

Les personnes ayant un rôle de confiance ne doivent pas souffrir de conflit d'intérêts préjudiciables à l'impartialité de leurs tâches.

Ces vérifications doivent être menées préalablement à l'affectation à un rôle de confiance et revues régulièrement (au minimum tous les 3 ans).

V.3.3. Exigences en matière de formation initiale

Le personnel doit être préalablement formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité qu'il met en œuvre et qu'il doit respecter, correspondant à la composante au sein de laquelle il opère.

Les personnels doivent avoir connaissance et comprendre les implications des opérations dont ils ont la responsabilité.

V.3.4. Exigences et fréquence en matière de formation continue

Le personnel concerné doit recevoir une information et une formation adéquates préalablement à toute évolution dans les systèmes, dans les procédures, dans l'organisation, etc. en fonction de la nature de ces évolutions.

V.3.5. Fréquence et séquence de rotation entre différentes attributions

La présente PC Type ne formule pas d'exigence spécifique sur le sujet. À préciser par l'AC dans sa DPC.

V.3.6. Sanctions en cas d'actions non autorisées

À préciser par l'AC dans sa DPC.

V.3.7. Exigences vis-à-vis du personnel des prestataires externes

Le personnel des prestataires externes intervenant dans les locaux et/ou sur les composantes de l'IGC doit également respecter les exigences du présent chapitre V.3. Ceci doit être traduit en clauses adéquates dans les contrats avec ces prestataires.

V.3.8. Documentation fournie au personnel

Chaque personnel doit disposer au minimum de la documentation adéquate concernant les procédures opérationnelles et les outils spécifiques qu'il met en œuvre ainsi que les politiques et pratiques générales de la composante au sein de laquelle il travaille. En particulier, il doit lui être remis la ou les politique(s) de sécurité l'impactant.

V.4. Procédures de constitution des données d'audit

La journalisation d'évènements consiste à les enregistrer de façon manuelle ou automatique. Les fichiers

résultants, sous forme papier ou électronique, doivent rendre possible la traçabilité et l'imputabilité des opérations effectuées.

V.4.1. Type d'évènements à enregistrer

Concernant les systèmes liés aux fonctions qui sont mises en œuvre dans le cadre de l'IGC, chaque entité opérant une composante de l'IGC doit au minimum journaliser les évènements tels que décrits ci- dessous, sous forme électronique. La journalisation doit être automatique, dès le démarrage d'un système et sans interruption jusqu'à l'arrêt de ce système.

- Création / modification / suppression de comptes utilisateur (droits d'accès) et des données d'authentification correspondantes (mots de passe, certificats, etc.) ;
- Démarrage et arrêt des systèmes informatiques et des applications ;
- Évènements liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de journalisation, actions prises suite à une défaillance de la fonction de journalisation ;
- Connexion / déconnexion des utilisateurs ayant des rôles de confiance, et les tentatives non réussies correspondantes.

D'autres évènements doivent aussi être recueillis, par des moyens électroniques ou manuels. Ce sont ceux concernant la sécurité et qui ne sont pas produits automatiquement par les systèmes informatiques, notamment :

- Les accès physiques ;
- Les actions de maintenance et de changements de la configuration des systèmes ;
- Les changements apportés au personnel ;
- Les actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation, renseignements personnels sur les porteurs,...).

En plus de ces exigences de journalisation communes à toutes les composantes et toutes les fonctions de l'IGC, des évènements spécifiques aux différentes fonctions de l'IGC doivent également être journalisés, notamment[36] :

- Réception d'une demande de certificat (initiale et renouvellement) ;
- Validation / rejet d'une demande de certificat ;
- Évènements liés aux clés de signature et aux certificats d'AC (génération (cérémonie des clés), sauvegarde / récupération, révocation, renouvellement, destruction,...) ;
- Le cas échéant, génération des éléments secrets du porteur (bi-clé, codes d'activation,…) ;
- Génération des certificats des porteurs ;
- Transmission des certificats aux porteurs et, selon les cas, acceptations / rejets explicites par les porteurs ;
- Le cas échéant, remise de son dispositif de protection des éléments secrets au porteur ;

[36] Les évènements à journaliser doivent être adaptés à l'organisation et l'architecture de l'IGC. Notamment, les échanges entre fonctions de l'IGC et/ou entre composantes de l'IGC peuvent nécessiter une journalisation pour assurer une traçabilité des actions.

- Publication et mise à jour des informations liées à l'AC (PC, certificats d'AC, conditions générales d'utilisation, etc.) ;
- Réception d'une demande de révocation ;
- Validation / rejet d'une demande de révocation ;
- Génération puis publication des LCR (et éventuellement des deltaLCR) ou des, requêtes / réponses OCSP.

[Confidentialité]		
En plus de ces exigences de journalisation communes à toutes les composantes et toutes les fonctions de l'IGC, des évènements spécifiques aux différentes fonctions de l'IGC doivent également être journalisés, notamment[37] : ➢ Le cas échéant, séquestre d'une clé privée de porteur ; ➢ Réception d'une demande de recouvrement ; ➢ Validation / rejet d'une demande de recouvrement ; ➢ Recouvrement d'une clé privée ; ➢ Remise d'une clé privée recouvrée au demandeur du recouvrement/A6].		

Chaque enregistrement d'un évènement dans un journal doit contenir au minimum les champs suivants :

- Type de l'évènement ;
- Nom de l'exécutant ou référence du système déclenchant l'évènement ;
- Date et heure de l'évènement (l'heure exacte des évènements significatifs de l'AC concernant l'environnement, la gestion de clé et la gestion de certificat doit être enregistrée) ;
- Résultat de l'évènement (échec ou réussite).

L'imputabilité d'une action revient à la personne, à l'organisme ou au système l'ayant exécutée. Le nom ou l'identifiant de l'exécutant doit figurer explicitement dans l'un des champs du journal d'évènements.

De plus, en fonction du type de l'évènement, chaque enregistrement devra également contenir les champs suivants :

- Destinataire de l'opération ;
- Nom du demandeur de l'opération ou référence du système effectuant la demande ;
- Nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes) ;
- Cause de l'évènement ;
- Toute information caractérisant l'évènement (par exemple, pour la génération d'un certificat, le numéro de série de ce certificat).

Les opérations de journalisation doivent être effectuées au cours du processus.

[37] Les évènements à journaliser doivent être adaptés à l'organisation et l'architecture de l'IGC. Notamment, les échanges entre fonctions de l'IGC et/ou entre composantes de l'IGC peuvent nécessiter une journalisation pour assurer une traçabilité des actions.

En cas de saisie manuelle, l'écriture doit se faire, sauf exception, le même jour ouvré que l'évènement.

Les évènements et données spécifiques à journaliser doivent être documentés par l'AC.

V.4.2. Fréquence de traitement des journaux d'évènements

Cf. chapitre V.4.8 ci-dessous.

V.4.3. Période de conservation des journaux d'évènements

Les journaux d'évènements doivent être conservés sur site pendant au moins un (1) mois. Ils doivent être archivés le plus rapidement possible après leur génération et au plus tard sous un (1) mois (recouvrement possible entre la période de conservation sur site et la période d'archivage).

V.4.4. Protection des journaux d'évènements

La journalisation doit être conçue et mise en œuvre de façon à limiter les risques de contournement, de modification ou de destruction des journaux d'évènements. Des mécanismes de contrôle d'intégrité doivent permettre de détecter toute modification, volontaire ou accidentelle, de ces journaux.

Les journaux d'évènements doivent être protégés en disponibilité (contre la perte et la destruction partielle ou totale, volontaire ou non).

Le système de datation des évènements doit respecter les exigences du chapitre VI.8.

La définition de la sensibilité des journaux d'évènements dépend de la nature des informations traitées et du métier. Elle peut entraîner un besoin de protection en confidentialité.

V.4.5. Procédure de sauvegarde des journaux d'évènements

Chaque entité opérant une composante de l'IGC doit mettre en place les mesures requises afin d'assurer l'intégrité et la disponibilité des journaux d'évènements pour la composante considérée, conformément aux exigences de la présente PC Type.

V.4.6. Système de collecte des journaux d'évènements

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

V.4.7. Notification de l'enregistrement d'un évènement au responsable de l'évènement

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

V.4.8. Évaluation des vulnérabilités

Chaque entité opérant une composante de l'IGC doit être en mesure de détecter toute tentative de violation de l'intégrité de la composante considérée.

Les journaux d'évènements doivent être contrôlés une (1) fois pas jour ouvré, afin d'identifier des anomalies liées à des tentatives en échec.

Les journaux doivent être analysés dans leur totalité au minimum selon la fréquence suivante :

Description	**Niveau ***	**Niveau ****	**Niveau*****
Fréquence d'analyse complète des journaux d'évènements	1 fois toutes les 2 semaines et dès la détection d'une anomalie	1 fois par semaine et dès la détection d'une anomalie	1 fois par jour ouvré et dès la détection d'une anomalie

Cette analyse donnera lieu à un résumé dans lequel les éléments importants sont identifiés, analysés et expliqués. Le résumé doit faire apparaître les anomalies et les falsifications constatées.

Par ailleurs, un rapprochement entre les différents journaux d'évènements de fonctions qui interagissent entre elles (autorité d'enregistrement et fonction de génération, fonction de gestion des révocations et fonction d'information sur l'état des certificats, etc.) doit être effectué à une fréquence au moins égale à celle déterminée dans le tableau suivant , ceci afin de vérifier la concordance entre évènements dépendants et contribuer ainsi à révéler toute anomalie.

Description	**Niveau* ****	**Niveau ****	**Niveau *****
Fréquence de rapprochement des journaux d'évènements	1 fois par mois		1 fois par semaine

V.5. Archivage des données

V.5.1. Types de données à archiver

Des dispositions en matière d'archivage doivent également être prises par l'AC. Cet archivage doit permettre d'assurer la pérennité des journaux constitués par les différentes composantes de l'IGC.

Il doit également permettre la conservation des pièces papier liées aux opérations de certification, ainsi que leur disponibilité en cas de nécessité.

Les données à archiver sont au moins les suivantes :

- Les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- Les PC ;
- Les DPC ;
- Les conditions générales d'utilisation ;
- Les accords contractuels avec d'autres AC ;
- Les certificats, LCR ou réponses OCSP tels qu'émis ou publiés ;
- Les récépissés ou notifications (à titre informatif) ;
- Les engagements signés des MC ;
- Les justificatifs d'identité des porteurs et, le cas échéant, de leur entité de rattachement ;
- Les journaux d'évènements des différentes entités de l'IGC.

V.5.2. Période de conservation des archives

Dossiers de demande de certificat

Tout dossier de demande de certificat accepté doit être archivé aussi longtemps que nécessaire, et pendant au moins sept (7) ans, pour les besoins de fourniture de la preuve de la certification dans des procédures légales, conformément à la loi applicable.

Les facteurs à prendre en compte dans la détermination de la «loi applicable» sont la loi du pays dans lequel l'AC est établie.

Lorsque les porteurs sont enregistrés par une autorité d'enregistrement dans un autre pays que celui ou l'AC est établie, alors il convient que cette AE applique également la réglementation de son propre pays.

Lorsque des MC sont également dans un autre pays, alors il convient de prendre également en compte les

exigences contractuelles et légales applicables à ces MC.

La durée de conservation des dossiers d'enregistrement doit être portée à la connaissance du porteur ou du MC.

Au cours de cette durée d'opposabilité des documents, le dossier de demande de certificat doit pouvoir être présenté par l'AC lors de toute sollicitation par les autorités habilitées.

Ce dossier, complété par les mentions consignées par l'AE ou le MC, doit permettre de retrouver l'identité réelle des personnes physiques désignées dans le certificat émis par l'AC.

[Confidentialité]		
Tout dossier de demande de recouvrement accepté doit être archivé pendant au moins cinq ans, comptés à partir de la fin du séquestre par l'AC de la clé privée correspondante. Au cours de cette durée d'opposabilité des documents, le dossier de demande de recouvrement doit pouvoir être présenté par l'AC lors de toute sollicitation par les autorités habilitées. Ce dossier doit permettre de retrouver l'identité réelle de la personne physique ayant demandé et obtenu le recouvrement.		

Certificats, LCR et réponses OCSP émis par l'AC

Les certificats de clés de porteurs et d'AC, ainsi que les LCR / LAR produites, doivent être archivés pendant au moins cinq (5) années après leur expiration.

Les réponses OCSP produites doivent être archivées pendant au moins trois mois après leur expiration.

Journaux d'évènements

Les journaux d'évènements traités au chapitre V.4 seront archivés pendant sept (7) années après leur génération. Les moyens mis en œuvre par lAC pour leur archivage devront offrir le même niveau de sécurité que celui visé lors de leur constitution. En particulier, l'intégrité des enregistrements devra être assurée tout au long de leur cycle de vie.

Autres journaux

Pour l'archivage des journaux autres que les journaux d'évènements traités au chapitre V.4, aucune exigence n'est stipulée. L'AC précisera dans sa DPC les moyens mis en œuvre pour archiver ces journaux.

V.5.3. Protection des archives

Pendant tout le temps de leur conservation, les archives, et leurs sauvegardes, doivent :

- Être protégées en intégrité ;
- Être accessibles aux personnes autorisées ;
- Pouvoir être relues et exploitées.

L'AC précisera dans sa DPC les moyens mis en œuvre pour archiver les pièces en toute sécurité.

V.5.4. Procédure de sauvegarde des archives

La présente PC Type ne formule pas d'exigence spécifique sur le sujet. À préciser par l'AC dans ses PC et DPC. Le niveau de protection des sauvegardes doit être au moins équivalent au niveau de protection des archives.

V.5.5. Exigences d'horodatage des données

Cf. chapitre V.4.4 pour la datation des journaux d'évènements.

Le chapitre [VI.8] précise les exigences en matière de datation / horodatage.

V.5.6. Système de collecte des archives

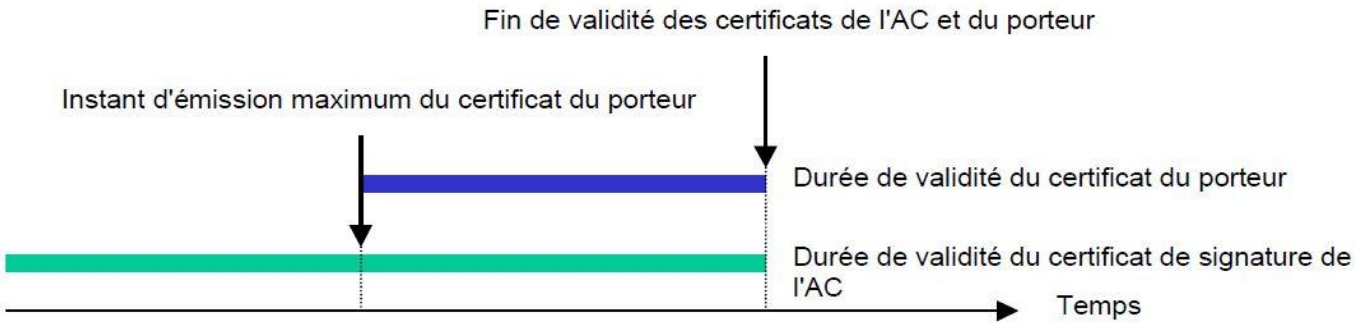
La présente PC Type ne formule pas d'exigence spécifique sur le sujet, si ce n'est que le système de collecte des archives, qu'il soit interne ou externe, doit respecter les exigences de protection des archives concernées.

V.5.7. Procédures de récupération et de vérification des archives

Les archives (papier et électroniques) doivent pouvoir être récupérées dans un délai inférieur à deux (2) jours ouvrés, sachant que seule l'AC peut accéder à toutes les archives (par opposition à une entité opérant une composante de l'IGC qui ne peut récupérer et consulter que les archives de la composante considérée).

V.6. Changement de clé d'AC

L'AC ne peut pas générer de certificat dont la date de fin serait postérieure à la date d'expiration du certificat correspondant de l'AC. Pour cela la période de validité de ce certificat de l'AC doit être supérieure à celle des certificats qu'elle signe.



Au regard de la date de fin de validité de ce certificat, son renouvellement doit être demandé dans un délai au moins égal à la durée de vie des certificats signés par la clé privée correspondante.

Dès qu'une nouvelle bi-clé d'AC est générée, seule la nouvelle clé privée doit être utilisée pour signer des certificats.

Le certificat précédent reste utilisable pour valider les certificats émis sous cette clé et ce jusqu'à ce que tous les certificats signés avec la clé privée correspondante aient expiré.

V.7. Reprise suite à compromission et sinistre

V.7.1. Procédures de remontée et de traitement des incidents et des compromissions

Chaque entité opérant une composante de l'IGC doit mettre en œuvre des procédures et des moyens de remontée et de traitement des incidents, notamment au travers de la sensibilisation et de la formation de ses personnels et au travers de l'analyse des différents journaux d'évènements. Ces procédures et moyens doivent permettre de minimiser les dommages dus à des incidents de sécurité et des dysfonctionnements.

Dans le cas d'un incident majeur, tel que la perte, la suspicion de compromission, la compromission, le vol de la clé privée de l'AC, l'évènement déclencheur est la constatation de cet incident au niveau de la

composante concernée, qui doit en informer immédiatement l'AC. Le cas de l'incident majeur doit être impérativement traité dès détection et la publication de l'information de révocation du certificat, s'il y a lieu, doit être faite dans la plus grande urgence, voire immédiatement, par tout moyen utile et disponible (presse, site Internet, récépissé …).

Si l'un des algorithmes, ou des paramètres associés, utilisés par l'AC ou ses porteurs devient insuffisant pour son utilisation prévue restante, alors l'AC doit :

- Informer tous les porteurs et les tiers utilisateurs de certificats avec lesquels l'AC a passé des accords ou à d'autres formes de relations établies. En complément, cette information doit être mise à disposition des autres utilisateurs de certificats ;
- Révoquer tout certificat concerné.

V.7.2. Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données)

Chaque composante de l'IGC doit disposer d'un plan de continuité d'activité permettant de répondre aux exigences de disponibilité des différentes fonctions de l'IGC découlant de la présente PC Type, des engagements de l'AC dans sa propre PC notamment en ce qui concerne les fonctions liées à la publication et / ou liées à la révocation des certificats.

Ce plan doit être testé au minimum suivant la fréquence ci-dessous :

Description	**Niveau ***	**Niveau ****	**Niveau *****
Fréquence de test du plan de continuité	1 fois tous les 3 ans	1 fois tous les 2 ans	1 fois par an

V.7.3. Procédures de reprise en cas de compromission de la clé privée d'une composante

Le cas de compromission d'une clé d'infrastructure ou de contrôle d'une composante doit être traité dans le plan de continuité de la composante en tant que sinistre.

Dans le cas de compromission d'une clé d'AC, le certificat correspondant doit être immédiatement révoqué : cf. chapitre IV.9.

En outre, l'AC doit au minimum respecter les engagements suivants :

- Informer les entités suivantes de la compromission : tous les porteurs, MC et les autres entités avec lesquelles l'AC a passé des accords ou a d'autres formes de relations établies, parmi lesquelles des tiers utilisateurs et d'autres AC. En complément, cette information doit être mise à disposition des autres tiers utilisateurs ;
- Indiquer que les certificats et les informations de statut de révocation délivrés en utilisant cette clé d'AC peuvent ne plus être valables.

V.7.4. Capacités de continuité d'activité suite à un sinistre

Les différentes composantes de l'IGC doivent disposer des moyens nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les exigences de la présente PC Type et de la PC de l'AC.

V.8. Fin de vie de l'IGC

Une ou plusieurs composantes de l'IGC peuvent être amenées à cesser leur activité ou à la transférer à une autre entité pour des raisons diverses.

L'AC doit prendre les dispositions nécessaires pour couvrir les coûts permettant de respecter ces exigences minimales dans le cas où l'AC serait en faillite ou pour d'autres raisons serait incapable de couvrir ces coûts par elle-même, ceci, autant que possible, en fonction des contraintes de la législation applicable en matière de faillite.

Le transfert d'activité est défini comme la fin d'activité d'une composante de l'IGC ne comportant pas d'incidence sur la validité des certificats émis antérieurement au transfert considéré et la reprise de cette activité organisée par l'AC en collaboration avec la nouvelle entité.

La cessation d'activité est définie comme la fin d'activité d'une composante de l'IGC comportant une incidence sur la validité des certificats émis antérieurement à la cessation concernée.

Transfert d'activité ou cessation d'activité[38] affectant une composante de l'IGC

Afin d'assurer un niveau de confiance constant pendant et après de tels évènements, l'AC doit entre autres obligations :

1) Mettre en place des procédures dont l'objectif est d'assurer un service constant en particulier en matière d'archivage (notamment, archivage des certificats des porteurs et des informations relatives aux certificats, archivage de séquestre le cas échéant).

2) Assurer la continuité de la révocation (prise en compte d'une demande de révocation et publication de l'état des certificats), conformément aux exigences de disponibilité pour ses fonctions définies dans la présente PC Type. À défaut, les applications de l'Administration refuseront les certificats émis par des AC dont les informations sur l'état de révocation des certificats en cours de validité ne seraient plus accessibles, même si le certificat du porteur est encore valide.

Des précisions quant aux engagements suivants doivent ainsi être annoncées par l'AC dans sa PC.

Dans la mesure où les changements envisagés peuvent avoir des répercussions sur les engagements vis-à-vis des porteurs ou des utilisateurs de certificats, l'AC doit les en aviser aussitôt que nécessaire et, au moins, sous le délai d'un (1) mois.

Cessation d'activité affectant l'AC

La cessation d'activité peut être totale ou partielle (par exemple : cessation d'activité pour une famille de certificats donnée seulement). La cessation partielle d'activité doit être progressive de telle sorte que seules les obligations visées aux 1), 2), et 3) ci-dessous soient à exécuter par l'AC, ou une entité tierce qui reprend les activités, lors de l'expiration du dernier certificat émis par elle.

Dans l'hypothèse d'une cessation d'activité totale, l'AC ou, en cas d'impossibilité, toute entité qui lui serait substituée de par l'effet d'une loi, d'un règlement, d'une décision de justice ou bien d'une convention antérieurement conclue avec cette entité, devra assurer la révocation des certificats et la publication des LCR conformément aux engagements pris dans sa PC.

L'AC doit stipuler dans ses pratiques les dispositions prises en cas de cessation de service. Elles doivent inclure :

- La notification des entités affectées ;
- Le transfert de ses obligations à d'autres parties ;
- La gestion du statut de révocation pour les certificats non-expirés qui ont été délivrés.

[38] Cessation d'activité d'une composante autre que l'AC

Lors de l'arrêt du service, l'AC doit :

1) S'interdire de transmettre la clé privée lui ayant permis d'émettre des certificats ;
2) Prendre toutes les mesures nécessaires pour la détruire ou la rendre inopérante ;
3) Révoquer son certificat ;
4) Révoquer tous les certificats qu'elle a signés et qui seraient encore en cours de validité ;
5) Informer (par exemple par récépissé) tous les MC et/ou porteurs des certificats révoqués ou à révoquer, ainsi que leur entité de rattachement le cas échéant (cf. chapitre III.2.3).

VI. Mesures de sécurité techniques

Les exigences définies dans la suite du présent chapitre sont les exigences minimales que l'AC doit respecter. Elles doivent être complétées et déclinées en mesures de sécurité en fonction de l'environnement réel de l'IGC.

VI.1. Génération et installation de bi-clés

VI.1.1. Génération des bi-clés

VI.1.1.1. Clés d'AC

La génération des clés de signature d'AC doit être effectuée dans un environnement sécurisé (cf. chapitre V).

Les clés de signature d'AC doivent être générées et mises en œuvre dans un module cryptographique conforme aux exigences du chapitre XI ci-dessous pour le niveau de sécurité considéré.

La génération des clés de signature d'AC doit être effectuée dans des circonstances parfaitement contrôlées, par des personnels dans des rôles de confiance (cf. chapitre V.2.1), dans le cadre de «cérémonies de clés». Ces cérémonies doivent se dérouler suivant des scripts préalablement définis.

Selon le cas, l'initialisation de l'IGC et/ou la génération des clés de signature d'AC peut s'accompagner de la génération de parts de secrets d'IGC. Ces parts de secrets sont des données permettant de gérer et de manipuler, ultérieurement à la cérémonie de clés, les clés privées de signature d'AC, notamment, de pouvoir initialiser ultérieurement de nouveaux modules cryptographiques avec les clés de signatures d'AC.

Par exemple, ces parts de secrets peuvent être des parties de la (ou des) clé(s) privée(s) d'AC, décomposée(s) suivant un schéma à seuil de Shamir (n parties parmi m sont nécessaires et suffisantes pour reconstituer la clé privée), ou encore, il peut s'agir de données permettant de déclencher le chargement sécurisé, dans un nouveau module cryptographique, de la (ou des) clé(s) privée(s) d'AC sauvegardée(s) lors de la cérémonie de clés.

Suite à leur génération, les parts de secrets doivent être remises à des porteurs de parts de secrets désignés au préalable et habilités à ce rôle de confiance par l'AC. Quelle qu'en soit la forme (papier, support magnétique ou confiné dans une carte à puce ou une clé USB), un même porteur ne peut détenir plus d'une part de secrets d'une même AC à un moment donné. Chaque part de secrets doit être mise en œuvre par son porteur. Ce dernier peut le cas échéant, en accord avec le responsable de l'IGC, notamment en cas d'indisponibilité au moment ou la cérémonie de clé doit être opérée, transférer temporairement ou définitivement cette part de secret à un personnel désigné.

	Niveau (***)	
Les cérémonies de clés doivent se dérouler sous le contrôle d'au moins deux personnes ayant des rôles de confiance et en présence de plusieurs témoins dont au moins deux sont externes à l'AC et sont impartiaux. Les témoins attestent, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement défini. Il est recommandé qu'il y ait parmi les témoins un officier public (huissier ou notaire). Toute manipulation de données secrètes en clair (clés privées d'AC, clés privées des porteurs, parts de secrets d'IGC) doit se faire dans un environnement protégé contre les rayonnements parasites compromettant : matériels protégés, cage de Faraday, locaux limitant les risques de fuites d'information par observation visuelle ou rayonnements électromagnétiques, etc.		

	Niveau (**)	

Les cérémonies de clés doivent se dérouler sous le contrôle d'au moins deux personnes ayant des rôles de confiance et en présence de plusieurs témoins dont au moins un est externe à l'AC et est impartial. Les témoins attestent, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement défini.

	Niveau (*)	
Les cérémonies de clés doivent se dérouler sous le contrôle d'au moins une personne ayant au moins un rôle de confiance et en présence de plusieurs témoins. Les témoins attestent, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement défini.		

VI.1.1.2. Clés porteurs générées par l'AC

Les exigences de ce paragraphe ne s'appliquent que si la bi-clé du porteur est générée par l'AC.

La génération des clés des porteurs doit être effectuée dans un environnement sécurisé (cf. chapitre V).

Les bi-clés des porteurs doivent être générées :

- Soit directement dans le dispositif de protection des éléments secrets destiné au porteur conforme aux exigences du chapitre XII ci-dessous pour le niveau de sécurité considéré,
- Soit dans un module cryptographique conforme aux exigences du chapitre XI ci-dessous pour le niveau de sécurité considéré, puis transférées de manière sécurisée dans le dispositif de protection des éléments secrets destiné au porteur.

[Confidentialité]		
Dans ce dernier cas, un séquestre de la bi-clé peut être généré par l'AC conformément à sa PC et à sa DPC.		

VI.1.1.3. Clés porteurs générées par le porteur

Dans le cas où le porteur génère sa bi-clé, cette génération doit être effectuée dans un dispositif répondant aux exigences du chapitre XII ci-dessous pour le niveau de sécurité considéré. L'AC doit s'assurer que la clé publique exportée réside effectivement dans le dispositif de protection des éléments secrets du porteur.

VI.1.2. Transmission de la clé privée à son propriétaire

Si l'AC génère la bi-clé du porteur (cf. chapitre VI.1.1.2), la clé privée doit être transmise au porteur de manière sécurisée, afin d'en assurer la confidentialité et l'intégrité. Cette transmission doit se faire directement dans le dispositif de protection des éléments secrets du porteur, ou suivant un moyen équivalent.

	Niveau (***)	
Si la vérification de l'identité du porteur par l'AE via un face-à-face physique n'a pas eu lieu au moment de l'enregistrement du porteur (chapitre III.2.3), celle-ci doit être effectuée lors de la remise de la bi-clé générée par l'AC en présence du porteur.		

	Niveau (**)	
Si la vérification de l'identité du porteur par l'AE via un face-à-face physique ou via l'emploi d'un procédé de signature électronique conforme au minimum aux exigences du niveau (**) n'a pas eu lieu au moment de l'enregistrement du porteur (chapitre III.2.3), celle-ci doit être effectuée lors de la remise de la bi-clé générée par l'AC en présence du porteur.		

[Signature]	**Niveau (***)**	
Une fois remise, la clé privée doit être maintenue sous le seul contrôle du porteur.		

VI.1.3. Transmission de la clé publique à l'AC

En cas de transmission de la requête de demande de certificat du porteur au format PKCS#10, ou tout autre conteneur offrant les mêmes fonctions, vers une composante de l'AC (cas où la bi-clé est générée par le porteur), la clé devra être protégée en intégrité et son origine devra en être authentifiée.

VI.1.4. Transmission de la clé publique de l'AC aux utilisateurs de certificats

Les clés publiques de vérification de signature de l'AC doivent être diffusées auprès des utilisateurs de certificats par un moyen qui en assure l'intégrité de bout en bout et qui en authentifie l'origine.

Une clé publique d'AC peut être diffusée dans un certificat qui est soit un certificat racine autosigné, soit un certificat rattaché à une hiérarchie d'AC jusqu'à une AC racine (cf. chapitre I.5.1.1. ci-dessus).

Un certificat racine autosigné ne permet pas de garantir par lui-même que la clé publique correspondante appartient bien à l'AC considérée. Sa diffusion doit s'accompagner de la diffusion, via des sources de confiance, de l'empreinte numérique du certificat, et éventuellement de la clé publique, ainsi que d'une déclaration qu'il s'agit bien d'une clé publique de l'AC.

La clé publique de l'AC, ainsi que les informations correspondantes (certificat, empreintes numériques, déclaration d'appartenance) doivent pouvoir être récupérées aisément par les utilisateurs de certificats.

VI.1.5. Tailles des clés

Les clés d'AC et de porteurs doivent respecter les exigences de caractéristiques (tailles, algorithmes, etc.) du document [RGS_A4].

VI.1.6. Vérification de la génération des paramètres des bi-clés et de leur qualité

L'équipement de génération de bi-clés doit utiliser des paramètres respectant les normes de sécurité propres à l'algorithme correspondant à la bi-clé (cf. [RGS_A4]).

Les paramètres et les algorithmes utilisés doivent être documentés par l'AC.

VI.1.7. Objectifs d'usage de la clé

L'utilisation d'une clé privée d'AC et du certificat associé est strictement limitée à la signature de certificats, de LCR / LAR et/ou de réponses OCSP (cf. [RGS_A4]).

L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée à la fonction de sécurité concernée (cf. chapitres I.5.1.1, IV.5 et le [RGS_A4]).

VI.2. Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques

VI.2.1. Standards et mesures de sécurité pour les modules cryptographiques

VI.2.1.1. Modules cryptographiques de l'AC

Les modules cryptographiques, utilisés par l'AC, pour la génération et la mise en œuvre de ses clés de signature, ainsi que le cas échéant pour la génération des clés des porteurs, doivent être des modules cryptographiques répondant au minimum aux exigences du chapitre XI ci-dessous pour le niveau de sécurité considéré.

VI.2.1.2. Dispositifs de protection des éléments secrets des porteurs

Les dispositifs de protection des éléments secrets des porteurs, pour la mise en œuvre de leurs clés privées de personne, doivent respecter les exigences du chapitre XII ci-dessous pour le niveau de sécurité considéré.

Si l'AC ne fournit pas elle-même ce dispositif au porteur, elle doit s'assurer auprès du porteur de la conformité de son dispositif de protection des éléments secrets, au minimum au travers d'un engagement contractuel clair et explicite du porteur vis-à-vis de l'AC.

En revanche, lorsque l'AC fournit ce dispositif au porteur, directement ou indirectement, elle doit s'assurer que :

- La préparation des dispositifs de protection des éléments secrets est contrôlée de façon sécurisée par le prestataire de service ;
- Les dispositifs de protection des éléments secrets sont stockés et distribués de façon sécurisée ;
- Les désactivations et réactivations des dispositifs de protection des éléments secrets sont contrôlées de façon sécurisée.

Note : L'AC peut s'inspirer du document [ExigencesSitesPerso] pour répondre à ces exigences.

VI.2.2. Contrôle de la clé privée par plusieurs personnes

Ce chapitre porte sur le contrôle de la clé privée de l'AC pour l'exportation / l'importation hors / dans un module cryptographique. La génération de la bi-clé est traitée au chapitre VI.1.1.1, l'activation de la clé privée au chapitre VI.2.8 et sa destruction au chapitre VI.2.10.

	Niveaux (**) et (***)	

Le contrôle des clés privées de signature de l'AC doit être assuré par du personnel de confiance (porteurs de secrets d'IGC) et via un outil mettant en œuvre le partage des secrets (systèmes où n exploitants parmi m doivent s'authentifier, avec n au moins égal à 2).

	Niveau (*)	
Le contrôle des clés privées de signature de l'AC doit être assuré par du personnel de confiance (porteurs de secrets d'IGC).		

VI.2.3. Séquestre de la clé privée

Seules les clés privées associées aux certificats électroniques dont l'usage est la confidentialité (chiffrement) peuvent être séquestrées, conformément aux dispositions prévues dans la PC et la DPC de l'AC et en respectant les exigences de séquestre et de recouvrement du chapitre IV.12.

VI.2.4. Copie de secours de la clé privée

Hormis pour les clés privées à usage de confidentialité, les clés privées des porteurs ne doivent faire l'objet d'aucune copie de secours par l'AC.

Les clés privées d'AC peuvent faire l'objet de copies de secours, soit dans un module cryptographique conforme aux exigences du chapitre XI ci-dessous, soit hors d'un module cryptographique mais dans ce cas sous forme chiffrée et avec un mécanisme de contrôle d'intégrité. Le chiffrement correspondant doit offrir un niveau de sécurité équivalent ou supérieur au stockage au sein du module cryptographique et, notamment, s'appuyer sur un algorithme, une longueur de clé et un mode opératoire capables de résister aux attaques par cryptanalyse pendant au moins la durée de vie de la clé ainsi protégée. Les règles à respecter sont définies dans le document [RGS_B_1].

Les opérations de chiffrement et de déchiffrement doivent être effectuées à l'intérieur du module cryptographique de telle manière que les clés privées d'AC ne soient à aucun moment en clair en dehors du module cryptographique.

Le contrôle des opérations de chiffrement / déchiffrement doit être conforme aux exigences du chapitre VI.2.2.

[Confidentialité]		
Les clés privées des porteurs séquestrées par l'AC peuvent faire l'objet de copies de secours par l'AC, moyennant le respect des exigences de sécurité pour le séquestre des clés.		

VI.2.5. Archivage de la clé privée

Les clés privées de l'AC ne doivent en aucun cas être archivée.

Les clés privées des porteurs ne doivent en aucun cas être archivées ni par l'AC ni par aucune des composantes de l'IGC.

VI.2.6. Transfert de la clé privée vers / depuis le module cryptographique

Si l'AC génère les clés privées des porteurs en dehors du dispositif du porteur, le transfert doit se faire conformément aux exigences du chapitre VI.1.1.2 ci-dessus.

Pour les clés privées d'AC, tout transfert doit se faire sous forme chiffrée, conformément aux exigences du chapitre VI.2.4.

VI.2.7. Stockage de la clé privée dans un module cryptographique

Il est recommandé de stocker les clés privées d'AC dans un module cryptographique répondant au minimum aux exigences du chapitre XI ci-dessous pour le niveau de sécurité considéré.

Cependant, dans le cas des copies de secours, le stockage peut être effectué en dehors d'un module cryptographique moyennant le respect des exigences du chapitre VI.2.4.

Quel que soit le moyen utilisé, l'AC doit garantir que les clés privées d'AC ne sont pas compromises pendant leur stockage ou leur transport.

VI.2.8. Méthode d'activation de la clé privée

VI.2.8.1. Clés privées d'AC

La méthode d'activation des clés privées d'AC dans un module cryptographique doit permettre de répondre aux exigences définies dans le chapitre XI pour le niveau de sécurité considéré.

	Niveaux (**) et (***)	
L'activation des clés privées d'AC dans un module cryptographique doit être contrôlée via des données d'activation (cf. chapitre VI.4) et doit faire intervenir au moins deux personnes dans des rôles de confiance (par exemple, responsable sécurité et opérateur).		

	Niveau (*)	
L'activation des clés privées d'AC dans un module cryptographique doit être contrôlée via des données d'activation (cf. chapitre VI.4) et doit faire intervenir au moins une personne ayant au moins un rôle de confiance (par exemple, responsable sécurité).		

VI.2.8.2. Clés privées des porteurs

La méthode d'activation de la clé privée du porteur dépend du dispositif utilisé. L'activation de la clé privée du porteur doit au minimum être contrôlée via des données d'activation (cf. chapitre VI.4) et doit permettre de répondre aux exigences définies dans le chapitre XII pour le niveau de sécurité considéré.

VI.2.9. Méthode de désactivation de la clé privée

VI.2.9.1. Clés privées d'AC

La désactivation des clés privées d'AC dans un module cryptographique doit être automatique dès que l'environnement du module évolue : arrêt ou déconnexion du module, déconnexion de l'opérateur, etc. Une clé privée d'AC peut également être désactivée après une certaine période d'inactivité. Ces conditions de désactivation doivent permettre de répondre aux exigences définies dans le chapitre XI pour le niveau de sécurité considéré.

VI.2.9.2. Clés privées des porteurs

Les conditions de désactivation de la clé privée d'un porteur doivent permettre de répondre aux exigences définies dans le chapitre XII pour le niveau de sécurité considéré.

VI.2.10. Méthode de destruction des clés privées

VI.2.10.1. Clés privées d'AC

La méthode de destruction des clés privées d'AC doit permettre de répondre aux exigences définies dans le chapitre XI pour le niveau de sécurité considéré.

En fin de vie d'une clé privée d'AC, normale ou anticipée (révocation), cette clé doit être systématiquement détruite, ainsi que toute copie et tout élément permettant de la reconstituer.

VI.2.10.2. Clés privées des porteurs

Si les clés privées des porteurs sont générées par l'AC dans un module cryptographique hors du dispositif de protection des éléments secrets, la méthode de destruction de ces clés privées après leur exportation hors du module cryptographique doit permettre de répondre aux exigences définies dans le chapitre XII pour le niveau de sécurité considéré.

En fin de vie de la clé privée d'un porteur, la méthode de destruction de cette clé privée doit permettre de répondre aux exigences définies dans le chapitre XII pour le niveau de sécurité considéré.

[Confidentialité]		
Lorsque la clé privée d'un porteur n'est plus nécessaire (cf. nota ci-dessous), la méthode de destruction de cette clé privée doit permettre de répondre aux exigences définies dans le chapitre XII pour le niveau de sécurité considéré. *Nota* - À la fin de la période de validité d'un certificat, le passage à une nouvelle clé privée peut se faire au niveau du porteur : ➢ Soit en conservant l'ancienne et la nouvelle clé privée, afin que le porteur continue à accéder aux données précédemment chiffrées avec son ancienne clé privée, ➢ Soit en procédant à un transchiffrement de l'ancienne clé privée vers la nouvelle, dans ce cas l'ancienne clé n'a pas à être conservée. Cela dépend de l'application et est hors du cadre de la présente PC Type.		

VI.2.11. Niveau de qualification du module cryptographique et des dispositifs de protection des éléments secrets

Les exigences de qualification des produits de sécurité de type module cryptographique et dispositif de protection des éléments secrets ne s'appliquent que lorsque :

- le PSCE fait l'objet d'une procédure de qualification de son offre de certificats électroniques et
- les dispositifs de protection des éléments secrets sont délivrés par le PSCE.

Ces exigences sont précisées aux chapitres XI et XII.

VI.3. Autres aspects de la gestion des bi-clés

VI.3.1. Archivage des clés publiques

Les clés publiques de l'AC et des porteurs sont archivées dans le cadre de l'archivage des certificats correspondants.

VI.3.2. Durées de vie des bi-clés et des certificats

Les bi-clés et les certificats des porteurs couverts par la présente PC Type doivent avoir une durée de vie maximale de :

• Particulier	5 ans	5 ans	5 ans
• Agent	3 ans	3 ans	3 ans
• Entreprise	3 ans	3 ans	3 ans

Cette durée de vie s'entend à compter de la première utilisation de la clé, ou de la première émission d'un certificat associé à cette clé. La clé doit respecter les exigences de caractéristiques (tailles, algorithmes, etc.) de l'annexe B1 du RGS (taille, algorithme) du document [RGS_A4] au démarrage de sa durée de vie.

La fin de validité d'un certificat d'AC doit être postérieure à la fin de vie des certificats porteurs qu'elle émet. L'AC doit préciser dans sa PC la durée de vie des clés de signature d'AC et des certificats correspondants. Cette durée de vie doit être cohérente avec les caractéristiques de l'algorithme et la longueur de clé utilisés (cf. [RGS_B1]) et de la date de fin de validité de l'AC qui l'a émise.

À titre d'exemple, et sous réserve que les algorithmes et longueurs soient conformes aux exigences de l'annexe [RGS_B1], une clé d'AC racine a une durée de vie de 12 ans, une AC intermédiaire une durée de vie de 6 ans et un certificat délivré à une personne physique une durée de vie de 3 ans.

VI.4. Données d'activation

VI.4.1. Génération et installation des données d'activation

VI.4.1.1. Génération et installation des données d'activation correspondant à la clé privée de l'AC

La génération et l'installation des données d'activation d'un module cryptographique de l'IGC doivent se faire lors de la phase d'initialisation et de personnalisation de ce module. Si les données d'activation ne sont pas choisies et saisies par les responsables de ces données eux-mêmes, elles doivent leur être transmises de manière à en garantir la confidentialité et l'intégrité. Ces données d'activation ne doivent être connues que par les responsables nommément identifiés dans le cadre des rôles qui leurs sont attribués (cf. chapitre V.2.1).

VI.4.1.2. Génération et installation des données d'activation correspondant à la clé privée du porteur

Si l'AC génère la clé privée du porteur, elle a pour obligation de transmettre au porteur les données d'activation correspondantes par le biais d'un chemin garantissant la protection en intégrité et en

confidentialité des données. Notamment, la remise de la donnée d'activation doit être séparée dans le temps ou dans l'espace de la remise de la clé privée.

Par exemple : si les éléments secrets d'un porteur sont gérés sur un support matériel dont la mise en œuvre est conditionnée par l'utilisation d'un code personnel, la fourniture du support et celle du code personnel doivent être réalisées par des moyens différents (par exemple retrait du support à un guichet de l'AE et envoi du code par un autre canal).

Si les données d'activation sont sous forme de mots de passe, le porteur doit être informé de la politique de constitution des mots de passe (par exemple, longueur d'au moins 8 caractères, présence d'au moins un caractère spécial, etc.).

VI.4.2. Protection des données d'activation

VI.4.2.1. Protection des données d'activation correspondant à la clé privée de l'AC

Les données d'activation qui sont générées par l'AC pour les modules cryptographiques de l'IGC doivent être protégées en intégrité et en confidentialité jusqu'à la remise à leur destinataire. Ce destinataire a ensuite la responsabilité d'en assurer la confidentialité, l'intégrité et la disponibilité.

VI.4.2.2. Protection des données d'activation correspondant aux clés privées des porteurs

Si les données d'activation des dispositifs de protection des éléments secrets des porteurs sont générées par l'AC, elles doivent être protégées en intégrité et en confidentialité jusqu'à la remise aux porteurs.

Si ces données d'activation sont également sauvegardées par l'AC, elles doivent être protégées en intégrité et en confidentialité.

VI.4.3. Autres aspects liés aux données d'activation

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

VI.5. Mesures de sécurité des systèmes informatiques

Les mesures de sécurité relatives aux systèmes informatiques doivent satisfaire aux objectifs de sécurité qui découlent de l'analyse de risque que l'AC peut mener (cf. chapitre I.4.1).

Une analyse des objectifs de sécurité peut être effectuée en amont de tout projet d'IGC par l'AC, de façon à garantir la prise en compte de la sécurité dans les systèmes informatiques.

Le PSCE doit être en mesure de justifier, par tout moyen, qu'il a pris les mesures nécessaires pour assurer la protection des échanges d'information entre les différentes composantes de l'IGC. Il vérifie périodiquement les mesures de sécurité prises dans ce cadre. Le moyen privilégié consiste en un audit technique réalisé par un prestataire d'audit de la sécurité des systèmes d'information qualifié.

VI.5.1. Exigences de sécurité technique spécifiques aux systèmes informatiques

Un niveau minimal d'assurance de la sécurité offerte sur les systèmes informatiques de l'IGC doit être défini dans la DPC de l'AC. Il doit au moins répondre aux objectifs de sécurité suivants :

- Identification et authentification forte des utilisateurs pour l'accès au système (authentification à deux facteurs, de nature physique et/ou logique),
- Gestion des droits des utilisateurs (permettant de mettre en œuvre la politique de contrôle d'accès définie par l'AC, notamment pour implémenter les principes de moindres privilèges, de contrôles multiples et de séparation des rôles),
- Gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur),

- Protection contre les virus informatiques et toutes formes de logiciels compromettants ou non-autorisés et mises à jour des logiciels,
- Gestion des comptes des utilisateurs, notamment la modification et la suppression rapide des droits d'accès,
- Protection du réseau contre toute intrusion d'une personne non autorisée,
- Protection du réseau afin d'assurer la confidentialité et l'intégrité des données qui y transitent,
- Fonctions d'audits (non-répudiation et nature des actions effectuées),
- Éventuellement, gestion des reprises sur erreur.

Les applications utilisant les services des composantes peuvent requérir des besoins de sécurité complémentaires.

La protection en confidentialité et en intégrité des clés privées ou secrètes d'infrastructure et de contrôle doit faire l'objet de mesures particulières qui peuvent découler de l'analyse de risque.

Des dispositifs de surveillance (avec alarme automatique) et des procédures d'audit des paramétrages du système (en particulier des éléments de routage) doivent être mis en place.

VI.5.2. Niveau de qualification des systèmes informatiques

	Niveaux (**) et (***)	
Lorsque le PSCE souhaite faire qualifier son offre de certificats électroniques, il est recommandé que les systèmes informatiques de l'IGC mettant en œuvre le module cryptographique fassent l'objet d'une qualification conformément à la loi du pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices, au niveau standard défini par le [RGS] et en respectant les exigences du [CWA 14167-1].		

VI.6. Mesures de sécurité des systèmes durant leur cycle de vie

Les mesures de sécurité relatives aux cycles de vie des systèmes informatiques doivent satisfaire aux objectifs de sécurité qui découlent de l'analyse de risque que l'AC peut mener (cf. rappel au début du présent chapitre VI).

VI.6.1 Mesures de sécurité liées au développement des systèmes

L'implémentation d'un système permettant de mettre en œuvre les composantes de l'IGC doit être documentée et doit respecter dans la mesure du possible des normes de modélisation et d'implémentation. La configuration du système des composantes de l'IGC ainsi que toute modification et mise à niveau doivent être documentées et contrôlées.

L'AC doit :

- Garantir que les objectifs de sécurité sont définis lors des phases de spécification et de conception
- Utiliser des systèmes et des produits fiables qui sont protégés contre toute modification

VI.6.2 Mesures liées à la gestion de la sécurité

Toute évolution significative d'un système d'une composante de l'IGC doit être signalée à l'AC pour validation. Elle doit être documentée et doit apparaître dans les procédures de fonctionnement interne de la composante concernée et être conforme au schéma de maintenance de l'assurance de conformité, dans le cas de produits évalués.

VI.6.3 Niveau d'évaluation sécurité du cycle de vie des systèmes

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

VI.7. Mesures de sécurité réseau

L'interconnexion vers des réseaux publics doit être protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement de la composante au sein de l'IGC.

L'AC doit garantir que les composants du réseau local (routeurs, par exemple) sont maintenus dans un environnement physiquement sécurisé et que leurs configurations sont périodiquement auditées en vue de vérifier leur conformité avec les exigences spécifiées par l'AC.

De plus, les échanges entre composantes au sein de l'IGC peuvent nécessiter la mise en place de mesures particulières en fonction du niveau de sensibilité des informations (utilisation de réseaux séparés / isolés, mise en œuvre de mécanismes cryptographiques à l'aide de clés d'infrastructure et de contrôle, etc.).

VI.8. Horodatage / Système de datation

Plusieurs exigences de la présente PC Type nécessitent la datation par les différentes composantes de l'IGC d'évènements liés aux activités de l'IGC (cf. chapitre V.4).

Pour dater ces évènements, les différentes composantes de l'IGC peuvent recourir :

- Soit à une autorité d'horodatage, interne ou externe à l'IGC, conforme à la politique d'horodatage [RGS_A5] ;
- Soit en utilisant l'heure système de l'IGC en assurant une synchronisation des horloges des systèmes de l'IGC entre elles, au minimum à la minute près, et par rapport à une source fiable de temps UTC, au minimum à la seconde près. Pour les opérations faites hors ligne (ex : administration d'une AC Racine), cette précision de synchronisation par rapport au temps UTC n'est pas requise. Le système devra toutefois pouvoir ordonner les évènements avec une précision suffisante. Pour la synchronisation par rapport au temps UTC, il est recommandé de se référer à un système comprenant au moins deux sources indépendantes de temps.

VII. Profils des certificats, OCSP et des LCR

Le document [RGS_A4] liste les règles concernant les profils des certificats, des listes de révocation (LCR) et OCSP. Elles portent notamment sur :

- Les algorithmes et longueurs des clés cryptographiques ;
- Limitation exclusive de l'usage du certificat électronique.

VIII. Audit de conformité et autres évaluations

Le présent chapitre concerne les audits et les évaluations que doit réaliser, ou faire réaliser, l'AC afin de s'assurer que l'ensemble de son IGC, ainsi que le cas échéant le ou les MC, est bien conforme à ses engagements affichés dans sa PC et aux pratiques identifiées dans sa DPC.

VIII.1. Fréquences et / ou circonstances des évaluations

Avant la première mise en service d'une composante de son IGC ou suite à toute modification significative au sein d'une composante, l'AC doit procéder à un contrôle de conformité de cette composante.

L'AC doit également procéder régulièrement à un contrôle de conformité de l'ensemble de son IGC, selon la fréquence suivante :

Description	**Niveau ***	**Niveau ****	**Niveau *****
Fréquence de contrôle de conformité de l'ensemble de l'IGC	1 fois tous les 3 ans	1 fois tous les 2 ans	1 fois par an

VIII.2. Identités / qualifications des évaluateurs

Le contrôle d'une composante doit être assigné par l'AC à une équipe d'auditeurs compétents en sécurité des systèmes d'information et dans le domaine d'activité de la composante contrôlée.

VIII.3. Relations entre évaluateurs et entités évaluées

L'équipe d'audit ne doit pas appartenir à l'entité opérant la composante de l'IGC contrôlée, quelle que soit cette composante, et être dûment autorisée à pratiquer les contrôles visés.

VIII.4. Sujets couverts par les évaluations

Les contrôles de conformité portent sur une composante de l'IGC (contrôles ponctuels) ou sur l'ensemble de l'architecture de l'IGC (contrôles périodiques) et visent à vérifier le respect des engagements et pratiques définies dans la PC de l'AC et dans la DPC qui y répond ainsi que des éléments qui en découlent (procédures opérationnelles, ressources mises en œuvre, etc.).

Le PSCE doit également être en mesure de justifier, par tout moyen, aux auditeurs, qu'il a pris les mesures nécessaires pour assurer la protection des échanges d'information entre les différentes composantes de l'IGC. Il vérifie périodiquement les mesures de sécurité prises dans ce cadre. Le moyen privilégié consiste en un audit technique réalisé par un prestataire d'audit de la sécurité des systèmes d'information qualifié.

VIII.5. Actions prises suite aux conclusions des évaluations

À l'issue d'un contrôle de conformité, l'équipe d'audit rend à l'AC, un avis parmi les suivants : « réussite », « échec », « à confirmer ».

Selon l'avis rendu, les conséquences du contrôle sont les suivantes :

- En cas d'échec, et selon l'importance des non-conformités, l'équipe d'audit émet des recommandations à l'AC qui peuvent être la cessation (temporaire ou définitive) d'activité, la révocation du certificat de la composante, la révocation de l'ensemble des certificats émis depuis le dernier contrôle positif, etc. Le choix de la mesure à appliquer est effectué par l'AC et doit respecter ses politiques de sécurité internes.
- En cas de résultat «à confirmer», l'AC remet à la composante un avis précisant sous quel délai les non-conformités doivent être levées. Puis, un contrôle de « confirmation « permettra de vérifier que tous les points critiques ont bien été résolus.

- En cas de réussite, l'AC confirme à la composante contrôlée la conformité aux exigences de la PC et la DPC.

VIII.6. Communication des résultats

Les résultats des audits de conformité doivent être tenus à la disposition de l'organisme de qualification en charge de la qualification de l'AC.

IX. Autres problématiques métiers et légales

IX.1. Tarifs

IX.1.1. Tarifs pour la fourniture ou le renouvellement de certificats

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

IX.1.2. Tarifs pour accéder aux certificats

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

IX.1.3. Tarifs pour accéder aux informations d'état et de révocation des certificats

L'accès aux LCR et, éventuellement, deltaLCR doit être en accès libre en lecture.

IX.1.4. Tarifs pour d'autres services

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

IX.1.5. Politique de remboursement

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

IX.2. Responsabilité financière

Conformément à ses obligations, l'AC doit prendre les dispositions nécessaires pour couvrir, éventuellement financièrement, ses responsabilités liées à ses opérations et/ou activités.

IX.2.1. Couverture par les assurances

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

IX.2.2. Autres ressources

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

IX.2.3. Couverture et garantie concernant les entités utilisatrices

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

IX.3. Confidentialité des données professionnelles

IX.3.1. Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont au moins les suivantes :

- La partie non-publique de la DPC de l'AC,
- Les clés privées de l'AC, des composantes et des porteurs de certificats,
- Les données d'activation associées aux clés privées d'AC et des porteurs[39],
- Tous les secrets de l'IGC,

[39] La confidentialité des données d'activation des clés privées des porteurs doit être garantie par l'AC tant qu'elle les détient.

- Les journaux d'évènements des composantes de l'IGC,
- Les dossiers d'enregistrement des porteurs,
- Les causes de révocations, sauf accord explicite du porteur.

[Confidentialité]		
Les clés privées de l'AC, des composantes et des porteurs de certificats (notamment lorsqu'elles sont séquestrées) sont aussi considérées comme des informations confidentielles.		

IX.3.2. Informations hors du périmètre des informations confidentielles

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

IX.3.3. Responsabilités en termes de protection des informations confidentielles

L'AC est tenue d'appliquer des procédures de sécurité pour garantir la confidentialité des informations identifiées au chapitre IX.3.1, en particulier en ce qui concerne l'effacement définitif ou la destruction des supports ayant servi à leur stockage.

De plus, lorsque ces données sont échangées, l'AC doit en garantir l'intégrité.

L'AC est notamment tenue de respecter la législation et la réglementation en vigueur sur le territoire français. En particulier, elle peut devoir mettre à disposition les dossiers d'enregistrement des porteurs à des tiers dans le cadre de procédures légales. Elle doit également donner l'accès à ces informations au porteur et au MC.

IX.4. Protection des données à caractère personnel

IX.4.1. Politique de protection des données à caractère personnel

Il est entendu que toute collecte et tout usage de données à caractère personnel par l'AC et l'ensemble de ses composantes sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, en particulier de la loi [CNIL].

IX.4.2. Données à caractère personnel

Les données considérées comme personnelles sont au moins les suivantes :

- Les causes de révocation des certificats des porteurs (qui sont considérées comme confidentielles sauf accord explicite du porteur) ;
- Le dossier d'enregistrement du porteur.

IX.4.3. Données à caractère non personnel

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

IX.4.4. Responsabilité en termes de protection des données à caractère personnel

Cf. législation et réglementation en vigueur sur le territoire français (notamment cf. chapitre X ci-dessous)

IX.4.5. Notification et consentement d'utilisation des données à caractère personnel

Conformément à la législation et réglementation en vigueur sur le territoire français, les informations personnelles remises par les porteurs à l'AC ne doivent ni ne être divulguées ni transférées à un tiers sauf dans les cas suivants : consentement préalable du porteur, décision judiciaire ou autre autorisation légale.

IX.4.6. Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives

Cf. législation et réglementation en vigueur sur le territoire français (notamment cf. chapitre X ci-dessous).

IX.4.7. Autres circonstances de divulgation de données à caractère personnel

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

IX.5. Droits de propriété intellectuelle

La présente PC Type ne formule pas d'exigence spécifique sur le sujet. Application de la législation et de la réglementation en vigueur sur le territoire français.

IX.6. Interprétations contractuelles et garanties

Les obligations communes aux composantes de l'IGC sont les suivantes :

- Protéger et garantir l'intégrité et la confidentialité de leurs clés secrètes et/ou privées,
- N'utiliser leurs clés cryptographiques (publiques, privées et/ou secrètes) qu'aux fins prévues lors de leur émission et avec les outils spécifiés dans les conditions fixées par la PC de l'AC et les documents qui en découlent,
- Respecter et appliquer la partie de la DPC leur incombant (cette partie doit être communiquée à la composante correspondante),
- Se soumettre aux contrôles de conformité effectués par l'équipe d'audit mandatée par l'AC (cf. chapitre VII-VIII) et l'organisme de qualification,
- Respecter les accords ou contrats qui les lient entre elles ou aux porteurs,
- Documenter leurs procédures internes de fonctionnement,
- Mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles elles s'engagent dans des conditions garantissant qualité et sécurité.

IX.6.1. Autorités de Certification

L'AC a pour obligation de :

- Pouvoir démontrer aux utilisateurs de ses certificats qu'elle a émis un certificat pour un porteur donné et que ce porteur a accepté le certificat, conformément aux exigences du chapitre IV.4 ci-dessus.
- Garantir et maintenir la cohérence de sa DPC avec sa PC.
- Prendre toutes les mesures raisonnables pour s'assurer que ses porteurs sont au courant de leurs droits et obligations en ce qui concerne l'utilisation et la gestion des clés, des certificats ou encore de l'équipement et des logiciels utilisés aux fins de l'IGC. La relation entre un porteur et l'AC est formalisée par un lien contractuel / hiérarchique / réglementaire précisant les droits et obligations des parties et notamment les garanties apportées par l'AC.

L'AC est responsable de la conformité de sa Politique de Certification avec les exigences émises dans la présente PC Type pour le niveau de sécurité considéré. L'AC assume toute conséquence dommageable résultant du non-respect de sa PC, conforme aux exigences de la présente PC Type, par elle-même ou l'une de ses composantes. Elle doit prendre les dispositions nécessaires pour couvrir ses responsabilités liées à ses opérations et/ou activités et posséder la stabilité financière et les ressources exigées pour fonctionner en conformité avec la présente politique.

De plus, l'AC reconnaît engager sa responsabilité en cas de faute ou de négligence, d'elle-même ou de l'une de ses composantes, quelle qu'en soit la nature et la gravité, qui aurait pour conséquence la lecture, l'altération ou le détournement des données personnelles des porteurs à des fins frauduleuses, que ces données soient contenues ou en transit dans les applications de gestion des certificats de l'AC.

Par ailleurs, l'AC reconnaît avoir à sa charge un devoir général de surveillance, quant à la sécurité et l'intégrité des certificats délivrés par elle-même ou l'une de ses composantes. Elle est responsable du maintien du niveau de sécurité de l'infrastructure technique sur laquelle elle s'appuie pour fournir ses services. Toute modification ayant un impact sur le niveau de sécurité fourni doit être approuvée par les instances de haut niveau de l'AC.

En cas de non-respect ponctuel des obligations décrites dans la présente PC Type, l'Administration se réserve le droit de refuser temporairement ou définitivement les certificats de l'AC conformément à la réglementation en vigueur.

IX.6.2. Service d'enregistrement

Cf. les obligations pertinentes du chapitre IX.6.1.

IX.6.3. Porteurs de certificats

Le porteur a le devoir de :

- Communiquer des informations exactes et à jour lors de la demande ou du renouvellement du certificat ;
- Protéger sa clé privée par des moyens appropriés à son environnement ;
- Protéger ses données d'activation et, le cas échéant, les mettre en œuvre ;
- Protéger l'accès à sa base de certificats ;
- Respecter les conditions d'utilisation de sa clé privée et du certificat correspondant ;
- Informer l'AC de toute modification concernant les informations contenues dans son certificat ;
- Faire, sans délai, une demande de révocation de son certificat auprès de l'AE, du MC de son entreprise ou de l'AC en cas de compromission ou de suspicion de compromission de sa clé privée (ou de ses données d'activation).

La relation entre le porteur et l'AC ou ses composantes est formalisée par un engagement du porteur visant à certifier l'exactitude des renseignements et des documents fournis.

Ces informations s'appliquent également aux MC.

IX.6.4. Utilisateurs de certificats

Les utilisateurs de la sphère publique utilisant les certificats doivent :

- Vérifier et respecter l'usage pour lequel un certificat a été émis ;
- Pour chaque certificat de la chaîne de certification, du certificat du porteur jusqu'à l'AC Racine, vérifier la signature numérique de l'AC émettrice du certificat considéré et contrôler la validité de ce certificat (dates de validité, statut de révocation) ;
- Vérifier et respecter les obligations des utilisateurs de certificats exprimées dans la présente
- PC Type.

[Confidentialité]		
Les utilisateurs de la sphère publique utilisant les certificats doivent de plus contrôler que le certificat émis par l'AC est référencé au niveau de sécurité et pour le service de confiance requis par l'application.		

L'AC ne doit pas émettre dans sa propre PC d'obligations supplémentaires, par rapport aux obligations de la présente PC Type, à l'encontre des utilisateurs de la sphère publique.

IX.6.5. Autres participants

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

IX.7. Limite de garantie

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

IX.8. Limite de responsabilité

[Signature]		
Il est rappelé que les AC qualifiées suivant la PC type Signature pour le niveau *** délivrent des certificats qualifiés au sens du décret [SIG]. Par conséquent, leur régime de responsabilité est défini par l'article 33 de la [LCEN].		

IX.9. Indemnités

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

IX.10. Durée et fin anticipée de validité de la PC

IX.10.1. Durée de validité

La PC de l'AC doit rester en application au moins jusqu'à la fin de vie du dernier certificat émis au titre de cette PC.

IX.10.2. Fin anticipée de validité

La publication d'une nouvelle version de la présente PC Type peut entraîner, en fonction des évolutions apportées, la nécessité pour l'AC de faire évoluer sa PC correspondante.

En fonction de la nature et de l'importance des évolutions apportées à la PC Type, le délai de mise en conformité sera arrêté conformément aux modalités prévues par la réglementation en vigueur.

De plus, la mise en conformité n'impose pas le renouvellement anticipé des certificats déjà émis, sauf cas exceptionnel lié à la sécurité.

IX.10.3. Effets de la fin de validité et clauses restant applicables

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

IX.11. Notifications individuelles et communications entre les participants

En cas de changement de toute nature intervenant dans la composition de l'IGC, l'AC devra :

- Au plus tard un mois avant le début de l'opération, faire valider ce changement au travers d'une expertise technique, afin d'évaluer les impacts sur le niveau de qualité et de sécurité des fonctions

de l'AC et de ses différentes composantes.

- Au plus tard un mois après la fin de l'opération, en informer l'organisme de qualification.

IX.12. Amendements à la PC

IX.12.1. Procédures d'amendements

L'AC devra contrôler que tout projet de modification de sa PC reste conforme aux exigences de la présente

PC Type et des éventuels documents complémentaires du [RGS]. En cas de changement important, il est recommandé à l'AC de faire appel à une expertise technique pour en contrôler l'impact.

IX.12.2. Mécanisme et période d'information sur les amendements

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

IX.12.3. Circonstances selon lesquelles l'OID doit être changé

L'OID de la PC de l'AC étant inscrit dans les certificats qu'elle émet, toute évolution de cette PC ayant un impact majeur sur les certificats déjà émis (par exemple, augmentation des exigences en matière d'enregistrement des porteurs, qui ne peuvent donc pas s'appliquer aux certificats déjà émis) doit se traduire par une évolution de l'OID, afin que les utilisateurs puissent clairement distinguer quels certificats correspondent à quelles exigences.

En particulier, l'OID de la PC de l'AC doit évoluer dès lors qu'un changement majeur (et qui sera signalé comme tel, notamment par une évolution de l'OID de la présente PC Type) intervient dans les exigences de la présente PC Type applicable à la famille de certificats considérée.

IX.13. Dispositions concernant la résolution de conflits

L'AC doit mettre en place des politiques et procédures pour le traitement des réclamations et le règlement des litiges émanant des entités pour lesquelles elle fournit des services électroniques de confiance ou d'autres points qui y sont liés.

IX.14. Juridictions compétentes

La présente PC Type ne formule pas d'exigence spécifique sur le sujet. Application de la législation et de la réglementation en vigueur sur le territoire français.

IX.15. Conformité aux législations et réglementations

Les textes législatifs et réglementaires applicables à la présente PC Type sont, notamment, ceux indiqués au chapitre X ci-dessous.

L'AC est notamment soumise aux dispositions prévues par l'article 31 de la [LSQ] concernant la remise des clés privées des porteurs, si celles-ci sont séquestrées par l'AC.

IX.16. Dispositions diverses

IX.16.1. Accord global

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

IX.16.2. Transfert d'activités

Cf. chapitre V.8-11.

IX.16.3. Conséquences d’une clause non valide

La présente PC Type ne formule pas d’exigence spécifique sur le sujet.

IX.16.4. Application et renonciation

La présente PC Type ne formule pas d’exigence spécifique sur le sujet.

IX.16.5. Force majeure

Sont considérés comme cas de force majeure tous ceux habituellement retenus par les tribunaux français, notamment le cas d’un évènement irrésistible, insurmontable et imprévisible.

IX.17. Autres dispositions

La présente PC Type ne formule pas d’exigence spécifique sur le sujet.

X. Annexe 1 : Documents cités en référence

X.1. Réglementation

[CNIL]	Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004
[ORDONNANCE]	Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives
[LSQ]	Loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne.
[LCEN]	Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, notamment son article 31 concernant la déclaration de fourniture de cryptologie et son article 33 qui précise le régime de responsabilité des prestataires de services de certification électronique délivrant des certificats électroniques qualifiés.
[SIG]	Décret n° 2001-272 du 30 mars 2001 pris pour application de l'article 1316-4 du code civil et relatif à la signature électronique.
[LOIDUPAYS]	Loi du pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices

X.2. Documents techniques

[RGS]	Référentiel Général de Sécurité – Version 1.0
[RGS_A1]	RGS - Fonction de sécurité - Version 1.0
[RGS_A4]	RGS - Politiques de Certification Types - Profils de certificats, de LCR et OCSP et algorithmes cryptographiques – Version 1.0
[CWA14167-1]	CWA 14167-1 (2003-06) Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1
[CWA14167-2]	CWA 14167-2 (2003-10) Cryptographic Module for CSP Signing Operations with Backup - Protection Profile (CMCSOB-PP). Ce PP a été certifié EAL4+.
[CWA14167-3]	CWA 14167-3 (2003-10) Cryptographic Module for CSP Key Generation Services -Protection Profile (CMCKG-PP)
[CWA14167-4]	CWA 14167-4 (2003-10) Cryptographic Module for CSP Signing Operations - Protection Profile (CMCSO-PP). Ce PP a été certifié EAL4+.
[CWA14169]	CWA 14169 (2002-04) Secure Signature Creation Devices (SSCD). Ce PP a été certifié EAL4+.
[ExigencesSitesPerso]	Exigences de sécurité des sites de personnalisation, V1.0 (août 2007) http://www.references.modernisation.gouv.fr/sites/default/files/Exigences_sites_de_perso
	V1 _0.pdf

[ETSI_NQCP]	ETSI TS 102 042 V1.3.4 (décembre 2007) applicable Policy Requirements for Certification Authorities issuing public key certificates
[ETSI_QCP]	ETSI TS 101 456 V1.4.3 (mai 2007) Policy Requirements for Certification Authorities issuing qualified certificates
[ETSI_SigPol]	ETSI TR 102 272 - ASN.1 format for signature policies V1.1.1 (décembre 2003) ETSI TR 102 038 - XML format for signature policies V1.1.1 (avril 2002)
[PROG_ACCRED]	COFRAC - Programme d'accréditation pour la qualification des prestataires de services de confiance – CEPE REF 21 -publié cf www.cofrac.fr
[RFC3647]	IETF - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practice Framework - novembre 2003
[RGS_B_1]	Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, Version 1.0
[X.509]	Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks, Recommendation X.509, version d'août 2005 (complétée par les correctifs techniques Corrigendum 1 de janvier 2007 et Corrigendum 2 de novembre 2008)
[972-1]	DCSSI - Guide Technique pour la confidentialité des informations enregistrées sur les disques durs à recycler ou exporter – N° 972-1/SGDN/DCSSI du 17/07/2003

XI. Annexe 2 : Exigences de sécurité du module cryptographique de l'AC

XI.1. Exigences sur les objectifs de sécurité

Le module cryptographique, utilisé par l'AC pour générer et mettre en œuvre ses clés de signature (pour la génération des certificats électroniques, des LCR / LAR ou des réponses OCSP), ainsi que, le cas échéant, générer les bi-clés des porteurs, doit répondre aux exigences de sécurité suivantes.

- si les bi-clés des porteurs sont générées par ce module, garantir que ces générations sont réalisées exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique des bi-clés générées ;
- si les bi-clés des porteurs sont générées par ce module, assurer la confidentialité des clés privées et l'intégrité des clés privées et publiques des porteurs lorsqu'elles sont sous la responsabilité de l'AC et pendant leur transfert vers le dispositif de protection des éléments secrets du porteur et assurer leur destruction sûre après ce transfert ;
- assurer la confidentialité et l'intégrité des clés privées de signature de l'AC durant tout leur cycle de vie, et assurer leur destruction sûre en fin de vie ;
- être capable d'identifier et d'authentifier ses utilisateurs ;
- limiter l'accès à ses services en fonction de l'utilisateur et du rôle qui lui a été assigné ;
- être capable de mener une série de tests pour vérifier qu'il fonctionne correctement et entrer dans un état sûr s'il détecte une erreur ;
- permettre de créer une signature électronique sécurisée, pour signer les certificats générés par l'AC, qui ne révèle pas les clés privées de l'AC et qui ne peut pas être falsifiée sans la connaissance de ces clés privées ;
- créer des enregistrements d'audit pour chaque modification concernant la sécurité ;
- si une fonction de sauvegarde et de restauration des clés privées de l'AC est offerte, garantir la confidentialité et l'intégrité des données sauvegardées et réclamer au minimum un double contrôle des opérations de sauvegarde et de restauration.

	Niveaux (**) et (***)	
Il est recommandé que le module cryptographique de l'AC détecte les tentatives d'altérations physiques et entre dans un état sûr quand une tentative d'altération est détectée.		

XI.2. Exigences sur la qualification

Les exigences suivantes ne sont applicables que lorsque le PSCE souhaite faire qualifier son offre de certificats électroniques au(x) niveau(x) de sécurité considéré(s) selon les modalités prévues par l'article LP 22 de la [LOIDUPAYS] et déclinées au chapitre 5 du corps de texte du [RGS].

	Niveau (***)	

Le module cryptographique utilisé par l'AC doit être qualifié au niveau renforcé[40], selon le processus décrit dans le [RGS], et être conforme aux exigences[41] du chapitre XI.1 ci-dessus.

	Niveau (**)	
Le module cryptographique utilisé par l'AC doit être qualifié au minimum au niveau standard[42], selon le processus décrit dans le [RGS], et être conforme aux exigences du chapitre XI.1 ci-dessus. Il est toutefois recommandé d'utiliser un module cryptographique qualifié au niveau renforcé.		

	Niveau (*)	
Le module cryptographique utilisé par l'AC doit être qualifié au minimum au niveau élémentaire[43], selon le processus décrit dans le [RGS], et être conforme aux exigences du chapitre XI.1 ci-dessus. Il est toutefois recommandé d'utiliser un module cryptographique qualifié au niveau standard.		

[40] Sous réserve qu'il existe au moins une telle référence sur la liste de référence des produits de sécurité visée à l'article LP 22 de la loi du pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices. Dans le cas contraire, le PSCE souhaitant faire qualifier son offre de certificats de porteur final doit obtenir une dérogation de l'ANSSI.

[41] Une cible de sécurité conforme au profil de protection [CWA14167-4] (ou [CWA14167-2] s'il y a une fonction de sauvegarde des clés privées de l'AC) permet au module cryptographique d'être considéré comme conforme aux exigences de la présente annexe (hors génération des bi-clés des porteurs). Les exigences de génération des bi-clés des porteurs peuvent être remplies lorsque la cible de sécurité respecte le profil de protection [CWA14167-3].

[42] Cf. note de bas de page n° 31.

[43] Cf. note de bas de page n° 31.

XII. Annexe 3 : Exigences de sécurité du dispositif de protection des éléments secrets

XII.1. Exigences sur les objectifs de sécurité

Le dispositif de protection des éléments secrets du porteur, utilisé par le porteur pour stocker et mettre en œuvre sa clé privée et, le cas échéant, générer sa bi-clé, doit répondre aux exigences de sécurité suivantes :

- Si la bi-clé du porteur est générée par le dispositif, garantir que cette génération est réalisée exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique de la bi-clé générée ;
- Détecter les défauts lors des phases d'initialisation, de personnalisation et d'opération et disposer de techniques sûres de destruction des clés privées ;
- Garantir la confidentialité et l'intégrité des clés privées ;
- Assurer la correspondance entre la clé privée et la clé publique ;
- Générer une fonction de sécurité qui ne peut être falsifiée sans la connaissance de la clé privée ;
- Assurer la fonction de sécurité pour le porteur légitime uniquement et protéger la clé privée contre toute utilisation par des tiers ;
- Permettre de garantir l'authenticité et l'intégrité de la clé publique lors de son export hors du dispositif.

[Confidentialité]		
Le dispositif de protection des éléments secrets du porteur doit répondre aux exigences de sécurité supplémentaires suivantes : ➢ Assurer la fonction de déchiffrement, de clés symétriques de fichier ou de message, pour le porteur légitime uniquement et protéger la clé privée contre toute utilisation par des tiers ; ➢ Permettre de garantir l'authenticité et l'intégrité de la clé symétrique de fichier ou de message, une fois déchiffrée, lors de son export hors du dispositif à destination de l'application de déchiffrement des données ; ➢ Le cas échéant, permettre de garantir la confidentialité, l'authenticité et l'intégrité de la clé privée lors de son export hors du dispositif, à destination d'une fonction de séquestre ou d'archivage des clés privées.		

XII.2. Exigences sur la qualification

Les exigences suivantes ne sont applicables que lorsque le PSCE souhaite faire qualifier son offre de certificats électronique au(x) niveau(x) de sécurité considéré(s) selon les modalités prévues par l'article LP 22 de la [LOIDUPAYS] et déclinées au chapitre 5 du corps de texte du [RGS] et que le PSCE fournit au porteur le dispositif de protection des éléments secrets adéquat.

	Niveau (***)	
Le dispositif de protection des éléments secrets utilisé par le porteur doit être qualifié au niveau		

renforcé[44], selon le processus décrit dans le [RGS], et être conforme aux exigences du chapitre XII.1 ci-dessus.

	Niveau (**)	
Le dispositif de protection des éléments secrets utilisé par le porteur doit être qualifié au minimum au niveau standard[45], selon le processus décrit dans le [RGS], et être conforme aux exigences du chapitre XII.1 ci-dessus. Il est toutefois recommandé d'utiliser le dispositif de protection des éléments secrets qualifié au niveau renforcé.		

	Niveau (*)	
Le dispositif de protection des éléments secrets utilisé par le porteur doit être qualifié au minimum au niveau élémentaire[46], selon le processus décrit dans le [RGS], et être conforme aux exigences du chapitre XII.1 ci-dessus. Il est toutefois recommandé d'utiliser dispositif de protection des éléments secrets qualifié au niveau standard.		

[44] Sous réserve qu'il existe au moins une telle référence sur la liste de référence des produits de sécurité visée à l'article LP 22 de la loi du pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices. Dans le cas contraire, le PSCE souhaitant faire qualifier son offre de certificats de porteur final doit obtenir une dérogation de l'ANSSI.

[45] Cf. note de bas de page 35.

[46] Cf. note de bas de page 35.

Annexe A 3

Politique de Certification Type
« Certificats électroniques de services applicatifs »

Historique des versions		
Date	**Version**	**Evolution du document**
xxx	1.0	Publication de la première version de l'annexe A3 du référentiel général de sécurité

Avant-propos

Le présent document fait partie du référentiel général de sécurité (RGS), pris en application de l'article LP 20 de la loi du pays n° 2017-30 du 22 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices, et de son arrêté d'application.

Le présent document et ses annexes sont une copie adaptée du RGS A3 – Politique de Certification Type « services applicatifs », en vigueur en métropole, version 3.0 du 27 février 2014.

Le texte fait des renvois à des documents publiés par l'Agence nationale de la sécurité des systèmes d'information[47] (ANSSI) ou encore disponibles sur son site internet www.ssi.gouv.fr, en ce qu'ils reflètent l'état de l'art en matière de sécurité informatique.

Le référentiel et ses annexes sont disponibles en ligne sur le site internet www.lexpol.pf, et leur mise à jour est assurée par la Direction générale de l'économie numérique.

[47] L'ANSSI est un service à compétence nationale rattaché au Secrétaire général de la défense et de la sécurité nationale, l'autorité chargée d'assister le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale. Parmi ses nombreux objectifs, l'un d'eux consiste à promouvoir un espace de confiance pour les services en ligne. Elle y participe en ce sens notamment au travers de la règlementation (référentiels) et ses labels (certification des produits de sécurité et qualification des produits de sécurité et des prestataires de service de confiance).

I. Introduction

I.1. Présentation générale

I.1.1. Objet du document

Le présent document « Politique de Certification Type, certificats électroniques de services applicatifs « (PC Type Services applicatifs) fait partie du Référentiel Général de Sécurité [RGS]. Il en constitue l'annexe [RGS_A3].

Ce référentiel technique liste les règles que les prestataires de services de certification électronique (PSCE), délivrant des certificats électroniques à des services applicatifs doivent respecter. Les PSCE délivrant des certificats électroniques à des personnes se reporteront à l'annexe [RGS_A2].

Ce document distingue trois niveaux de sécurité aux exigences croissantes : *, ** et ***. Il distingue par ailleurs trois usages de certificats électroniques : cachet, signature de codes et authentification de serveurs. Enfin, les certificats électroniques délivrés dans le cadre de ce document concernent le secteur public ([Administration]) et le secteur privé ([Privé]). En outre, cette politique de certification (PC) Type concerne les certificats pour des serveurs de type serveur SSL/TLS, serveur IPsec ou des serveurs qui lors de l'établissement d'une session sécurisée avec un autre serveur se trouve être en mode client. Les exigences spécifiques à l'un ou à l'autre de ces types de serveurs, lorsqu'elles existent, sont clairement identifiées en faisant précéder le paragraphe concerné respectivement par [SERVEUR-SERVEUR] ou [SERVEUR-CLIENT].

Conformément à la [LOIDUPAYS], il est du ressort de l'autorité administrative (AA) de déterminer le niveau de sécurité ainsi que les fonctions de sécurité qu'elle souhaite mettre en place au sein de son SI. Elle peut, par conséquent, décider de recourir à la fonction de sécurité « Cachet «, « Signature de codes « ou « Authentification serveur « basée sur des mécanismes cryptographiques asymétriques nécessitant l'usage de certificats électroniques. Le cas échéant, une fois le niveau de sécurité déterminé parmi *, ** et ***, l'AA doit recourir à des certificats électroniques délivrés par des PSCE conformes à la présente PC Type au dit niveau.

Un PSCE peut demander la qualification de son offre de services conformément à l'article LP 22 de la [LOIDUPAYS]. Cette qualification permet d'attester de la conformité de l'offre du PSCE aux exigences du présent document, pour un ou plusieurs niveaux de sécurité, un ou plusieurs usages de certificats électroniques et secteurs.

Les exigences, communes à tous les niveaux et particulières à un niveau donné, spécifiées dans la présente PC Type doivent être respectées intégralement par les PSCE moyennant l'exception suivante : dans la présente PC Type, un certain nombre de recommandations sont formulées. Les PSCE sont incités à les respecter également dès maintenant car ces recommandations, qui ne sont pas d'application obligatoire dans la présente version de ce document, devraient le devenir dans une version ultérieure.

Cette PC Type n'est pas une PC à part entière : elle ne peut pas être utilisée telle quelle par un PSCE en tant que PC pour être mentionnée dans ses certificats et sa déclaration des pratiques de certification (DPC). Un PSCE souhaitant être qualifié par rapport à un des niveaux de sécurité de la présente PC Type doit en reprendre, dans sa propre PC, l'ensemble des exigences correspondant au niveau visé. La structure de la PC du PSCE devant être conforme au [RFC3647] (préférentiellement au [RFC2527]), la structure de la présente PC Type est également conforme au [RFC3647] pour en faciliter l'incorporation dans la PC du PSCE.

Afin de favoriser l'interopérabilité, dans le cadre de la sécurisation des échanges électroniques entre AA et usagers et entre AA, des règles et recommandations sur les formats de certificats et de listes de révocations, compatibles avec la norme [X.509] sont formulées dans le document [RGS_A4].

I.1.2. Conventions de rédaction

De manière à mettre en exergue les règles spécifiques à un niveau de sécurité, à un type d'usage ou à un secteur, celles-ci seront présentées dans un encadré, le titre du cadre précisant son périmètre d'application (niveau de sécurité, usage du certificat électronique, secteur). La forme est la suivante :

[Usage]	**[Niveau de sécurité]**	**[Secteur]**
Intitulé de la règle …		

Les exigences qui ne sont pas encadrées s'appliquent de manière identique aux trois niveaux. En respectant la forme suivante.

1.2. Identification du document

La présente PC Type est dénommée «RGS - Politique de Certification Type – certificats électroniques de services applicatifs». Elle peut être identifiée par son nom, numéro de version et sa date de mise à jour.

1.3. Définitions et acronymes

I.3.1. Acronymes

Les acronymes utilisés dans la présente PC Type sont les suivants :

AA	Autorité Administrative
AC	Autorité de Certification
AE	Autorité d'Enregistrement
AED	Autorité d'Enregistrement Déléguée
AH	Autorité d'Horodatage
ANSSI	Agence nationale de la sécurité des systèmes d'information
CEN	Comité Européen de Normalisation
DGME	Direction Générale de la Modernisation de l'État
DN	Distinguished Name
DNS	Domain Name System
DPC	Déclaration des Pratiques de Certification
ETSI	European Telecommunications Standards Institute
FQDN	Fully Qualified Domain Name
IGC	Infrastructure de Gestion de Clés
LAR	Liste des certificats d'AC Révoqués
LCR	Liste des Certificats Révoqués
MC	Mandataire de Certification
OC	Opérateur de Certification
OCSP	Online Certificate Status Protocol

OID	Object Identifier
PC	Politique de Certification
PP	Profil de Protection
PSCE	Prestataire de Services de Certification Électronique
RC	Responsable du Certificat de service applicatif
RSA	Rivest Shamir Adelman
SP	Service de Publication
SSI	Sécurité des Systèmes d'Information
SSL	Secure Sockets Layer
TLS	Transport Layer Security
URL	Uniform Resource Locator

I.3.2. Définitions

Les termes utilisés dans la présente PC Type sont les suivants :

Agent - Personne physique agissant pour le compte d'une autorité administrative.

Applications utilisatrices - Services applicatifs exploitant les certificats émis par l'Autorité de Certification pour des besoins d'authentification, de chiffrement ou de signature du porteur du certificat ou des besoin d'authentification ou de cachet du service applicatif auquel le certificat est rattaché.

Autorités administratives - Ce terme générique, défini à l'article LP 1 de la [LOIDUPAYS], désigne la Polynésie française, ses établissements publics, les autorités administratives indépendantes, les organismes de protection sociale et les autres organismes et personnes de droit public et de droit privé chargés d'une mission de service public administratif ;

Autorité d'horodatage - Autorité responsable de la gestion d'un service d'horodatage (cf. politique d'horodatage type du [RGS]).

Autorité de certification (AC) - Au sein d'un PSCE, une Autorité de Certification a en charge, au nom et sous la responsabilité de ce PSCE, l'application d'au moins une politique de certification et est identifiée comme telle, en tant qu'émetteur (champ «issuer» du certificat), dans les certificats émis au titre de cette politique de certification. Dans le cadre de la présente PC Type, le terme de PSCE n'est pas utilisé en dehors du présent chapitre et du chapitre I.1 et le terme d'AC est le seul utilisé. Il désigne l'AC chargée de l'application de la politique de certification, répondant aux exigences de la présente PC Type, au sein du PSCE souhaitant faire qualifier la famille de certificats correspondante.

Cachet serveur - Signature numérique effectuée par un serveur applicatif sur des données dans le but de pouvoir être utilisée soit dans le cadre d'un service d'authentification de l'origine des données, soit dans le cadre d'un service de non répudiation dans le cadre d'échanges dématérialisés entre usagers et AA ou entre AA.

Certificat électronique - Document sous forme électronique attestant du lien entre une clé publique et l'identité de son propriétaire (personne physique ou service applicatif). Cette attestation prend la forme d'une signature électronique réalisée par un prestataire de service de certification électronique (PSCE). Il est délivré par une Autorité de Certification. Le certificat est valide pendant une durée donnée précisée dans celui-ci. Les usages des certificats électroniques régis par le présent document sont le cachet électronique et l'authentification de serveur.

Composante - Plate-forme opérée par une entité et constituée d'au moins un poste informatique, une application et, le cas échéant, un moyen de cryptologie et jouant un rôle déterminé dans la mise en œuvre opérationnelle d'au moins une fonction de l'IGC. L'entité peut être le PSCE lui-même ou une entité externe liée au PSCE par voie contractuelle, réglementaire ou hiérarchique.

Déclaration des pratiques de certification (DPC) - Une DPC identifie les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que l'AC applique dans le cadre de la fourniture de ses services de certification électronique aux usagers et en conformité avec la ou les politiques de certification qu'elle s'est engagée à respecter.

Dispositif de protection des éléments secret - Un dispositif de protection des éléments secrets désigne un dispositif de stockage des éléments secrets remis au RC (exemples : clé privée, code PIN, etc). Il peut prendre la forme d'une carte à puce, d'une clé USB à capacités cryptographique ou se présenter au format logiciel (exemple fichier PKCS#12).

Entité - Désigne une autorité administrative ou une entreprise au sens le plus large, c'est-à-dire également les personnes morales de droit privé de type associations.

FQDN (Fully qualified domain name) : nom de domaine pleinement qualifié indiquant la position absolue d'un nœud dans l'arborescence DNS et précisant les domaines de niveau supérieur jusqu'à la racine. Ex. : ssi.gouv.fr.

Infrastructure de gestion de clés (IGC) - Ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs certificats utilisés par des services de confiance. Une IGC peut être composée d'une autorité de certification, d'un opérateur de certification, d'une autorité d'enregistrement centralisée et/ou locale, de mandataires de certification, d'une entité d'archivage, d'une entité de publication, etc.

Politique de certification (PC) - Ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une AC se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes. Une PC peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les RC et les utilisateurs de certificats.

Porteur de certificat - Personne physique identifiée dans le certificat et qui est la détentrice de la clé privée correspondant à la clé publique.

Prestataire de services de certification électronique (PSCE) - Un PSCE est un type de prestataire de services de confiance (PSCO) particulier. Un PSCE se définit comme toute personne ou entité qui est responsable de la gestion de certificats électroniques tout au long de leur cycle de vie, vis-à-vis des porteurs et utilisateurs de ces certificats. Un PSCE peut fournir différentes familles de certificats correspondant à des finalités différentes et/ou des niveaux de sécurité différents. Un PSCE comporte au moins une AC mais peut en comporter plusieurs en fonction de son organisation. Les différentes AC d'un PSCE peuvent être indépendantes les unes des autres et/ou liées par des liens hiérarchiques ou autres (AC Racines / AC Filles). Un PSCE est identifié dans un certificat dont il a la responsabilité au travers de son AC ayant émis ce certificat et qui est elle-même directement identifiée dans le champ «émetteur» du certificat.

Produit de sécurité - Un dispositif matériel ou logiciel, ou les composants correspondants du dispositif matériel ou logiciel, qui sont destinés à être utilisés pour la fourniture de services de confiance et nécessaires à la sécurisation d'une information ou d'un système.

Promoteur d'application - Un responsable d'un service de la sphère publique accessible par voie électronique.

Qualification d'un prestataire de services de certification électronique - La qualification d'un PSCE

permet d'attester de la conformité de l'offre de certification électronique d'un PSCE à un niveau de sécurité du [RGS]. Conformément à l'article LP 22 de la [LOIDUPAYS], cette qualification correspond à la qualification délivrée par les autorités de métropole en application de l'[ORDONNANCE].

Qualification d'un produit de sécurité - La qualification d'un produit de sécurité permet d'attester de la conformité d'un produit à un niveau de sécurité du [RGS]. Conformément à l'article LP 22 de la [LOIDUPAYS], cette qualification correspond à la qualification délivrée par les autorités de métropole en application de l'[ORDONNANCE].

Responsable du certificat – Personne en charge et responsable du certificat électronique de service applicatif de cachet ou d'authentification du serveur.

Système d'information – Tout ensemble de moyens destinés à élaborer, traiter, stocker ou transmettre des informations faisant l'objet d'échanges par voie électronique entre autorités administratives et usagers ainsi qu'entre autorités administratives.

Usager - Toute personne physique ou toute personne morale de droit privé, à l'exception de celles qui sont chargées d'une mission de service public lorsqu'est en cause l'exercice de cette mission. Selon le contexte, un usager peut être un porteur ou un utilisateur de certificats.

Utilisateur de certificat - Entité ou personne physique qui utilise un certificat et qui s'y fie pour vérifier une signature électronique ou une valeur d'authentification provenant d'un porteur de certificat ou chiffrer des données à destination d'un porteur de certificat.

I.4. Entités intervenant dans l'IGC

I.4.1. Autorités de certification

La notion d'Autorité de Certification (AC) telle qu'utilisée dans la présente PC Type est définie au chapitre I.6.2 ci-dessous.

L'AC a en charge la fourniture des prestations de gestion des certificats tout au long de leur cycle de vie (génération, diffusion, renouvellement, révocation...) et s'appuie pour cela sur une infrastructure technique : une infrastructure de gestion de clés (IGC).

Les prestations de l'AC sont le résultat de différentes fonctions qui correspondent aux différentes étapes du cycle de vie des bi-clés et des certificats.

Afin de clarifier et faciliter l'identification des exigences, et en cohérence avec les documents de l'ETSI dans le domaine (cf. [ETSI_NQCP]), la décomposition fonctionnelle d'une IGC qui est retenue dans la présente PC Type est la suivante[48] :

- **Autorité d'enregistrement (AE) [49] -** Cette fonction vérifie et valide les informations d'identification du futur responsable du certificat (RC) et du service applicatif auquel le certificat

[48] Cette décomposition est donnée à titre d'illustration pour les besoins de la présente PC Type et n'impose aucune restriction sur la décomposition d'une implémentation effective d'une IGC.

[49] Les documents de l'ETSI, notamment [ETSI_NQCP], utilisent le terme Service d'Enregistrement. Le [RFC3647] utilise le terme Autorité d'Enregistrement. En cohérence avec ce dernier document, il est conservé l'utilisation du terme Autorité d'Enregistrement, mais qui doit être compris, dans la présente PC Type, en tant que fonction et non pas en tant que composante technique de l'IGC.

doit être rattaché, ainsi qu'éventuellement d'autres attributs spécifiques, avant de transmettre la demande correspondante à la fonction adéquate de l'IGC, en fonction des services rendus et de l'organisation de l'IGC. L'AE a également en charge, lorsque cela est nécessaire, la revérification des informations du RC ou du service applicatif lors du renouvellement du certificat.

- **Fonction de génération des certificats** - Cette fonction génère (création du format, signature électronique avec la clé privée de l'AC) les certificats à partir des informations transmises par l'autorité d'enregistrement et de la clé publique du service provenant soit du RC, soit de la fonction de génération des éléments secrets du service, si c'est cette dernière qui génère la bi-clé du service applicatif.
- **Fonction de génération des éléments secrets du service applicatif** - Cette fonction génère les éléments secrets du service à destination du RC, si l'AC a en charge une telle génération, et les prépare en vue de leur remise au RC (par exemple, personnalisation d'une carte à puce ou d'une carte cryptographique destinée au service applicatif, courrier sécurisé avec le code d'activation, etc.). De tels éléments secrets peuvent être, par exemple, directement la bi-clé du service applicatif, les codes (activation / déblocage) liés au dispositif de protection des éléments secrets ou encore des codes ou clés temporaires permettant au RC de mener à distance le processus de génération / récupération du certificat électronique de service applicatif.
- **Fonction de remise au RC** - Cette fonction remet au RC au minimum le certificat du service applicatif ainsi que, le cas échéant, les autres éléments fournis par l'AC (dispositif de protection des éléments secrets, clé privée du service applicatif, codes d'activation…).
- **Fonction de publication** - Cette fonction met à disposition des différentes parties concernées, les conditions générales, politiques et pratiques publiées par l'AC, les certificats d'AC et toute autre information pertinente destinée aux RC ou aux utilisateurs de certificats, hors informations d'état des certificats. Elle peut également mettre à disposition, en fonction de la politique de l'AC, les certificats valides des services applicatifs.
- **Fonction de gestion des révocations** - Cette fonction traite les demandes de révocation (notamment identification et authentification du demandeur) et détermine les actions à mener. Les résultats des traitements sont diffusés via la fonction d'information sur l'état des certificats.
- **Fonction d'information sur l'état des certificats** - Cette fonction fournit aux utilisateurs de certificats des informations sur l'état des certificats (révoqués, suspendus, etc.). Cette fonction peut être mise en œuvre selon un mode de publication d'informations mises à jour à intervalles réguliers (LCR, LAR) ou selon un mode requête / réponse temps réel (OCSP).

Les fonctions ci-dessus sont les fonctions minimales que doit obligatoirement mettre en œuvre une IGC gérant des certificats de service applicatif, à l'exception de la fonction de génération des éléments secrets du service applicatif qui est optionnelle et qui dépend des prestations effectivement offertes par l'AC.

Un certain nombre d'entités / personnes physiques externes à l'IGC interagissent avec cette dernière. Il s'agit notamment :

- **Responsable du certificat (RC)** - La personne physique responsable du certificat électronique de service applicatif (cachet ou authentification serveur), notamment de l'utilisation de ce certificat et de la bi-clé correspondante, pour le compte de l'entité dont dépend le service applicatif identifié dans le certificat.
- **Mandataire de certification (MC)** - Le mandataire de certification est désigné par et placé sous la responsabilité de l'entité cliente. Il est en relation directe avec l'AE. Il assure pour elle un certain nombre de vérifications concernant l'identité et, éventuellement, les attributs des RC et

des services applicatifs de cette entité (il assure notamment le face-à-face pour l'identification des RC lorsque celui-ci est requis).

- **Utilisateur de certificat** - L'entité ou la personne physique qui reçoit un certificat et qui s'y fie pour vérifier une valeur de cachet ou d'authentification serveur provenant du service applicatif auquel le certificat est rattaché, ou pour établir une clé de session.
- **Personne autorisée** - Il s'agit d'une personne autre que le RC et le mandataire de certification et qui est autorisée par la politique de certification de l'AC ou par contrat avec l'AC à mener certaines actions pour le compte du RC (demande de révocation, de renouvellement, …). Typiquement, dans une entreprise ou une administration, il peut s'agir d'un responsable hiérarchique du RC ou d'un responsable des ressources humaines.

L'organisation et l'ordonnancement des différentes fonctions de l'IGC les unes par rapport aux autres dépendent du modèle adopté par l'AC. La présente PC Type n'impose aucun modèle particulier, dans la limite où l'AC respecte les exigences qui y sont définies.

Cependant, les parties de l'AC concernées par la génération de certificat et la gestion des révocations doivent être indépendantes d'autres organisations en ce qui concerne leurs décisions concernant la mise en place, la fourniture, le maintien et la suspension des services ; en particulier, leurs cadres dirigeants, leur personnel d'encadrement et leur personnel ayant des rôles de confiance, doivent être libres de toute pression d'ordre commercial, financier ou autre, qui pourraient influer négativement sur la confiance dans les services fournis par l'AC. Les parties de l'AC concernées par la génération de certificat et de la gestion des révocations doivent avoir une structure documentée qui préserve l'impartialité des opérations.

L'organisation adoptée dépend notamment des prestations fournies par l'AC : génération ou non de la bi-clé du service applicatif, fourniture ou non du dispositif de protection des éléments secrets et, si oui, fourniture avant ou après génération de la bi-clé du service applicatif, etc.

L'AC doit préciser dans sa PC les prestations effectivement fournies et son organisation fonctionnelle correspondante.

Dans la pratique, la mise en œuvre opérationnelle de ces fonctions peut être effectuée par une ou plusieurs composante(s) de l'IGC (opérateurs techniques et/ou autorités tel que OC, AE, SP, AH, …), qui peuvent être internes à l'AC et/ou opérées par des entités externes.

La Déclaration des Pratiques de Certification (DPC) de l'AC doit décrire l'organisation opérationnelle de son IGC et la répartition des rôles entre les différentes composantes en fonction de l'organisation fonctionnelle et de la définition des rôles décrites dans sa PC.

Quelle que soit l'organisation opérationnelle mise en œuvre, l'AC reste in fine responsable vis-à-vis de toute partie externe à l'IGC (utilisateurs, autorités publiques, etc.) des prestations fournies et doit garantir le respect des engagements pris dans sa PC et sa DPC, relatifs à son activité de certification. Le cadre contractuel entre l'AC et ses différentes composantes opérées par des entités externes doit être clairement documenté. En particulier, les politiques et les procédures, en fonction desquelles l'AC fonctionne, doivent être non-discriminatoires. Le cadre contractuel entre l'AC et ses différentes composantes opérées par des entités externes doit être clairement documenté.

Une AC qualifiée pour son offre de certificats électroniques de service applicatif (niveau de sécurité, types d'usage et de porteur) conformément à l'article LP 22 de la [LOIDUPAYS] respecte les exigences décrites dans la présente PC Type et s'engage à ce que les composantes de l'IGC, internes et externes à l'AC, respectent aussi les exigences qui les concernent.

Dans le cadre de ses fonctions opérationnelles, qu'elle assume directement ou qu'elle sous-traite à des entités externes, les exigences qui incombent à l'AC en tant que responsable de l'ensemble de l'IGC sont les

suivantes :

- Être une entité légale au sens de la règlementation.
- Être en relation par voie contractuelle / hiérarchique / réglementaire avec l'entité pour laquelle elle a en charge la gestion des certificats de services applicatifs de cette entité. L'AC peut aussi, le cas échéant, être en relation contractuelle / hiérarchique / réglementaire avec le ou les mandataires de certification choisis par l'entité.
- Rendre accessible l'ensemble des prestations déclarées dans sa PC aux promoteurs d'application d'échanges dématérialisés de l'administration, aux RC, aux utilisateurs de certificats, ceux qui mettent en œuvre ses certificats.
- S'assurer que les exigences de la PC et les procédures de la DPC sont appliquées par chacune des composantes de l'IGC et sont adéquates et conformes aux normes en vigueur.
- Mettre en œuvre les différentes fonctions identifiées dans sa PC, correspondant au minimum aux fonctions obligatoires de la présente PC Type, notamment en matière de génération des certificats, de remise au RC, de gestion des révocations et d'information sur l'état des certificats.
- Élaborer, mettre en œuvre, contrôler et maintenir de façon itérative les mesures de sécurité et les procédures opérationnelles, concernant ses installations, ses systèmes et ses biens informationnels.

	Niveau (***)	
➢ > L'AC doit mener une analyse de risque permettant de déterminer les objectifs de sécurité propres à couvrir les risques métiers de l'ensemble de l'IGC et les mesures de sécurité techniques et non techniques correspondantes à mettre en œuvre. Elle élabore sa DPC en fonction de cette analyse.		

	Niveaux (*) et (**)	
➢ > Il est recommandé que l'AC mène une analyse de risque.		

- Mettre en œuvre tout ce qui est nécessaire pour respecter les engagements définis dans sa PC, et correspondant au minimum aux exigences de la présente PC Type, notamment en termes de fiabilité, de qualité et de sécurité. À ce titre, elle doit posséder un ou des systèmes de gestion de la qualité et de la sécurité de l'information adaptés aux services de certification qu'elle assure.
- Générer, et renouveler lorsque nécessaire, ses bi-clés et les certificats correspondants (signature de certificats, de LCR et de réponses OCSP), ou faire renouveler ses certificats si l'AC est rattachée à une AC hiérarchiquement supérieure. Diffuser ses certificats d'AC aux RC et utilisateurs de certificats.
- Suivre les demandes en capacité et réaliser des projections concernant les futurs besoins en capacité afin de garantir la disponibilité du service, notamment en matière de capacités de traitement et de stockage.

I.4.2. Autorité d'enregistrement

L'AE a pour rôle de vérifier l'identité du futur RC et les informations liées au service applicatif, tel que défini au chapitre I.6.2 de la présente PC Type. Pour cela, l'AE assure les tâches suivantes :

- La prise en compte et la vérification des informations du futur RC et du service applicatif, ainsi que de leur entité de rattachement et la constitution du dossier d'enregistrement correspondant ;

- Le cas échéant, la prise en compte et la vérification des informations du futur MC (cf. dernier paragraphe du I.4.2) et de son entité de rattachement et la constitution du dossier d'enregistrement correspondant ;
- L'établissement et la transmission de la demande de certificat à la fonction adéquate de l'IGC suivant l'organisation de cette dernière et les prestations offertes ;
- L'archivage des pièces du dossier d'enregistrement (ou l'envoi vers la composante chargée de l'archivage) ;
- La conservation et la protection en confidentialité et en intégrité des données personnelles d'authentification du RC ou, le cas échéant, du MC, y compris lors des échanges de ces données avec les autres fonctions de l'IGC (notamment, elle respecte la législation relative à la protection des données personnelles).

L'AE peut s'appuyer sur un MC désigné et placé sous la responsabilité de l'entité cliente pour effectuer tout ou partie des opérations de vérification des informations (cf. chapitre I.4.5.2 ci-dessous). Dans ce cas, l'AE doit s'assurer que les demandes sont complètes et exactes et effectuées par un MC dûment autorisé.

Dans tous les cas, l'archivage des pièces du dossier d'enregistrement (sous forme électronique et/ou papier) est de la responsabilité de l'AE (cf. chapitre V.5).

L'AE, en tant que de besoin, peut déléguer tout ou partie de ses fonctions à des unités de proximité désignées sous le nom d'autorités d'enregistrement déléguées (AED).

I.4.3. Responsables de certificats électroniques de services applicatifs

Dans le cadre de la présente PC Type, un RC est une personne physique qui est responsable de l'utilisation du certificat électronique identifié dans le certificat et de la clé privée correspondant à ce certificat, pour le compte de l'entité également identifiée dans ce certificat. Le RC a un lien contractuel /hiérarchique / réglementaire avec cette entité.

Le RC respecte les conditions qui lui incombent définies dans la PC de l'AC, qui doit reprendre les conditions définies dans la présente PC Type.

Il est à noter que le certificat étant attaché au service applicatif et non au RC, ce dernier peut être amené à changer en cours de validité du certificat : départ du RC de l'entité, changement d'affectation et de responsabilités au sein de l'entité, etc.

L'entité doit signaler à l'AC préalablement, sauf cas exceptionnel et dans ce cas sans délai, le départ d'un RC de ses fonctions et lui désigner un successeur. Une AC doit révoquer un certificat électronique pour lequel il n'y a plus de RC explicitement identifié.

1.4.4. Utilisateurs de certificats

[Cachet]		
Un utilisateur (ou accepteur) de certificats électroniques de cachet peut être notamment : - Un usager destinataire de données signées par un service applicatif de cachet et qui utilise le certificat électronique du cachet ainsi qu'un module de vérification de cachet afin d'authentifier l'origine de ces données transmises. - Un service applicatif destinataire de données provenant d'un autre service applicatif et qui utilise le certificat électronique de cachet et un module de vérification de cachet afin d'authentifier l'origine de ces données transmises.		

➢ Un service applicatif qui signe des données électroniques.

[Authentification serveur]		
Un utilisateur (ou accepteur) de certificats électroniques d'authentification serveur peut être notamment : ➢ Une personne accédant à un serveur et qui utilise le certificat du serveur et un module de vérification d'authentification afin d'authentifier le serveur auquel il accède, qui est identifié dans le certificat du serveur, afin d'établir une clé de session partagée entre son poste et le serveur. ➢ Un service applicatif accédant à un serveur informatique et qui utilise un certificat et un applicatif de vérification d'authentification afin d'authentifier le serveur auquel il accède, qui est identifié dans le certificat, et afin d'établir une clé de session partagée entre les deux serveurs.		

I.4.5. Autres participants

I.4.5.1. Composantes de l'IGC

La décomposition en fonctions de l'IGC est présentée au chapitre I.4.1 ci-dessus. Les composantes de l'IGC mettant en œuvre ces fonctions devront être présentées dans la DPC de l'AC.

I.4.5.2. Mandataire de certification

Le recours à un mandataire de certification (MC) n'est pas obligatoire pour une entité. Une même entité peut s'appuyer sur un ou plusieurs MC.

Dans le cas où elle y a recours, le MC doit être formellement désigné par un représentant légal de l'entité concernée. Le MC est en relation directe avec l'AE de l'IGC.

Les engagements du MC à l'égard de l'AC doivent être précisés dans un contrat écrit avec l'entité responsable du MC. Ce contrat stipule notamment que le MC doit :

- effectuer correctement et de façon indépendante les contrôles d'identité et des éventuels attributs des futurs RC et services applicatifs de l'entité pour laquelle il est MC ;
- respecter les parties de la PC et de la DPC de l'AC qui lui incombent.

L'entité doit signaler à l'AC, si possible préalablement mais au moins sans délai, le départ du MC de ses fonctions et, éventuellement, lui désigner un successeur.

Le MC ne doit en aucun cas avoir accès aux moyens qui lui permettraient d'activer et d'utiliser la clé privée associée à la clé publique contenue dans le certificat électronique délivré au RC.

I.5. Usage des certificats

I.5.1. Domaines d'utilisation applicables

I.5.1.1. Bi-clés et certificats du service applicatif

Usages :

[Cachet]		
Lorsque le certificat électronique délivré par le PSCE est un certificat de cachet, les usages sont la signature électronique de données et la vérification de signature électronique. Ces données peuvent être, par exemple, un accusé de réception suite à la transmission d'informations par un usager à un service applicatif, une réponse automatique à une demande formulée par un usager, un jeton d'horodatage, un		

code applicatif, un certificat de répondeur OCSP, ou encore une archive.

[Authentification Serveur]		
Lorsque le certificat électronique délivré par le PSCE est un certificat d'authentification de serveur, les usages sont l'authentification du serveur auprès d'autres serveurs ou auprès de personnes, dans le cadre de l'établissement de sessions sécurisées, de type SSL / TLS ou IPsec visant à établir une clé symétrique de session afin que les échanges au sein de ces sessions soient chiffrés. L'établissement de la clé de session peut se faire par un mécanisme cryptographique asymétrique, de type RSA (génération de la clé symétrique par le client et chiffrement de cette clé symétrique par la clé publique du serveur) ou de type Diffie-Hellman (obtention de la clé symétrique via un algorithme combinant la clé privée du client et la clé publique du serveur, et inversement).		

Niveaux de sécurité

	Niveau (***)	
Les certificats électronique objets de la présente PC Type sont utilisés par des applications pour lesquelles les besoins de sécurité sont très forts eu égard aux risques très élevés qui les menacent.		

	Niveau (**)	
Les certificats électronique objets de la présente PC Type sont utilisés par des applications pour lesquelles les besoins de sécurité sont forts eu égard aux risques élevés qui les menacent.		

	Niveau (*)	
Les certificats électronique objets de la présente PC Type sont utilisés par des applications pour lesquelles les besoins de sécurité sont moyens eu égard aux risques qui les menacent.		

I.5.1.2. Bi-clés et certificats d'AC et de composantes

Cette PC Type comporte également des exigences, lorsque nécessaire, concernant les bi-clés et certificats de l'AC (signature des certificats de services applicatifs, des LCR / LAR ou des réponses OCSP) ainsi que des clés, bi-clés et certificats des composantes de l'IGC (sécurisation des échanges entre composantes, authentification des opérateurs, etc.).

L'AC génère et signe différents types d'objets : certificats, LCR / LAR ou des réponses OCSP. Pour signer ces objets, l'AC dispose d'au moins une bi-clé, mais il est recommandé qu'elle mette en œuvre des bi-clés séparées pour ces différents types.

Les certificats des clés publiques de ces bi-clés peuvent être générés par différentes AC. Les cas les plus courants sont les suivants :

1) L'AC dispose d'une seule bi-clé et le certificat correspondant est rattaché à une AC de niveau supérieur (hiérarchie d'AC).
2) L'AC dispose d'une seule bi-clé et le certificat correspondant est un certificat racine (certificat autosigné non rattaché à une AC de niveau supérieur).
3) L'AC dispose de bi-clés séparées, le certificat correspondant à la bi-clé de signature de certificats est un certificat racine (certificat autosigné non rattaché à une AC de niveau supérieur) et les certificats des autres bi-clés sont signés par cette bi-clé de signature de certificats de l'AC.
4) L'AC dispose de bi-clés séparées, le certificat correspondant à la bi-clé de signature de certificats

est rattaché à une AC de niveau supérieur (hiérarchie d'AC) et les certificats correspondant aux autres bi-clés sont signés par cette bi-clé de signature de certificats de l'AC.

5) L'AC dispose de bi-clés séparées, les certificats correspondant à ces bi-clés sont rattachés à une AC de niveau supérieur (hiérarchie d'AC).

La présente PC Type recommande la mise en œuvre de ce dernier cas, qui permet notamment à l'AC de niveau supérieur de générer et diffuser de manière plus simple des LAR en cas de révocations des certificats d'AC de niveau inférieur.

Quelle que soit l'approche retenue par l'AC (bi-clés séparées ou non), les bi-clés et certificats de l'AC pour la signature de certificats, de LCR / LAR ou de réponses OCSP ne doivent être utilisés qu'à cette fin. Ils ne doivent notamment être utilisés ni à des fins de confidentialité, ni à des fins d'authentification.

Conformément au [CWA14167-1], les différentes clés internes à l'IGC peuvent être décomposées suivant les catégories suivantes :

- la (ou les) clé(s) de signature d'AC, utilisée(s) pour signer les certificats générés par l'AC ainsi que les informations sur l'état des certificats (LCR / LAR ou réponses OCSP) ;
- les clés d'infrastructure, utilisées par les systèmes intervenant dans l'IGC à des fins d'authentification, de signature des journaux d'évènements, de chiffrement des données échangées ou stockées au sein de l'IGC, etc. ;
- les clés de contrôle, assignées au personnel de l'IGC afin de s'authentifier vis-à-vis des différents systèmes, de signer et/ou de chiffrer des messages ou des données échangés, etc.

Les deux derniers types de clés peuvent être des clés asymétriques et/ou symétriques.

Ces différents types de clés, et éventuellement les certificats correspondants, doivent être couverts par leurs propres engagements, complets et à part entière. Ces engagements doivent faire partie directement de la propre PC de l'AC, couvrant les certificats de services applicatifs (cf. chapitre I.1), ou bien faire l'objet de PC séparées (par exemple, PC d'une AC Racine couvrant les certificats d'AC).

La PC de l'AC répondant à la présente PC Type doit au minimum reprendre les exigences de cette dernière sur les certificats d'AC et de composantes. En cas de traitement de ces certificats dans des PC séparées, ces PC doivent être cohérentes avec les exigences de la PC de l'AC et de la présente PC Type.

I.5.2. Domaines d'utilisation interdits

Les restrictions d'utilisation des bi-clés et des certificats sont définies au chapitre IV.5 ci-dessous, en fonction du niveau de sécurité. L'AC doit respecter ces restrictions et imposer leur respect par les RC auxquels elle délivre des certificats de service applicatif et les utilisateurs de ces certificats.

À cette fin, elle doit communiquer à tous les RC, MC et utilisateurs potentiels les termes et conditions relatives à l'utilisation du certificat.

I.6. Gestion de la PC

I.6.1. Entité gérant la PC

La direction de l'AC est responsable de la validation et de la gestion de la PC répondant aux exigences de la présente PC Type.

I.6.2. Point de contact

À préciser dans la PC de l'AC.

I.6.3. Entité déterminant la conformité d'une DPC avec cette PC

L'AC doit être pourvue d'une direction ayant autorité et une responsabilité finale pour déterminer la conformité de la DPC avec la PC.

I.6.4. Procédures d'approbation de la conformité de la DPC

L'AC doit mettre en place un processus d'approbation de la conformité de la DPC avec la PC.

L'AC est responsable de la gestion (mise à jour, révisions) de la DPC. Toute demande de mise à jour de la DPC doit suivre le processus d'approbation mis en place. Toute nouvelle version de la DPC doit être publiée, conformément aux exigences du paragraphe II.2 sans délai.

II. Responsabilités concernant la mise à disposition des informations devant être publiées

II.1. Entités chargées de la mise à disposition des informations

Pour la mise à disposition des informations devant être publiées à destination des RC et des utilisateurs de certificats, l'AC doit mettre en œuvre au sein de son IGC une fonction de publication et une fonction d'information sur l'état des certificats (cf. chapitre I.4.1 ci-dessus).

La PC de l'AC doit préciser les méthodes de mise à disposition et les URL correspondantes (annuaire accessible en protocole LDAP et/ou HTTP, serveur Web, serveur OCSP, etc.).

II.2. Informations devant être publiées

L'AC a pour obligation de publier au minimum les informations suivantes à destination des RC et utilisateurs de certificats :

- sa politique de certification, couvrant l'ensemble des rubriques du [RFC3647] et conforme à la présente PC Type ;
- l'état des certificats émis par l'AC, selon le ou les moyens indiqués dans sa PC ;
- les certificats de l'AC en cours de validité ;
- si l'AC est rattachée à une hiérarchie d'AC, les certificats en cours de validité des AC de cette hiérarchie et les différentes politiques de certification correspondantes, ceci jusqu'à l'AC Racine ;
- pour les certificats d'AC autosignés (AC Racine), les informations permettant aux utilisateurs de certificats de s'assurer de l'origine de ces certificats (cf. chapitre VI.1.4) et de leur état (cf. chapitre IV.10).

L'AC peut publier sa déclaration des pratiques de certification (DPC) ainsi que toute autre documentation pertinente pour rendre possible l'évaluation de la conformité avec sa politique de certification. Cependant, elle n'est en général pas tenue de rendre publics tous les détails relatifs à ses pratiques. Ces informations devront néanmoins être communiquées aux auditeurs et aux personnes appliquant ces pratiques.

L'AC a également pour obligation de publier, à destination des RC, les différents formulaires nécessaires pour la gestion des certificats (demande d'enregistrement, demande de révocation, demande de renouvellement, etc.).

De plus, compte tenu de la complexité de lecture d'une PC pour des personnes non spécialistes du domaine, il est recommandé que l'AC publie également des conditions générales d'utilisation correspondant aux «PKI Disclosure Statement» (PDS) définis par [ETSI_NQCP] et [RFC3647]. Il est recommandé que ces conditions générales aient une structure conforme à celle décrite en annexe B de [ETSI_NQCP] et reprennent ainsi, à destination des RC et des utilisateurs de certificats, les informations pertinentes de la PC de l'AC :

- L'identifiant (OID) de la PC applicable, la mention du type de population à laquelle les certificats peuvent être délivrés, les exigences de la PC en matière de protection de la bi-clé et des supports de certificats ;
- Les conditions d'usages des certificats et leurs limites ;
- Les obligations et responsabilités des différentes parties, notamment les exigences relatives à la vérification du statut de révocation d'un certificat pour les utilisateurs ;
- Les informations expliquant comment vérifier un certificat ;
- Les garanties et limites de garanties de l'AC ;

- La durée de conservation des dossiers d'enregistrement et des journaux d'évènements ;
- Les procédures pour la résolution des réclamations et des litiges ;
- Le système légal applicable ;
- Si l'AC a été déclarée conforme à la politique identifiée et dans ce cas au travers de quel schéma.

Ces conditions générales font notamment partie intégrante du dossier d'enregistrement.

Le moyen utilisé pour la publication de ces informations est libre mais doit être précisé dans la PC de l'AC. Il doit garantir l'intégrité, la lisibilité et la clarté des informations publiées.

L'AC doit employer la langue française pour la rédaction de ces documents, et pourra les traduire en autant de langues que nécessaire pour la bonne compréhension des porteurs des certificats.

II.3. Délais et fréquences de publication

Les informations liées à l'IGC (nouvelle version de la PC, formulaires, etc.) doivent être publiées dès que nécessaire afin que soit assurée à tout moment la cohérence entre les informations publiées et les engagements, moyens et procédures effectifs de l'AC.

En particulier, toute nouvelle version doit être communiquée au RC ou MC lors d'une demande de renouvellement de clé et doit faire l'objet d'un nouvel accord. Les systèmes publiant ces informations doivent au moins être disponibles les jours ouvrés.

Les certificats d'AC doivent être diffusés préalablement à toute diffusion de certificats de services applicatifs et/ou de LCR correspondants et les systèmes les publiant doivent avoir une disponibilité 24h/24 et 7j/7.

Les délais et fréquences de publication des informations d'état des certificats ainsi que les exigences de disponibilité des systèmes les publiant sont décrites aux chapitres IV.9 et IV.10.

Il est à noter qu'une perte d'intégrité d'une information mise à disposition (présence de l'information et intégrité de son contenu) est considérée comme une indisponibilité de cette information.

II.4. Contrôle d'accès aux informations publiées

L'ensemble des informations publiées à destination des utilisateurs de certificats doit être libre d'accès en lecture.

	Niveau (***)	
L'accès en modification aux systèmes de publication (ajout, suppression, modification des informations publiées) doit être strictement limité aux fonctions internes habilitées de l'IGC, au travers d'un contrôle d'accès fort (basé sur une authentification au moins à deux facteurs).		

	Niveau (**)	
L'accès en modification aux systèmes de publication des informations d'état des certificats (ajout, suppression, modification des informations publiées) doit être strictement limité aux fonctions internes habilitées de l'IGC au travers d'un **contrôle d'accès fort** (basé sur une authentification au moins à deux facteurs). L'accès en modification aux systèmes de publication des autres informations doit être strictement limité aux fonctions internes habilitées de l'IGC, au moins au travers d'un **contrôle d'accès de type mots de passe** basé sur une politique de gestion stricte des mots de passe.		

	Niveau (*)	
L’accès en modification aux systèmes de publication (ajout, suppression, modification des informations publiées) doit être strictement limité aux fonctions internes habilitées de l’IGC, au moins au travers d’un contrôle d’accès de type mots de passe longs basé sur une politique de gestion stricte des mots de passe.		

III. Identification et authentification

III.1. Nommage

III.1.1. Types de noms

Les noms utilisés doivent être conformes aux spécifications de la norme [X.500].

Dans chaque certificat conforme à la norme [X.509], l'AC émettrice (issuer) et le service applicatif de cachet ou d'authentification du serveur (subject) sont identifiés par un «Distinguished Name» (DN) répondant aux exigences de la norme [X.501].

Des règles sur la construction du DN de ces champs sont précisées dans le document [RGS_A4].

III.1.2. Nécessité d'utilisation de noms explicites

Les noms choisis pour désigner les services applicatifs dans les certificats doivent être explicites.

L'identification de l'entité à laquelle le service applicatif est rattaché est obligatoire.

Authentification Serveur		
Le champ « DN « du certificat du service applicatif contient son FQDN (« Fully Qualified Domain Name « ou nom de domaine totalement qualifié. Exemple : www.monHote.monDomaine.fr) auquel le service applicatif est rattaché. *Nota* – Le certificat d'authentification serveur est associé au FQDN et pas au serveur physique sur lequel la bi-clé est déployée. Autrement dit, une bi-clé d'authentification serveur peut être déployée sur plusieurs machines physiques rattachées à ce FQDN (cas notamment d'architecture de répartition de charge), ou vice-versa plusieurs bi-clés peuvent être déployées sur un même serveur hébergeant plusieurs services applicatifs dotés de FQDN distincts.		

[Cachet]		
Le champ « DN « du certificat du service applicatif contient son nom du service de création de cachet. Exemple : [Nom de l'organisme].[Nom du bureau responsable du serveur].[Nom du service applicatif] pour lequel le service de création de cachet est rattaché. *Nota* – Le certificat de cachet est associé au nom du service et pas au serveur physique sur lequel la bi-clé est déployée. Autrement dit, une bi-clé de cachet peut être déployée sur plusieurs machines physiques rattachées au nom du service de cachet (cas notamment d'architecture de répartition de charge), ou vice-versa plusieurs bi-clés peuvent être déployées sur un même serveur hébergeant plusieurs services applicatifs dotés de noms de services de cachet distincts.		

III.1.3. Anonymisation ou pseudonymisation des services applicatifs

S'agissant de certificats délivrés à des services applicatifs, les notions d'anonymisation ou de pseudonymisation sont sans objet.

III.1.4. Règles d'interprétation des différentes formes de nom

Le document [RGS_A4] fournit des règles à ce sujet. Le cas échéant des précisions seront fournies par l'AC dans sa PC.

III.1.5. Unicité des noms

Afin d'assurer l'identification unique du service applicatif (cachet ou authentification du serveur) au sein du domaine de l'AC ainsi que l'entité à laquelle ce service est rattaché, notamment dans le cas du renouvellement du certificat associé et pour éviter toute ambiguïté, le DN du champ «subject» de chaque certificat électronique doit permettre d'identifier de façon unique ce service (Triplet [Nom de l'organisme].[Nom du bureau responsable du serveur].[Nom du service applicatif] dans le cas d'un service de cachet ; FQDN ou nom interne du serveur / entité dans le cas d'un service d'authentification serveur).

Authentification Serveur		
Durant toute la durée de vie de l'AC, le FQDN d'un serveur rattaché à une entité ne peut être attribué à une autre entité		

[Cachet]		
Durant toute la durée de vie de l'AC, le nom du service de création de cachet rattaché à une entité ne peut être attribué à une autre entité.		

III.1.6. Identification, authentification et rôle des marques déposées

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

L'AC est responsable de l'unicité des noms des services applicatifs utilisés dans ses certificats et de la résolution des litiges portant sur la revendication d'utilisation d'un nom.

Des précisions seront fournies dans la PC de l'AC.

III.2. Validation initiale de l'identité

L'enregistrement d'un service applicatif pour lequel un certificat doit être délivré se fait via l'enregistrement du RC correspondant.

Authentification Serveur		
[SERVEUR-SERVEUR] Le RC devra démontrer qu'il dispose du droit d'utiliser le nom de domaine inclus dans le FQDN (titularité des droits sur le nom de domaine ou droit d'utilisation de la part de l'entité titulaire des droits).		

L'AC doit préciser dans sa PC les preuves retenues.

Un RC peut être amené à changer en cours de validité du certificat électronique correspondant (cf. chapitre I.3.3). Dans ce cas, tout nouveau RC doit également faire l'objet d'une procédure d'enregistrement.

L'enregistrement d'un RC, et du service applicatif objet de la demande, peut se faire soit directement auprès de l'AE, soit via un mandataire de certification de l'entité. Dans ce dernier cas, le MC doit être préalablement enregistré par l'AE.

La validation initiale de l'identité d'une entité ou d'une personne physique est ainsi réalisée dans les cas suivants :

- Enregistrement d'un RC sans MC pour un certificat de service applicatif à émettre : validation par l'AE de l'identité «personne morale» de l'entité de rattachement du RC, de l'identité «personne physique» du futur RC, de son habilitation à être RC pour le service applicatif considéré et pour l'entité considérée, et du nom de domaine du serveur.

- Enregistrement d'un nouveau RC sans MC pour un certificat de service applicatif déjà émis : validation par l'AE de l'identité «personne physique» du futur RC et de son habilitation à être RC pour le service applicatif considéré et pour l'entité considérée.
- Enregistrement d'un MC : validation de l'identité «personne morale» de l'entité pour laquelle le MC interviendra, du rattachement du futur MC à l'entité et de l'identité «personne physique» du futur MC.
- Enregistrement d'un RC via un MC pour un certificat de service applicatif à émettre ou d'un nouveau RC pour un certificat de service applicatif déjà émis : validation par le MC de l'identité «personne physique» du futur RC, de son habilitation à être RC pour le service applicatif considéré et pour l'entité considérée, et des preuves de droit d'usage ou de propriété du nom de domaine et des adresses IP du service applicatif considéré.

Pour des raisons de simplicité de présentation, ces différents cas sont regroupés dans le chapitre III.2.3.

III.2.1. Méthode pour prouver la possession de la clé privée

Lorsque la bi-clé du service applicatif n'est pas générée par l'AC, le RC doit alors fournir à l'AC, via le MC le cas échéant, une preuve de possession de la clé privée correspondant à la clé publique contenue dans la demande de certificat électronique. Cette exigence ne s'applique pas aux unités d'horodatage dédiées à la génération de jetons. En effet, le protocole défini dans la RFC 3161 permet de vérifier en temps réel la possession de la clé privée.

III.2.2. Validation de l'identité d'un organisme

Cf. chapitre III.2.3

III.2.3. Validation de l'identité d'un individu

III.2.3.1. Enregistrement d'un RC sans MC pour un certificat de service applicatif à émettre

L'enregistrement du futur RC représentant une entité nécessite l'identification de cette entité, l'identification de la «personne physique» du futur RC, la vérification de son habilitation à être RC pour le service applicatif considéré et pour l'entité considérée, la justification de l'appartenance du nom de domaine du serveur (FQDN) à l'entité et la justification de l'existence d'une application au sein de l'entité.

Le dossier d'enregistrement, déposé directement auprès de l'AE, doit au moins comprendre :

- Une demande de certificat écrite, datée de moins de 3 mois, signée par un représentant légal de l'entité et comportant le nom du service applicatif concerné par cette demande (FQDN, nom interne du serveur ou nom du service applicatif hébergé par un serveur) ;
- Un mandat, daté de moins de 3 mois, désignant le futur RC comme étant habilité à être responsable pour le service applicatif pour lequel le certificat doit être délivré. Ce mandat doit être signé par un représentant légal de l'entité et co-signé, pour acceptation, par le futur RC ;
- [Entreprise] toute pièce, valide lors de la demande de certificat (extrait Kbis ou situation au Répertoire Territoriale des Entreprises, ...), attestant de l'existence de l'entreprise et portant le numéro TAHITI de celle-ci, ou, à défaut, une autre pièce attestant l'identification unique de l'entreprise qui figurera dans le certificat ;
- [Entreprise] tout document attestant de la qualité du signataire de la demande de certificat ;
- [Administration] une pièce, valide au moment de l'enregistrement, portant délégation de l'autorité responsable de la structure administrative ;

- Un document officiel d'identité en cours de validité du futur RC comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour), qui est présenté à l'AE qui en conserve une copie ;
- Les conditions générales d'utilisation signées ;
- L'adresse postale ou l'adresse mail permettant à l'AC de contacter le RC.

Nota - Le RC doit être informé que les informations personnelles d'identité pourront être utilisées comme éléments d'authentification lors de la demande de révocation, dans le cas où l'AC s'appuie sur un tel mécanisme. En complément, ou à la place, de l'utilisation de ces informations personnelles, il pourra être convenu avec l'AC d'un jeu de questions/réponses ou équivalent.

	Niveau (***)	
La vérification de l'identité du RC par l'AE est réalisée lors d'un face-à-face physique[50].		

	Niveau (**)	
L'authentification du RC par l'AE est réalisée lors d'un face-à-face physique [51] ou sous forme dématérialisée à condition que la demande soit signée par le RC à l'aide d'un procédé de signature électronique conforme au minimum aux exigences du niveau (**)[52] décrites dans le document [RGS_A1] et que la signature soit vérifiée et valide au moment de l'enregistrement.		

	Niveau (*)	
L'authentification du RC peut notamment se faire : ➢ Soit par l'envoi du dossier papier à l'AE accompagné d'une photocopie des documents d'identité de chacun des signataires des pièces du dossier (représentant légal, RC) certifiée conforme par le signataire concerné (date, de moins de 3 mois, et signature de la personne concernée sur la photocopie de ses papiers d'identité précédées de la mention «copie certifiée conforme à l'original»). ➢ Soit via une demande d'enregistrement dématérialisée signée électroniquement par le futur RC à l'aide d'un procédé de signature électronique conforme aux exigences du niveau (*) décrites dans le document [RGS_A1] et que la signature soit vérifiée et valide au moment de l'enregistrement. ➢ Soit par la communication d'un élément propre au futur RC permettant de l'identifier au sein		

[50] Le face-à-face physique peut être réalisé lors de la remise par l'AC au RC du certificat ainsi que du dispositif de protection de la bi-clé si et seulement si cette dernière est générée par l'AC. Si tel est le cas, l'AC décrira dans sa PC la façon dont elle s'assure de la fiabilité des informations contenues dans le dossier d'enregistrement du RC. Il est toutefois recommandé de procéder au face-à-face physique dès la phase d'enregistrement.

[51] Le face-à-face physique peut être réalisé lors de la remise par l'AC au RC du certificat ainsi que du dispositif de protection de la bi-clé si et seulement si cette dernière est générée par l'AC. Si tel est le cas, l'AC décrira dans sa PC la façon dont elle s'assure de la fiabilité des informations contenues dans le dossier d'enregistrement du RC. Il est toutefois recommandé de procéder au face-à-face physique dès la phase d'enregistrement.

[52] Il est recommandé que le procédé de signature électronique soit conforme aux exigences du niveau (***) afin que la signature soit présumée fiable.

d'une base de données administrative pré-établie.

III.2.3.2. Enregistrement d'un nouveau RC sans MC pour un certificat électronique déjà émis

Dans le cas de changement d'un RC en cours de validité d'un certificat électronique, le nouveau RC doit être enregistré en tant que tel par l'AC en remplacement de l'ancien RC.

L'enregistrement du nouveau RC (personne physique) représentant une entité, nécessite l'identification de la personne physique et la vérification de son habilitation en tant que représentant de l'entité à laquelle le service applicatif est rattaché et en tant que RC pour le service applicatif considéré.

Le dossier d'enregistrement, déposé directement auprès de l'AE, doit au moins comprendre :

- Un mandat, daté de moins de 3 mois, désignant le futur RC comme étant habilité à être le nouveau RC pour le service applicatif auquel le certificat a été délivré, en remplacement du RC précédent. Ce mandat doit être signé par un représentant légal de l'entité et co-signé, pour acceptation, par le futur RC,
- [Entreprise] tout document attestant de la qualité du signataire du mandat,
- [Administration] une pièce, valide au moment de l'enregistrement, portant délégation ou subdélégation de l'autorité responsable de la structure administrative,
- Un document officiel d'identité en cours de validité du futur RC comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour), qui est présenté à l'AE qui en conserve une copie,
- Les conditions générales d'utilisation signées.

Nota - Le RC doit être informé que les informations personnelles d'identité pourront être utilisées comme éléments d'authentification lors de la demande de révocation, dans le cas où l'AC s'appuie sur un tel mécanisme. En complément, ou à la place, de l'utilisation de ces informations personnelles, il pourra être convenu avec l'AC d'un jeu de questions/réponses ou équivalent.

	Niveau (***)	
La vérification de l'identité du RC par l'AE est réalisée lors d'un face-à-face physique[53].		

	Niveau (**)	
L'authentification du RC par l'AE est réalisée lors d'un face-à-face physique [54] ou sous forme dématérialisée à condition que la demande soit signée par le RC à l'aide d'un procédé de signature électronique conforme au minimum aux exigences du niveau (**)[55] décrites dans le document [RGS_A1]		

[53] Le face-à-face physique peut être réalisé lors de la remise par l'AC au RC du certificat ainsi que du dispositif de protection de la bi-clé si et seulement si cette dernière est générée par l'AC. Si tel est le cas, l'AC décrira dans sa PC la façon dont elle s'assure de la fiabilité des informations contenues dans le dossier d'enregistrement du RC. Il est toutefois recommandé de procéder au face-à-face physique dès la phase d'enregistrement.

[54] Cf. note de bas de page 7.

[55] Il est recommandé que le procédé de signature électronique soit conforme aux exigences du niveau (***) afin que la signature soit présumée fiable.

et que la signature soit vérifiée et valide au moment de l'enregistrement.

	Niveau (*)	
L'authentification du RC peut notamment se faire : ➢ Soit par l'envoi du dossier papier à l'AE accompagné d'une photocopie des documents d'identité de chacun des signataires des pièces du dossier (représentant légal, RC) certifiée conforme par le signataire concerné (date, de moins de 3 mois, et signature de la personne concernée sur la photocopie de ses papiers d'identité précédées de la mention «copie certifiée conforme à l'original»). ➢ Soit via une demande d'enregistrement dématérialisée signée électroniquement par le futur RC à l'aide d'un procédé de signature électronique conforme aux exigences du niveau (*) décrites dans le document [RGS_A1] et que la signature soit vérifiée et valide au moment de l'enregistrement. ➢ Soit par la communication d'un élément propre au futur RC permettant de l'identifier au sein d'une base de données administrative pré-établie		

III.2.3.3. Enregistrement d'un Mandataire de Certification

Une AE est amenée à constituer un dossier d'enregistrement pour un Mandataire de Certification pour répondre aux besoins suivants :

- Utilisation du dossier du MC comme référence pour les données d'identification de l'entité de tous les RC présentés par le MC.
- Éventuellement, fourniture d'un certificat au MC pour qu'il puisse signer les dossiers d'enregistrement de certificats de services applicatifs de l'entité qu'il représente et les transmettre sous forme électronique.

Le dossier d'enregistrement d'un MC doit comprendre :

- Une demande écrite, datée de moins de 3 mois, signée par un représentant légal de l'entité,
- Un mandat, daté de moins de 3 mois, désignant le MC. Ce mandat doit être signé par un représentant légal de l'entité et co-signé, pour acceptation, par le MC,
- Un engagement signé, et daté de moins de 3 mois, du MC, auprès de l'AC, à effectuer correctement et de façon indépendante les contrôles des dossiers des demandeurs,
- Un engagement signé, et daté de moins de 3 mois, du MC à signaler à l'AE son départ de l'entité,
- [Entreprise] toute pièce, valide lors de la demande de certificat (extrait Kbis ou situation au Répertoire Territoriale des Entreprises, ...), attestant de l'existence de l'entreprise et portant le numéro TAHITI de celle-ci, ou, à défaut, une autre pièce attestant l'identification unique de l'entreprise qui figurera dans le certificat,
- [Entreprise] tout document attestant de la qualité du signataire de la demande,
- [Administration] une pièce, valide au moment de l'enregistrement, portant délégation de l'autorité responsable de la structure administrative,
- Un document officiel d'identité en cours de validité du MC comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour), qui est présenté à l'AE qui en conserve une copie.

Nota - Le MC doit être informé que les informations personnelles d'identité pourront être utilisées comme éléments d'authentification lors de la demande de révocation, dans le cas où l'AC s'appuie sur un tel mécanisme. En complément, ou à la place, de l'utilisation de ces informations personnelles, il pourra être convenu avec l'AC d'un jeu de questions/réponses ou équivalent.

	Niveau (***)	
La vérification de l'identité du MC par l'AE est réalisée lors d'un face-à-face physique[56].		

	Niveau (**)	
L'authentification du MC par l'AE est réalisée lors d'un face-à-face physique [57] ou sous forme dématérialisée à condition que la demande soit signée par le MC à l'aide d'un procédé de signature électronique conforme au minimum aux exigences du niveau (**)[58] décrites dans le document [RGS_A1] et que la signature soit vérifiée et valide au moment de l'enregistrement.		

	Niveau (*)	
L'authentification du MC par l'AE peut se faire par l'envoi du dossier papier par courrier accompagné d'une photocopie des documents d'identité de chacun des signataires des pièces du dossier (représentant légal, MC) certifiée conforme par le signataire concerné (date, de moins de 3 mois, et signature de la personne concernée sur la photocopie de ces papiers d'identité, précédées de la mention «copie certifiée conforme à l'original»). Cette authentification peut également se faire sous forme dématérialisée à condition que les différentes pièces justificatives du dossier soient signées à l'aide d'un procédé de signature électronique conforme aux exigences du niveau (*) décrites dans le document [RGS_A_3] et que la signature soit vérifiée et valide au moment de l'enregistrement.		

III.2.3.4. Enregistrement d'un RC via un MC pour un certificat électronique à émettre

Le dossier d'enregistrement, déposé auprès d'un MC, doit au moins comprendre :

Le dossier d'enregistrement, déposé directement auprès de l'AE, doit au moins comprendre :

- Une demande de certificat écrite, datée de moins de 3 mois, signée par le MC et comportant le nom du service applicatif concerné par cette demande (FQDN) ;
- Un mandat, daté de moins de 3 mois, désignant le futur RC comme étant habilité à être responsable pour le service applicatif pour lequel le certificat doit être délivré. Ce mandat doit être signé par le MC et co-signé, pour acceptation, par le futur RC ;

[56] Le face-à-face physique peut être réalisé lors de la remise par l'AC au MC du certificat ainsi que du dispositif de protection de la bi-clé si et seulement si cette dernière est générée par l'AC. Si tel est le cas, l'AC décrira dans sa PC la façon dont elle s'assure de la fiabilité des informations contenues dans le dossier d'enregistrement du MC. Il est toutefois recommandé de procéder au face-à-face physique dès la phase d'enregistrement.

[57] Cf. note de bas de page 10.

[58] Il est recommandé que le procédé de signature électronique soit conforme aux exigences du niveau (***) afin que la signature soit présumée fiable.

- Un document officiel d'identité en cours de validité du futur RC comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour), qui est présenté au MC qui en conserve une copie ;
- Les conditions générales d'utilisation signées ;
- L'adresse postale ou l'adresse mail permettant à l'AC de contacter le RC.

Authentification		
➢ [SERVEUR] une preuve de possession par l'entité du nom de domaine correspondant au FQDN du serveur. ➢ [CACHET], une preuve de possession par l'entité de l'existence du serveur et du nom de l'application que ce dernier héberge.		

Nota - Le RC doit être informé que les informations personnelles d'identité pourront être utilisées comme éléments d'authentification lors de la demande de révocation, dans le cas où l'AC s'appuie sur un tel mécanisme. En complément, ou à la place, de l'utilisation de ces informations personnelles, il pourra être convenu avec l'AC d'un jeu de questions/réponses ou équivalent.

	Niveau (***)	
La vérification de l'identité du RC par le MC est réalisée lors d'un face-à-face physique[59].		

	Niveau (**)	
L'authentification du RC par le MC est réalisée lors d'un face-à-face physique[60] ou sous forme dématérialisée à condition que la demande soit signée par le RC à l'aide d'un procédé de signature électronique conforme au minimum aux exigences du niveau (**)[61] décrites dans le document [RGS_A1] et que la signature soit vérifiée et valide au moment de l'enregistrement.		

	Niveau (*)	
L'authentification du RC peut notamment se faire : ➢ Soit par l'envoi du dossier papier au MC accompagné d'une photocopie des documents d'identité de chacun des signataires des pièces du dossier (représentant légal, RC) certifiée conforme par le signataire concerné (date, de moins de 3 mois, et signature de la personne concernée sur la photocopie de ses papiers d'identité précédées de la mention «copie certifiée conforme à l'original»).		

[59] Le face-à-face physique peut être réalisé lors de la remise par l'AC au RC du certificat ainsi que du dispositif de protection de la bi-clé si et seulement si cette dernière est générée par l'AC. Si tel est le cas, l'AC décrira dans sa PC la façon dont elle s'assure de la fiabilité des informations contenues dans le dossier d'enregistrement du futur RC. Il est toutefois recommandé de procéder au face-à-face physique dès la phase d'enregistrement.

[60] Cf. note de bas de page 13.

[61] Il est recommandé que le procédé de signature électronique soit conforme aux exigences du niveau (***) afin que la signature soit présumée fiable.

- Soit via une demande d'enregistrement dématérialisée signée électroniquement par le futur RC à l'aide d'un procédé de signature électronique conforme aux exigences du niveau (*) décrites dans le document [RGS_A1] et que la signature soit vérifiée et valide au moment de l'enregistrement.
- Soit par la communication d'un élément propre au futur RC permettant de l'identifier au sein d'une base de données administrative pré-établie.

Lors de la transmission des dossiers de RC par le MC, celui-ci doit s'authentifier auprès de l'AE :

- soit à l'aide d'un certificat électronique remis par l'AC,
- soit au cours d'un face-à-face et/ou par le paraphe du MC apposé sur les différentes pages du dossier de demande, complété par sa signature sur les principales pages.

III.2.3.5. Enregistrement d'un nouveau RC via un MC pour un certificat électronique déjà émis

Dans le cas de changement d'un RC pour un certificat électronique en cours de validité de ce certificat, le nouveau RC doit être enregistré en tant que tel par l'AC en remplacement de l'ancien RC.

Le dossier d'enregistrement, déposé auprès d'un MC, doit au moins comprendre :

- un mandat, daté de moins de 3 mois, désignant le futur RC comme étant habilité à être le nouveau RC pour le service applicatif auquel le certificat a été délivré, en remplacement du RC précédent. Ce mandat doit être signé par le MC et co-signé, pour acceptation, par le futur RC,
- un document officiel d'identité en cours de validité du RC comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour), qui est présenté au MC qui en transmet une copie à l'AE pour conservation,
- les conditions générales d'utilisation signées.

Nota - Le RC doit être informé que les informations personnelles d'identité pourront être utilisées comme éléments d'authentification lors de la demande de révocation, dans le cas où l'AC s'appuie sur un tel mécanisme. En complément, ou à la place, de l'utilisation de ces informations personnelles, il pourra être convenu avec l'AC d'un jeu de questions/réponses ou équivalent.

	Niveau (***)	
La vérification de l'identité du RC par le MC est réalisée lors d'un face-à-face physique[62].		

	Niveau (**)	
L'authentification du RC par le MC est réalisée lors d'un face-à-face physique[63] ou sous forme dématérialisée à condition que la demande soit signée par le RC à l'aide d'un procédé de signature		

[62] Le face-à-face physique peut être réalisé lors de la remise par l'AC au RC du certificat ainsi que du dispositif de protection de la bi-clé si et seulement si cette dernière est générée par l'AC. Si tel est le cas, l'AC décrira dans sa PC la façon dont elle s'assure de la fiabilité des informations contenues dans le dossier d'enregistrement du futur RC. Il est toutefois recommandé de procéder au face-à-face physique dès la phase d'enregistrement.

[63] Cf. note de bas de page 16.

électronique conforme au minimum aux exigences du niveau (**)[64] décrites dans le document [RGS_A1] et que la signature soit vérifiée et valide au moment de l'enregistrement.

	Niveau (*)	
L'authentification du RC peut notamment se faire : ➢ Soit par l'envoi du dossier papier au MC accompagné d'une photocopie des documents d'identité de chacun des signataires des pièces du dossier (représentant légal, RC) certifiée conforme par le signataire concerné (date, de moins de 3 mois, et signature de la personne concernée sur la photocopie de ses papiers d'identité précédées de la mention «copie certifiée conforme à l'original»). ➢ Soit via une demande d'enregistrement dématérialisée signée électroniquement par le futur RC à l'aide d'un procédé de signature électronique conforme aux exigences du niveau (*) décrites dans le document [RGS_A1] et que la signature soit vérifiée et valide au moment de l'enregistrement. ➢ Soit par la communication d'un élément propre au futur RC permettant de l'identifier au sein d'une base de données administrative pré-établie.		

Lors de la transmission des dossiers de RC par le MC, celui-ci doit s'authentifier auprès de l'AE :

- soit à l'aide d'un certificat électronique remis par l'AC,
- soit au cours d'un face-à-face et/ou par le paraphe du MC apposé sur les différentes pages du dossier de demande, complété par sa signature sur les principales pages.

III.2.4. Informations non vérifiées du RC et du service applicatif

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

III.2.5. Validation de l'autorité du demandeur

Cette étape est effectuée en même temps que la validation de l'identité de la personne physique (directement par l'AE ou par le MC).

III.3. Identification et validation d'une demande de renouvellement des clés

Le renouvellement de la bi-clé d'un service applicatif entraîne automatiquement la génération et la fourniture d'un nouveau certificat. De plus, un nouveau certificat de service applicatif ne peut pas être fourni au RC sans renouvellement de la bi-clé correspondante (cf. chapitre IV.6).

Ce chapitre concerne aussi bien le cas où la bi-clé est générée au niveau du service applicatif que le cas où elle est générée par l'AC.

III.3.1. Identification et validation pour un renouvellement courant

	Niveau (, ***)**	

[64] Il est recommandé que le procédé de signature électronique soit conforme aux exigences du niveau (***) afin que la signature soit présumée fiable.

Lors du premier renouvellement, l'AC doit au minimum s'assurer que les informations du dossier d'enregistrement initial sont toujours valides et que le certificat à renouveler existe, et est toujours valide.

	Niveau (*)	
Lors du premier renouvellement, la vérification de l'identité du porteur est optionnelle. Elle est laissée à l'appréciation de l'AC qui engage sa responsabilité quant à la validité des informations contenues dans le certificat renouvelé.		

Lors du renouvellement suivant, l'AE, saisie de la demande, identifiera le RC et le service applicatif selon la même procédure que pour l'enregistrement initial ou une procédure offrant un niveau de garantie équivalent.

III.3.2. Identification et validation pour un renouvellement après révocation

Suite à la révocation définitive d'un certificat, quelle qu'en soit la cause, la procédure d'identification et de validation de la demande de renouvellement doit être identique à la procédure d'enregistrement initial ou doit être une procédure offrant un niveau de garantie équivalent.

III.4. Identification et validation d'une demande de révocation

Les exigences concernant les informations à fournir dans une demande de révocation sont décrites au chapitre IV.9.3.

	Niveau (***)	
Si la demande de révocation est faite via un service téléphonique ou via un service en ligne (serveur web), le demandeur doit être formellement authentifié : vérification de l'identité du demandeur et de son autorité par rapport au certificat à révoquer. Par exemple : série d'au moins 4 ou 5 questions / réponses sur des informations propres au demandeur, dont au moins une réponse ne peut réellement être connue que du demandeur (question d'identification personnelle liée au demandeur et/ou dont la réponse a été choisie au moment de l'enregistrement ou lors du retrait du certificat (cf. chapitre III.2.3), utilisation d'un identifiant / mot de passe envoyé préalablement au demandeur de façon sécurisée).		

	Niveau (**)	
Si la demande de révocation est faite via un service téléphonique ou via un service en ligne (serveur web), le demandeur doit être formellement authentifié : vérification de l'identité du demandeur et de son autorité par rapport au certificat à révoquer. Par exemple : série d'au moins 3 ou 4 questions / réponses sur des informations propres au demandeur, dont au moins une réponse ne peut réellement être connue que du demandeur (question d'identification personnelle liée au demandeur et/ou dont la réponse a été choisie au moment de l'enregistrement ou lors du retrait du certificat, utilisation d'un identifiant / mot de passe envoyé préalablement au demandeur de façon sécurisée).		

	Niveau (*)	
Si la demande de révocation est faite via un service téléphonique ou via un service en ligne (serveur web), elle doit faire l'objet d'un minimum d'authentification : vérification d'une ou deux informations		

de base du demandeur (adresse, n° de téléphone, etc.) et de son autorité par rapport au certificat à révoquer.

Une demande de révocation peut également être faite par courrier ou par télécopie. Elle doit alors être signée par le demandeur et le service de gestion des révocations doit s'assurer de l'identité du demandeur (vérification de la signature manuscrite par rapport à une signature préalablement enregistrée) et de son autorité par rapport au certificat à révoquer.

IV. Exigences opérationnelles sur le cycle de vie des certificats

IV.1. Demande de certificat

IV.1.1. Origine d'une demande de certificat

Un certificat peut être demandé par un représentant légal de l'entité ou un MC dûment mandaté pour cette entité, avec dans tous les cas consentement préalable du futur RC.

IV.1.2. Processus et responsabilités pour l'établissement d'une demande de certificat

Les informations suivantes doivent au moins faire partie de la demande de certificat (cf. chapitre III.2 ci-dessus) :

- [SERVEUR] le FQDN du serveur à utiliser dans le certificat ;
- [CACHET], le nom du service applicatif à utiliser dans le certificat.
- les données personnelles d'identification du RC ;
- les données d'identification de l'entité (sauf si l'enregistrement est effectué par l'intermédiaire d'un MC).

Le dossier de demande est établi soit directement par le futur RC à partir des éléments fournis par son entité, soit par son entité et signé par le futur RC. Si l'entité n'a pas mis en place de MC, le dossier est transmis directement à l'AE. Si l'entité a mis en place un MC, le dossier lui est remis.

Par ailleurs, l'AE doit s'assurer de disposer d'une information permettant de contacter le MC ou le futur RC du certificat.

IV.2. Traitement d'une demande de certificat

IV.2.1. Exécution des processus d'identification et de validation de la demande

Les identités «personne physique» et «personne morale» sont vérifiées conformément aux exigences du chapitre III.2.

L'AE, ou le MC le cas échéant, doit effectuer les opérations suivantes :

- Valider l'identité du futur RC ;
- Vérifier la cohérence des justificatifs présentés ;
- S'assurer que le futur RC a pris connaissance des modalités applicables pour l'utilisation du certificat (voir les conditions générales d'utilisation).

Authentification		
➢ [SERVEUR] valider le FQDN du serveur informatique auquel le certificat doit être rattaché. Il peut utiliser le service d'interrogation whoIs de l'AFNIC par exemple pour vérifier les FQDN se terminant par « .fr «. Il peut utiliser le service whoIs de Mana par exemple pour le « .pf ». Par ailleurs l'AE, ou le MC, vérifiera que le FQDN du serveur est correctement formaté et ne contient pas le caractère NUL. ➢ [CACHET], valider l'existence du serveur et du nom de l'application que ce dernier héberge et à laquelle le certificat doit être rattachée.		

Dans le cas d'une demande via un MC, celui-ci retransmet le dossier à l'AE après avoir effectué les

opérations ci-dessus. L'AE doit alors s'assurer que la demande correspond bien au mandat du MC.

Une fois ces opérations effectuées, l'AE émet la demande de génération du certificat et, le cas échéant, de la bi-clé vers la fonction adéquate de l'IGC (cf. chapitre I.4.1).

L'AE conserve ensuite une trace des justificatifs présentés :

- si le dossier est au format papier, sous la forme d'une photocopie signée à la fois par le futur RCC et par l'AE, ou le MC le cas échéant, les signatures étant précédées de la mention «copie certifiée conforme à l'original» ;
- si le dossier est au format électronique, les différents justificatifs sous une forme électronique ayant valeur légale.

IV.2.2. Acceptation ou rejet de la demande

En cas de rejet de la demande, l'AE en informe le RC, ou le MC le cas échéant, en justifiant le rejet.

IV.2.3. Durée d'établissement du certificat

La présente PC Type ne formule pas d'exigence spécifique sur le sujet. A préciser par l'AC dans sa PC, en visant une durée d'établissement la plus courte possible.

IV.3. Délivrance du certificat

IV.3.1. Actions de l'AC concernant la délivrance du certificat

Suite à l'authentification de l'origine et à la vérification de l'intégrité de la demande provenant de l'AE, l'AC déclenche les processus de génération et de préparation des différents éléments destinés au RC : au minimum, le certificat[65], et, selon les cas, la bi-clé du service applicatif, le dispositif de protection associé, les codes d'activation, etc. (cf. chapitre I.4.1).

Si l'AC génère la bi-clé du service applicatif, le processus de génération du certificat doit être lié de manière sécurisée au processus de génération de la bi-clé : l'ordonnancement des opérations doit être assuré ainsi que, le cas échéant en fonction de l'architecture de l'IGC, l'intégrité et l'authentification des échanges entres les composantes. Par ailleurs, la clé privée doit être transmise de façon sécurisée au RC, en en garantissant l'intégrité et la confidentialité.

Les conditions de génération des clés et des certificats et les mesures de sécurité à respecter sont précisées aux chapitres V et VI ci-dessous, notamment la séparation des rôles de confiance (cf. chapitre V.2).

IV.3.2. Notification par l'AC de la délivrance du certificat au RC

	Niveau (**) et (***)	
La remise du certificat doit se faire en mains propres (face-à-face) au minimum dans le cas où l'authentification du RC se fait via un face-à-face et que ce face-à-face n'a pas eu lieu au moment de l'enregistrement (cf. chapitre III.2). Si la remise du certificat ne se fait pas en mains propres, l'AC précisera dans sa PC comment elle s'assure		

[65] Si la bi-clé est générée au niveau du serveur, la clé publique doit être transmise à l'AC (cf. chapitre VI.1.3).

que le certificat est bien remis au bon RC ou à une personne dûment autorisée (par exemple, envoi sur carte à puce ou sur disquette en courrier recommandé, téléchargement grâce à un code d'accès préalablement fourni au RC, ...).

	Niveau (***)	
De plus, si l'AC n'a pas généré elle-même la bi-clé du porteur, elle doit s'assurer que le certificat est bien associé, dans l'environnement du porteur, à la clé privée correspondante (par exemple, mise à disposition d'une application en ligne permettant de réaliser une authentification de test). Il s'agit notamment du cas où le certificat est associé à une clé privée stockée sur une carte à puce non fournie par l'AC : le certificat doit alors être téléchargé sur la bonne carte à puce.		

	Niveau (*)	
Le certificat peut être transmis par message électronique à une adresse fournie par le porteur, ou bien l'URL permettant de télécharger le certificat peut être envoyée à une telle adresse.		

Le certificat complet et exact doit être mis à la disposition du MC ou du RC.

Nota – Si la remise du certificat doit se faire en main propre auprès de l'AE, le RC ou MC sera également tributaire des modalités d'accueil de l'AE.

IV.4. Acceptation du certificat

IV.4.1. Démarche d'acceptation du certificat

	Niveau (***)	
L'AC doit obtenir confirmation de l'acceptation explicite du certificat par le RC sous la forme d'un accord signé (papier ou électronique). L'AC doit garder une trace de l'acceptation du certificat par le porteur.		

	Niveau (**)	
L'AC doit obtenir confirmation de l'acceptation du certificat par le RC, si possible de façon explicite sous la forme d'un accord signé (papier ou électronique). Si la remise du certificat au RC, ou le cas échéant à son MC, peut faire l'objet d'une date connue avec un degré suffisant de certitude, l'AC peut s'appuyer sur un mécanisme d'acceptation tacite du certificat moyennant un délai maximum laissé au RC, à compter de la date de réception de son certificat, pour signaler sa non-acceptation du certificat. La première utilisation du certificat peut également valoir acceptation tacite. Dans le cas d'une acceptation tacite, les obligations du porteur et le délai correspondant doivent être clairement mentionnés dans la PC de l'AC ainsi que dans les conditions générales d'utilisation (cf. chapitre II.2) et/ou le contrat porteur. L'AC doit garder une trace de l'acceptation du certificat par le porteur si celle-ci est explicite.		

	Niveau (*)	
L'acceptation peut être tacite à compter de la date d'envoi du certificat (ou des informations de téléchargement) au RC. Le processus d'acceptation du certificat et les obligations correspondantes du porteur doivent être clairement mentionnés dans la PC de l'AC ainsi que dans les conditions générales		

d'utilisation (cf. chapitre II.2) et/ou le contrat porteur.

IV.4.2. Publication du certificat

Si le certificat fait l'objet d'une publication par l'AC, les conditions d'une telle publication doivent être précisées par l'AC dans sa PC. Notamment, cette publication ne peut avoir lieu sans l'accord du RC et qu'après acceptation du contenu du certificat par celui-ci.

IV.4.3. Notification par l'AC aux autres entités[66] de la délivrance du certificat

L'AC informe l'AE de la délivrance du certificat, qui se charge d'en informer le MC le cas échéant.

IV.5. Usages de la bi-clé et du certificat

IV.5.1. Utilisation de la clé privée et du certificat par le RC

L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée à la fonction de sécurité concernée (cf. chapitre I.5.1.1). Les RC doivent respecter strictement les usages autorisés des bi-clés et des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.

L'usage autorisé de la bi-clé du service applicatif et du certificat associé doit par ailleurs être indiqué dans le certificat lui-même, via les extensions concernant les usages des clés (cf. [RGS_A4]). Cet usage doit également être clairement explicité dans la PC de l'AC, ainsi que dans les conditions générales d'utilisation et/ou le contrat pour le certificat électronique considéré. Faisant partie du dossier d'enregistrement, les conditions générales sont portées à la connaissance du RC ou du MC par l'AC avant d'entrer en relation contractuelle.

IV.5.2. Utilisation de la clé publique et du certificat par l'utilisateur du certificat

Cf. chapitre précédent et chapitre I.5.

Les utilisateurs de certificats doivent respecter strictement les usages autorisés des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.

IV.6. Renouvellement d'un certificat

Conformément au [RFC3647], la notion de «renouvellement de certificat» correspond à la délivrance d'un nouveau certificat pour lequel seules les dates de validité sont modifiées, toutes les autres informations sont identiques au certificat précédent (y compris la clé publique du service applicatif).

Dans le cadre de la présente PC Type, il ne peut pas y avoir de renouvellement de certificat sans renouvellement de la bi-clé correspondante. Aussi, si c'est l'AC qui génère les bi-clés des services applicatifs, elle doit garantir qu'un certificat correspondant à une bi-clé existante ne peut pas être renouvelé au sens du [RFC3647]. Dans le cas contraire, elle doit s'en assurer auprès du RC, au minimum au travers d'un engagement contractuel clair et explicite du RC vis-à-vis de l'AC.

IV.7. Délivrance d'un nouveau certificat suite à changement de la bi-clé

Conformément au [RFC3647], ce chapitre traite de la délivrance d'un nouveau certificat électronique liée à

[66] Internes et/ou externes à l'IGC.

la génération d'une nouvelle bi-clé.

IV.7.1. Causes possibles de changement d'une bi-clé

Les bi-clés doivent être périodiquement renouvelées afin de minimiser les possibilités d'attaques cryptographiques. Ainsi les bi-clés des services applicatifs, et les certificats correspondants, seront renouvelés au minimum à une fréquence définie au point VI.3.2.

Nota : Dans le cadre de la délivrance de certificats électroniques SSL EV (cf. [GEVC]), il est exigé que la durée de validité du certificat soit inférieure à 27 mois et il est recommandé qu'elle soit d'un an.

Par ailleurs, une bi-clé et un certificat peuvent être renouvelés par anticipation, suite à la révocation du certificat du service applicatif (cf. chapitre IV.9, notamment le chapitre [IV.9.1.1] pour les différentes causes possibles de révocation).

Nota - Dans la suite du présent chapitre, le terme utilisé est «fourniture d'un nouveau certificat». Ce terme recouvre également, dans le cas où elle est générée par l'AC, la fourniture de la nouvelle bi-clé du service applicatif.

IV.7.2. Origine d'une demande d'un nouveau certificat

Le déclenchement de la fourniture d'un nouveau certificat électronique peut-être automatique ou bien à l'initiative du RC.

L'entité, via son MC le cas échéant, peut également être à l'initiative d'une demande de fourniture d'un nouveau certificat pour un service applicatif qui lui est rattaché.

IV.7.3. Procédure de traitement d'une demande d'un nouveau certificat

L'identification et la validation d'une demande de fourniture d'un nouveau certificat sont précisées au chapitre III.3 ci-dessus.

Pour les actions de l'AC, cf. chapitre IV.3.1.

IV.7.4. Notification au RC de l'établissement du nouveau certificat

Cf. chapitre IV.3.2.

IV.7.5. Démarche d'acceptation du nouveau certificat

Cf. chapitre IV.4.1.

IV.7.6. Publication du nouveau certificat

Cf. chapitre IV.4.2.

IV.7.7. Notification par l'AC aux autres entités de la délivrance du nouveau certificat

Cf. chapitre IV.4.3.

IV.8. Modification du certificat

Conformément au [RFC3647], la modification d'un certificat correspond à des modifications d'informations sans changement de la clé publique (cf. chapitre IV.7) et autres qu'uniquement la modification des dates de validité (cf. chapitre IV.6).

La modification de certificat n'est pas recommandée dans la présente PC Type. Toutefois, si elle est mise en

œuvre, elle doit modifier le numéro de série du certificat, révoquer le certificat initial et ne concerner que les certificats d'utilisateurs finaux.

IV.9. Révocation et suspension des certificats

IV.9.1. Causes possibles d'une révocation

IV.9.1.1. Certificats de services applicatifs

Les circonstances suivantes peuvent être à l'origine de la révocation du certificat électronique :

- Les informations du service figurant dans le certificat ne sont plus en conformité avec l'identité du service ou l'utilisation prévue dans le certificat (par exemple, modification du FQDN), ceci avant l'expiration normale du certificat ;
- Le RC n'a pas respecté les modalités applicables d'utilisation du certificat ;
- Le RC et/ou, le cas échéant, le MC / l'entité n'ont pas respecté leurs obligations découlant de la PC de l'AC ;
- Une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement ;
- La clé privée du service applicatif est suspectée de compromission, est compromise, est perdue ou est volée, (éventuellement les données d'activation associées) ;
- Le RC ou une entité autorisée (représentant légal de l'entité ou MC par exemple) demande la révocation du certificat (notamment dans le cas d'une destruction ou altération de la clé privée du service applicatif et/ou de son support) ;
- L'arrêt définitif du service applicatif ou la cessation d'activité de l'entité du RC de rattachement du service applicatif.

Lorsqu'une des circonstances ci-dessus se réalise et que l'AC en a connaissance (elle en est informée ou elle obtient l'information au cours d'une de ses vérifications, lors de la délivrance d'un nouveau certificat notamment), le certificat concerné doit être révoqué.

IV 9.1.2. Certificats d'une composante de l'IGC

Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat d'une composante de l'IGC (y compris un certificat d'AC pour la génération de certificats, de LCR et/ou de réponses OCSP) :

- Suspicion de compromission, compromission, perte ou vol de la clé privée de la composante ;
- Décision de changement de composante de l'IGC suite à la détection d'une non-conformité des procédures appliquées au sein de la composante avec celles annoncées dans la DPC (par exemple, suite à un audit de qualification ou de conformité négatif) ;
- Cessation d'activité de l'entité opérant la composante.

IV.9.2. Origine d'une demande de révocation

IV.9.2.1. Certificats de services applicatifs

Les personnes / entités qui peuvent demander la révocation d'un certificat électronique sont les suivantes :

- Le RC pour le service applicatif considéré ;
- Le MC ;
- Un représentant légal de l'entité ;

- L'AC émettrice du certificat ou l'une de ses composantes (AE).

Nota : Le RC doit être informé des personnes / entités susceptibles d'effectuer une demande de révocation pour le certificat dont il a la responsabilité.

IV.9.2.2. Certificats d'une composante de l'IGC

La révocation d'un certificat d'AC ne peut être décidée que par l'entité responsable de l'AC, ou par les autorités judiciaires via une décision de justice.

La révocation des autres certificats de composantes est décidée par l'entité opérant la composante concernée qui doit en informer l'AC sans délai.

IV.9.3. Procédure de traitement d'une demande de révocation

IV.9.3.1. Révocation d'un certificat électronique

Les exigences d'identification et de validation d'une demande de révocation, effectuée hors ligne ou en ligne par la fonction de gestion des révocations, sont décrites au chapitre III.4.

L'AC doit préciser dans sa PC comment la fonction de gestion des révocations est organisée et quels sont les points d'accès à cette fonction pour les demandeurs de révocation.

Les informations suivantes doivent au moins figurer dans la demande de révocation de certificat :

- Le nom du service applicatif figurant dans le certificat (FQDN pour les certificats de serveur ou nom d'application pour les certificats de cachet) ;
- Le nom du demandeur de la révocation ;
- Toute information permettant de retrouver rapidement et sans erreur le certificat à révoquer (n° de série...) ;
- Éventuellement, la cause de révocation.

Une fois la demande authentifiée et contrôlée, la fonction de gestion des révocations révoque le certificat correspondant en changeant son statut, puis communique ce nouveau statut à la fonction d'information sur l'état des certificats.

L'information de révocation doit être diffusée au minimum selon l'une des solutions suivantes :

- Via une LCR signée par l'AC elle-même ou par une entité désignée par l'AC ;
- Via un service OCSP dont la réponse est soit signée par l'AC ayant émis le certificat à révoquer ou par un certificat de répondeur OCSP lui-même signé par l'AC ayant émis le certificat à révoquer (cf. chapitre IV.9.9).

Nota : Dans le cadre de l'émission de certificats électroniques SSL de type « Extended validation « (SSL EV), il est exigé que soit mis en œuvre par le PSCE un service de répondeur OCSP. L'ensemble des exigences du CA Browser Forum pour l'émission de certificats SSL EV se trouve dans le document [GEVC].

Le demandeur de la révocation doit être informé du bon déroulement de l'opération et de la révocation effective du certificat.

L'opération est enregistrée dans les journaux d'évènements avec, le cas échéant, suffisamment d'informations sur les causes initiales ayant entraîné la révocation du certificat.

IV.9.3.2. Révocation d'un certificat d'une composante de l'IGC

L'AC précisera dans sa DPC les procédures à mettre en œuvre en cas de révocation d'un certificat d'une

composante de l'IGC.

En cas de révocation d'un des certificats de la chaîne de certification, l'AC doit informer dans les plus brefs délais et par tout moyen (et si possible par anticipation) l'ensemble des RC concernés que leurs certificats de services applicatifs correspondants ne sont plus valides. Pour cela, l'IGC pourra par exemple envoyer des récépissés aux AE et aux MC. Ces derniers devront informer les RC en leur indiquant explicitement que leurs certificats de services applicatifs ne sont plus valides car un des certificats de la chaîne de certification n'est plus valide.

Afin de faciliter la révocation du certificat de l'AC, il est recommandé que le certificat associé à la clé de l'AC signant les certificats de services applicatifs soit signé par une autre AC et ne soit pas uniquement autosigné (cf. chapitre I.4.1.2).

IV.9.4. Délai accordé au RC pour formuler la demande de révocation

Dès que le RC (ou une personne autorisée) a connaissance qu'une des causes possibles de révocation, de son ressort, est effective, il doit formuler sa demande de révocation sans délai.

IV.9.5. Délai de traitement par l'AC d'une demande de révocation

IV.9.5.1. Révocation d'un certificat électronique

Par nature, une demande de révocation doit être traitée en urgence.

IV.9.5.2. Disponibilité du système de traitement des demandes de révocation

La fonction de gestion des révocations doit être disponible aux heures ouvrées au niveau * et 24h/24 et 7j/7 aux niveaux ** et ***. Cette fonction doit avoir une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) conforme au tableau suivant :

escription	**Niveau ***	**Niveau ****	**Niveau *****
Durée maximale d'indisponibilité par interruption (panne ou maintenance) de la fonction de gestion des révocations	2h (jours ouvrées)	2h	1h

Cette fonction doit avoir une durée maximale totale d'indisponibilité par mois conforme au tableau suivant :

Description	**Niveau ***	**Niveau ****	**Niveau *****
Durée maximale totale d'indisponibilité par mois de la fonction de gestion des révocations	16h (jours ouvrées)	8h	4h

Toute demande de révocation d'un certificat porteur doit être traitée dans un délai inférieur à 72h pour un niveau * et inférieur à 24h pour les niveaux ** et ***. Ce délai s'entend entre la réception de la demande de révocation authentifiée et la mise à disposition de l'information de révocation auprès des utilisateurs.

IV.9.5.3. Révocation d'un certificat d'une composante de l'IGC

La révocation d'un certificat d'une composante de l'IGC doit être effectuée dès la détection d'un évènement décrit dans les causes de révocation possibles pour ce type de certificat. La révocation du certificat est effective lorsque le numéro de série du certificat est introduit dans la liste de révocation de l'AC qui a émis le certificat, et que cette liste est accessible au téléchargement.

La révocation d'un certificat de signature de l'AC (signature de certificats, de LCR / LAR ou de réponses OCSP) doit être effectuée immédiatement, particulièrement dans le cas de la compromission de la clé.

IV.9.6. Exigences de vérification de la révocation par les utilisateurs de certificats

L'utilisateur d'un certificat électronique est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante. La méthode utilisée (LCR, dLCR, OCSP…) est à l'appréciation de l'utilisateur selon leur disponibilité et les contraintes liées à son application.

IV.9.7. Fréquence d'établissement et durée de validité des LCR

Lorsque l'information sur l'état de la révocation d'un certificat est assurée au travers de la mise en place d'un service de LCR et, le cas échéant, de dLCR, la fréquence minimale de leur publication doit être de 72h pour le niveau * et 24h pour les niveaux ** et ***.

Afin d'assurer une continuité du service dans le cas où un incident sur la publication des LCR survient, il est recommandé que la durée de validité des LCR (et dLCR) soit le double de leur fréquence de publication. En aucun cas cette durée de validité ne pourra excéder 6 jours.

Une LAR est un LCR qui ne contient que des certificats d'AC. Il est recommandé que les LAR soient publiées au minimum à fréquence mensuelle.

IV.9.8. Délai maximum de publication d'une LCR

Lorsque l'information sur l'état de la révocation d'un certificat est assurée au travers de la mise en place d'un service de LCR et, le cas échéant, de dLCR, celles-ci doivent être publiées et disponibles pour le téléchargement au maximum dans les 30 minutes suivant leur génération[67].

IV.9.9. Exigences sur la vérification en ligne de la révocation et de l'état des certificats

Lorsque l'information sur l'état de la révocation d'un certificat est assurée au travers de la mise en place d'un service OCSP, celui-ci doit respecter les exigences d'intégrité, de disponibilité et de délai de publication décrites dans cette PC Type.

Nota : Dans le cadre de la délivrance de certificats électroniques SSL EV, il est exigé que les données exploitées par le répondeur OCSP soient renouvelées au moins tous les 4 jours ouvrés, et les réponses doivent avoir une date d'expiration de 10 jours

IV.9.10. Autres moyens disponibles d'information sur les révocations

Ces autres moyens d'information sur les révocations peuvent être mis en place à condition qu'ils respectent les exigences d'intégrité, de disponibilité et de délai de publication décrites dans la présente PC Type.

À préciser par l'AC dans sa PC.

IV.9.11. Exigences spécifiques en cas de compromission de la clé privée

Pour les certificats de services applicatifs, les entités autorisées à effectuer une demande de révocation sont tenues de le faire dans les meilleurs délais après avoir eu connaissance de la compromission de la clé privée.

Pour les certificats d'AC, outre les exigences du chapitre IV.9.3.2 ci-dessus, la révocation suite à une compromission de la clé privée doit faire l'objet d'une information clairement diffusée au moins sur le site Internet de l'AC et éventuellement relayée par d'autres moyens (autres sites Internet institutionnels, journaux,

[67] Recommandation d'immédiateté.

etc.).

	Niveau (***)	
L'AC doit imposer au RC ou au MC qu'en cas de compromission de la clé privée du porteur ou de connaissance de la compromission de la clé privée de l'AC ayant émis son certificat, le RC s'oblige à interrompre immédiatement et définitivement l'usage de sa clé privée et de son certificat associé.		

IV.9.12. Causes possibles d'une suspension

La suspension de certificats n'est pas autorisée dans la présente PC Type.

IV.9.13. Origine d'une demande de suspension

Sans objet.

IV.9.14. Procédure de traitement d'une demande de suspension

Sans objet.

IV.9.15. Limites de la période de suspension d'un certificat

Sans objet.

IV.10. Fonction d'information sur l'état des certificats

IV.10.1. Caractéristiques opérationnelles

L'AC doit fournir aux utilisateurs de certificats les informations leur permettant de vérifier et de valider, préalablement à son utilisation, le statut d'un certificat et de l'ensemble de la chaîne de certification correspondante (jusqu'à et y compris l'AC Racine), c'est-à-dire de vérifier également les signatures des certificats de la chaîne, les signatures garantissant l'origine et l'intégrité des LCR / LAR ou des jetons OCSP et l'état du certificat de l'AC Racine.

La fonction d'information sur l'état des certificats doit au moins mettre à la disposition des utilisateurs de certificats une solution : LCR ou OCSP.

Lorsqu'un service de LCR / LAR est proposé, alors celles-ci doivent être au format V2.

IV.10.2. Disponibilité de la fonction d'information sur l'état des certificats

La fonction d'information sur l'état des certificats doit être disponible 24h/24 7j/7.

Cette fonction doit avoir une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) conforme au tableau suivant :

Description	**Niveau ***	**Niveau ****	**Niveau*****

Durée maximale d'indisponibilité par interruption (panne ou maintenance) de la fonction d'information sur l'état des certificats	4h (jours ouvrés)	4h	2h[68]

Cette fonction doit avoir une durée maximale totale d'indisponibilité par mois conforme au tableau suivant :

Description	**Niveau ***	**Niveau ****	**Niveau*****
Durée maximale totale d'indisponibilité par mois de la fonction d'information sur l'état des certificats	32h (jours ouvrés)	16h	8h

Lorsque la fonction de vérification en ligne du statut d'un certificat (OCSP) est mise en œuvre, le temps de réponse du serveur à la requête reçue[69] doit être au maximum de 10 secondes.

IV.10.3. Dispositifs optionnels

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

IV.11. Fin de la relation entre le RC et l'AC

En cas de fin de relation contractuelle / hiérarchique / réglementaire entre l'AC et l'entité de rattachement du service applicatif avant la fin de validité du certificat, pour une raison ou pour une autre, ce dernier doit être révoqué.

De plus, l'AC doit révoquer un certificat électronique pour lequel il n'y a plus de RC explicitement identifié.

IV.12. Séquestre de clé et recouvrement

Le séquestre des clés privées des services applicatifs est interdit par la présente PC Type.

Les clés privées d'AC ne doivent pas non plus être séquestrées.

IV.12.1. Politique et pratiques de recouvrement par séquestre des clés

Sans objet.

IV.12.2. Politique et pratiques de recouvrement par encapsulation des clés de session

Sans objet.

[68] Il est recommandé que cette durée soit de 1h lorsque le PSCE délivre des certificats d'authentification (personne ou machine), chiffrement et de cachet à des fins de signature de contremarques de temps.

[69] Durée mesurée au niveau du serveur (requête reçue par le serveur et réponse au départ du serveur)

V. Mesures de sécurité non techniques

Les exigences définies dans la suite du présent chapitre sont les exigences minimales que l'AC doit respecter. Elles doivent être complétées et déclinées en mesures de sécurité en fonction de l'environnement réel de l'IGC.

V.1. Mesures de sécurité physique

V.1.1. Situation géographique et construction des sites

La présente PC Type ne formule pas d'exigence spécifique concernant la localisation géographique de l'IGC et de ses composantes.

La construction des sites doit respecter les règlements et normes en vigueur ainsi qu'éventuellement des exigences spécifiques face à des risques de type tremblement de terre ou explosion (proximité d'une zone d'usines ou d'entrepôts de produits chimiques...).

V.1.2. Accès physique

Afin d'éviter toute perte, dommage et compromission des ressources de l'IGC et l'interruption des services de l'AC, les accès aux locaux des différentes composantes de l'IGC doivent être contrôlés.

En outre, toute personne entrant dans ces zones physiquement sécurisées ne doit pas être laissée, pendant une période de temps significative, sans la surveillance d'une personne autorisée.

	Niveau (***)	
Pour les fonctions de génération des certificats, de génération des éléments secrets du RC et de gestion des révocations et, le cas échéant, pour les fonctions de gestion des recouvrements et de séquestre et recouvrement : L'accès doit être strictement limité aux seules personnes nominativement autorisées à pénétrer dans les locaux et la traçabilité des accès doit être assurée. En dehors des heures ouvrables, la sécurité doit être renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logique. Afin d'assurer la disponibilité des systèmes, l'accès aux machines doit être limité aux seules personnes autorisées à effectuer des opérations nécessitant l'accès physique aux machines. Pour cela, les composantes concernées de l'IGC doivent définir un périmètre de sécurité physique où sont installées ces machines. La mise en œuvre de ce périmètre doit permettre de respecter la séparation des rôles de confiance telle que prévue dans la PC de l'AC, en conformité avec la présente PC Type. Notamment, il est recommandé que tout local utilisé en commun avec d'autres fonctions que les fonctions rendues par la composante concernée soit en dehors de ce périmètre de sécurité.		

	Niveau (**)	
Pour les fonctions de génération des certificats, de génération des éléments secrets du RC et de gestion des révocations et, le cas échéant, pour les fonctions de gestion des recouvrements et de séquestre et recouvrement : L'accès doit être strictement limité aux seules personnes autorisées à pénétrer dans les locaux et la traçabilité des accès doit être assurée. En dehors des heures ouvrables, la sécurité doit être renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logique Afin d'assurer la disponibilité des systèmes, il est recommandé que l'accès aux machines soit limité aux seules personnes autorisées à effectuer des opérations nécessitant l'accès physique aux machines.		

Nota - On entend par machines l'ensemble des serveurs, boîtiers cryptographiques, stations et éléments actifs du réseau utilisés pour la mise en œuvre de ces fonctions.

V.1.3. Alimentation électrique et climatisation

Les caractéristiques des équipements d'alimentation électrique et de climatisation doivent permettre de respecter les conditions d'usage des équipements de l'IGC telles que fixées par leurs fournisseurs.

Elles doivent également permettre de respecter les exigences de la présente PC Type, ainsi que les engagements pris par l'AC dans sa PC, en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

V.1.4. Vulnérabilité aux dégâts des eaux

Les moyens de protection contre les dégâts des eaux doivent permettre de respecter les exigences de la présente PC Type, ainsi que les engagements pris par l'AC dans sa PC, en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

V.1.5. Prévention et protection incendie

Les moyens de prévention et de lutte contre les incendies doivent permettre de respecter les exigences de la présente PC Type, ainsi que les engagements pris par l'AC dans sa PC, en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

V.1.6. Conservation des supports

Les différentes informations intervenant dans les activités de l'IGC doivent être identifiées et leurs besoins de sécurité définis (en confidentialité, intégrité et disponibilité). L'AC doit maintenir un inventaire de ces informations. L'AC doit mettre en place des mesures pour éviter la compromission et le vol de ces informations.

Les supports (papier, disque dur, disquette, CD, etc.) correspondant à ces informations doivent être gérés selon des procédures conformes à ces besoins de sécurité. En particulier, ils doivent être manipulés de manière sécurisée afin de protéger les supports contre les dommages, le vol et les accès non autorisés.

Des procédures de gestion doivent protéger ces supports contre l'obsolescence et la détérioration pendant la période de temps durant laquelle l'AC s'engage à conserver les informations qu'ils contiennent.

V.1.7. Mise hors service des supports

En fin de vie, les supports devront être, soit détruits, soit réinitialisés en vue d'une réutilisation, en fonction du niveau de confidentialité des informations correspondantes.

Les procédures et moyens de destruction et de réinitialisation doivent être conformes à ce niveau de confidentialité (voir notamment le guide [972-1]).

V.1.8. Sauvegardes hors site

En complément de sauvegardes sur sites, il est recommandé que les composantes de l'IGC mettent en œuvre des sauvegardes hors sites de leurs applications et de leurs informations. Ces sauvegardes doivent être organisées de façon à assurer une reprise des fonctions de l'IGC après incident le plus rapidement possible, et conforme aux exigences de la présente PC Type et aux engagements de l'AC dans sa PC en matière de disponibilité, en particulier pour les fonctions de gestion des révocations et d'information sur l'état des certificats (cf. chapitres IV.9.5.1 et IV.10.2).

Les informations sauvegardées hors site doivent respecter les exigences de la présente PC Type en matière de protection en confidentialité et en intégrité de ces informations.

	Niveaux (**) et (***)	
Les composantes de l'IGC en charge des fonctions de gestion des révocations et d'information sur l'état des certificats, au moins, doivent obligatoirement mettre en œuvre des sauvegardes hors site permettant une reprise rapide de ces fonctions suite à la survenance d'un sinistre ou d'un évènement affectant gravement et de manière durable la réalisation de ces prestations (destruction du site, etc.). Les fonctions de sauvegarde et de restauration doivent être effectuées par les rôles de confiance appropriés et conformément aux mesures de sécurité procédurales.		

V.2. Mesures de sécurité procédurales

V.2.1. Rôles de confiance

Chaque composante de l'IGC doit distinguer au moins les cinq rôles fonctionnels[70] de confiance suivante :

- **Responsable de sécurité** - Le responsable de sécurité est chargé de la mise en œuvre et du contrôle de la politique de sécurité d'une ou plusieurs composantes de l'IGC. Il gère les contrôles d'accès physiques aux équipements des systèmes de la composante. Il est habilité à prendre connaissance des archives et des journaux d'évènements. Il est responsable des opérations de génération et de révocation des certificats.
- **Responsable d'application** - Le responsable d'application est chargé, au sein de la composante à laquelle il est rattaché, de la mise en œuvre de la politique de certification et de la déclaration des pratiques de certification de l'IGC au niveau de l'application dont il est responsable. Sa responsabilité couvre l'ensemble des fonctions rendues par cette application et des performances correspondantes.
- **Ingénieur système** - Il est chargé de la mise en route, de la configuration et de la maintenance technique des équipements informatiques de la composante. Il assure l'administration technique des systèmes et des réseaux de la composante.
- **Opérateur** - Un opérateur au sein d'une composante de l'IGC réalise, dans le cadre de ses attributions, l'exploitation au quotidien des applications pour les fonctions mises en œuvre par la composante.
- **Contrôleur** - Personne autorisée à accéder et en charge de l'analyse régulière des archives et de l'analyse des journaux d'évènements afin de détecter tout incident, anomalie, tentative de compromission, etc.

En plus de ces rôles de confiance au sein de chaque composante de l'IGC, et en fonction de l'organisation de l'IGC et des outils mis en œuvre, l'AC peut être amenée à distinguer également en tant que rôle de confiance, les rôles de porteur de parts de secrets d'IGC : cf. chapitres VI.1 et VI.2.

Ces porteurs de parts de secrets ont la responsabilité d'assurer la confidentialité, l'intégrité et la disponibilité

[70] En fonction de la taille de l'entité concernée, de la charge de travail correspondant au rôle, etc., ainsi qu'en fonction des exigences de sécurité et de continuité d'activité, un même rôle fonctionnel peut / doit être tenu par différentes personnes.

des parts qui leur sont confiés.

De manière générale, des procédures doivent être établies et appliquées pour tous les rôles administratifs et les rôles de confiance ayant trait à la fourniture de services de certification. Ces rôles doivent être décrits et définis dans la description des postes propre à chaque entité opérant une des composantes de l'IGC sur les principes de séparation des responsabilités et du moindre privilège. Ces rôles doivent déterminer la sensibilité du poste, en fonction des responsabilités et des niveaux d'accès, des vérifications des antécédents et de la formation et de la sensibilité des employés.

Lorsqu'appropriées, ces descriptions doivent différencier entre les fonctions générales et les fonctions spécifiques à l'AC. L'AC doit implémenter techniquement ce principe de moindre privilège via les mécanismes de contrôle d'accès qu'elle met en œuvre.

De plus, les opérations de sécurité de l'AC doivent être séparées des opérations normales. Les responsabilités des opérations de sécurité incluent :

- Les procédures et responsabilités opérationnelles ;
- La planification et la validation des systèmes sécurisés ;
- La protection contre les logiciels malicieux ;
- L'entretien ;
- La gestion de réseaux ;
- La surveillance active des journaux d'audit, l'analyse des évènements et les suites ;
- La manipulation et la sécurité des supports ;
- L'échange de données et de logiciels.

Ces responsabilités sont gérées par les opérations de sécurité de l'AC, mais peuvent être effectivement réalisées par du personnel opérationnel non spécialiste (en étant supervisé), tel que défini dans la politique de sécurité appropriée et les documents relatifs aux rôles et responsabilités.

Des mesures doivent être mises en place pour empêcher que des équipements, des informations, des supports et des logiciels ayant trait aux services de l'AC soient sortis du site sans autorisation.

V.2.2. Nombre de personnes requises par tâches

Selon le type d'opération effectuée, le nombre et la qualité des personnes devant nécessairement être présentes, en tant qu'acteurs ou témoins, peuvent être différents.

Pour des raisons de sécurité, il est demandé de répartir les fonctions sensibles sur plusieurs personnes. La présente PC Type définit un certain nombre d'exigences concernant cette répartition, notamment pour les opérations liées aux modules cryptographiques de l'IGC (cf. chapitre VI).

La DPC de l'AC devra préciser quelles sont les opérations nécessitant l'intervention de plusieurs personnes et quelles sont les contraintes que ces personnes doivent respecter (positions dans l'organisation, liens hiérarchiques, etc.).

V.2.3. Identification et authentification pour chaque rôle

Chaque entité opérant une composante de l'IGC doit faire vérifier l'identité et les autorisations de tout membre de son personnel amené à travailler au sein de la composante avant de lui attribuer un rôle et les droits correspondants, notamment :

- Que son nom soit ajouté aux listes de contrôle d'accès aux locaux de l'entité hébergeant la

composante concernée par le rôle ;

- Que son nom soit ajouté à la liste des personnes autorisées à accéder physiquement à ces systèmes ;
- Le cas échéant et en fonction du rôle, qu'un compte soit ouvert à son nom dans ces systèmes ;
- Éventuellement, que des clés cryptographiques et/ou un certificat lui soient délivrés pour accomplir le rôle qui lui est dévolu dans l'IGC.

Ces contrôles doivent être décrits dans la DPC de l'AC et doivent être conformes à la politique de sécurité de la composante.

Chaque attribution d'un rôle à un membre du personnel de l'IGC doit être notifiée par écrit. Ce rôle doit être clairement mentionné et décrit dans sa fiche de poste.

V.2.4. Rôles exigeant une séparation des attributions

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre. Pour les rôles de confiance, il est néanmoins recommandé qu'une même personne ne détienne pas plusieurs rôles et, au minimum, les exigences ci-dessous de non cumul doivent être respectées.

Les attributions associées à chaque rôle doivent être décrites dans la DPC de l'AC et être conformes à la politique de sécurité de la composante concernée.

	Niveaux (**) et (***)	
Concernant les rôles de confiance, les cumuls suivants sont interdits : ➢ Responsable de sécurité et ingénieur système / opérateur / contrôleur ; ➢ Ingénieur système, opérateur et contrôleur.		

	Niveau (*)	
Concernant les rôles de confiance, le cumul suivant est interdit ➢ Responsable de sécurité et ingénieur système.		

V.3. Mesures de sécurité vis-à-vis du personnel

V.3.1. Qualifications, compétences et habilitations requises

Tous les personnels amenés à travailler au sein de composantes de l'IGC doivent être soumis à une clause de confidentialité vis-à-vis de leur employeur. Dans le cas des agents, ceux-ci sont soumis à leur devoir de réserve.

Chaque entité opérant une composante de l'IGC doit s'assurer que les attributions de ses personnels, amenés à travailler au sein de la composante, correspondent à leurs compétences professionnelles.

Le personnel d'encadrement doit posséder l'expertise appropriée à son rôle et être familier des procédures de sécurité en vigueur au sein de l'IGC.

L'AC doit informer toute personne intervenant dans des rôles de confiance de l'IGC :

- de ses responsabilités relatives aux services de l'IGC,
- des procédures liées à la sécurité du système et au contrôle du personnel, auxquelles elle doit se

conformer.

En particulier, les personnes intervenant dans des rôles de confiance doivent y être formellement affectées par l'encadrement supérieur chargé de la sécurité.

V.3.2. Procédures de vérification des antécédents

Chaque entité opérant une composante de l'IGC doit mettre en œuvre tous les moyens légaux dont elle peut disposer pour s'assurer de l'honnêteté de ses personnels amenés à travailler au sein de la composante. Ces personnels ne doivent notamment pas avoir de condamnation de justice en contradiction avec leurs attributions.

A ce titre, l'employeur peut demander à ces personnels la communication d'une copie du bulletin n°3 de leur casier judiciaire.

L'employeur peut décider en cas de refus de communiquer cette copie ou en cas de présence de condamnation de justice incompatible avec les attributions de la personne, de lui retirer ces attributions.

Les personnes ayant un rôle de confiance ne doivent pas souffrir de conflit d'intérêts préjudiciables à l'impartialité de leurs tâches.

Ces vérifications doivent être menées préalablement à l'affectation à un rôle de confiance et revues régulièrement (au minimum tous les 3 ans).

V.3.3. Exigences en matière de formation initiale

Le personnel doit être préalablement formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité qu'il met en œuvre et qu'il doit respecter, correspondant à la composante au sein de laquelle il opère.

Les personnels doivent avoir connaissance et comprendre les implications des opérations dont ils ont la responsabilité.

V.3.4. Exigences et fréquence en matière de formation continue

Le personnel concerné doit recevoir une information et une formation adéquates préalablement à toute évolution dans les systèmes, dans les procédures, dans l'organisation, etc. en fonction de la nature de ces évolutions.

V.3.5. Fréquence et séquence de rotation entre différentes attributions

La présente PC Type ne formule pas d'exigence spécifique sur le sujet. A préciser par l'AC dans sa DPC.

V.3.6. Sanctions en cas d'actions non autorisées

À préciser par l'AC dans sa DPC.

V.3.7. Exigences vis-à-vis du personnel des prestataires externes

Le personnel des prestataires externes intervenant dans les locaux et/ou sur les composantes de l'IGC doit également respecter les exigences du présent chapitre V.3. Ceci doit être traduit en clauses adéquates dans les contrats avec ces prestataires.

V.3.8. Documentation fournie au personnel

Chaque personnel doit disposer au minimum de la documentation adéquate concernant les procédures opérationnelles et les outils spécifiques qu'il met en œuvre ainsi que les politiques et pratiques générales de

la composante au sein de laquelle il travaille. En particulier, il doit lui être remis la ou les politique(s) de sécurité l'impactant.

V.4. Procédures de constitution des données d'audit

La journalisation d'évènements consiste à les enregistrer de façon manuelle ou automatique. Les fichiers résultants, sous forme papier ou électronique, doivent rendre possible la traçabilité et l'imputabilité des opérations effectuées.

V.4.1. Type d'évènements à enregistrer

Concernant les systèmes liés aux fonctions qui sont mises en œuvre dans le cadre de l'IGC, chaque entité opérant une composante de l'IGC doit au minimum journaliser les évènements tels que décrits ci-dessous, sous forme électronique. La journalisation doit être automatique, dès le démarrage d'un système et sans interruption jusqu'à l'arrêt de ce système.

- Création / modification / suppression de comptes utilisateur (droits d'accès) et des données d'authentification correspondantes (mots de passe, certificats, etc.) ;
- Démarrage et arrêt des systèmes informatiques et des applications ;
- Évènements liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de journalisation, actions prises suite à une défaillance de la fonction de journalisation ;
- Connexion / déconnexion des utilisateurs ayant des rôles de confiance, et les tentatives non réussies correspondantes.

D'autres évènements doivent aussi être recueillis, par des moyens électroniques ou manuels. Ce sont ceux concernant la sécurité et qui ne sont pas produits automatiquement par les systèmes informatiques, notamment :

- Les accès physiques ;
- Les actions de maintenance et de changements de la configuration des systèmes ;
- Les changements apportés au personnel ;
- les actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation, renseignements personnels sur les RC,...).

En plus de ces exigences de journalisation communes à toutes les composantes et toutes les fonctions de l'IGC, des évènements spécifiques aux différentes fonctions de l'IGC doivent également être journalisés, notamment[71] :

- Réception d'une demande de certificat (initiale et renouvellement) ;
- Validation / rejet d'une demande de certificat ;
- Évènements liés aux clés de signature et aux certificats d'AC (génération (cérémonie des clés), sauvegarde / récupération, révocation, renouvellement, destruction...) ;

[71] Les évènements à journaliser doivent être adaptés à l'organisation et l'architecture de l'IGC. Notamment, les échanges entre fonctions de l'IGC et/ou entre composantes de l'IGC peuvent nécessiter une journalisation pour assurer une traçabilité des actions.

- Le cas échéant, génération des éléments secrets du service applicatif (bi-clé, codes d'activation…) ;
- Génération des certificats de services applicatifs ;
- Transmission des certificats aux RC et, selon les cas, acceptations / rejets explicites par les RC ;
- Le cas échéant, remise du dispositif de protection du service applicatif au RC ;
- Publication et mise à jour des informations liées à l'AC (PC, certificats d'AC, conditions générales d'utilisation, etc.) ;
- Réception d'une demande de révocation ;
- Validation / rejet d'une demande de révocation ;
- Génération puis publication des LCR (et éventuellement des deltaLCR) ou des, requêtes / réponses OCSP ;

Chaque enregistrement d'un évènement dans un journal doit contenir au minimum les champs suivants :

- Type de l'évènement ;
- Nom de l'exécutant ou référence du système déclenchant l'évènement ;
- Date et heure de l'évènement (l'heure exacte des évènements significatifs de l'AC concernant l'environnement, la gestion de clé et la gestion de certificat doit être enregistrée) ;
- Résultat de l'évènement (échec ou réussite).

L'imputabilité d'une action revient à la personne, à l'organisme ou au système l'ayant exécutée. Le nom ou l'identifiant de l'exécutant doit figurer explicitement dans l'un des champs du journal d'évènements.

De plus, en fonction du type de l'évènement, chaque enregistrement devra également contenir les champs suivants :

- Destinataire de l'opération ;
- Nom du demandeur de l'opération ou référence du système effectuant la demande ;
- Nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes) ;
- Cause de l'évènement ;
- Toute information caractérisant l'évènement (par exemple, pour la génération d'un certificat, le numéro de série de ce certificat).

Les opérations de journalisation doivent être effectuées au cours du processus.

En cas de saisie manuelle, l'écriture doit se faire, sauf exception, le même jour ouvré que l'évènement.

Les évènements et données spécifiques à journaliser doivent être documentés par l'AC.

V.4.2. Fréquence de traitement des journaux d'évènements

Cf. chapitre V.4.8 ci-dessous.

V.4.3. Période de conservation des journaux d'évènements

Les journaux d'évènements doivent être conservés sur site pendant au moins un (1) mois. Ils doivent être archivés le plus rapidement possible après leur génération et au plus tard sous un (1) mois (recouvrement possible entre la période de conservation sur site et la période d'archivage).

V.4.4. Protection des journaux d'évènements

La journalisation doit être conçue et mise en œuvre de façon à limiter les risques de contournement, de modification ou de destruction des journaux d'évènements. Des mécanismes de contrôle d'intégrité doivent permettre de détecter toute modification, volontaire ou accidentelle, de ces journaux.

Les journaux d'évènements doivent être protégés en disponibilité (contre la perte et la destruction partielle ou totale, volontaire ou non).

Le système de datation des évènements doit respecter les exigences du chapitre VI.8.

La définition de la sensibilité des journaux d'évènements dépend de la nature des informations traitées et du métier. Elle peut entraîner un besoin de protection en confidentialité.

V.4.5. Procédure de sauvegarde des journaux d'évènements

Chaque entité opérant une composante de l'IGC doit mettre en place les mesures requises afin d'assurer l'intégrité et la disponibilité des journaux d'évènements pour la composante considérée, conformément aux exigences de la présente PC Type.

V.4.6. Système de collecte des journaux d'évènements

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

V.4.7. Notification de l'enregistrement d'un évènement au responsable de l'évènement

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

V.4.8. Évaluation des vulnérabilités

Chaque entité opérant une composante de l'IGC doit être en mesure de détecter toute tentative de violation de l'intégrité de la composante considérée.

Les journaux d'évènements doivent être contrôlés une (1) fois par jour ouvré, afin d'identifier des anomalies liées à des tentatives en échec.

Les journaux doivent être analysés dans leur totalité au minimum selon la fréquence suivante :

Description	**Niveau ***	**Niveau ****	**Niveau *****
Fréquence d'analyse complète des journaux d'évènements	1 fois toutes les 2 semaines et dès la détection d'une anomalie	1 fois par semaine et dès la détection d'une anomalie	1 fois par jour ouvré et dès la détection d'une anomalie

Cette analyse donnera lieu à un résumé dans lequel les éléments importants sont identifiés, analysés et expliqués. Le résumé doit faire apparaître les anomalies et les falsifications constatées.

Par ailleurs, un rapprochement entre les différents journaux d'évènements de fonctions qui interagissent entre elles (autorité d'enregistrement et fonction de génération, fonction de gestion des révocations et fonction d'information sur l'état des certificats, etc.) doit être effectué à une fréquence au moins égale à celle déterminée dans le tableau suivant, ceci afin de vérifier la concordance entre évènements dépendants et contribuer ainsi à révéler toute anomalie.

Description	**Niveau ***	**Niveau ****	**Niveau *****

Fréquence de rapprochement des journaux d'évènements	1 fois par mois	1 fois par semaine

V.5. Archivage des données

V.5.1. Types de données à archiver

Des dispositions en matière d'archivage doivent également être prises par l'AC. Cet archivage doit permettre d'assurer la pérennité des journaux constitués par les différentes composantes de l'IGC.

Il doit également permettre la conservation des pièces papier liées aux opérations de certification, ainsi que leur disponibilité en cas de nécessité.

Les données à archiver sont au moins les suivantes :

- Les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- Les PC ;
- Les DPC ;
- Les conditions générales d'utilisation ;
- Les accords contractuels avec d'autres AC ;
- Les certificats et LCR ou réponses OCSP tels qu'émis ou publiés ;
- Les récépissés ou notifications (à titre informatif) ;
- Les engagements signés des MC ;
- Les justificatifs d'identité des RC et, le cas échéant, de leur entité de rattachement ;
- Les justificatifs de possession des services applicatifs ainsi que leurs noms (FQDN pour les certificats de serveur ou nom d'application pour les certificats de cachet) ;
- Les journaux d'évènements des différentes entités de l'IGC.

V.5.2. Période de conservation des archives

Dossiers de demande de certificat

Tout dossier de demande de certificat accepté doit être archivé aussi longtemps que nécessaire, et pendant au moins sept (7) ans, pour les besoins de fourniture de la preuve de la certification dans des procédures légales, conformément à la loi applicable.

Les facteurs à prendre en compte dans la détermination de la «loi applicable» sont la loi du pays dans lequel l'AC est établie.

Lorsque les RC sont enregistrés par une autorité d'enregistrement dans un autre pays que celui ou l'AC est établie, alors il convient que cette AE applique également la réglementation de son propre pays.

Lorsque des MC sont également dans un autre pays, alors il convient de prendre également en compte les exigences contractuelles et légales applicables à ces MC.

La durée de conservation des dossiers d'enregistrement doit être portée à la connaissance du RC ou du MC.

Au cours de cette durée d'opposabilité des documents, le dossier de demande de certificat doit pouvoir être présenté par l'AC lors de toute sollicitation par les autorités habilitées.

Ce dossier, complété par les mentions consignées par l'AE ou le MC, doit permettre de retrouver l'identité réelle du RC responsable, à un instant «t» du service applicatif désigné dans le certificat émis par l'AC.

Certificats et LCR et réponses OCSP émis par l'AC

Les certificats de services applicatifs et d'AC, ainsi que les LCR / LAR, doivent être archivés pendant au moins cinq (5) années après leur expiration.

Les réponses OCSP produites doivent être archivées pendant au moins trois mois après leur expiration.

Journaux d'évènements

Les journaux d'évènements traités au chapitre V.4 seront archivés pendant sept (7) années après leur génération. Les moyens mis en œuvre par l'AC pour leur archivage devront offrir le même niveau de sécurité que celui visé lors de leur constitution. En particulier, l'intégrité des enregistrements devra être assurée tout au long de leur cycle de vie.

Autres journaux

Pour l'archivage des journaux autres que les journaux d'évènements traités au chapitre V.4, aucune exigence n'est stipulée. L'AC précisera dans sa DPC les moyens mis en œuvre pour archiver ces journaux.

V.5.3. Protection des archives

Pendant tout le temps de leur conservation, les archives, et leurs sauvegardes, doivent :

- Être protégées en intégrité ;
- Être accessibles aux personnes autorisées ;
- Pouvoir être relues et exploitées.

L'AC précisera dans sa DPC les moyens mis en œuvre pour archiver les pièces en toute sécurité.

V.5.4. Procédure de sauvegarde des archives

La présente PC Type ne formule pas d'exigence spécifique sur le sujet. À préciser par l'AC dans ses PC et DPC. Le niveau de protection des sauvegardes doit être au moins équivalent au niveau de protection des archives.

V.5.5. Exigences d'horodatage des données

Cf. chapitre V.4.4 pour la datation des journaux d'évènements.

Le chapitre VI.8 précise les exigences en matière de datation / horodatage.

V.5.6. Système de collecte des archives

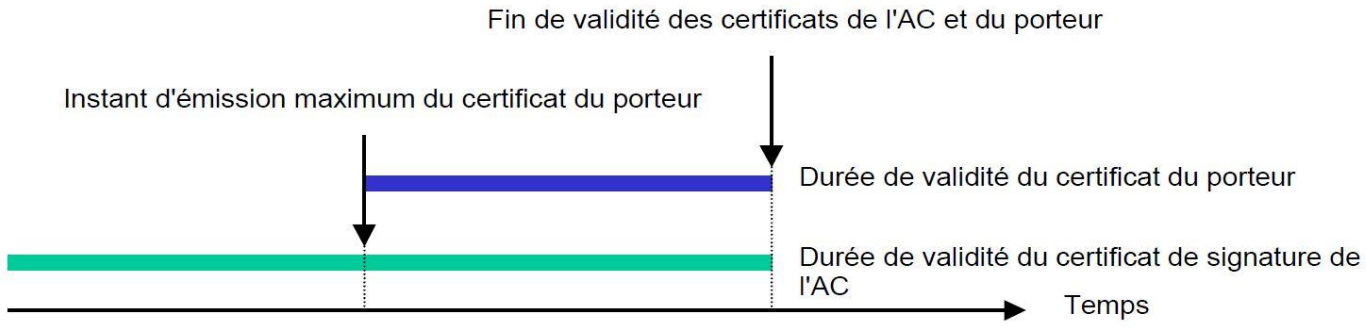
La présente PC Type ne formule pas d'exigence spécifique sur le sujet, si ce n'est que le système de collecte des archives, qu'il soit interne ou externe, doit respecter les exigences de protection des archives concernées.

V.5.7. Procédures de récupération et de vérification des archives

Les archives (papier et électroniques) doivent pouvoir être récupérées dans un délai inférieur à deux (2) jours ouvrés, sachant que seule l'AC peut accéder à toutes les archives (par opposition à une entité opérant une composante de l'IGC qui ne peut récupérer et consulter que les archives de la composante considérée).

V.6. Changement de clé d'AC

L'AC ne peut pas générer de certificat dont la date de fin serait postérieure à la date d'expiration du certificat correspondant de l'AC. Pour cela la période de validité de ce certificat de l'AC doit être supérieure à celle des certificats qu'elle signe.



Au regard de la date de fin de validité de ce certificat, son renouvellement doit être demandé dans un délai au moins égal à la durée de vie des certificats signés par la clé privée correspondante.

Dès qu'une nouvelle bi-clé d'AC est générée, seule la nouvelle clé privée doit être utilisée pour signer des certificats.

Le certificat précédent reste utilisable pour valider les certificats émis sous cette clé et ce jusqu'à ce que tous les certificats signés avec la clé privée correspondante aient expiré.

V.7. Reprise suite à compromission et sinistre

V.7.1. Procédures de remontée et de traitement des incidents et des compromissions

Chaque entité opérant une composante de l'IGC doit mettre en œuvre des procédures et des moyens de remontée et de traitement des incidents, notamment au travers de la sensibilisation et de la formation de ses personnels et au travers de l'analyse des différents journaux d'évènements. Ces procédures et moyens doivent permettre de minimiser les dommages dus à des incidents de sécurité et des dysfonctionnements.

Dans le cas d'un incident majeur, tel que la perte, la suspicion de compromission, la compromission, le vol de la clé privée de l'AC, l'évènement déclencheur est la constatation de cet incident au niveau de la composante concernée, qui doit en informer immédiatement l'AC. Le cas de l'incident majeur doit être impérativement traité dès détection et la publication de l'information de révocation du certificat, s'il y a lieu, doit être faite dans la plus grande urgence, voire immédiatement, par tout moyen utile et disponible (presse, site Internet, récépissé …).

Si l'un des algorithmes, ou des paramètres associés, utilisés par l'AC ou ses serveurs devient insuffisant pour son utilisation prévue restante, alors l'AC doit :

- Informer tous les RC et les tiers utilisateurs de certificats avec lesquels l'AC a passé des accords ou a d'autres formes de relations établies. En complément, cette information doit être mise à disposition des autres utilisateurs de certificats ;
- Révoquer tout certificat concerné.

V.7.2. Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données)

Chaque composante de l'IGC doit disposer d'un plan de continuité d'activité permettant de répondre aux exigences de disponibilité des différentes fonctions de l'IGC découlant de la présente PC Type, des engagements de l'AC dans sa propre PC notamment en ce qui concerne les fonctions liées à la publication et / ou liées à la révocation des certificats.

Ce plan doit être testé au minimum suivant la fréquence ci-dessous :

Description	**Niveau***	**Niveau****	**Niveau*****
Fréquence de test du plan de continuité	1 fois tous les 3 ans	1 fois tous les 2 ans	1 fois par an

V.7.3. Procédures de reprise en cas de compromission de la clé privée d'une composante

Le cas de compromission d'une clé d'infrastructure ou de contrôle d'une composante doit être traité dans le plan de continuité de la composante (cf. chapitre V.7.2) en tant que sinistre.

Dans le cas de compromission d'une clé d'AC, le certificat correspondant doit être immédiatement révoqué : cf. chapitre IV.9.

En outre, l'AC doit au minimum respecter les engagements suivants :

- Informer les entités suivantes de la compromission : tous les RC, MC et les autres entités avec lesquelles l'AC a passé des accords ou à d'autres formes de relations établies, parmi lesquelles des tiers utilisateurs et d'autres AC. En complément, cette information doit être mise à disposition des autres tiers utilisateurs ;
- Indiquer que les certificats et les informations de statut de révocation délivrés en utilisant cette clé d'AC peuvent ne plus être valables.

V.7.4. Capacités de continuité d'activité suite à un sinistre

Les différentes composantes de l'IGC doivent disposer des moyens nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les exigences de la présente PC Type et de la PC de l'AC (cf. chapitre V.7.2).

V.8. Fin de vie de l'IGC

Une ou plusieurs composantes de l'IGC peuvent être amenées à cesser leur activité ou à la transférer à une autre entité pour des raisons diverses.

L'AC doit prendre les dispositions nécessaires pour couvrir les coûts permettant de respecter ces exigences minimales dans le cas où l'AC serait en faillite ou pour d'autres raisons serait incapable de couvrir ces coûts par elle-même, ceci, autant que possible, en fonction des contraintes de la législation applicable en matière de faillite.

Le transfert d'activité est défini comme la fin d'activité d'une composante de l'IGC ne comportant pas d'incidence sur la validité des certificats émis antérieurement au transfert considéré et la reprise de cette activité organisée par l'AC en collaboration avec la nouvelle entité.

La cessation d'activité est définie comme la fin d'activité d'une composante de l'IGC comportant une incidence sur la validité des certificats émis antérieurement à la cessation concernée.

Transfert d'activité ou cessation d'activité[72] affectant une composante de l'IGC

Afin d'assurer un niveau de confiance constant pendant et après de tels évènements, l'AC doit entre autres obligations :

1) Mettre en place des procédures dont l'objectif est d'assurer un service constant en particulier en matière d'archivage (notamment, archivage des certificats de services applicatifs et des informations relatives aux certificats).
2) Assurer la continuité de la révocation (prise en compte d'une demande de révocation et publication de l'état des certificats), conformément aux exigences de disponibilité pour ses fonctions définies dans la présente PC Type. À défaut, les applications de l'Administration refuseront les certificats émis par des AC dont les informations sur l'état de révocation des certificats en cours de validité ne seraient plus accessibles, même si le certificat électronique est encore valide.

Des précisions quant aux engagements suivants doivent ainsi être annoncées par l'AC dans sa PC.

Dans la mesure où les changements envisagés peuvent avoir des répercussions sur les engagements vis à vis des RC ou des utilisateurs de certificats, l'AC doit les en aviser aussitôt que nécessaire et, au moins, sous le délai d'un (1) mois.

Cessation d'activité affectant l'AC

La cessation d'activité peut être totale ou partielle (par exemple : cessation d'activité pour une famille de certificats donnée seulement). La cessation partielle d'activité doit être progressive de telle sorte que seules les obligations visées aux 1), 2), et 3) ci-dessous soient à exécuter par l'AC, ou une entité tierce qui reprend les activités, lors de l'expiration du dernier certificat émis par elle.

Dans l'hypothèse d'une cessation d'activité totale, l'AC ou, en cas d'impossibilité, toute entité qui lui serait substituée de par l'effet d'une loi, d'un règlement, d'une décision de justice ou bien d'une convention antérieurement conclue avec cette entité, devra assurer la révocation des certificats et la publication des LCR conformément aux engagements pris dans sa PC.

L'AC doit stipuler dans ses pratiques les dispositions prises en cas de cessation de service. Elles doivent inclure :

- La notification des entités affectées ;
- Le transfert de ses obligations à d'autres parties ;
- La gestion du statut de révocation pour les certificats non-expirés qui ont été délivrés.

Lors de l'arrêt du service, l'AC doit :

1) S'interdire de transmettre la clé privée lui ayant permis d'émettre des certificats ;
2) Prendre toutes les mesures nécessaires pour la détruire ou la rendre inopérante ;
3) Révoquer son certificat ;
4) Révoquer tous les certificats qu'elle a signés et qui seraient encore en cours de validité ;
5) Informer (par exemple par récépissé) tous les MC et/ou RC des certificats révoqués ou à révoquer,

[72] Cessation d'activité d'une composante autre que l'AC.

ainsi que leur entité de rattachement le cas échéant (cf. chapitre III.2.3)

VI. Mesures de sécurité technique

Les exigences définies dans la suite du présent chapitre sont les exigences minimales que l'AC doit respecter. Elles doivent être complétées et déclinées en mesures de sécurité en fonction de l'environnement réel de l'IGC.

VI.1. Génération et installation de bi-clés

VI.1.1. Génération des bi-clés

VI.1.1.1. Clés d'AC

La génération des clés de signature d'AC doit être effectuée dans un environnement sécurisé (cf. chapitre V).

Les clés de signature d'AC doivent être générées et mises en œuvre dans un module cryptographique conforme aux exigences du chapitre XI ci-dessous pour le niveau de sécurité considéré.

La génération des clés de signature d'AC doit être effectuée dans des circonstances parfaitement contrôlées, par des personnels dans des rôles de confiance (cf. chapitre V.2.1), dans le cadre de «cérémonies de clés». Ces cérémonies doivent se dérouler suivant des scripts préalablement définis.

Selon le cas, l'initialisation de l'IGC et/ou la génération des clés de signature d'AC peut s'accompagner de la génération de parts de secrets d'IGC. Ces parts de secrets sont des données permettant de gérer et de manipuler, ultérieurement à la cérémonie de clés, les clés privées de signature d'AC, notamment, de pouvoir initialiser ultérieurement de nouveaux modules cryptographiques avec les clés de signatures d'AC.

Par exemple, ces parts de secrets peuvent être des parties de la (ou des) clé(s) privée(s) d'AC, décomposée(s) suivant un schéma à seuil de Shamir (n parties parmi m sont nécessaires et suffisantes pour reconstituer la clé privée), ou encore, il peut s'agir de données permettant de déclencher le chargement sécurisé, dans un nouveau module cryptographique, de la (ou des) clé(s) privée(s) d'AC sauvegardée(s) lors de la cérémonie de clés.

Suite à leur génération, les parts de secrets doivent être remises à des porteurs de parts de secrets désignés au préalable et habilités à ce rôle de confiance par l'AC. Quelle qu'en soit la forme (papier, support magnétique ou confiné dans une carte à puce ou une clé USB), un même porteur ne peut détenir plus d'une part de secrets d'une même AC à un moment donné. Chaque part de secrets doit être mise en œuvre par son porteur. Ce dernier peut le cas échéant, en accord avec le responsable de l'IGC, notamment en cas d'indisponibilité au moment où la cérémonie des clés doit être opérée, transférer temporairement ou définitivement cette part de secret à un personnel désigné.

	Niveau (***)	
Les cérémonies de clés doivent se dérouler sous le contrôle d'au moins deux personnes ayant des rôles de confiance et en présence de plusieurs témoins dont au moins deux sont externes à l'AC et sont impartiaux. Les témoins attestent, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement défini. Il est recommandé qu'il y ait parmi les témoins un officier public (huissier ou notaire). Toute manipulation de données secrètes en clair (clés privées d'AC, clés privées des services applicatifs, parts de secrets d'IGC) doit se faire dans un environnement protégé contre les rayonnements parasites compromettant : matériels protégés, cage de Faraday, locaux limitant les risques de fuites d'information par observation visuelle ou rayonnements électromagnétiques, etc.		

	Niveau (**)	
Les cérémonies de clés doivent se dérouler sous le contrôle d'au moins deux personnes ayant des rôles de confiance et en présence de plusieurs témoins dont au moins un est externe à l'AC et est impartial. Les témoins attestent, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement défini.		

	Niveau (*)	
Les cérémonies de clés doivent se dérouler sous le contrôle d'au moins une personne ayant au moins un rôle de confiance et en présence de plusieurs témoins. Les témoins attestent, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement défini.		

VI.1.1.2. Clés du service applicatif générées par l'AC

Les exigences de ce paragraphe ne s'appliquent que si la bi-clé du service applicatif est générée par l'AC.

La génération des clés des services applicatifs doit être effectuée dans un environnement sécurisé (cf. chapitre V).

Les bi-clés des services applicatifs doivent être générées :

- soit directement dans le dispositif de protection des éléments secrets du service applicatif conforme aux exigences du chapitre XII ci-dessous pour le niveau de sécurité considéré,
- soit dans un module cryptographique conforme aux exigences du chapitre XI ci-dessous pour le niveau de sécurité considéré, puis transférées de manière sécurisée dans le dispositif de protection des éléments secrets du service applicatif sans que l'AC n'en garde aucune copie.

VI.1.1.3. Clés du service applicatif générées au niveau du service applicatif

Dans le cas où la bi-clé est générée au niveau du service applicatif, cette génération doit être effectuée dans un dispositif répondant aux exigences du chapitre XII ci-dessous pour le niveau de sécurité considéré. L'AC doit s'en assurer auprès du RC, au minimum au travers d'un engagement contractuel clair et explicite du RC vis-à-vis de l'AC.

VI.1.2. Transmission de la clé privée au service applicatif

Si l'AC génère la bi-clé du service applicatif (cf. chapitre VI.1.1.2), la clé privée doit être transmise au service applicatif de manière sécurisée, afin d'en assurer la confidentialité et l'intégrité. Cette transmission doit se faire. Les réponses OCSP produites doivent être archivées pendant au moins trois mois après leur expiration, directement dans le dispositif de protection des éléments secrets destiné au service applicatif, ou suivant un moyen équivalent.

	Niveau (***)	
Si la vérification de l'identité du RC par l'AE via un face-à-face physique n'a pas eu lieu au moment de l'enregistrement du porteur (chapitre III.2.3), celle-ci doit être effectuée lors de la remise de la bi-clé générée par l'AC en présence du RC.		

	Niveau (**)	
Si la vérification de l'identité du RC par l'AE via un face-à-face physique ou via l'emploi d'un procédé de signature électronique conforme au minimum aux exigences du niveau (**) n'a pas eu lieu au moment de l'enregistrement du porteur (chapitre III.2.3), celle-ci doit être effectuée lors de la remise de la bi-clé		

générée par l'AC en présence du RC.

Il est interdit à l'autorité de certification de conserver ou de dupliquer cette clé privée.

VI.1.3. Transmission de la clé publique à l'AC

En cas de transmission de la requête de demande de certificat de service applicatif au format PKCS10, ou tout autre conteneur offrant les mêmes garanties de sécurité, vers une composante de l'AC (cas où la bi-clé est générée au niveau du service applicatif), la clé devra être protégée en intégrité et son origine devra en être authentifiée.

VI.1.4. Transmission de la clé publique de l'AC aux utilisateurs de certificats

Les clés publiques de vérification de signature de l'AC doivent être diffusées auprès des utilisateurs de certificats par un moyen qui en assure l'intégrité de bout en bout et qui en authentifie l'origine.

Une clé publique d'AC peut être diffusée dans un certificat qui est soit un certificat racine autosigné, soit un certificat rattaché à une hiérarchie d'AC jusqu'à une AC racine (cf. chapitre I.4.1.2 ci-dessus).

Un certificat racine autosigné ne permet pas de garantir par lui-même que la clé publique correspondante appartient bien à l'AC considérée. Sa diffusion doit s'accompagner de la diffusion, via des sources de confiance, de l'empreinte numérique du certificat, et éventuellement de la clé publique, ainsi que d'une déclaration qu'il s'agit bien d'une clé publique de l'AC.

La clé publique de l'AC, ainsi que les informations correspondantes (certificat, empreintes numériques, déclaration d'appartenance) doivent pouvoir être récupérées aisément par les utilisateurs de certificats.

VI.1.5. Tailles des clés

Les clés d'A et de services applicatifs doivent respecter les exigences de caractéristiques (tailles, algorithmes, etc.) du document [RGS_A4].

VI.1.6. Vérification de la génération des paramètres des bi-clés et de leur qualité

L'équipement de génération de bi-clés doit utiliser des paramètres respectant les normes de sécurité propres à l'algorithme correspondant à la bi-clé (cf. [RGS_A4]).

Les paramètres et les algorithmes utilisés doivent être documentés par l'AC.

VI.1.7. Objectifs d'usage de la clé

L'utilisation d'une clé privée d'AC et du certificat associé est strictement limitée à la signature de certificats, de LCR / LAR et/ou de réponses OCSP (cf. chapitre I.4.1.2 et document [RGS_A_4]).

L'utilisation de la clé privée du service applicatif et du certificat associé est strictement limitée à la fonction de sécurité concernée (cf. chapitres I.5.1.1, IV.5 et le [RGS_A4]).

VI.2. Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques

VI.2.1. Standards et mesures de sécurité pour les modules cryptographiques

VI.2.1.1. Modules cryptographiques de l'AC

Les modules cryptographiques, utilisés par l'AC, pour la génération et la mise en œuvre de ses clés de signature, ainsi que le cas échéant pour la génération des clés des services applicatifs, doivent être des modules cryptographiques répondant au minimum aux exigences du chapitre XI ci-dessous pour le niveau

de sécurité considéré.

VI.2.1.2. Dispositifs de protection des éléments secrets du service applicatif

Les dispositifs de protection des clés privées des services applicatifs, pour la mise en œuvre de leurs clés privées, doivent respecter les exigences du chapitre XII ci-dessous pour le niveau de sécurité considéré.

Si l'AC ne fournit pas elle-même ce dispositif au RC, elle doit s'assurer auprès du RC de la conformité du dispositif mis en œuvre par le serveur, au minimum au travers d'un engagement contractuel clair et explicite du RC vis-à-vis de l'AC.

En revanche, lorsque l'AC fournit ce dispositif au RC, directement ou indirectement, elle doit s'assurer que :

- La préparation des dispositifs de protection est contrôlée de façon sécurisée ;
- Les dispositifs de protection sont stockés et distribués de façon sécurisée ;
- Les désactivations et réactivations des dispositifs protection sont contrôlées de façon sécurisée.

Note : L'AC peut s'inspirer du document [ExigencesSitesPerso] pour répondre à ces exigences.

VI.2.2. Contrôle de la clé privée par plusieurs personnes

Ce chapitre porte sur le contrôle de la clé privée de l'AC pour l'exportation / l'importation hors / dans un module cryptographique. La génération de la bi-clé est traitée au chapitre VI.1.1.1, l'activation de la clé privée au chapitre VI.2.8 et sa destruction au chapitre VI.2.10.

	Niveaux (**) et (***)	
Le contrôle des clés privées de signature de l'AC doit être assuré par du personnel de confiance (porteurs de secrets d'IGC) et via un outil mettant en œuvre le partage des secrets (systèmes où n exploitants parmi m doivent s'authentifier, avec n au moins égal à 2).		

	Niveau (*)	
Le contrôle des clés privées de signature de l'AC doit être assuré par du personnel de confiance (porteurs de secrets d'IGC).		

VI.2.3. Séquestre de la clé privée

Ni les clés privées d'AC, ni les clés privées des services applicatifs ne doivent en aucun cas être séquestrées.

VI.2.4. Copie de secours de la clé privée

Les clés privées des services applicatifs ou d'AC peuvent faire l'objet de copie de secours.

Ces copies peuvent être effectuées, soit dans un module cryptographique conforme aux exigences du chapitre XI ci-dessous, soit hors d'un module cryptographique mais dans ce cas sous forme chiffrée et avec un mécanisme de contrôle d'intégrité. Le chiffrement correspondant doit offrir un niveau de sécurité équivalent ou supérieur au stockage au sein du module cryptographique et, notamment, s'appuyer sur un algorithme, une longueur de clé et un mode opératoire capables de résister aux attaques par cryptanalyse pendant au moins la durée de vie de la clé ainsi protégée. Les règles à respecter sont définies dans le document [RGS_B_1].

Les opérations de chiffrement et de déchiffrement doivent être effectuées à l'intérieur du module cryptographique de telle manière que les clés privées d'AC ne soient à aucun moment en clair en dehors du module cryptographique.

Le contrôle des opérations de chiffrement / déchiffrement doit être conforme aux exigences du chapitre VI.2.2.

VI.2.5. Archivage de la clé privée

Les clés privées de l'AC ne doivent en aucun cas être archivée.

Les clés privées des services applicatifs ne doivent en aucun cas être archivées ni par l'AC ni par aucune des composantes de l'IGC.

VI.2.6. Transfert de la clé privée vers / depuis le module cryptographique

Si l'AC génère les clés privées des services applicatifs en dehors du dispositif de protection des éléments secrets du service applicatif, le transfert doit se faire conformément aux exigences du chapitre VI.1.1.2 ci-dessus.

Pour les clés privées d'AC, tout transfert doit se faire sous forme chiffrée, conformément aux exigences du chapitre VI.2.4.

VI.2.7. Stockage de la clé privée dans un module cryptographique

Il est recommandé de stocker les clés privées d'AC dans un module cryptographique répondant au minimum aux exigences du chapitre XI ci-dessous pour le niveau de sécurité considéré.

Cependant, dans le cas des copies de secours, le stockage peut être effectué en dehors d'un module cryptographique moyennant le respect des exigences du chapitre VI.2.4.

Quel que soit le moyen utilisé, l'AC doit garantir que les clés privées d'AC ne sont pas compromises pendant leur stockage ou leur transport.

VI.2.8. Méthode d'activation de la clé privée

VI.2.8.1. Clés privées d'AC

La méthode d'activation des clés privées d'AC dans un module cryptographique doit permettre de répondre aux exigences définies dans le chapitre XI pour le niveau de sécurité considéré.

	Niveaux (**) et (***)	
L'activation des clés privées d'AC dans un module cryptographique doit être contrôlée via des données d'activation (cf. chapitre VI.4) et doit faire intervenir au moins deux personnes dans des rôles de confiance (par exemple, responsable sécurité et opérateur).		

	Niveau (*)	
L'activation des clés privées d'AC dans un module cryptographique doit être contrôlée via des données d'activation (cf. chapitre VI.4) et doit faire intervenir au moins une personne ayant au moins un rôle de confiance (par exemple, responsable sécurité).		

VI.2.8.2. Clés privées des services applicatifs

La méthode d'activation de la clé privée du service applicatif dépend du dispositif utilisé. L'activation de la clé privée du service applicatif doit au minimum être contrôlée via des données d'activation (cf. chapitre VI.4) et doit permettre de répondre aux exigences définies dans le chapitre XII pour le niveau de sécurité considéré.

VI.2.9. Méthode de désactivation de la clé privée

VI.2.9.1. Clés privées d'AC

La désactivation des clés privées d'AC dans un module cryptographique doit être automatique dès que l'environnement du module évolue : arrêt ou déconnexion du module, déconnexion de l'opérateur, etc. Une clé privée d'AC peut également être désactivée après une certaine période d'inactivité. Ces conditions de désactivation doivent permettre de répondre aux exigences définies dans le chapitre XI pour le niveau de sécurité considéré.

VI 2.9.2. Clés privées des services applicatifs

Les conditions de désactivation de la clé privée d'un service applicatif doivent permettre de répondre aux exigences définies dans le chapitre XII pour le niveau de sécurité considéré.

VI.2.10. Méthode de destruction des clés privées

VI.2.10.1. Clés privées d'AC

La méthode de destruction des clés privées d'AC doit permettre de répondre aux exigences définies dans le chapitre XI pour le niveau de sécurité considéré.

En fin de vie d'une clé privée d'AC, normale ou anticipée (révocation), cette clé doit être systématiquement détruite, ainsi que toute copie et tout élément permettant de la reconstituer.

VI.2.10.2. Clés privées des services applicatifs

Si les clés privées des services applicatifs sont générées par l'AC dans un module cryptographique hors du dispositif de protection des éléments secrets, la méthode de destruction de ces clés privées après leur exportation hors du module cryptographique doit permettre de répondre aux exigences définies dans le chapitre XII pour le niveau de sécurité considéré.

En fin de vie de la clé privée d'un service applicatif, la méthode de destruction de cette clé privée doit permettre de répondre aux exigences définies dans le chapitre XII pour le niveau de sécurité considéré.

VI.2.11. Niveau de qualification du module cryptographique et des dispositifs de protection

Les exigences de qualification des produits de sécurité de type module cryptographique et dispositif de protection des éléments secrets ne s'appliquent que lorsque :

- le PSCE fait l'objet d'une procédure de qualification de son offre de certificats électronique, et
- les dispositifs de protection sont délivrés par le PSCE.

Ces exigences sont précisées aux chapitres XI et XII.

VI.3. Autres aspects de la gestion des bi-clés

VI.3.1. Archivage des clés publiques

Les clés publiques de l'AC et des services applicatifs sont archivées dans le cadre de l'archivage des certificats correspondants.

VI.3.2. Durées de vie des bi-clés et des certificats

Les bi-clés et les certificats des services applicatifs couverts par la présente PC Type doivent avoir une durée de vie maximale de 3 ans.

La fin de validité d'un certificat d'AC doit être postérieure à la fin de vie des certificats de services applicatifs

qu'elle émet. L'AC doit préciser dans sa PC la durée de vie des clés de signature d'AC et des certificats correspondants. Cette durée de vie doit être cohérente avec les caractéristiques de l'algorithme et la longueur de clé utilisés (cf. [RGS_B1]) et de la date de fin de validité de l'AC qui l'a émise.

A titre d'exemple, en 2012, un certificat d'AC racine peut avoir une durée de vie de 12 ans, celui d'une AC intermédiaire une durée de vie de 6 ans et un certificat délivré à une personne physique une durée de vie de 3 ans.

VI.4. Données d'activation

VI.4.1. Génération et installation des données d'activation

VI.4.1.1. Génération et installation des données d'activation correspondant à la clé privée de l'AC

La génération et l'installation des données d'activation d'un module cryptographique de l'IGC doivent se faire lors de la phase d'initialisation et de personnalisation de ce module. Si les données d'activation ne sont pas choisies et saisies par les responsables de ces données eux-mêmes, elles doivent leur être transmises de manière à en garantir la confidentialité et l'intégrité. Ces données d'activation ne doivent être connues que par les responsables nommément identifiés dans le cadre des rôles qui leurs sont attribués (cf. chapitre V.2.1).

VI.4.1.2. Génération et installation des données d'activation correspondant à la clé privée du service applicatif

Si l'AC génère la clé privée du service applicatif, elle a pour obligation de transmettre au RC les données d'activation correspondantes par le biais d'un chemin garantissant la protection en intégrité et en confidentialité des données. Notamment, la remise de la donnée d'activation doit être séparée dans le temps ou dans l'espace de la remise de la clé privée.

Par exemple : si les éléments secrets d'un service applicatif sont gérés sur un support matériel dont la mise en œuvre est conditionnée par l'utilisation d'un code personnel, la fourniture du support et celle du code personnel doivent être réalisées par des moyens différents (par exemple retrait du support à un guichet de l'AE et envoi du code par un autre canal).

Si les données d'activation sont sous forme de mots de passe, le RC doit être informé de la politique de constitution des mots de passe (par exemple, longueur d'un moins 8 caractères, présence d'un moins un caractère spécial, etc.).

VI.4.2. Protection des données d'activation

VI.4.2.1. Protection des données d'activation correspondant à la clé privée de l'AC

Les données d'activation qui sont générées par l'AC pour les modules cryptographiques de l'IGC doivent être protégées en intégrité et en confidentialité jusqu'à la remise à leur destinataire. Ce destinataire a ensuite la responsabilité d'en assurer la confidentialité, l'intégrité et la disponibilité.

VI.4.2.2. Protection des données d'activation correspondant aux clés privées des services applicatifs

Si les données d'activation des dispositifs de protection des clés privées des services applicatifs sont générées par l'AC, elles doivent être protégées en intégrité et en confidentialité jusqu'à la remise aux RC.

Si ces données d'activation sont également sauvegardées par l'AC, elles doivent être protégées en intégrité et en confidentialité.

VI.4.3. Autres aspects liés aux données d'activation

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

VI.5. Mesures de sécurité des systèmes informatiques

Les mesures de sécurité relatives aux systèmes informatiques doivent satisfaire aux objectifs de sécurité qui découlent de l'analyse de risque que l'AC peut mener (cf. chapitre I.4.1).

Une analyse des objectifs de sécurité peut être effectuée en amont de tout projet d'IGC par l'AC, de façon à garantir la prise en compte de la sécurité dans les systèmes informatiques.

Le PSCE doit être en mesure de justifier, par tout moyen, qu'il a pris les mesures nécessaires pour assurer la protection des échanges d'information entre les différentes composantes de l'IGC. Il vérifie périodiquement les mesures de sécurité prises dans ce cadre. Le moyen privilégié consiste en un audit technique réalisé par un prestataire d'audit de la sécurité des systèmes d'information qualifié.

VI.5.1. Exigences de sécurité technique spécifiques aux systèmes informatiques

Un niveau minimal d'assurance de la sécurité offerte sur les systèmes informatiques de l'IGC doit être défini dans la DPC de l'AC. Il doit au moins répondre aux objectifs de sécurité suivants :

- Identification et authentification forte des utilisateurs pour l'accès au système (authentification à deux facteurs, de nature physique et/ou logique),
- gestion des droits des utilisateurs (permettant de mettre en œuvre la politique de contrôle d'accès définie par l'AC, notamment pour implémenter les principes de moindres privilèges, de contrôles multiples et de séparation des rôles),
- gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur),
- protection contre les virus informatiques et toutes formes de logiciels compromettants ou non-autorisés et mises à jour des logiciels,
- gestion des comptes des utilisateurs, notamment la modification et la suppression rapide des droits d'accès,
- protection du réseau contre toute intrusion d'une personne non autorisée,
- protection du réseau afin d'assurer la confidentialité et l'intégrité des données qui y transitent,
- fonctions d'audits (non-répudiation et nature des actions effectuées),
- éventuellement, gestion des reprises sur erreur.

Les applications utilisant les services des composantes peuvent requérir des besoins de sécurité complémentaires.

La protection en confidentialité et en intégrité des clés privées ou secrètes d'infrastructure et de contrôle (cf. chapitre I.4.1.2) doit faire l'objet de mesures particulières, qui peuvent découler de l'analyse de risque.

Des dispositifs de surveillance (avec alarme automatique) et des procédures d'audit des paramétrages du système (en particulier des éléments de routage) doivent être mis en place.

VI.5.2. Niveau de qualification des systèmes informatiques

	Niveaux (**) et (***)	
Lorsque le PSCE souhaite faire qualifier son offre de certificats électroniques, il est recommandé que les systèmes informatiques de l'IGC mettant en œuvre le module cryptographique fassent l'objet d'une qualification conformément à la [LOIDUPAYS], au niveau standard défini par le [RGS] et en respectant		

les exigences du [CWA 14167-1].

VI.6. Mesures de sécurité des systèmes durant leur cycle de vie

Les mesures de sécurité relatives aux cycles de vie des systèmes informatiques doivent satisfaire aux objectifs de sécurité qui découlent de l'analyse de risque que l'AC peut mener (cf. rappel au début du présent chapitre VI).

VI.6.1. Mesures de sécurité liées au développement des systèmes

L'implémentation d'un système permettant de mettre en œuvre les composantes de l'IGC doit être documentée et doit respecter dans la mesure du possible des normes de modélisation et d'implémentation. La configuration du système des composantes de l'IGC ainsi que toute modification et mise à niveau doivent être documentées et contrôlées.

L'AC doit :

- Garantir que les objectifs de sécurité sont définis lors des phases de spécification et de conception,
- utiliser des systèmes et des produits fiables qui sont protégés contre toute modification

VI.6.2. Mesures liées à la gestion de la sécurité

Toute évolution significative d'un système d'une composante de l'IGC doit être signalée à l'AC pour validation. Elle doit être documentée et doit apparaître dans les procédures de fonctionnement interne de la composante concernée et être conforme au schéma de maintenance de l'assurance de conformité, dans le cas de produits évalués.

VI.6.3. Niveau d'évaluation sécurité du cycle de vie des systèmes

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

VI.7. Mesures de sécurité réseau

L'interconnexion vers des réseaux publics doit être protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement de la composante au sein de l'IGC.

L'AC doit garantir que les composants du réseau local (routeurs, par exemple) sont maintenus dans un environnement physiquement sécurisé et que leurs configurations sont périodiquement auditées en vue de vérifier leur conformité avec les exigences spécifiées par l'AC.

De plus, les échanges entre composantes au sein de l'IGC peuvent nécessiter la mise en place de mesures particulières en fonction du niveau de sensibilité des informations (utilisation de réseaux séparés / isolés, mise en œuvre de mécanismes cryptographiques à l'aide de clés d'infrastructure et de contrôle, etc.).

VI.8. Horodatage / Système de datation

Plusieurs exigences de la présente PC Type nécessitent la datation par les différentes composantes de l'IGC d'évènements liés aux activités de l'IGC (cf. chapitre V.4).

Pour dater ces évènements, les différentes composantes de l'IGC peuvent recourir :

- Soit à une autorité d'horodatage, interne ou externe à l'IGC, conforme à la politique d'horodatage [RGS_A5] ;
- Soit en utilisant l'heure système de l'IGC en assurant une synchronisation des horloges des systèmes de l'IGC entre elles, au minimum à la minute près, et par rapport à une source fiable de

temps UTC, au minimum à la seconde près. Pour les opérations faites hors ligne (ex : administration d'une AC Racine), cette précision de synchronisation par rapport au temps UTC n'est pas requise. Le système devra toutefois pouvoir ordonner les évènements avec une précision suffisante. Pour la synchronisation par rapport au temps UTC, il est recommandé de se référer à un système comprenant au moins deux sources indépendantes de temps.

VII. Profils des certificats, OCSP et des LCR

Le document [RGS_A4] liste les règles concernant les profils des certificats, des listes de révocation (LCR) et OCSP. Elles portent notamment sur :

- Les algorithmes et longueurs des clés cryptographiques ;
- Limitation exclusive de l'usage du certificat à la signature électronique.

VIII. Audit de conformité et autres évaluations

Le présent chapitre concerne les audits et les évaluations que doit réaliser, ou faire réaliser, l'AC afin de s'assurer que l'ensemble de son IGC, ainsi que le cas échéant le ou les MC, est bien conforme à ses engagements affichés dans sa PC et aux pratiques identifiées dans sa DPC.

VIII.1. Fréquences et / ou circonstances des évaluations

Avant la première mise en service d'une composante de son IGC ou suite à toute modification significative au sein d'une composante, l'AC doit procéder à un contrôle de conformité de cette composante.

L'AC doit également procéder régulièrement à un contrôle de conformité de l'ensemble de son IGC, suivant la fréquence suivante :

Description	**Niveau ***	**Niveau ****	**Niveau *****
Fréquence de contrôle de conformité de l'ensemble de l'IGC	1 fois tous les 3 ans	1 fois tous les 2 ans	1 fois par an

VIII.2. Identités / qualifications des évaluateurs

Le contrôle d'une composante doit être assigné par l'AC à une équipe d'auditeurs compétents en sécurité des systèmes d'information et dans le domaine d'activité de la composante contrôlée.

VIII.3. Relations entre évaluateurs et entités évaluées

L'équipe d'audit ne doit pas appartenir à l'entité opérant la composante de l'IGC contrôlée, quelle que soit cette composante, et être dûment autorisée à pratiquer les contrôles visés.

VIII.4. Sujets couverts par les évaluations

Les contrôles de conformité portent sur une composante de l'IGC (contrôles ponctuels) ou sur l'ensemble de l'architecture de l'IGC (contrôles périodiques) et visent à vérifier le respect des engagements et pratiques définies dans la PC de l'AC et dans la DPC qui y répond ainsi que des éléments qui en découlent (procédures opérationnelles, ressources mises en œuvre, etc.).

Le PSCE doit être en mesure de justifier, par tout moyen, aux auditeurs, qu'il a pris les mesures nécessaires pour assurer la protection des échanges d'information entre les différentes composantes de l'IGC. Il vérifie périodiquement les mesures de sécurité prises dans ce cadre. Le moyen privilégié consiste en un audit technique réalisé par un prestataire d'audit de la sécurité des systèmes d'information qualifié.

VIII.5. Actions prises suite aux conclusions des évaluations

À l'issue d'un contrôle de conformité, l'équipe d'audit rend à l'AC, un avis parmi les suivants : «réussite», «échec», «à confirmer».

Selon l'avis rendu, les conséquences du contrôle sont les suivantes

En cas d'échec, et selon l'importance des non-conformités, l'équipe d'audit émet des recommandations à l'AC qui peuvent être la cessation (temporaire ou définitive) d'activité, la révocation du certificat de la composante, la révocation de l'ensemble des certificats émis depuis le dernier contrôle positif, etc. Le choix de la mesure à appliquer est effectué par l'AC et doit respecter ses politiques de sécurité internes.

En cas de résultat «à confirmer», l'AC remet à la composante un avis précisant sous quel délai les non-conformités doivent être levées. Puis, un contrôle de « confirmation « permettra de vérifier que tous les

points critiques ont bien été résolus.

En cas de réussite, l'AC confirme à la composante contrôlée la conformité aux exigences de la PC et la DPC.

VIII.6. Communication des résultats

Les résultats des audits de conformité doivent être tenus à la disposition de l'organisme de qualification en charge de la qualification de l'AC.

IX. Autres problématiques métiers et légales

IX.1. Tarifs

IX.1.1. Tarifs pour la fourniture ou le renouvellement de certificats

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

IX.1.2. Tarifs pour accéder aux certificats

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

IX.1.3. Tarifs pour accéder aux informations d'état et de révocation des certificats

L'accès aux LCR et, éventuellement, deltaLCR doit être en accès libre en lecture.

IX.1.4. Tarifs pour d'autres services

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

IX.1.5. Politique de remboursement

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

IX.2. Responsabilité financière

Conformément à ses obligations, l'AC doit prendre les dispositions nécessaires pour couvrir, éventuellement financièrement, ses responsabilités liées à ses opérations et/ou activités.

IX.2.1. Couverture par les assurances

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

IX.2.2. Autres ressources

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

IX.2.3. Couverture et garantie concernant les entités utilisatrices

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

IX.3. Confidentialité des données professionnelles

IX.3.1. Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont au moins les suivantes :

- La partie non-publique de la DPC de l'AC,
- les clés privées de l'AC, des composantes et des serveurs,
- les données d'activation associées aux clés privées d'AC et des services applicatifs[73],

[73] La confidentialité des données d'activation des clés privées des serveurs doit être garantie par l'AC tant qu'elle les détient.

- tous les secrets de l'IGC,
- les journaux d'évènements des composantes de l'IGC,
- les dossiers d'enregistrement des services applicatifs et des RC,
- les causes de révocations, sauf accord explicite du RC.

IX.3.2. Informations hors du périmètre des informations confidentielles

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

IX.3.3. Responsabilités en termes de protection des informations confidentielles

L'AC est tenue d'appliquer des procédures de sécurité pour garantir la confidentialité des informations identifiées au chapitre IX.3.1, en particulier en ce qui concerne l'effacement définitif ou la destruction des supports ayant servi à leur stockage.

De plus, lorsque ces données sont échangées, l'AC doit en garantir l'intégrité.

L'AC est tenue de respecter la législation et la réglementation en vigueur sur le territoire français. En particulier, elle peut devoir mettre à disposition les dossiers d'enregistrement des certificats de services applicatifs à des tiers dans le cadre de procédures légales. Elle doit également donner l'accès à ces informations au RC et au MC.

IX.4. Protection des données à caractère personnel

IX.4.1. Politique de protection des données à caractère personnel

Il est entendu que toute collecte et tout usage de données à caractère personnel par l'AC et l'ensemble de ses composantes sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, en particulier de la loi [CNIL].

IX.4.2. Données à caractère personnel

Les données considérées comme personnelles sont au moins les suivantes :

- Les causes de révocation des certificats des services applicatifs (qui sont considérées comme confidentielles sauf accord explicite du RC) ;
- Les dossiers d'enregistrement des RC.

IX.4.3. Données à caractère non personnel

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

IX.4.4. Responsabilité en termes de protection des données à caractère personnel

Cf. législation et réglementation en vigueur sur le territoire français (notamment cf. chapitre X ci-dessous)

IX.4.5. Notification et consentement d'utilisation des données à caractère personnel

Conformément à la législation et réglementation en vigueur sur le territoire français, les informations personnelles remises par les porteurs à l'AC ne doivent ni être divulguées ni transférées à un tiers sauf dans les cas suivants : consentement préalable du porteur, décision judiciaire ou autre autorisation légale.

IX.4.6. Conditions de divulgation de données personnelles aux autorités judiciaires ou administratives

Cf. législation et réglementation en vigueur sur le territoire français (notamment cf. Chapitre X ci-dessous).

IX.4.7. Autres circonstances de divulgation de données personnelles

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

IX.5. Droits de propriété intellectuelle

La présente PC Type ne formule pas d'exigence spécifique sur le sujet. Application de la législation et de la réglementation en vigueur sur le territoire français.

IX.6. Interprétations contractuelles et garanties

Les obligations communes aux composantes de l'IGC sont les suivantes :

- Protéger et garantir l'intégrité et la confidentialité de leurs clés secrètes et/ou privées,
- n'utiliser leurs clés cryptographiques (publiques, privées et/ou secrètes) qu'aux fins prévues lors de leur émission et avec les outils spécifiés dans les conditions fixées par la PC de l'AC et les documents qui en découlent,
- respecter et appliquer la partie de la DPC leur incombant (cette partie doit être communiquée à la composante correspondante),
- se soumettre aux contrôles de conformité effectués par l'équipe d'audit mandatée par l'AC (cf. chapitre VIII) et l'organisme de qualification,
- respecter les accords ou contrats qui les lient entre elles ou aux RC,
- documenter leurs procédures internes de fonctionnement,
- mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles elles s'engagent dans des conditions garantissant qualité et sécurité.

IX.6.1. Autorités de Certification

L'AC a pour obligation de :

- Pouvoir démontrer aux utilisateurs de ses certificats qu'elle a émis un certificat pour un service applicatif donné et que le RC correspondant a accepté le certificat, conformément aux exigences du chapitre IV.4 ci-dessus.
- Garantir et maintenir la cohérence de sa DPC avec sa PC.
- Prendre toutes les mesures raisonnables pour s'assurer que ses RC sont au courant de leurs droits et obligations en ce qui concerne l'utilisation et la gestion des clés, des certificats ou encore de l'équipement et des logiciels utilisés aux fins de l'IGC. La relation entre un RC et l'AC est formalisée par un lien contractuel / hiérarchique / réglementaire précisant les droits et obligations des parties et notamment les garanties apportées par l'AC.

L'AC est responsable de la conformité de sa Politique de Certification, avec les exigences émises dans la présente PC Type pour le niveau de sécurité considéré. L'AC assume toute conséquence dommageable résultant du non-respect de sa PC, conforme aux exigences de la présente PC Type, par elle-même ou l'une de ses composantes. Elle doit prendre les dispositions nécessaires pour couvrir ses responsabilités liées à ses opérations et/ou activités et posséder la stabilité financière et les ressources exigées pour fonctionner en

conformité avec la présente politique.

De plus, l'AC reconnaît engager sa responsabilité en cas de faute ou de négligence, d'elle-même ou de l'une de ses composantes, quelle qu'en soit la nature et la gravité, qui aurait pour conséquence la lecture, l'altération ou le détournement des données personnelles des RC à des fins frauduleuses, que ces données soient contenues ou en transit dans les applications de gestion des certificats de l'AC.

Par ailleurs, l'AC reconnaît avoir à sa charge un devoir général de surveillance, quant à la sécurité et l'intégrité des certificats délivrés par elle-même ou l'une de ses composantes. Elle est responsable du maintien du niveau de sécurité de l'infrastructure technique sur laquelle elle s'appuie pour fournir ses services. Toute modification ayant un impact sur le niveau de sécurité fourni doit être approuvée par les instances de haut niveau de l'AC.

En cas de non-respect ponctuel des obligations décrites dans la présente PC Type, l'Administration se réserve le droit de refuser temporairement ou définitivement les certificats de l'AC conformément à la réglementation en vigueur.

IX.6.2. Service d'enregistrement

Cf. les obligations pertinentes du chapitre IX.6.1.

IX.6.3. RC

Le RC a le devoir de :

- Communiquer des informations exactes et à jour lors de la demande ou du renouvellement du certificat ;
- Protéger la clé privée du service applicatif dont il a la responsabilité par des moyens appropriés à son environnement ;
- Protéger les données d'activation de cette clé privée et, le cas échéant, les mettre en œuvre ;
- Protéger l'accès à la base de certificats du service applicatif ;
- Respecter les conditions d'utilisation de la clé privée du service applicatif et du certificat correspondant ;
- Informer l'AC de toute modification concernant les informations contenues dans le certificat électronique ;
- Faire, sans délai, une demande de révocation du certificat électronique dont il est responsable auprès de l'AE, du MC de son entreprise ou de l'AC en cas de compromission ou de suspicion de compromission de la clé privée correspondante (ou de ses données d'activation).

La relation entre le RC et l'AC ou ses composantes est formalisée par un engagement du RC visant à certifier l'exactitude des renseignements et des documents fournis.

Ces informations s'appliquent également aux MC.

IX.6.4. Utilisateurs de certificats

Les utilisateurs de la sphère publique utilisant les certificats doivent :

- Vérifier et respecter l'usage pour lequel un certificat a été émis ;
- Contrôler que le certificat émis par l'AC est référencé au niveau de sécurité et pour le service de confiance requis par l'application ;

- Pour chaque certificat de la chaîne de certification, du certificat du service applicatif jusqu'à l'AC Racine, vérifier la signature numérique de l'AC émettrice du certificat considéré et contrôler la validité de ce certificat (dates de validité, statut de révocation) ;
- Vérifier et respecter les obligations des utilisateurs de certificats exprimées dans la présente PC Type.

L'AC ne doit pas émettre dans sa propre PC d'obligations supplémentaires, par rapport aux obligations de la présente PC Type, à l'encontre des utilisateurs de la sphère publique.

IX.6.5. Autres participants

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

IX.7. Limite de garantie

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

IX.8. Limite de responsabilité

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

IX.9. Indemnités

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

IX.10. Durée et fin anticipée de validité de la PC

IX.10.1. Durée de validité

La PC de l'AC doit rester en application au moins jusqu'à la fin de vie du dernier certificat émis au titre de cette PC.

IX.10.2. Fin anticipée de validité

La publication d'une nouvelle version de la présente PC Type peut entraîner, en fonction des évolutions apportées, la nécessité pour l'AC de faire évoluer sa PC correspondante.

En fonction de la nature et de l'importance des évolutions apportées à la PC Type, le délai de mise en conformité sera arrêté conformément aux modalités prévues par la réglementation en vigueur.

De plus, la mise en conformité n'impose pas le renouvellement anticipé des certificats déjà émis, sauf cas exceptionnel lié à la sécurité.

IX.10.3. Effets de la fin de validité et clauses restant applicables

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

IX.11. Notifications individuelles et communications entre les participants

En cas de changement de toute nature intervenant dans la composition de l'IGC, l'AC devra :

- Au plus tard un mois avant le début de l'opération, faire valider ce changement au travers d'une expertise technique, afin d'évaluer les impacts sur le niveau de qualité et de sécurité des fonctions de l'AC et de ses différentes composantes.
- Au plus tard un mois après la fin de l'opération, en informer l'organisme de qualification.

IX.12. Amendements à la PC

IX.12.1. Procédures d'amendements

L'AC devra contrôler que tout projet de modification de sa PC reste conforme aux exigences de la présente PC Type et des éventuels documents complémentaires du [RGS]. En cas de changement important, il est recommandé à l'AC de faire appel à une expertise technique pour en contrôler l'impact.

IX.12.2. Mécanisme et période d'information sur les amendements

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

IX.12.3. Circonstances selon lesquelles l'OID doit être changé

L'OID de la PC de l'AC étant inscrit dans les certificats qu'elle émet, toute évolution de cette PC ayant un impact majeur sur les certificats déjà émis (par exemple, augmentation des exigences en matière d'enregistrement des RC, qui ne peuvent donc pas s'appliquer aux certificats déjà émis) doit se traduire par une évolution de l'OID, afin que les utilisateurs puissent clairement distinguer quels certificats correspondent à quelles exigences.

En particulier, l'OID de la PC de l'AC doit évoluer dès lors qu'un changement majeur (et qui sera signalé comme tel, notamment par une évolution de l'OID de la présente PC Type) intervient dans les exigences de la présente PC Type applicable à la famille de certificats considérée.

IX.13. Dispositions concernant la résolution de conflits

L'AC doit mettre en place des politiques et procédures pour le traitement des réclamations et le règlement des litiges émanant des entités pour lesquelles elle fournit des services électroniques de confiance ou d'autres points qui y sont liés.

IX.14. Juridictions compétentes

La présente PC Type ne formule pas d'exigence spécifique sur le sujet. Application de la législation et de la réglementation en vigueur sur le territoire français.

IX.15. Conformité aux législations et réglementations

Les textes législatifs et réglementaires applicables à la présente PC Type sont, notamment, ceux indiqués au chapitre X ci-dessous.

IX.16. Dispositions diverses

IX.16.1. Accord global

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

IX.16.2. Transfert d'activités

Cf. chapitre V.8.

IX.16.3. Conséquences d'une clause non valide

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

IX.16.4. Application et renonciation

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

IX.16.5. Force majeure

Sont considérés comme cas de force majeure tous ceux habituellement retenus par les tribunaux français, notamment le cas d'un évènement irrésistible, insurmontable et imprévisible.

IX.17. Autres dispositions

La présente PC Type ne formule pas d'exigence spécifique sur le sujet.

X Annexe 1 : Documents cités en référence

X.1. Réglementation

Renvoi	Document
[CNIL]	Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004.
[ORDONNANCE]	Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.
[DécretRGS]	Décret pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005.
[LOIDUPAYS]	Loi du pays n° 2017-31 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices

X.2. Documents techniques

Renvoi	Document
[RGS]	Référentiel Général de Sécurité – Version 1.0
[RGS_A1]	RGS - Fonction de sécurité « Signature « - Version 1.0
[RGS_A4]	RGS - Politiques de Certification Types - Profils de certificats, de LCR et OCSP et algorithmes cryptographiques – Version 1.0
[RGS_B_1]	Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, Version 1.0
[GEVC]	Exigences relatives à l'émission et à la gestion des certificats électroniques SSL Extended Validation, CA Browser Forum, 1er octobre 2009, version 1.2.
[CWA14167-1]	CWA 14167-1 (2003-06) Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1
[ETSI_NQCP]	ETSI TS 102 042 V1.3.4 (décembre 2007) Policy Requirements for Certification Authorities issuing public key certificates
[ExigencesSitesPerso]	Exigences de sécurité des sites de personnalisation, V1.0 (août 2007) http://www.references.modernisation.gouv.fr/sites/default/files/Exigences_sites_de_perso_V1_0.pdf
[PROG_ACCRED]	COFRAC - Programme d'accréditation pour la qualification des prestataires de services de confiance – CEPE REF 21 – disponible : www.cofrac.fr
[RFC3647]	IETF - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practice Framework - novembre 2003

[RFC2527]	IETF - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practice Framework - march 1999
[X.509]	Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks, Recommendation X.509, version d'août 2005 (complétée par les correctifs techniques Corrigendum 1 de janvier 2007et Corrigendum 2 de novembre 2008)
[972-1]	DCSSI - Guide Technique pour la confidentialité des informations enregistrées sur les disques durs à recycler ou exporter – N° 972-1/SGDN/DCSSI du 17/07/2003

XI. Annexe 2 : Exigences de sécurité du module cryptographique de l'AC

XI.1. Exigences sur les objectifs de sécurité

Le module cryptographique, utilisé par l'AC pour générer et mettre en œuvre ses clés de signature (pour la génération des certificats électroniques, des LCR / LAR et, éventuellement, des réponses OCSP), ainsi que, le cas échéant, générer les bi-clés des services applicatifs, doit répondre aux exigences de sécurité suivantes :

- si les bi-clés des services applicatifs sont générées par ce module, garantir que ces générations sont réalisées exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique des bi-clés générées ;
- si les bi-clés des services applicatifs sont générées par ce module, assurer la confidentialité des clés privées et l'intégrité des clés privées et publiques des services applicatifs lorsqu'elles sont sous la responsabilité de l'AC et pendant leur transfert vers le dispositif de protection des éléments secrets du service applicatif et assurer leur destruction sûre après ce transfert ;
- assurer la confidentialité et l'intégrité des clés privées de signature de l'AC durant tout leur cycle de vie, et assurer leur destruction sûre en fin de vie ;
- être capable d'identifier et d'authentifier ses utilisateurs ;
- limiter l'accès à ses services en fonction de l'utilisateur et du rôle qui lui a été assigné ;
- être capable de mener une série de tests pour vérifier qu'il fonctionne correctement et entrer dans un état sûr s'il détecte une erreur ;
- permettre de créer une signature électronique sécurisée, pour signer les certificats générés par l'AC, qui ne révèle pas les clés privées de l'AC et qui ne peut pas être falsifiée sans la connaissance de ces clés privées ;
- créer des enregistrements d'audit pour chaque modification concernant la sécurité ;
- si une fonction de sauvegarde et de restauration des clés privées de l'AC est offerte, garantir la confidentialité et l'intégrité des données sauvegardées et réclamer au minimum un double contrôle des opérations de sauvegarde et de restauration.

	Niveau (et ***)**	
Il est recommandé que le module cryptographique de l'AC détecte les tentatives d'altérations physiques et entre dans un état sûr quand une tentative d'altération est détectée.		

XI.2. Exigences sur la qualification

Les exigences suivantes ne sont applicables que lorsque le PSCE souhaite faire qualifier son offre de certificats de service applicatif au(x) niveau(x) de sécurité considéré(s) les modalités prévues par l'article LP 22 de la [LOIDUPAYS] et déclinées au chapitre 5 du corps de texte du [RGS].

	Niveau (***)	

Le module cryptographique utilisé par l'AC doit être qualifié au niveau renforcé[74], selon le processus décrit dans le [RGS], et être conforme aux exigences[75] du chapitre XI.1 ci-dessus.

	Niveau (**)	
Le module cryptographique utilisé par l'AC doit être qualifié au minimum au niveau standard[76], selon le processus décrit dans le [RGS], et être conforme aux exigences du chapitre XI.1 ci-dessus. Il est toutefois recommandé d'utiliser un module cryptographique qualifié au niveau renforcé.		

	Niveau (*)	
Le module cryptographique utilisé par l'AC doit être qualifié au minimum au niveau élémentaire[77], selon le processus décrit dans le [RGS], et être conforme aux exigences du chapitre XI.1 ci-dessus. Il est toutefois recommandé d'utiliser un module cryptographique qualifié au niveau standard.		

[74] Sous réserve qu'il existe au moins une telle référence sur la liste de référence des produits de sécurité visée à l'article LP 22 de la [LOIDUPAYS]. Dans le cas contraire, le PSCE souhaitant faire qualifier son offre de certificats de machine doit obtenir une dérogation de l'ANSSI.

[75] Une cible de sécurité conforme au profil de protection [CWA14167-4] (ou [CWA14167-2] s'il y a une fonction de sauvegarde des clés privées de l'AC) permet au module cryptographique d'être considéré comme conforme aux exigences de la présente annexe (hors génération des bi-clés des porteurs). Les exigences de génération des bi-clés des services applicatifs peuvent être remplies lorsque la cible de sécurité respecte le profil de protection [CWA14167-3].

[76] Sous réserve qu'il existe au moins une telle référence au catalogue des produits qualifiés par l'ANSSI. Dans le cas contraire, le PSCE souhaitant faire qualifier son offre de certificats de service applicatif doit obtenir une dérogation de l'ANSSI.

[77] Sous réserve qu'il existe au moins une telle référence au catalogue des produits qualifiés par l'ANSSI. Dans le cas contraire, le PSCE souhaitant faire qualifier son offre de certificats de machine doit obtenir une dérogation de l'ANSSI.

XII. Annexe 3 : Exigences de sécurité du dispositif de protection

Le dispositif de protection des éléments secrets, utilisé par le service applicatif pour stocker et mettre en œuvre sa clé privée et, le cas échéant, générer sa bi-clé, doit répondre aux exigences de sécurité suivantes :

- Si la bi-clé du service applicatif est générée par le dispositif, garantir que cette génération est réalisée exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique de la bi-clé générée ;
- Assurer la correspondance entre la clé privée et la clé publique ;
- Générer un cachet ou une authentification qui ne peut être falsifiée sans la connaissance de la clé privée.

Par ailleurs, des mesures de sécurité organisationnelles, procédurales ou techniques doivent être mises en place afin de :

- Détecter les défauts lors des phases d'initialisation, et d'opération et disposer de techniques sûres de destruction de la clé privée en cas de régénération de la clé privée ;
- Garantir la confidentialité et l'intégrité de la clé privée ;
- Permettre de garantir l'authenticité et l'intégrité de la clé publique lors de son export hors du dispositif.

Cachet
➢ Assurer pour le serveur légitime uniquement la fonction de génération des cachets électroniques et protéger la clé privée contre toute utilisation par des tiers.

Authentification Serveur
➢ Assurer pour le serveur légitime uniquement, d'une part, la fonction d'authentification et, d'autre part, la fonction de déchiffrement de clés symétriques de session, et protéger la clé privée contre toute utilisation par des tiers ; ➢ Permettre de garantir l'authenticité et l'intégrité de la clé symétrique de session, une fois déchiffrée, lors de son export hors du dispositif à destination de l'application de déchiffrement des données.

Nota - Les dispositifs matériels, de types cartes à puces ou modules cryptographiques figurant sur la liste de référence visée à l'article LP 22 de la [LOIDUPAYS] respectent ces exigences. Toutefois, des solutions logicielles sont susceptibles de respecter ces exigences pourvues que des mesures de sécurité additionnelles propres à l'environnement dans lequel est déployé la clé privée soient mises en place. Cet environnement dans lequel est déployée la clé privée doit faire l'objet d'un audit de sécurité.

Annexe A4

Profils de Certificats / LCR / OCSP et Algorithmes Cryptographiques

Historique des versions		
Date	**Version**	**Evolution du document**
xxx	1.0	Publication de la première version de l'annexe A4 du référentiel général de sécurité

Avant propos

Le présent document fait partie du référentiel général de sécurité (RGS), pris en application de l'article LP 20 de la loi du pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices, et de son arrêté d'application.

Le présent document et ses annexes sont une copie adaptée du RGS A4 – Profils de certificats, CRL, OCSP et algorithmes cryptographiques, en vigueur en métropole, version 3.0 du 27 février 2014.

Le texte fait des renvois à des documents publiés par l'Agence nationale de la sécurité des systèmes d'information[78] (ANSSI) ou encore disponibles sur son site internet www.ssi.gouv.fr, en ce qu'ils reflètent l'état de l'art en matière de sécurité informatique.

Le référentiel et ses annexes sont disponibles en ligne sur le site internet www.dgenpf, et leur mise à jour est assurée par la Direction générale de l'économie numérique.

[78] L'ANSSI est un service à compétence nationale rattaché au Secrétaire général de la défense et de la sécurité nationale, l'autorité chargée d'assister le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale. Parmi ses nombreux objectifs, l'un d'eux consiste à promouvoir un espace de confiance pour les services en ligne. Elle y participe en ce sens notamment au travers de la règlementation (référentiels) et ses labels (certification des produits de sécurité et qualification des produits de sécurité et des prestataires de service de confiance).

I. Introduction

Les politiques de certification types (PC Types), annexes du [RGS], contiennent des règles sur les formats des certificats, des LCR et des requêtes / réponses OCSP (état en ligne des certificats) ainsi que sur les mécanismes cryptographiques.

Ces règles, communes à toutes les fonctions de sécurité à base de certificats traitées dans les PC Types, ont été factorisées dans le présent document. Celui-ci précise, lorsqu'il y en a, les différences entre les fonctions de sécurité et/ou les niveaux de sécurité.

II. Certificats

II.1. Certificats d'AC

Ce chapitre porte sur les certificats de clés d'AC utilisées pour la signature de certificats de porteurs ou de services applicatifs, et à la signature de LCR.

II.1.1. Champs de base

Le tableau ci-dessous reprend l'ensemble des champs de base d'un certificat X.509v3. Un certificat d'AC conforme au [RGS] doit respecter, de base, les exigences correspondantes du [RFC5280], moyennant les compléments et/ou modifications d'exigences définis dans ce tableau.

Champ	**Intitulé de l'exigence**
Version	La valeur de ce champ doit être « 2 », indiquant qu'il s'agit d'un certificat version 3.
Serial number	Il doit être généré pour être unique. Il est recommandé que le Serial Number soit non prédictible. Les AC en service lors de la parution de la V2.0 du RGS qui ne respecteraient pas cette exigence doivent le faire lors du renouvellement de leur certificat.
Signature	Cf. chapitre V ci-dessous sur les exigences en matière d'algorithmes et de longueurs de clés.
Issuer	Ce champ doit être un DN répondant aux exigences du chapitre VII ci-dessous.
Validity	Pas d'exigence supplémentaire par rapport au [RFC5280]
Subject	Ce champ doit respecter les mêmes exigences que le champ « Issuer ».
Subject Public Key Info	Cf. chapitre V ci-dessous sur les exigences en matière d'algorithmes et de longueurs de clés.
Unique Identifiers (issuer et subject)	Les PC Types du [RGS] imposant l'unicité des DN des champs Issuer et Subject au sein du domaine de l'AC, les champs Unique Identifiers ne doivent pas être utilisés.
Extensions	Cf. chapitre suivant.

II.1.2. Extensions

Une extension d'un certificat est caractérisée par :

- Sa présence obligatoire ou non dans le certificat. Ceci indique si l'AC émettrice du certificat a l'obligation ou non d'intégrer l'extension dans tous les certificats qu'elle émet.
- Sa criticité. Ceci indique comment les utilisateurs de certificats doivent traiter l'extension et le certificat correspondant, ceci conformément aux principes de gestion de la criticité définis dans [X.509].

Le tableau ci-dessous présente les exigences requises par le [RGS] en complément des exigences définies dans [RFC5280], en précisant le caractère obligatoire de chaque extension (colonne «O», O(ui)/N(on)) et sa criticité (colonne «C», O(ui)/N(on)).

Les extensions qui apparaissent dans ce tableau doivent respecter l'ensemble des exigences correspondantes du [RFC5280], moyennant les compléments et/ou modifications d'exigences définis ici.

Les autres extensions traitées dans le [RFC5280] et qui n'apparaissent pas dans ce tableau doivent respecter strictement les exigences du [RFC5280]. Notamment, les extensions obligatoires pour les certificats d'AC (Basic Constraints, Authority / Subject Key Identifiers...) doivent être intégrées. La prise en compte des extensions non obligatoires est laissée au choix de l'AC.

L'intégration de ces autres extensions (obligatoires et non obligatoires) doit respecter les exigences de criticité imposées par le [RFC5280]. Lorsque le [RFC5280] n'impose pas d'exigence de criticité, l'extension doit être systématiquement marquée «non critique». De même, l'AC peut intégrer des extensions non traitées ni dans le [RFC5280] ni dans le présent document, y compris des extensions propriétaires, mais ces extensions doivent obligatoirement être marquées « non critiques ».

Champ	**O**	**C**	**Intitulé de l'exigence**
Identifiant de la clé de l'autorité / Authority Key Identifier	O	N	Cette extension doit être présente, être marquée « non critique » et contenir l'identifiant de la clé publique de l'AC émettrice (même valeur que le champ « Subject Key Identifier » du certificat de cette AC émettrice).
Usages de la clé / Key Usage	O	O	Cette extension doit être marquée « critique ». Les bits keyCertSign et cRLSign doivent être à 1. Si l'AC signe des réponses OCSP, le bit digitalSignature doit être à 1.
Politique de certification / *Certificate Policies*	O	N	Cette extension doit être conforme aux exigences du chapitre 4.2.1.4 du [RFC5280].
Autre nom de l'objet / de l'émetteur *Subject Alternative Name*	N	N	L'identification des AC via les DN des champs Subject et Issuer étant obligatoire dans les PC Types du [RGS], les champs Subject Alternative Name et Issuer Alternative Name peuvent être présents, mais ils doivent obligatoirement être marqués «non critique» et être conformes aux exigences du chapitre 4.1.2.4 du [RFC5280].
Point de publication des listes de certificats révoqués / CRL Distribution Points	N	N	S'il est proposé un service de LCR pour vérifier le statut de révocation du certificat d'AC concerné (à l'exception des certificats racines auto-signés), alors cette extension doit être présente, marquée « non critique ». La règle générale est qu'il doit y avoir au moins une manière de vérifier le statut de révocation du certificat d'AC ; si cette extension n'est pas présente, alors l'extension suivante doit l'être.
Accès aux informations publiées par l'AC / Authority Information Access	N	N	S'il est proposé un service de validation de certificat en ligne (type serveur OCSP pour « Online Certificate Service Protocol »), alors cette extension doit être renseignée du type de service proposé et de la méthode à suivre pour l'atteindre, conformément au chapitre 4.2.2.1 de [RFC5280]. Si cette extension n'est pas présente, alors l'extension précédente doit l'être.
Basic Constraints	O	O	Pour les certificats d'AC utilisés pour la signature de certificats de personnes physiques ou de services applicatifs, le champ *pathLenConstraint* doit être positionné à « 0 « .

II.2. Certificats porteurs

II.2.1. Champs de base

Le tableau ci-dessous reprend l'ensemble des champs de base d'un certificat X.509v3. Un certificat porteur conforme au [RGS] doit respecter, de base, les exigences correspondantes du [RFC5280], du [RFC3739] et de [ETSI_QC] pour les certificats qualifiés, moyennant les compléments et/ou modifications d'exigences définis dans ce tableau.

Champ	**Intitulé de l'exigence**
Version	La valeur de ce champ doit être « 2 », indiquant qu'il s'agit d'un certificat version 3.
Serial number	Il doit avoir été généré pour être unique. Il est recommandé que le Serial Number soit non prédictible. Les AC en service lors de la parution de la V2.0 du RGS qui ne respecteraient pas cette exigence doivent le faire sous trois ans.
Signature	Cf. chapitre V ci-dessous sur les exigences en matière d'algorithmes et de longueurs de clés.
Issuer	Ce champ est un DN répondant aux exigences du chapitre VII ci-dessous.
Validity	Pas d'exigence supplémentaire par rapport au [RFC5280]
Subject	Ce champ doit être un DN répondant aux exigences du chapitre VII ci-dessous.
Subject Public Key Info	Cf. chapitre V ci-dessous sur les exigences en matière d'algorithmes et de longueurs de clés.
Unique Identifiers (issuer et subject)	Les PC Types du [RGS] imposant l'unicité des DN des champs Issuer et Subject au sein du domaine de l'AC, les champs Unique Identifiers ne doivent pas être utilisés.
Extensions	Cf. chapitre suivant.

II.2.2. Extensions

Une extension d'un certificat est caractérisée par :

- Sa présence obligatoire ou non dans le certificat. Ceci indique si l'AC émettrice du certificat a l'obligation ou non d'intégrer l'extension dans tous les certificats qu'elle émet.
- Sa criticité. Ceci indique comment les utilisateurs de certificats doivent traiter l'extension et le certificat correspondant, ceci conformément aux principes de gestion de la criticité définis dans [X.509].

Le tableau ci-dessous présente les exigences requises par le [RGS] en complément des exigences définies dans [RFC5280], en précisant le caractère obligatoire de chaque extension (colonne « O », O(ui)/N(on)) et sa criticité (colonne « C », O(ui)/N(on)).

Les extensions qui apparaissent dans ce tableau doivent respecter l'ensemble des exigences correspondantes du [RFC5280], moyennant les compléments et/ou modifications d'exigences définis ici.

Les autres extensions traitées dans le [RFC5280] et qui n'apparaissent pas dans ce tableau doivent respecter strictement les exigences du [RFC5280]. La prise en compte des extensions non obligatoires est laissée au choix de l'AC.

L'intégration de ces autres extensions (obligatoires et non obligatoires) doit respecter les exigences de criticité imposées par le [RFC5280]. Lorsque le [RFC5280] n'impose pas d'exigence de criticité, 15 l'extension doit être systématiquement marquée « non critique ». De même, l'AC peut intégrer des extensions non traitées ni dans le [RFC5280] ni dans le présent document, y compris des extensions propriétaires, mais ces extensions doivent obligatoirement être marquées «non critiques».

Champ	**Intitulé de l'exigence**					
	O	**C**	**PC Type Signature**	**PC Type Authentification**	**PC TypeAuthentification**	**PC Type Confidentialité**
Authority Key Identifier	O	N	Pour tous les certificats porteurs, cette extension doit être présente, être marquée «non critique» et contenir l'identifiant de la clé publique de l'AC émettrice (même valeur que le champ «Subject Key Identifier» du certificat de cette AC émettrice).			
Key Usage	O	O	Le bit «nonRepudiation »[79] doit être à «1», les autres bits à «0».	Le bit « digitalSignature » doit être à «1», les autres bits à «0».	Les bits « nonRepudiation » et « digitalSignature » doivent être à «1», les autres bits à «0».	Le bit « keyEncipherment » pour une clé RSA ou (exclusif) le bit « keyAgreement » ou (exclusif) le bit « dataEncipherment » doit être à «1», les autres bits
Certificate Policies	O	N	Cette extension doit être conforme aux exigences du chapitre 3.2.3 du [RFC3739].			
Subject Alternative Name	N	N	L'identification du porteur via le DN du champ Subject étant obligatoire dans les PC Types du [RGS], le champ Subject Alternative Name peut être présent, mais il doit obligatoirement être marqué «non critique» et être conforme aux exigences du chapitre 4.1.2.4 du [RFC5280].			
Issuer Alternative Name	N	N	L'identification de l'AC émettrice via le DN du champ Issuer étant obligatoire dans les PC Types du [RGS], le champ Issuer Alternative Name peut être présent, mais il doit obligatoirement être marqué « non critique ».			
Subject Directory Attributes	N	N	Si cette extension est utilisée, elle doit être conforme aux exigences du chapitre 3.2.2 du [RFC3739].			
CRL Distribution Points	N	N	S'il est proposé un service de CRL pour vérifier le statut de révocation du certificat concerné, alors cette extension doit être présente, marquée «non critique» et être conforme aux exigences du chapitre 5.4.14 de [ETSI_CERT]. La règle générale est qu'il doit y avoir au moins une manière de vérifier le statut de révocation du certificat (par CRL ou par OCSP).			

[79] Le bit nonRepudiation est désormais nommé contentCommitment

Freshest CRL	N [80]	N	Si l'AC utilise des deltaLCR (ce qui est recommandé par les PC Types du [RGS]), cette extension doit être présente. La syntaxe de cette extension étant identique à celle de «CRL Distribution Points», elle doit être également conforme aux exigences du chapitre 5.4.14 de [ETSI_CERT].
Authority Information Access	N	N	S'il est proposé un service OCSP pour vérifier le statut de révocation du certificat concerné, alors cette extension doit être présente, marquée «non critique» et être conforme aux exigences du chapitre 3.1 du [RFC2560]. La règle générale est qu'il doit y avoir au moins une manière de vérifier le statut de révocation du certificat (par CRL ou par OCSP).
QCStatements	Applicable uniquement pour les certificats de signature électronique (***). Les exigences sont décrites ci-après.		

Extension QCStatements :

Pour les certificats de signature électronique (***), cette extension doit contenir a minima les deux OID évoqués aux chapitres 5.2.1 et 5.2.4 du document [ETSI_QC] :

- esi4-qcStatement-QcCompliance : indique que le certificat émis est qualifié conformément à la législation en vigueur dans le pays dans lequel est établie l'AC :
- esi4-qcStatement-QcSSCD : indique que la clé privée correspondante est stockée dans un dispositif sécurisé de création de signature électronique (SSCD).

En Polynésie française, le PSCE peut faire qualifier son offre de certificat de signature électronique conformément à l'article LP 22 de la [LOIDUPAYS].

II.3. Certificats de services applicatifs

II.3.1. Champs de base

Le tableau ci-dessous reprend l'ensemble des champs de base d'un certificat X.509v3. Un certificat de services applicatifs (serveur par exemple), conforme aux exigences de la PC Type « authentification serveur » ou de la PC Type « cachet », doit respecter, de base, les exigences correspondantes du [RFC5280], moyennant les compléments et/ou modifications d'exigences définis dans ce tableau.

Champ	**Intitulé de l'exigence**
Version	La valeur de ce champ doit être « 2 », indiquant qu'il s'agit d'un certificat version 3.
Serial number	Il doit avoir été généré pour être unique. Il est recommandé que le Serial Number soit non prédictible.
Signature	Cf. chapitre V ci-dessous sur les exigences en matière d'algorithmes et de longueurs de clés.

[80] Si l'AC émet des deltaLCR, ce champ doit être présent. Inversement, si ce champ est présent, l'AC doit fournir le service correspondant.

Issuer	Ce champ est un DN répondant aux exigences du chapitre VII ci-dessous.
Validity	Pas d'exigence supplémentaire par rapport au [RFC5280]
Subject	Ce champ doit être un DN répondant aux exigences du chapitre VII ci-dessous
Subject Public Key Info	Cf. chapitre V ci-dessous sur les exigences en matière d'algorithmes et de longueurs de clés.
Unique Identifiers (issuer et subject)	Les PC Types du [RGS] imposant l'unicité des DN des champs Issuer et Subject au sein du domaine de l'AC, les champs Unique Identifiers ne doivent pas être utilisés.
Extensions	Cf. chapitre suivant.

II.3.2. Extensions

Une extension d'un certificat est caractérisée par :

- Sa présence obligatoire ou non dans le certificat. Ceci indique si l'AC émettrice du certificat a l'obligation ou non d'intégrer l'extension dans tous les certificats qu'elle émet.
- Sa criticité. Ceci indique comment les utilisateurs de certificats doivent traiter l'extension et le certificat correspondant, ceci conformément aux principes de gestion de la criticité définis dans [X.509].

Le tableau ci-dessous présente les exigences requises par le [RGS] en complément des exigences définies dans [RFC5280], en précisant le caractère obligatoire de chaque extension (colonne « O », O(ui)/N(on)) et sa criticité (colonne « C », O(ui)/N(on)).

Les extensions qui apparaissent dans ce tableau doivent respecter l'ensemble des exigences correspondantes du [RFC5280], moyennant les compléments et/ou modifications d'exigences définis ici.

Les autres extensions traitées dans le [RFC5280] et qui n'apparaissent pas dans ce tableau doivent respecter strictement les exigences du [RFC5280]. La prise en compte des extensions non obligatoires est laissée au choix de l'AC.

L'intégration de ces autres extensions (obligatoires et non obligatoires) doit respecter les exigences de criticité imposées par le [RFC5280]. Lorsque le [RFC5280] n'impose pas d'exigence de criticité, l'extension doit être systématiquement marquée «non critique». De même, l'AC peut intégrer des extensions non traitées ni dans le [RFC5280] ni dans le présent document, y compris des extensions propriétaires, mais ces extensions doivent obligatoirement être marquées « non critiques ».

Champ	**O**	**C**	**Intitulé de l'exigence**
Authority Key Identifier	O	N	Pour tous les certificats de services applicatifs, cette extension doit être présente, être marquée « non critique » et contenir l'identifiant de la clé publique de l'AC émettrice (même valeur que le champ « Subject Key Identifier » du certificat de cette AC émettrice).
Key Usage	O	O	*Pour les certificats d'authentification de type serveur SSL/TLS ou de type serveur IPsec :*

			– si le mécanisme d'échange de clé est le chiffrement RSA, le bit « keyEncipherment » doit être à 1 ; – si le mécanisme d'échange de clé est Diffie-Hellman éphémère signé, le bit « digitalSignature » doit être à 1 ; – si le mécanisme d'échange de clé est Diffie-Hellman avec une clé publique fixe, le bit « keyAgreement » doit être à 1. En particulier, cela signifie qu'une clé RSA (qui peut correspondre aux deux premiers cas), peut nécessiter d'avoir les deux bits « keyEncipherment » et « digital signature » à 1. *Pour les certificats d'authentification serveur de type client*- Les bits « digitalSignature » ou (exclusif) « keyAgreement » doivent être à « 1 », tous les autres bits à « 0 ». *Pour les certificats cachet* - Le bit « digitalSignature » (et éventuellement le bit « nonRepudiation ») doit être à «1», tous les autres bits à « 0 ». *Pour les certificats de signature de code* – Le bit « digitalSignature » doit être à « 1 », tous les autres bits à « 0 ».
Certificate Policies	O	N	Cette extension doit être conforme aux exigences du chapitre 4.2.1.4 du [RFC5280].
Subject Alternative Name	O	N	Pour les certificats serveurs de type SSL/TLS, le champ Subject Alternative Name doit être présent. Il doit contenir au moins une entrée de type DNS Name correspondant à l'un des FQDN du service applicatif hébergé par la machine.
Issuer Alternative Name	N	N	L'identification de l'AC émettrice via le DN du champ Issuer étant obligatoire dans les présentes PC Type, le champ Issuer Alternative Name peut être présent, mais il doit obligatoirement être marqué « non critique ».
Subject Directory Attributes	N	N	Si cette extension est utilisée, elle doit obligatoirement être marquée « non critique ».
CRL Distribution Points	N	N	S'il est proposé un service de CRL pour vérifier le statut de révocation du certificat concerné, alors cette extension doit être présente, marquée « non critique ». La règle générale est qu'il doit y avoir au moins une manière de vérifier le statut de révocation du certificat (par CRL ou par OCSP).
Freshest CRL	N	N	Si l'AC utilise des deltaLCR (ce qui est recommandé par les présentes PC Types), cette extension doit être présente. La syntaxe de cette extension étant identique à celle de «CRL Distribution Points», elle doit être également conforme aux exigences du chapitre 5.4.14 de [ETSI_CERT].

	81		
Authority Information Access	N	N	S'il est proposé un service OCSP pour vérifier le statut de révocation du certificat concerné, alors cette extension doit être présente, marquée «non critique» et être conforme aux exigences du chapitre 3.1 du [RFC2560]. La règle générale est qu'il doit y avoir au moins une manière de vérifier le statut de révocation du certificat (par CRL ou par OCSP).
Extended Key Usage	O	N [82]	Pour les certificats cachet dont la clé privée est utilisée pour signer des contremarques de temps, cette extension doit contenir l'identifiant « id-kp-timeStamping « à l'exclusion de tout autre. Pour les certificats dont la clé privée est utilisée pour signer des certificats de répondeurs OCSP, conformément au chapitre 4.2.2.2 de la [RFC2560], cette extension doit contenir l'identifiant « id-kp-OCSPSigning » à l'exclusion de tout autre. Pour les certificats de signature de code, cette extension doit contenir l'identifiant « id-kp-codeSigning « à l'exclusion de tout autre. Pour les certificats d'authentification serveur (authentification et sécurisation de session), tel que défini dans la [RFC5280] cette extension doit contenir les valeurs suivantes : – « id-kp-serverAuth » pour les serveurs de type serveur SSL/TLS ou de type serveur IPsec ; – « id-kp-clientAuth » pour les serveurs « clients ».

II.4. Certificats de recette

Les profils de certificat de recette sont identiques à ceux prévus par le présent document, avec les exceptions suivantes :

- Pour les certificats de personnes, les attributs commonName (CN), givenName (GN), surname (SN), s'ils sont présents dans le certificat, doivent débuter par la chaine de caractères « TEST », suivie d'une espace, suivie de la valeur du champ prévue par la PC de l'AC ;
- Pour les certificats de services applicatifs, l'attribut commonName (CN) doit être présent sauf dans le cas d'un certificat de serveur SSL/TLS ou d'un certificat de signature de code (cf. VIII.3). Si l'attribut CN est présent, il doit débuter par la chaine de caractères « TEST », suivie d'une espace,

[81] Si l'AC émet des deltaLCR, ce champ doit être présent. Inversement, si ce champ est présent, l'AC doit fournir le service correspondant.

[82] Pour les certificats cachet serveur dont la clé privée est utilisée pour signer des contremarques de temps, cette extension doit être marquée critique

suivie de la valeur du champ prévue par la PC de l'AC. Si l'attribut CN n'est pas présent, l'extension SubjectAlternativeName ou le champ OU doit débuter par la chaîne de caractère « TEST ».

Les certificats de recette seront révoqués à la fin de la période de recette.

III. Liste de Certificats Révoqués

III.1. Champs de base

Le tableau ci-dessous reprend l'ensemble des champs de base d'une LCR X.509v2. Une LCR conforme au [RGS] doit respecter, de base, les exigences correspondantes du [RFC5280], moyennant les compléments et/ou modifications d'exigences définis dans ce tableau.

Une LAR est un LCR qui ne contient que des certificats d'AC.

Champ	**Intitulé de l'exigence**
Version	La valeur de ce champ doit être « 1 », indiquant qu'il s'agit d'une LCR version 2.
Signature	Cf. chapitre V ci-dessous sur les exigences en matière d'algorithmes et de longueurs de clés.
Issuer	Ce champ doit être identique au champ « Subject » du certificat d'AC dont la clé privée est utilisée pour signer la LCR (cf. chapitre II.1.1).
This Update	Pas d'exigence supplémentaire par rapport au [RFC5280]
Next Update	Pas d'exigence supplémentaire par rapport au [RFC5280]. Il est recommandé que ce champ soit fonction de la fréquence de publication définie dans le document [RGS_A_13][83]
Revoked Certificates	- userCertificate : pas d'exigence supplémentaire par rapport au [RFC5280] - revocationDate : pas d'exigence supplémentaire par rapport au [RFC5280] - crlEntryExtensions : cf. chapitre III.3
Extensions de LCR	Cf. chapitre suivant.

III.2. Extensions de LCR

Une extension de LCR est caractérisée par :

- Sa présence obligatoire ou non dans la LCR. Ceci indique si l'AC émettrice de la LCR a obligation ou non d'intégrer l'extension dans toutes les LCR qu'elle émet.
- Sa criticité. Ceci indique comment les utilisateurs de la LCR doivent traiter l'extension correspondante, ceci conformément aux principes de gestion de la criticité définis dans [X.509].

Le tableau ci-dessous présente les exigences requises par le [RGS] pour certaines extensions en complément

[83] Exemples :

(*) : next update = this update + 72h*2

(**) : next update = this update + 24h*2

(***) : next update = this update + 36h

de celles du [RFC5280]. Ce tableau précise le caractère obligatoire de chaque extension (colonne « O », O(ui)/N(on)) et sa criticité (colonne « C », O(ui)/N(on)).

Les autres extensions traitées dans le [RFC5280] et qui n'apparaissent pas dans ce tableau doivent respecter strictement les exigences du [RFC5280]. La prise en compte des extensions non obligatoires est laissée au choix de l'AC.

L'intégration de ces autres extensions (obligatoires et non obligatoires) doit respecter les exigences de criticité imposées par le [RFC5280]. Lorsque le [RFC5280] n'impose pas d'exigence de criticité, l'extension doit être systématiquement marquée «non critique». De même, l'AC peut intégrer des extensions non traitées ni dans le [RFC5280] ni dans le présent document, y compris des extensions propriétaires, mais ces extensions doivent obligatoirement être marquées «non critiques».

Champ	**O**	**C**	**Intitulé de l'exigence**
Authority Key Identifier	O	N	Cette extension doit être présente, être marquée «non critique» et contenir l'identifiant de la clé publique de l'AC émettrice (même valeur que le champ «Subject Key Identifier» du certificat de cette AC émettrice).
Issuer Alternative Name	N	N	L'identification de l'AC émettrice via le DN du champ Issuer étant obligatoire dans les présentes PC Type, le champ Issuer Alternative Name peut être présent, mais il doit obligatoirement être marqué « non critique ».
CRL Number	O	N	Cette extension doit obligatoirement être présente, être marquée «non critique» et être conforme aux exigences du [RFC5280]. Ce numéro doit être incrémenté de 1 à chaque nouvelle CRL[84].
Delta CRL Indicator	O[85]	O[86]	S'il s'agit d'une deltaLCR, cette extension doit obligatoirement être présente, être marquée « critique » et être conforme aux exigences du [RFC5280].
Freshest CRL	O[87]	N	Si l'AC utilise des deltaLCR (ce qui est recommandé par les présentes PC Types), cette extension doit être présente dans les LCR complètes (et absente dans les deltaLCR) et son contenu doit être identique au contenu de l'extension « Freshest CRL » des certificats des porteurs couverts par cette LCR (cf. chapitre II.2.2).

III.3. Extensions d'entrée de LCR

Les extensions d'entrées de LCR doivent être conformes aux exigences du [RFC5280].

[84] Ceci permet à un téléservice qui se base sur ce champ d'avoir la garantie qu'il a effectivement récupéré la CRL attendue.

[85] Uniquement s'il s'agit d'une deltaLCR

[86] Uniquement s'il s'agit d'une deltaLCR

[87] Obligatoire uniquement dans les LCR complètes et si l'AC émet des deltaLCR. Inversement, si ce champ est présent, l'AC doit fournir le service correspondant.

Pour les LCR qui comportent des numéros de série correspondant à des certificats d'unité d'horodatage, il est obligatoire de supporter l'extension d'entrée LCR : reasonCode.

IV. Protocoles d'Etat en ligne des Certificats

Il n'y a pas d'exigence spécifique. Le service doit être conforme au [RFC2560].

V. Algorithmes et longueurs de clés

Les règles à respecter concernant le choix et le dimensionnement des algorithmes cryptographiques et des longueurs de clés sont fixées dans le document [RGS_B_1][88].

Conformément au [RFC3279], l'identifiant utilisé dans le champ « subjectPublicKeyInfo » des certificats permet de spécifier l'algorithme cryptographique correspondant à la clé certifiée[89], mais ne permet pas de spécifier l'éventuel algorithme de hachage à utiliser en liaison avec cet algorithme cryptographique. L'information concernant les fonctions de hachage est donc fournie dans ce document à destination des applications et non pas à destination des AC. Si ce n'est pas l'AC qui génère le bi-clé du porteur / serveur, elle doit s'assurer que celle-ci est conforme aux exigences de ce chapitre. Pour les algorithmes pouvant être utilisés pour divers usages cryptographiques (authentification, signature, confidentialité), l'usage de la clé doit être restreint au travers du champ « keyUsage » du certificat.

[88] rsaEncryption, id-dsa, id-ecPublicKey, dhpublicnumber, id-ecPublicKey.

[89] rsaEncryption, id-dsa, id-ecPublicKey, dhpublicnumber, id-ecPublicKey.

VI. Annexe 1 - Documents de référence

VI.1. Réglementation

Renvoi	Document
[LOIDUPAYS]	Loi du pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices
[RGS]	Référentiel Général de Sécurité – Version 1.0

VI.2. Documents techniques

Renvoi	Document
[ETSI_CERT]	ETSI - TS 102 280 - X.509 V3 Certificate Profile for Certificates Issued to Natural Persons, V1.1.1 mars 2004
[ETSI_QC]	ETSI - TS 101 862 - Qualified certificate Profile, V1.3.3 janvier 2006
[PKCS#1]	RSA Laboratories - PKCS #1 v2.1 - RSA Cryptography Standard, 14 juin 2002
[RFC2560]	IETF - Internet X.509 Public Key Infrastructure - Online Certificate Status Protocol, RFC 2560 - juin 1999
[RFC3279]	IETF - Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure -Certificate and Certificate Revocation List (CRL) Profil - avril 2002
[RFC3739]	IETF - Internet X.509 Public Key Infrastructure, Qualified Certificates Profile, RFC 3739 - mars 2004
[RFC5280]	IETF - Internet X.509 Public Key Infrastructure, Certificate and CRL Profile, RFC 5280-mai 2008
[RGS_B_1]	Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, Version 1.0
[X.509]	ITU - Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks, Recommendation X.509, version 08/2005 (complétée par les correctifs techniques Corrigendum 1 de 01/2007, Corrigendum 2 de 11/2008)

VII. Annexe 2 - Exigences sur les identifiants d'AC, de porteurs et de services applicatifs

VII.1. Identification d'une Autorité de Certification

Le DN qui se trouve dans le champ « Subject » d'un certificat d'AC, dans le champ « Issuer » d'un certificat d'AC ou d'utilisateur final, ainsi que dans le champ « Issuer » d'une LCR, doivent être conforme aux exigences des chapitres 4.1.2.4 de la RFC [5280], 3.1.1 de [RFC3739] et 5.2.4 de [ETSI_CERT], ainsi qu'aux exigences supplémentaires du présent chapitre.

Ce DN doit être encodé en printableString ou en UTF8String.

Le nom commun (attribut commonName) mentionné dans le champ « émetteur « des AC, doit identifier précisément l'AC émettrice ; il est recommandé de porter dans ce champ un libellé représentatif de l'activité de l'AC émettrice du certificat.

L'attribut countryName doit être présent et doit indiquer le pays de l'autorité compétente auprès de laquelle l'entité émettant le certificat est officiellement enregistrée (tribunal de commerce, ministère,…). Il doit être renseigné en lettres majuscules.

L'attribut organizationName doit être présent et doit contenir le nom officiel complet de l'entité tel qu'enregistré auprès des autorités compétentes (cf. [ETSI_CERT]). Un nom différent du nom officiel complet de l'entité peut être toléré si le nom utilisé est similaire au nom officiel et identifie l'entité de manière non-ambiguë.

Une instance de l'attribut organizationalUnitName doit être présente et doit contenir l'identification de l'entité. L'instance de cet attribut doit être structurée conformément à la norme ISO 6523 et le format retenu est « <ICD> <Identification de l'organisation> » :

- l'ICD est sur 4 caractères ;
- l'identification de l'organisation sur 35 caractères :
- le séparateur entre les deux chaînes est un espace.

Pour les entités établies en France métropolitaine :

- ICD = 0002 ;
- l'identification est le n° SIREN ou le n° SIRET (9 caractères pour le n° SIREN et de 14 caractères pour le n° SIRET). Cette identification ne doit pas comporter d'espace. Ceci est cohérent avec la formalisation XML proposée par l'INSEE.

Pour les entités non établies en France métropolitaine, plusieurs possibilités existent :

- soit il n'y a pas d'instance de l'attribut organizationalUnitName conforme à la norme ISO 6523 et auquel cas elle ne doit pas commencer par 4 chiffres
- soit l'attribut organizationalUnitName est présent mais avec un numéro ICD différent de 0002
- soit l'attribut organizationalUnitName est présent et avec un numéro ICD égal à 0002, auquel cas il doit impérativement être suivi d'un numéro SIREN ou SIRET puisqu'il s'agit d'un établissement enregistré en France métropolitaine.

D'autres instances de l'attribut organizationalUnitName peuvent être présentes mais ne doivent pas commencer par 4 chiffres.

Exemple de DN : C=FR, O= Société ABC, OU= 0002 243516879, OU= Centre de Paris

VII.2. Identification de porteur

Le DN qui se trouve dans le champ «Subject» d'un certificat remis à une personne (par opposition à une machine) doit être conforme aux exigences des chapitres 4.1.2.6 du [RFC5280], 3.1.2 du [RFC3739] et 5.2.6 de [ETSI_CERT], ainsi qu'aux exigences supplémentaires du présent chapitre.

Les attributs du DN doivent être encodés en printableString ou en UTF8String[90].

VII.2.1. Certificats [ENTREPRISE] et [ADMINISTRATION]

Si le certificat n'est pas un certificat pseudonyme, une identification de l'entité à laquelle le porteur est rattaché est obligatoire.

L'attribut countryName doit être présent et doit indiquer le pays de l'autorité compétente auprès de laquelle l'entité est officiellement enregistrée (tribunal de commerce, ministère, …). Il doit être renseigné en lettres majuscules.

L'attribut organizationName doit être présent et doit contenir le nom officiel complet de l'entité tel qu'enregistré auprès des autorités compétentes. Un nom différent du nom officiel complet de l'entité peut être toléré si le nom utilisé est similaire au nom officiel et identifie l'entité de manière non-ambiguë.

Une instance de l'attribut organizationalUnitName doit être présente et doit contenir l'identification de cette entité telle que définie au chapitre VII.1.

Si d'autres instances de l'attribut organizationalUnitName sont présentes, elles ne doivent pas commencer par 4 chiffres.

Le CN doit être conforme au § VII.2.2.

VII.2.2. Certificats [ENTREPRISE], [ADMINISTRATION], [PARTICULIER]

L'attribut countryName doit être présent.

Si le certificat est un certificat pseudonyme, l'attribut *pseudonym* doit être utilisé mais pas les attributs givenName (GN), surname (SN) et commonName (CN) conformément à la [RFC3739].

Si le certificat n'est pas un certificat pseudonyme, deux possibilités :

- utilisation des attributs givenName et surname : l'attribut givenName doit comporter le un des prénoms de l'état civil du porteur (si la pièce d'identité présentée pour l'enregistrement comporte d'autres prénoms, il n'y a pas d'obligation à mentionner ces autres prénoms dans le certificat, mais s'ils le sont, ils doivent l'être dans le même ordre que sur la pièce d'identité et séparés par une virgule sans espace ni avant ni après la virgule) et l'attribut surname doit comporter le nom de l'état civil ou le nom d'usage du porteur. Pour les prénoms et noms composés, le tiret est utilisé comme élément séparateur. L'attribut commonName peut également être utilisé, dans ce cas l'AC précise dans sa PC

[90] A l'exception des attributs `emailAddress` et `dc(domaincomponent)` qui, lorsque présents dans le DN du champ « Subject » doivent être en `IA5String` (afin de permettre la saisie du caractère « @ »).

son format et la sémantique correspondante. La distinction des cas d'homonymie au sein du domaine de l'AC peut se faire au travers de l'attribut commonName ;

- seul l'attribut commonName est utilisé : il doit comporter un des prénoms de l'état civil du porteur (si la pièce d'identité présentée pour l'enregistrement comporte d'autres prénoms, il n'y a pas d'obligation à mentionner ces autres prénoms dans le certificat, mais s'ils le sont, ils doivent l'être dans le même ordre que sur la pièce d'identité et séparés par une virgule sans espace ni avant ni après la virgule), suivi d'un espace, suivi du nom de l'état civil ou le nom d'usage du porteur. Pour les prénoms et noms composés, le tiret est utilisé comme élément séparateur. A la suite du nom d'état civil ou du nom d'usage, et en fonction des besoins de l'AC, d'autres informations peuvent être mentionnées dans cet attribut (séparées par des espaces), notamment des informations permettant de traiter les cas d'homonymie au sein du domaine de l'AC. L'AC doit préciser dans sa PC le format exact et la sémantique correspondante de l'attribut commonName.

Exemples de DN :

- C=FR, O= Société DEF, OU= 0002 243516879, OU= Site de Toulouse, CN= Michel Martin
- C=FR, O= Société DEF, OU= 0002 243516879, OU= Site de Toulouse, GN= Michel + SN = Martin

VII.3. Identification d'un service applicatif

Est entendu par « service applicatif « :

- un service de création de cachet tel que décrit dans la PC Type « Certificats électroniques de services applicatifs » ;
- «un service d'authentification de serveur tel que décrit dans la PC Type « Certificats électroniques de services applicatifs ».

Le DN qui se trouve dans le champ «Subject» d'un certificat remis à un service applicatif (par opposition à une personne physique) doit être conforme aux exigences des chapitres 4.1.2.6 du [RFC5280] et 5.2.6 de [ETSI_CERT], ainsi qu'aux exigences supplémentaires du présent chapitre.

Ce DN doit être encodé en printableString ou en UTF8String.

L'attribut countryName doit être présent et doit indiquer le pays de l'autorité compétente auprès de laquelle l'entité est officiellement enregistrée (tribunal de commerce, ministère…). Il doit être renseigné en lettres majuscules.

L'attribut organizationName doit être présent et doit contenir le nom officiel complet de l'entité tel qu'enregistré auprès des autorités compétentes et à laquelle le serveur est rattaché. Un nom différent du nom officiel complet de l'entité peut être toléré si le nom utilisé est similaire au nom officiel et identifie l'entité de manière non-ambiguë.

Une instance de l'attribut organizationalUnitName doit être présente et doit contenir l'identification de cette entité telle que définie au chapitre VII.1.

L'attribut commonName doit être utilisé et doit contenir un nom significatif du service applicatif, à l'exception des deux cas particuliers suivants :

- lorsqu'il s'agit d'un certificat serveur de type SSL/TLS, l'attribut commonName est facultatif. S'il est présent, il doit contenir un FQDN (Fully Qualified Domain Name) du serveur également présent dans l'extension SubjectAlternativeName. S'il est absent, l'extension SubjectAlternativeName doit

être critique ;

- lorsqu'il s'agit d'un certificat de signature de code, l'attribut commonName est facultatif. S'il est présent, il ne doit pas contenir un FQDN.

Les attributs givenName et surname ne doivent pas être utilisés.

Si un nom DNS (Domain Name System) est présent dans le commonName la [RFC1123] section 2.1 doit être appliquée en plus du [RFC1034]. Ceci permet de contrôler la validité du nom.

Si d'autres instances de l'attribut organizationalUnitName sont présentes, elles ne doivent pas commencer par 4 chiffres.

Exemple de DN : C=FR, O= Société ABC, OU= 0002 243516879, OU= Site de Toulouse, CN= www.abc.fr

Lorsqu'il s'agit d'un service de création de cachet, pour préserver l'unicité des noms, il est proposé la règle de nommage suivante pour le champ CN :

[Nom de l'organisme].[Nom du bureau responsable du serveur].[Nom du service applicatif]

Annexe A5

Politique d’Horodatage Type

Historique des versions		
Date	**Version**	**Évolution du document**
xxx	1.0	Publication de la première version de l'annexe A5 du référentiel général de sécurité

Avant-propos

Le présent document fait partie du référentiel général de sécurité (RGS), pris en application de l'article LP 20 de la loi du pays n° 2017-30 du xxx relative à la dématérialisation des actes des autorités administratives et aux téléservices, et de son arrêté d'application.

Le présent document et ses annexes sont une copie adaptée du RGS A5 – Politique d'Horodatage Type, en vigueur en métropole, version 3.0 du 27 février 2014.

Le texte fait des renvois à des documents publiés par l'Agence nationale de la sécurité des systèmes d'information[91] (ANSSI) ou encore disponibles sur son site internet www.ssi.gouv.fr, en ce qu'ils reflètent l'état de l'art en matière de sécurité informatique.

Le référentiel et ses annexes sont disponibles en ligne sur le site internet www.lexpol.pf, et leur mise à jour est assurée par la Direction générale de l'économie numérique.

[91] L'ANSSI est un service à compétence nationale rattaché au Secrétaire général de la défense et de la sécurité nationale, l'autorité chargée d'assister le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale. Parmi ses nombreux objectifs, l'un d'eux consiste à promouvoir un espace de confiance pour les services en ligne. Elle y participe en ce sens notamment au travers de la règlementation (référentiels) et ses labels (certification des produits de sécurité et qualification des produits de sécurité et des prestataires de service de confiance).

I. Introduction

I.1.Présentation générale

Le présent document fait partie des documents constitutifs du [RGS]. Il concerne la fonction de sécurité « horodatage « et constitue la politique d'horodatage type (PH Type) destinée aux prestataires de services d'horodatage électronique (PSHE) souhaitant fournir des contremarques de temps à des usagers, des agents ou des applications. Il a également pour objet de renseigner les usagers, les agents et promoteurs d'applications utilisant de telles contremarques de temps.

Le service d'horodatage est composé d'un seul niveau de sécurité.

Afin de sécuriser les systèmes d'informations sous la responsabilité d'une autorité administrative (AA), celle-ci peut recourir à la fonction de sécurité « horodatage «. Dès lors, l'autorité administrative doit utiliser des jetons d'horodatage délivrés par des PSHE conformes à la présente PH Type.

Un PSHE peut demander la qualification de son offre de service (délivrance de jetons d'horodatage) selon les modalités prévues par l'article LP 22 de la [LOIDUPAYS]. Cette qualification permet d'attester de la conformité de l'offre du PSHE au présent référentiel.

Les exigences spécifiées dans la présente PH Type doivent être respectées intégralement par les PSHE, moyennant l'exception suivante. Dans la présente PH Type, un certain nombre de recommandations sont formulées. Les PSHE sont incités à les respecter également dès maintenant car ces recommandations, qui ne sont pas d'application obligatoire dans la présente version de ce document, devraient le devenir dans une version ultérieure.

Cette PH Type n'est pas une PH à part entière : elle ne peut pas être utilisée telle quelle par un PSHE en tant que PH pour être mentionnée dans ses contremarques de temps et sa DPH. Un PSHE souhaitant être qualifié par rapport à la présente PH Type doit en reprendre, dans sa propre PH, l'ensemble des engagements.

La présente PH Type a été élaborée sur la base de la politique d'horodatage de l'ETSI [ETSI_PH]. Les différences entre la PH Type et [ETSI_PH] sont présentées au chapitre XIII.

I.2. Identification du document

La présente PH Type est dénommée « RGS - Politique d'Horodatage Type ». Elle peut être identifiée par son nom, numéro de version, et sa date de mise à jour.

1.3. Qu'est-ce que l'horodatage ?

- L'horodatage permet d'attester qu'une donnée existe à un instant donné. Pour cela, il convient d'associer une représentation sans équivoque d'une donnée, par exemple une valeur de hachage associée à un identifiant d'algorithme de hachage, à un instant dans le temps. La garantie de cette association est fournie au moyen d'une contremarque de temps qui est une structure signée qui contient en particulier :
- L'identifiant de la politique d'horodatage sous laquelle la contremarque de temps a été générée ;
- La valeur de hachage et l'algorithme de hachage de la donnée qui a été horodatée ;
- La date et le temps UTC ;
- L'identifiant du certificat de l'Unité d'horodatage (UH) qui a généré la contremarque de temps (qui contient aussi le nom de l'Autorité d'horodatage).

L'horodatage ne nécessite pas le déploiement d'une infrastructure étendue pour que la validité des certificats des unités d'horodatage puisse être vérifiée. En particulier, les utilisateurs finaux ne doivent pas nécessairement avoir des certificats eux-mêmes, mais doivent avoir accès aux informations de validité des certificats d'horodatage (chaîne de certification, LRC…) pour vérifier les contremarques de temps.

La clé privée ou les clés utilisées pour générer les contremarques de temps sont gérées par l'Autorité d'horodatage qui conserve la pleine et entière responsabilité pour satisfaire aux exigences définies dans le document actuel. Une Autorité d'horodatage peut faire fonctionner plusieurs unités d'horodatage (UH). Chaque unité d'horodatage dispose de sa propre bi-clé.

I.4. Comment établir la confiance en l'horodatage

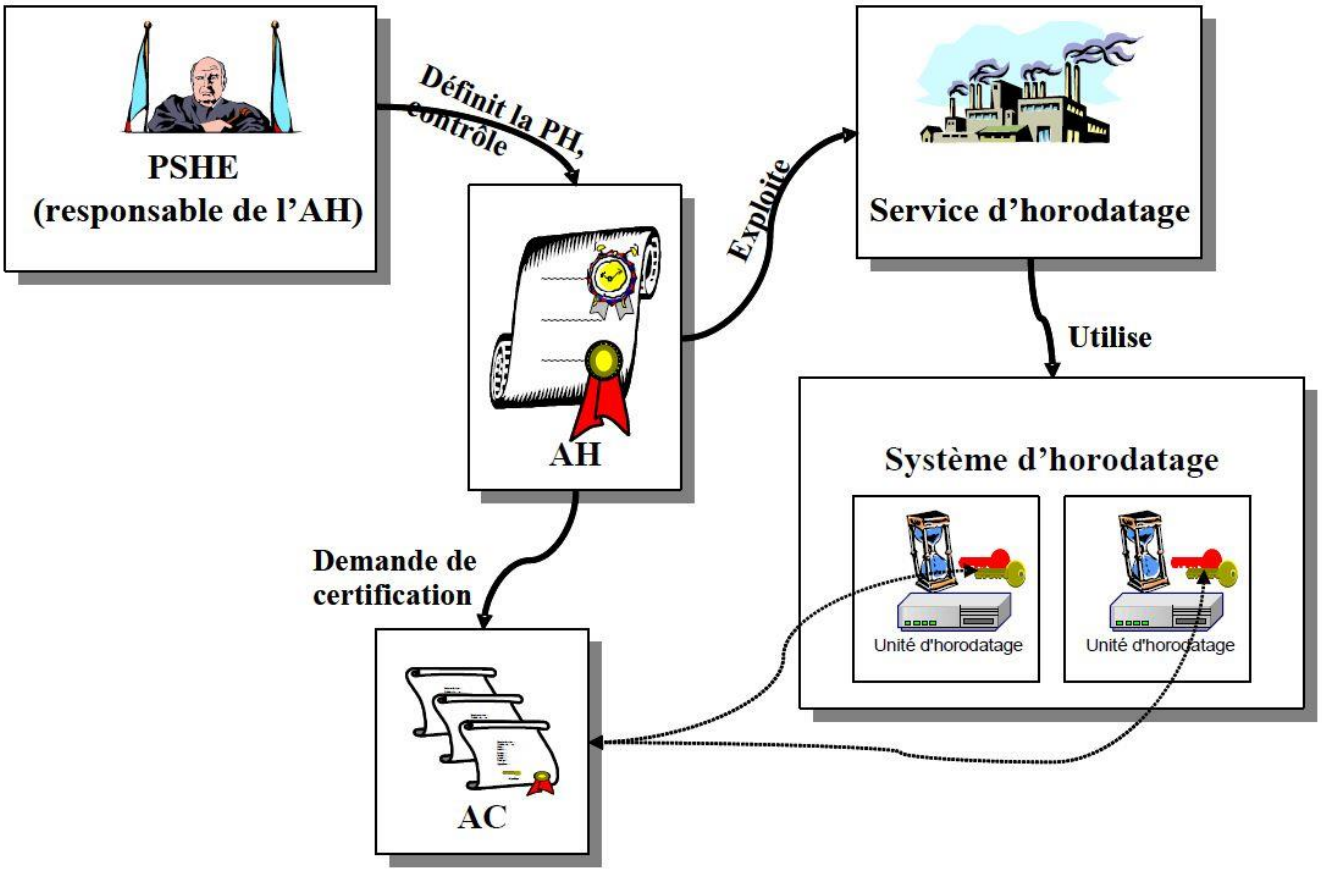
La garantie apportée par l'autorité d'horodatage s'appuie sur des éléments techniques (décrits précédemment) et des règles de gestion qui sont présentées dans la politique d'horodatage. La politique d'horodatage présente aux utilisateurs les engagements que prend l'autorité d'horodatage, notamment ceux pris en matière de sécurité, et décrit de façon macroscopique les moyens mis en œuvre pour tenir ces engagements. Elle revêt une grande importance car elle incarne le niveau de confiance atteint par le service d'horodatage. Elle traduit la reconnaissance formelle de l'importance accordée par l'autorité d'horodatage à la sécurité du service.

Les exigences pour les services d'horodatage décrits dans le document incluent des exigences portant, à la fois sur la gestion de l'horodatage et sur le fonctionnement des unités d'horodatage qui publient les contremarques de temps. L'Autorité d'horodatage, telle qu'identifiée dans la contremarque de temps, a la responsabilité d'assurer que ces exigences sont remplies (par exemple par des obligations contractuelles).

Elle peut sous-traiter à d'autres parties un sous-ensemble des services d'horodatage.

Par exemple, des organisations accueillant des unités d'horodatage peuvent exiger de contrôler l'utilisation du service et, au minimum, de savoir si le service est opérationnel ou être capable de mesurer le fonctionnement du service, par exemple le nombre de contremarques de temps produites pendant une période de temps. Un tel contrôle peut être considéré comme étant extérieur au service d'horodatage. La description des opérations de gestion décrites dans le corps principal du document n'est donc pas limitative. La surveillance des opérations, si elle est exécutée directement sur l'unité d'horodatage, peut être autorisée par le fournisseur du service d'horodatage.

I.5. Présentation des rôles et relations



La notion d'Autorité d'Horodatage (AH) telle qu'utilisée dans la présente PH Type est définie au chapitre II.1 ci-dessous.

L'AH exploite l'ensemble des services d'horodatage qui regroupe les diverses prestations organisationnelles et techniques nécessaires à la génération et à la gestion des contremarques de temps. Chaque UH signe ses contremarques de temps à l'aide d'une clé privée dont la clé publique correspondante a été certifiée au préalable par une autorité de certification (AC). Les clés privées sont conservées et mises en œuvre dans des modules d'horodatage.

I.6.Autres aspects

D'un point de vue technique, cette politique s'appuie sur un module d'horodatage pour la protection des clés de signature et de l'horloge.

II. Généralités

II.1. Définitions

Abonné - Entité ayant besoin de faire horodater des données par une Autorité d'horodatage et qui a accepté les conditions d'utilisation de ses services.

Autorité de Certification (AC) - Cf. les Politiques de Certification Types du [RGS].

Autorité d'horodatage (AH) - Au sein d'un PSHE, une Autorité d'Horodatage a en charge, au nom et sous la responsabilité de ce PSHE, l'application d'au moins une politique d'horodatage en s'appuyant sur une ou plusieurs Unités d'Horodatage. Dans le cadre de la présente PH Type, le terme de PSHE n'est pas utilisé en dehors du présent chapitre et du chapitre I.1 et le terme d'AH est le seul utilisé. Il désigne l'AH chargée de l'application de la politique d'horodatage, répondant aux exigences de la présente PH Type, au sein du PSHE souhaitant faire qualifier la famille de contremarques de temps correspondante.

Contremarque de temps - Donnée signée qui lie une représentation d'une donnée à un temps particulier, exprimé en heure UTC, établissant ainsi la preuve que la donnée existait à cet instant-là.

Coordinated Universal Time (UTC) - Echelle de temps liée à la seconde, telle que définie dans la recommandation ITU-R TF.460-5 [TF.460-5].

Nota - Pour la plupart des usages, le temps UTC est équivalent au temps solaire au méridien principal (0°). De manière plus précise, le temps UTC est un compromis entre le temps atomique particulièrement stable (Temps Atomique International -TAI) et le temps solaire dérivé de la rotation irrégulière de la terre lié au temps moyen sidéral de Greenwich (GMST) par une relation de convention.

Déclaration des pratiques d'horodatage (DPH) - Une DPH identifie les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que l'AH applique dans le cadre de la fourniture de ses services d'horodatage et en conformité avec la ou les politiques d'horodatage qu'elle s'est engagée à respecter.

Jeton d'horodatage - Voir contremarque de temps.

Module d'horodatage - Produit de sécurité comportant une ressource cryptographique et qui est dédié à la mise en œuvre des fonctions d'horodatage de l'UH, notamment la génération, la conservation et la mise en œuvre de la clé privée de signature de l'UH ainsi que la génération des contremarques de temps.

Politique d'horodatage (PH) - Ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une AH se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'une contremarque de temps à une communauté particulière et/ou une classe d'application avec des exigences de sécurité communes. Une PH peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les abonnés et les utilisateurs de contremarques de temps.

Prestataire de services d'horodatage (PSHE) - Un PSHE est un type de PSCO particulier. Un PSHE se définit comme toute personne ou entité qui est responsable de la génération et de la gestion de contremarques de temps, vis-à-vis de ses abonnés et des utilisateurs de ces contremarques de temps. Un PSHE peut fournir différentes familles de contremarques de temps correspondant à des finalités différentes et/ou des niveaux de sécurité différents. Un PSHE comporte au moins une AH mais peut en comporter plusieurs en fonction de son organisation. Un PSHE est identifié dans les certificats de clés publiques des UH dont il a la responsabilité au travers de ses AH.

Produit de sécurité - Un dispositif matériel ou logiciel, ou les composants correspondants du dispositif matériel ou logiciel, qui sont destinés à être utilisés pour la fourniture de services de confiance et nécessaires à la sécurisation d'une information ou d'un système.

Qualification d'un produit de sécurité - La qualification d'un produit de sécurité permet d'attester de la conformité d'un produit à un niveau de sécurité du [RGS]. Conformément à l'article LP 22 de la [LOIDUPAYS], cette qualification correspond à la qualification délivrée par les autorités de métropole en application de l'[ORDONNANCE]. **Qualification d'un prestataire de services d'horodatage** - La qualification d'un PSHE permet d'attester de la conformité de tout ou partie de l'offre d'horodatage d'un PSHE à un niveau de sécurité du [RGS]. Conformément à l'article LP 22 de la [LOIDUPAYS], cette qualification correspond à la qualification délivrée par les autorités de métropole en application de l'[ORDONNANCE].

Service d'horodatage - Ensemble des prestations nécessaires à la génération et à la gestion de contremarques de temps.

Système d'horodatage - Ensemble des unités d'horodatage et des composants d'administration et de supervision utilisés pour fournir des services d'horodatage.

Unité d'Horodatage (UH) - Ensemble de matériel et de logiciel en charge de la création de contremarques de temps caractérisé par un identifiant de l'unité d'horodatage accordé par une AC, et une clé unique de signature de contremarques de temps.

UTC(k) - Temps de référence réalisé par le laboratoire «k» et synchronisé avec précision avec le temps UTC, dans le but d'atteindre une précision de ±100 ns, selon la recommandation S5 (1993) du Comité Consultatif pour la définition de la Seconde. (Rec. ITU-R TF.536-1 [TF.536-1]).

Nota - Une liste des laboratoires UTC(k) est indiquée dans la section 1 de la Circulaire T publiée par le BIPM et est disponible sur le site web du BIPM (www.bipm.org).

Usager - Toute personne physique ou toute personne morale de droit privé, à l'exception de celles qui sont chargées d'une mission de service public lorsqu'est en cause l'exercice de cette mission. Selon le contexte, un usager peut être un porteur ou un utilisateur de certificats

Utilisateur de contremarque de temps – Entité (personne ou système) qui fait confiance à une contremarque de temps émise sous une politique d'horodatage donnée par une autorité d'horodatage donnée.

Utilisateur final - Abonné ou utilisateur de contremarques de temps.

II.2. Abréviations

Pour le présent document, les abréviations suivantes s'appliquent :

AC	Autorité de Certification
AH	Autorité d'horodatage
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CG	Conditions Générales d'utilisation du service d'horodatage
Delta-LRC	Liste de Révocation des Certificats partielle
DGME	Direction Générale de la Modernisation de l'Etat
DPH	Déclaration des Pratiques d'Horodatage
ETSI	European Telecommunications Standards Institute
LCR	Liste des Certificats Révoqués
IGC	Infrastructure de Gestion de Clés
OID	Object Identifier
PH	Politique d'Horodatage
PP	Profil de Protection
PSHE	Prestataire de Services d'Horodatag
UH	Unité d'Horodatage
UTC	Coordinated Universal Time

III. Politique d'horodatage

Pour cette politique, la date et le temps de chaque contremarque de temps doivent être synchronisés avec le temps UTC avec une exactitude précisée dans la déclaration des pratiques d'horodatage[92].

La présente PH Type impose un format de contremarque de temps spécifique, qui doit répondre aux exigences du chapitre VIII ci-dessous.

Cette politique n'impose pas l'usage d'un protocole d'horodatage spécifique pour demander et obtenir une contremarque de temps auprès d'une AH. Cependant, un protocole a été défini dans le [RFC3161] et profilé dans le document [ETSI_TSP] et son usage est recommandé.

Paramètres utilisés pour la politique d'horodatage

Les caractéristiques principales de cette politique sont comme suit :

- La protection des clés et de l'horloge doit respecter les exigences spécifiées au chapitre IX ci-dessous ;
- L'AC générant les certificats de clé publique pour les unités d'horodatage doit gérer le service de révocation pour chaque certificat publié.

[92] Il est recommandé que celle-ci soit d'une seconde. Elle ne doit en tout cas pas excéder la minute.

IV. Déclaration des Pratiques d'Horodatage

La déclaration des pratiques d'horodatage expose les mécanismes et les procédures mis en œuvre pour atteindre les objectifs de sécurité de la politique d'horodatage, en particulier les processus qu'une Autorité d'horodatage emploiera pour la création des contremarques de temps et le maintien de l'exactitude de ses horloges.

La déclaration des pratiques d'horodatage doit être une description détaillée des pratiques opérationnelles d'une Autorité d'horodatage mise en œuvre pour la délivrance des contremarques de temps et la gestion des services d'horodatage.

Une déclaration des pratiques d'horodatage doit définir comment l'Autorité d'horodatage se conforme aux exigences physiques, environnementales, procédurales, organisationnelles et techniques identifiées dans une politique d'horodatage. Une politique d'horodatage est ainsi un document moins spécifique qu'une déclaration des pratiques d'horodatage. Une politique d'horodatage est définie indépendamment des détails particuliers de l'environnement spécifique d'exploitation d'une Autorité d'horodatage, tandis qu'une déclaration des pratiques d'horodatage est façonnée à la structure organisationnelle, aux procédures d'exploitation, aux équipements et à l'environnement de travail d'une Autorité d'horodatage.

La déclaration des pratiques d'horodatage est toujours approuvée par le PSHE.

Contrairement à la politique d'horodatage, la DPH n'a pas pour objet d'être intégralement publiée. Cependant, l'Autorité d'horodatage est tenue de publier les parties publiques des déclarations des pratiques d'horodatage et en particulier :

- Le cadre d'application de la DPH ;
- Les coordonnées de l'AH ;
- La PH appliquée ;
- Les algorithmes de hachage autorisés pour constituer l'objet horodaté ;
- La durée minimum pendant laquelle il est possible de vérifier les contremarques de temps, à compter de leur date de génération ;
- La précision de la date des contremarques de temps par rapport à l'échelle de temps UTC ;
- Les obligations des abonnés ;
- Les obligations des utilisateurs de contremarque de temps ;
- Les informations permettant de vérifier la contremarque de temps ;
- Les limitations de responsabilité.

Ces informations publiques peuvent être présentées sous la forme d'un document indépendant (extrait de la DPH) ou bien intégrées aux conditions générales d'utilisation (cf. chapitre suivant).

V. Conditions générales d'utilisation

Compte tenu de la complexité de lecture d'une PH et d'une DPH pour des utilisateurs non-spécialistes du domaine, l'AH doit définir également des conditions générales d'utilisation correspondant aux «TSA Disclosure Statement» (TDS) définis par [ETSI_PH].

Ces conditions générales d'utilisation ne sont pas destinées à remplacer la politique d'horodatage ou la déclaration des pratiques d'horodatage mais sont destinées à des abonnés et à des utilisateurs de contremarques de temps non-techniciens afin qu'ils puissent facilement comprendre l'information essentielle dont ils doivent avoir connaissance.

Des conditions générales d'utilisation peuvent aider une Autorité d'horodatage à démontrer comment elle répond aux exigences réglementaires, en particulier celles liées à la protection du consommateur.

Une Autorité d'horodatage spécifiera dans ses conditions générales d'utilisation les identifiants des politiques d'horodatage supportées.

Les Autorités d'horodatage sont tenues de définir leurs propres conditions générales d'utilisation et de les rendre disponibles aux abonnés et aux utilisateurs de contremarques de temps sous une ou des forme(s) lisible(s), compréhensible(s) et pérenne(s).

Il est recommandé que ces conditions générales aient une structure conforme à celle décrite en annexe B de [ETSI_PH] et reprennent ainsi, à destination des abonnés et des utilisateurs, les informations pertinentes de la PH et la DPH de l'AH (conditions d'usages des contremarques de temps, obligations et responsabilités des différentes parties, garanties et limites de garanties de l'AH, etc. : cf. chapitre VI.1.6).

Ces conditions générales d'utilisation peuvent être présentées :

- sous la forme de documents indépendants, et/soit ;
- dans le contrat avec l'abonné et/ou les utilisateurs, et/soit ;
- dans la déclaration des pratiques d'horodatage à condition qu'elles soient compréhensibles au lecteur, dans ce cas cette partie de la DPH devra être publiée.

VI. Contenu de la politique d'horodatage

Ce chapitre décrit les dispositions générales ainsi que les exigences opérationnelles, physiques et environnementales, procédurales et organisationnelles et enfin de sécurité technique, auxquelles l'AH doit se conformer. Cet ensemble de règle précise le contenu d'une politique d'horodatage.

VI.1. Dispositions générales

VI.1.1. Obligations de l'Autorité d'horodatage

L'Autorité d'horodatage doit garantir la conformité des exigences et des procédures prescrites dans cette politique, même quand les fonctionnalités d'horodatage sont remplies par des sous-traitants.

L'Autorité d'horodatage doit garantir l'adhésion aux obligations complémentaires indiquées dans la contremarque de temps ou bien directement ou bien incorporée par référence.

L'Autorité d'horodatage doit fournir des services d'horodatage conformément à sa déclaration des pratiques d'horodatage.

L'Autorité d'horodatage doit remplir tous ses engagements tels que stipulés dans ses conditions générales d'utilisation.

VI.1.2. Obligations de l'abonné

Au-delà des exigences spécifiques incluses dans les conditions générales d'utilisation du service d'horodatage, et que doit respecter l'abonné, il est recommandé que ce dernier, au moment de l'obtention d'une contremarque de temps, vérifie que le certificat de l'unité d'horodatage n'est pas révoqué, mais cela dépend de l'environnement d'utilisation. En effet, si le certificat est émis par le système d'information, il peut être superflu de vérifier celui-ci systématiquement, l'organisme utilisateur doit apprécier l'impact d'une erreur découverte par échantillonnage et le risque de certificats erronés entre deux contrôles au regard des performances. Inversement, si les certificats d'UH proviennent d'AH différentes, une vérification systématique est fortement recommandée.

VI.1.3. Obligations de l'utilisateur de contremarques de temps

Les conditions générales d'utilisation disponibles pour les utilisateurs de contremarques de temps doivent inclure une obligation qui spécifie que, pour faire confiance à une contremarque de temps, il devra :

a) Vérifier que la contremarque de temps a été correctement signée, et que le certificat de l'unité d'horodatage est valide à l'instant de la vérification.

   Nota - Pendant la validité du certificat d'une unité d'horodatage, la validité de la clé de signature peut être vérifiée en utilisant l'état de révocation courant du certificat de l'unité d'horodatage. Si le temps de vérification excède la fin de la période de validité du certificat correspondant, voir le chapitre X ci-dessous.

b) Tenir compte des limitations sur l'utilisation de la contremarque de temps indiquées dans la politique d'horodatage, la déclaration des pratiques d'horodatage et les conditions générales d'utilisation.

VI.1.4. Obligations pour les AC fournissant les certificats des unités d'horodatage

Les certificats des clés publiques délivrés aux unités d'horodatage doivent être délivrés par des prestataires

de service de certification électronique (PSCE) conformes au RGS, c'est à dire respectant au minimum les exigences du niveau de sécurité une étoile (*) de la Politique de Certification Type «cachet serveur». Un prestataire de service d'horodatage (PSH) souhaitant faire qualifier son service d'horodatage devra recourir à un service de certification électronique d'un PSCE lui même qualifié

Nota - Les certificats des unités d'horodatage peuvent être générés par une Autorité de Certification opérée par la même organisation que l'Autorité d'horodatage, ou par une organisation différente.

VI.1.5. Déclarations des pratiques d'horodatage

L'Autorité d'horodatage doit garantir qu'elle possède la fiabilité nécessaire pour fournir des services d'horodatage. En particulier :

a) L'Autorité d'horodatage doit faire effectuer une évaluation de risques pour évaluer les actifs et les menaces pour ces actifs afin de déterminer les contrôles de sécurité nécessaires et les procédures opérationnelles.

b) L'Autorité d'horodatage doit avoir une déclaration des pratiques et des procédures utilisées pour adresser toutes les exigences identifiées dans chaque politique d'horodatage supportée.

   Nota - Cette politique n'impose aucune exigence quant à la structure de la déclaration des pratiques d'horodatage.

c) La déclaration des pratiques d'horodatage doit identifier les obligations de toutes les organisations externes participant à la fourniture des services d'horodatage, y compris la politique applicable et les pratiques. Cela inclut l'AC fournissant les certificats aux unités d'horodatage.

d) L'Autorité d'horodatage doit mettre à la disposition des abonnés et des utilisateurs de contremarques de temps les éléments publics de sa déclaration des pratiques d'horodatage, s'il y a lieu, et toute autre documentation appropriée, tel que nécessaire pour évaluer la conformité à la politique d'horodatage.

   Nota - Il n'est pas exigé que l'Autorité d'horodatage rende publics tous les détails de ses pratiques.

e) L'Autorité d'horodatage devra disposer d'une organisation adéquate pour l'approbation de la déclaration des pratiques d'horodatage et la vérification de la concordance entre cette déclaration et les politiques d'horodatage choisies.

f) Le responsable opérationnel de l'Autorité d'horodatage doit garantir que les pratiques sont correctement mises en œuvre.

g) L'Autorité d'horodatage doit définir une procédure de contrôle périodique de la conformité des pratiques, y compris les responsabilités, à la déclaration des pratiques d'horodatage.

h) L'Autorité d'horodatage doit informer au préalable les abonnés pour tout changement qu'elle a l'intention de faire dans la partie publique de sa déclaration des pratiques d'horodatage et, après l'approbation comme dans (e) ci-dessus, immédiatement mettre à la disposition des abonnés et des utilisateurs de contremarques de temps la partie publique révisée de la déclaration des pratiques d'horodatage comme exigé sous (d) ci-dessus.

i) Si l'Autorité d'horodatage a été évaluée pour être en conformité avec la Politique d'horodatage identifiée et si une modification envisagée à l'initiative de l'Autorité d'horodatage pouvait entraîner une non-conformité avec la politique d'horodatage ou avec la déclaration des pratiques d'horodatage, alors l'Autorité d'horodatage doit indiquer qu'elle soumettra cette modification à

l'organisme évaluateur indépendant pour avis.

Si elles ne font pas partie pas des conditions générales d'utilisation du service d'horodatage, les déclarations des pratiques d'horodatage doivent comporter, au moins pour chaque politique d'horodatage, supportée par l'Autorité d'horodatage :

a) Les obligations de l'abonné.

b) Les obligations des utilisateurs de contremarques de temps.

VI.1.6. Conditions générales d'utilisation

L'Autorité d'horodatage doit mettre à disposition de tous ses abonnés et des utilisateurs potentiels de contremarques de temps, au moins pour chaque politique d'horodatage supportée par l'Autorité d'horodatage :

a) Une information sur un point de contact pour l'Autorité d'horodatage.

b) Une description ou une référence de la politique d'horodatage appliquée.

c) Au moins un algorithme de hachage qui peut être utilisé pour représenter la donnée à horodater.

d) La période de temps minimum, hors cas de révocation, durant laquelle les contremarques de temps seront vérifiables.

e) L'exactitude du temps dans les contremarques de temps par rapport au temps UTC.

f) N'importe quelles limitations sur l'utilisation du service d'horodatage.

g) Les obligations de l'abonné, si elles ne font partie ni du contrat avec l'abonné, ni de la déclaration des pratiques d'horodatage.

h) Les obligations des utilisateurs de contremarques de temps, si elles ne font partie ni du contrat avec les utilisateurs de contremarques de temps, ni de la déclaration des pratiques d'horodatage.

i) L'information sur la manière de vérifier les contremarques de temps de telle façon que l'utilisateur de contremarques de temps puisse «raisonnablement avoir confiance» dans les contremarques de temps ainsi que les restrictions possibles sur sa période de validité.

j) La période de temps pendant laquelle les fichiers d'audit de l'Autorité d'horodatage sont conservés.

k) Le système légal applicable.

l) Les limitations de responsabilité.

m) Les procédures pour les plaintes et le règlement des conflits.

n) Le nom de l'organisme de qualification indépendant ayant validé la conformité avec la présente PH Type.

o) Les éléments permettant de valider la chaîne de certificats (du certificat de l'unité d'horodatage au certificat auto-signé). Un certificat racine auto-signé ne permet pas de garantir par lui-même que la clé publique correspondante appartient bien à l'AC considérée. Sa diffusion doit s'accompagner de la diffusion, via des sources de confiance, de l'empreinte numérique du certificat, et éventuellement de la clé publique, ainsi que d'une déclaration qu'il s'agit bien d'une clé publique de l'AC.

p) Le nom du pays dans lequel l'Autorité d'horodatage est établie et l'identifiant de l'Autorité d'horodatage (tel que figurant dans le certificat de l'unité d'horodatage).

L'autorité d'horodatage peut également mettre à disposition les conditions de disponibilité du service, par exemple le temps moyen d'indisponibilité du service d'horodatage, le temps moyen de rétablissement du service suite à une indisponibilité et les dispositions prises pour les plans de secours, y compris les services de secours prévus.

VI.1.7. Conformité avec les exigences légales

L'Autorité d'horodatage doit garantir la conformité avec les exigences légales. En particulier :

a) Des mesures techniques appropriées et organisationnelles doivent être prises contre le traitement non autorisé ou illégal des données personnelles (cf. [CNIL]), contre la perte accidentelle, la destruction de données personnelles ou les dégâts commis aux données personnelles.

b) Les informations fournies par les abonnés à l'Autorité d'horodatage ne doivent pas être divulguées, à moins de leur accord, d'une décision judiciaire ou d'une exigence légale.

VI.2. Exigences opérationnelles

VI.2.1. Gestion des requêtes de contremarques de temps

La fourniture d'une contremarque de temps en réponse à une demande (par exemple les performances et le prix du service) est à la discrétion de l'Autorité d'horodatage selon les conditions générales d'utilisation avec l'abonné. Il est toutefois recommandé que la réponse de la part du PSHE à une requête de création de contremarque de temps n'excède pas quelques secondes[93], ceci afin de ne pas nuire ni dégrader l'ergonomie de l'application appelante.

VI.2.2. Fichiers d'audit

L'Autorité d'horodatage doit garantir que toutes les informations appropriées concernant le fonctionnement du service d'horodatage sont enregistrées pendant une période de temps suffisante et précisée dans la déclaration des pratiques d'horodatage), en particulier dans le but de fournir une preuve en cas d'enquêtes légales.

En particulier :

<u>Général</u>

a) Les événements spécifiques et les données enregistrées doivent être documentés par l'Autorité d'horodatage.

b) La confidentialité et l'intégrité des enregistrements d'audit courants et archivés relatifs au

[93] Ce temps de réponse est le délai écoulé entre la réception par le PSHE de la requête et la signature de la contremarque de temps résultante.

fonctionnement des services d'horodatage doivent être assurée.

c) Les enregistrements relatifs à l'administration des services d'horodatage doivent être intégralement archivés et de manière adaptée à la sensibilité des informations.

d) Les enregistrements relatifs au fonctionnement des services d'horodatage doivent être disponibles si exigé dans le but de fournir une preuve d'un fonctionnement correct des services d'horodatage en cas d'enquêtes légales.

e) L'instant précis d'évènements significatifs concernant l'environnement de l'Autorité d'horodatage, la gestion des clés, et la synchronisation de l'horloge doit être enregistré.

f) Les enregistrements relatifs à l'administration du service d'horodatage doivent être gardés, après la date d'expiration de la validité de la clé de signature de l'unité d'horodatage durant une période de temps appropriée pour fournir des éléments de preuves nécessaires tel qu'indiqué dans les conditions générales d'utilisation de l'Autorité d'horodatage.

g) Les événements doivent être enregistrés de telle façon qu'ils ne puissent pas être facilement supprimés ou détruits (sauf s'ils sont transférés sur un support de sauvegarde) durant la période de temps où l'on exige qu'ils soient conservés.

Nota - Cela peut être réalisé, par exemple, à l'aide de supports qui ne peuvent être écrits qu'une seule fois, l'enregistrement de chaque support amovible utilisé et l'utilisation d'un site de sauvegarde hors-site.

h) Toute information enregistrée au sujet d'un abonné doit être tenue confidentielle sauf lorsqu'un accord est passé avec l'abonné pour une publication plus large.

Gestion des clés

i) Les enregistrements concernant tous les événements touchant au cycle de vie des clés doivent être effectués.

j) Les enregistrements concernant tous les événements touchant au cycle de vie des certificats des unités d'horodatage doivent être effectués.

Synchronisation de l'horloge

k) Les enregistrements concernant tous les événements touchant à une synchronisation de l'horloge des unités d'horodatage doivent être effectués. Cela doit inclure l'information concernant des recalibrages ou des synchronisations normales.

l) Les enregistrements concernant tous les événements touchant à la détection de perte de synchronisation doivent être effectués.

VI.2.3. Gestion de la durée de vie de la clé privée

L'Autorité d'horodatage doit garantir que les clés privées de signature des unités d'horodatage ne sont pas employées au-delà de la fin de leur cycle de vie. En particulier :

a) Des procédures opérationnelles ou techniques doivent être mises en place pour assurer qu'une nouvelle paire de clés est mise en place quand la fin de la période d'utilisation d'une clé privée d'unité d'horodatage a été atteinte.

b) Le système d'horodatage doit détruire la clé privée si la fin de la période d'utilisation de cette clé

privée a été atteinte.

VI.2.4. Synchronisation de l'horloge

L'Autorité d'horodatage doit garantir que son horloge est synchronisée avec le temps UTC selon l'exactitude déclarée. En particulier :

a) Le calibrage de chaque horloge d'unité d'horodatage doit être maintenu de telle manière que les horloges ne puissent pas normalement dériver à l'extérieur de l'exactitude déclarée.

b) Les horloges des unités d'horodatage doivent être protégées contre les menaces relatives à leur environnement qui pourraient aboutir à une désynchronisation avec le temps UTC en dehors de l'exactitude déclarée.

Nota - Une analyse des risques doit être conduite sur le système afin d'identifier les menaces contre lesquelles les horloges des unités d'horodatage doivent se protéger. Les menaces peuvent inclure des modifications par du personnel non autorisé, des ondes radio ou des chocs électriques.

c) L'Autorité d'horodatage devra garantir que, que si son horloge interne ne respecte plus l'exactitude déclarée, alors cela sera détecté.

d) *Nota* - L'information sur de tels événements doit être publiée à destination des utilisateurs de contremarques de temps.

e) Si l'horloge d'une unité d'horodatage est détectée comme étant en dehors de l'exactitude annoncée, alors les contremarques de temps ne doivent plus être générées.

f) L'Autorité d'horodatage doit garantir que la synchronisation de l'horloge est maintenue lorsqu'un saut de seconde est programmé comme notifié par l'organisme approprié. Le changement pour tenir compte du saut de seconde doit être effectué durant la dernière minute du jour où le saut de seconde est programmé. Un enregistrement du temps exact (selon l'exactitude déclarée) de l'instant de ce changement doit être effectué.

Nota - Un saut de seconde est un ajustement par rapport au temps UTC effectué en sautant ou en ajoutant une seconde durant la dernière minute d'un mois UTC. On donne la première préférence à la fin de décembre et juin et on donne la seconde préférence à la fin de mars et septembre.

VI.2.5. Exigences du contenu d'une contremarque de temps

L'Autorité d'horodatage doit garantir que les contremarques de temps sont générées en toute sécurité et incluent le temps correct. En particulier :

a) La contremarque de temps doit inclure l'identifiant du certificat de l'unité d'horodatage. Ce certificat doit inclure :

- Un identifiant du pays dans lequel l'Autorité d'horodatage est établie,
- Un identifiant de l'Autorité d'horodatage,
- Une identification de l'unité d'horodatage qui génère les contremarques de temps.

b) La contremarque de temps doit inclure un identifiant de la politique d'horodatage.

c) Chaque contremarque de temps doit comporter un identifiant unique.

d) Les informations de temps portées dans les contremarques de temps doivent pouvoir être reliées

à au moins un temps fourni par un laboratoire UTC (k).

Nota - Le Bureau des International Poids et Mesures (BIPM) calcule UTC sur la base des représentations locales UTC (k) d'un grand ensemble de montres atomiques dans des instituts de métrologie nationaux et des observatoires nationaux astronomiques autour du monde. Le BIPM dissémine le temps UTC par sa Circulaire mensuelle T. Celle-ci est disponible sur le site Web BIPM (www.BIPM.org) qui identifie officiellement tous les instituts ayant des échelles de temps UTC (k) reconnues.

e) Le temps inclus dans une contremarque de temps doit être synchronisé avec le temps UTC au moins avec l'exactitude définie dans la DPH.

f) Si une contremarque de temps inclut un temps qui est synchronisé avec le temps UTC avec une exactitude différente de la seconde, alors cette exactitude doit être indiquée dans la contremarque de temps.

g) La contremarque de temps doit inclure une représentation de la donnée à horodater (c'est-à-dire la valeur de hachage et l'identifiant d'algorithme de hachage) telle que fournie par le demandeur.

h) La contremarque de temps doit être signée en employant une clé produite exclusivement à cette fin.

i) La contremarque de temps doit, de plus, respecter les exigences du chapitre VIII ci-dessous

Nota - Dans le cas de demandes d'horodatage survenant durant un intervalle de temps correspondant à l'exactitude de l'horloge de l'unité d'horodatage, l'ordonnancement des contremarques de temps à l'intérieur de cet intervalle n'est pas requis.

VI.2.6. Compromission de l'AH

L'Autorité d'horodatage doit garantir dans le cas d'événements qui affectent la sécurité des services d'horodatage, incluant la compromission de la clé privée de signature d'une unité d'horodatage ou la perte détectée de calibrage qui pourrait affecter des contremarques de temps émises, qu'une information appropriée est mise à la disposition des abonnés et des utilisateurs de contremarques de temps. En particulier :

a) Le plan de secours de l'Autorité d'horodatage doit traiter le cas de la compromission réelle ou suspectée de la clé privée de signature d'une unité d'horodatage ou la perte de calibrage de l'horloge d'une unité d'horodatage, qui pourrait affecter des contremarques de temps émises.

b) Dans le cas d'une compromission, réelle ou suspectée, ou d'une perte de calibrage d'une unité d'horodatage, qui pourrait affecter des contremarques de temps émises, l'Autorité d'horodatage mettra à la disposition de tous les abonnés et utilisateurs de contremarques de temps une description de la compromission qui est survenue.

c) Dans le cas d'une compromission, réelle ou suspectée, ou d'une perte de calibrage d'une unité d'horodatage, qui pourrait affecter des contremarques de temps émises, l'Autorité d'horodatage prendra les mesures nécessaires pour que les contremarques de temps de cette unité ne soient plus générées jusqu'à ce que des actions soient faites pour restaurer la situation.

d) En cas d'un évènement majeur dans le fonctionnement de l'Autorité d'horodatage ou d'une une perte de calibrage, qui pourrait affecter des contremarques de temps émises, chaque fois que cela sera possible, l'Autorité d'horodatage mettra à la disposition de tous ses abonnés et des utilisateurs de contremarques de temps toute information pouvant être utilisée pour identifier les

contremarques de temps qui pourraient avoir été affectées, à moins que cela ne contrevienne à la vie privée des abonnés ou à la sécurité des services d'horodatage.

Nota - Dans le cas où une clé privée serait réellement compromise, un fichier d'audit de toutes les contremarques de temps produites par l'unité d'horodatage peut fournir le moyen de distinguer entre des contremarques de temps véritables et des fausses contremarques de temps antidatées. Deux contremarques de temps de deux unités d'horodatage différentes de la même Autorité d'horodatage ou, mieux, de deux Autorités d'horodatage différentes peuvent être une autre façon de résoudre ce problème (voir chapitre X ci-dessous).

VI.2.7. Fin d'activité

Il est nécessaire de définir les procédures de fin d'activité ou de reprise par un tiers. Dans ce cadre, l'Autorité d'horodatage doit garantir que les dérangements potentiels aux abonnés et aux utilisateurs de contremarques de temps seront réduits au minimum suite à la cessation d'activité du service d'horodatage et assurer en particulier la maintenance continue des informations nécessaires pour vérifier la justesse de contremarques de temps. En particulier :

a) Avant que l'Autorité d'horodatage ne termine ses services d'horodatage les procédures suivantes doivent être exécutées au minimum :

- L'Autorité d'horodatage rendra disponible à tous ses abonnés et aux utilisateurs de contremarques de temps l'information concernant sa fin d'activité ;
- L'Autorité d'horodatage doit abroger les autorisations données aux sous-traitants d'agir pour son compte dans l'exécution de n'importe quelles fonctions touchant au processus de génération des contremarques de temps ;
- L'Autorité d'horodatage transférera à un organisme fiable ses obligations de maintien des fichiers d'audit et des archives nécessaires pour démontrer son fonctionnement correct durant une période raisonnable ;
- L'Autorité d'horodatage maintiendra ou transférera à un organisme fiable ses obligations de rendre disponible aux utilisateurs de contremarques de temps pendant une période raisonnable ses clés publiques ainsi que ses certificats ;
- Les clés privées des unités d'horodatage doivent être détruites de telle façon que les clés privées ne puissent pas être recouvrées.

b) L'Autorité d'horodatage doit prendre les mesures nécessaires pour couvrir les dépenses pour accomplir ces exigences minimales dans le cas où l'Autorité d'horodatage tomberait en faillite ou pour d'autres raisons serait incapable de couvrir les dépenses par elle-même.

c) L'Autorité d'horodatage doit indiquer dans sa PH les dispositions prises pour la fin du service. Cela doit inclure :

- Un avis aux abonnés et aux utilisateurs de contremarques de temps ;
- Un transfert des obligations de l'Autorité d'horodatage à d'autres organismes.

VI.3. Exigences physiques et environnementales, procédurales et organisationnelles

VI.3.1. Exigences physiques et environnementales

L'Autorité d'horodatage doit garantir que l'accès physique aux services critiques est contrôlé et que les risques physiques d'atteinte à ses actifs sont réduits au minimum. En particulier :

a) A la fois pour la fourniture du service d'horodatage et la gestion de l'horodatage :

- L'accès physique aux équipements concernés par les services d'horodatage doit être limité aux individus autorisés ;
- Des contrôles doivent être mis en œuvre pour éviter la perte, des dégâts ou la compromission d'actifs et l'interruption des activités et ;
- Des contrôles doivent être mis en œuvre pour éviter la compromission ou le vol d'informations ou d'équipements informatiques.

b) Des contrôles d'accès doivent être appliqués aux modules d'horodatage pour remplir les exigences de sécurité des modules d'horodatage. Les contraintes sur l'environnement d'exploitation, identifiées dans la documentation liée à la certification du module (PP, cible de sécurité, ; cf. chapitre IX ci-dessous) doivent être remplies.

c) Les contrôles suivants complémentaires doivent être appliqués à la gestion du service d'horodatage :

- Le système d'horodatage doit fonctionner dans un environnement qui protège physiquement les services de la compromission au moyen d'un accès non autorisé aux systèmes ou aux données ;
- La protection physique doit être réalisée par la création d'un périmètre de sécurité dédié clairement défini (c'est-à-dire des barrières physiques) autour des unités d'horodatage ;
- Des contrôles de sécurité physique et environnementale doivent être mis en œuvre pour protéger l'environnement qui abrite les ressources du système, les ressources du système elles-mêmes et les équipements utilisés pour remplir leur fonction ; la politique de sécurité physique et environnementale de l'Autorité d'horodatage pour les systèmes concernés par la gestion de l'horodatage doit au minimum concerner le contrôle d'accès physique, la protection vis à vis des catastrophes naturelles, les facteurs de sécurité liés au feu, la défaillance des services de base (par exemple le secteur, les télécommunications), l'écroulement de la structure, des fuites de plomberie, la protection contre le vol, la casse et la pénétration et, le rétablissement de la sécurité après un désastre ;
- Des contrôles doivent être mis en œuvre pour empêcher des équipements, de l'information, des médias et du logiciel touchant aux services d'horodatage d'être enlevés du site sans autorisation.

VI.3.2. Exigences procédurales

L'Autorité d'horodatage doit garantir que les composants du système d'Horodatage sont sûrs et correctement opérés, avec un risque minimal d'échec. En particulier :

a) L'intégrité des composants du système d'horodatage et l'information doivent être protégés contre les virus, les logiciels malveillants et non autorisés.

b) Un rapport d'incident et des procédures de réponse aux incidents doivent être employés d'une telle façon que les dégâts liés aux incidents de sécurité et aux défaillances soient réduits au minimum.

c) Les supports employés dans les systèmes d'horodatage doivent être manipulés de manière sécuritaire pour les protéger des dégâts, du vol, de l'accès non autorisé et de l'obsolescence

Nota - Chaque membre du personnel avec des responsabilités de gestion est responsable de la planification et de l'exécution effective de la politique d'horodatage et des pratiques d'horodatage.

d) Des procédures doivent être établies et mises en œuvre pour tous les rôles de confiance et administratifs qui impactent la fourniture des services d'horodatage.

Manipulation et sécurité des supports

e) Tous les supports doivent être traités de manière sécuritaire conformément aux exigences de la classification de l'information. Les supports contenant des données sensibles doivent être retirés de manière sécuritaire quand ils ne sont plus utiles.

Planification de Système

f) Les charges doivent être contrôlées et des projections de charge dans le futur doivent être effectuées pour garantir que des puissances de traitement et des stockages adéquats seront disponibles.

Rapport d'incident et réponse

g) L'Autorité d'horodatage agira d'une façon opportune et coordonnée pour répondre rapidement aux incidents et limiter l'impact des infractions à la sécurité. Tous les incidents doivent être rapportés aussitôt que possible après l'incident.

Les contrôles complémentaires suivants doivent être appliqués à la gestion de l'horodatage :

Procédures de fonctionnement et responsabilités

h) Les opérations de sécurité doivent être séparées des autres opérations.

Nota - Les opérations de sécurité incluent :

- Les procédures opérationnelles et les responsabilités ;
- La planification et la qualification des systèmes sécurisés ;
- La protection vis-à-vis du logiciel malveillant ;
- La maintenance ;
- La gestion du réseau ;
- Le contrôle actif des journaux d'audit, l'analyse des événements et les suites à donner ;
- Le traitement et la sécurité des médias ;
- L'échange des données et du logiciel.

Ces opérations doivent être gérées par du personnel de confiance de l'Autorité d'horodatage, mais, peuvent aussi être exécutées par du personnel opérationnel non-spécialiste (sous surveillance), comme défini dans la politique de sécurité appropriée et, les documents sur les rôles et les responsabilités.

Gestion d'Accès au Système

L'Autorité d'horodatage doit garantir que l'accès au système d'horodatage est limité aux individus dûment autorisés. En particulier :

a) Des contrôles (par exemple, des pares-feux (firewalls)) doivent être mis en oeuvre pour protéger le réseau interne de l'Autorité d'horodatage d'accès non autorisés incluant l'accès par des abonnés et des tierces personnes.

Nota - Les pares-feux (firewalls) devraient aussi être configurés pour bloquer tous les protocoles et les accès non nécessaires au fonctionnement de l'Autorité d'horodatage.

b) L'Autorité d'horodatage doit garantir une administration efficace des utilisateurs (cela inclut les opérateurs, les administrateurs et les auditeurs), pour maintenir la sécurité du système, y compris la gestion des comptes des utilisateurs, l'audit, et la modification ou le retrait rapide d'accès.

c) L'Autorité d'horodatage doit garantir que l'accès aux fonctions du système, à l'information et aux applications est limité conformément à la politique de contrôle d'accès et que le système d'horodatage possède les contrôles informatiques de sécurité suffisants pour la séparation des rôles de confiance identifiés dans les pratiques d'horodatage, y compris la séparation des fonctions d'administrateur de sécurité et des fonctions opérationnelles. En particulier, l'utilisation de programmes systèmes utilitaires sera limitée et très contrôlée.

d) Le personnel de l'Autorité d'horodatage doit être correctement identifié et authentifier avant d'utiliser des applications critiques liées à l'horodatage.

e) Le personnel de l'Autorité d'horodatage sera tenu responsable de ses activités, par exemple en conservant des fichiers d'audit.

Les contrôles complémentaires suivants doivent être appliqués à la gestion de l'horodatage :

f) L'Autorité d'horodatage doit garantir que des composants de réseau locaux (par exemple les routeurs) seront mis dans un environnement physiquement sûr et que leurs configurations sont périodiquement vérifiées pour la conformité avec les exigences indiquées par l'Autorité d'horodatage.

g) Une surveillance permanente et des équipements d'alarme doivent être mis en œuvre pour permettre à l'Autorité d'horodatage de détecter, d'enregistrer et de réagir rapidement à n'importe quelle tentative non autorisée et/ou irrégulière d'accès à ses ressources.

Nota - On peut employer, par exemple, un système de détection d'intrusion, une surveillance de contrôle d'accès et des équipements d'alarme.

Déploiement et Maintenance

L'Autorité d'horodatage emploiera des produits et systèmes de confiance. Concernant les modules d'horodatage ils répondront aux exigences du chapitre IX ci-dessous.

Nota - L'analyse de risque effectuée sur les services d'horodatage devrait identifier les services critiques exigeant des systèmes évalués et les niveaux d'assurance exigés.

En particulier :

a) Une analyse des exigences de sécurité doit être effectuée au moment de la conception et de l'étape

de spécification des exigences pour tout projet de développement de systèmes entrepris par l'Autorité d'horodatage ou pour le compte de l'Autorité d'horodatage pour assurer que la sécurité fait partie du système d'information.

b) Des procédures de contrôle de changement doivent être appliquées pour les nouvelles versions, les modifications et les corrections d'anomalies de n'importe quel logiciel opérationnel.

VI.3.3. Exigences organisationnelles

L'Autorité d'horodatage doit garantir que le personnel et des pratiques d'embauche améliorent et concourent à la fiabilité des opérations de l'Autorité d'horodatage.

En particulier :

a) L'Autorité d'horodatage doit employer un personnel qui possède l'expertise, l'expérience et les qualifications nécessaires pour les services offerts, tels que l'exige la fonction.

Nota - Le personnel de l'Autorité d'horodatage devrait être en mesure de remplir l'exigence de «l'expertise, l'expérience et des qualifications» au moyen de la formation professionnelle et d'attestations professionnelles, de l'expérience réelle, ou d'une combinaison des deux.

Nota - Le personnel employé par l'Autorité d'horodatage inclut le personnel individuel contractuellement engagé dans l'exécution des fonctions pour supporter les services d'horodatage. Le personnel qui peut être impliqué dans la surveillance des services de l'Autorité d'horodatage n'a pas besoin de faire partie du personnel de l'Autorité d'horodatage.

b) Les rôles de sécurité et les responsabilités, comme spécifié dans la politique de sécurité de l'Autorité d'horodatage, doivent être documentés dans des descriptions de poste. Les rôles de confiance, sur lesquels la sécurité du fonctionnement de l'Autorité d'horodatage repose, doivent être clairement identifiés.

c) Des descriptions de fonctions doivent être définies pour le personnel de l'Autorité d'horodatage (aussi bien provisoire que permanent) du point de vue de la séparation des responsabilités et du principe du privilège minimum, selon la sensibilité de la fonction sur la base des responsabilités et des niveaux d'accès, et indiquer le type d'enquête à effectuer sur le passé, le type de formation appropriée et les particularités de la fonction. Quand cela est nécessaire, ces descriptions de fonctions doivent faire la différence entre les fonctions générales et les fonctions spécifiques à l'Autorité d'horodatage. Ces descriptions de fonctions devraient inclure des exigences d'expérience et de compétences.

d) Le personnel doit effectuer des procédures administratives et de gestion ainsi que des processus en accord avec les procédures de gestion de sécurité de l'information de l'Autorité d'horodatage.

Les contrôles complémentaires suivants doivent être appliqués à la gestion de l'horodatage

e) le personnel de gestion employé doit posséder :

- La connaissance de la technologie de l'horodatage et ;
- La connaissance de technologie de la signature numérique et ;
- La connaissance des mécanismes pour le calibrage ou la synchronisation des horloges des unités d'horodatage avec le temps UTC et ;
- Pour le personnel avec des responsabilités de sécurité, une bonne connaissance des

procédures de sécurité, et ;

- L'expérience avec la sécurité de l'information et l'évaluation des risques.

f) Tout le personnel de l'Autorité d'horodatage dans des rôles de confiance doit être libre de conflit d'intérêt qui pourrait porter préjudice à l'impartialité des opérations de l'Autorité d'horodatage.

g) Les rôles de confiance incluent les rôles qui impliquent les responsabilités suivantes :

- Les officiers chargés de la sécurité : responsabilité complète d'administrer la mise en œuvre des pratiques de sécurité ;
- Les administrateurs système : autorisés à installer, configurer et maintenir les modules d'horodatage de l'Autorité d'horodatage pour la gestion de l'horodatage ;
- Les opérateurs système : responsables pour faire fonctionner les modules d'horodatage de l'Autorité d'horodatage de manière quotidienne. Autorisés pour effectuer les opérations de sauvegarde et des secours ;
- Les auditeurs de système : autorisés à consulter les archives et les fichiers d'audit des modules d'horodatage.

h) Le personnel de l'Autorité d'horodatage doit être formellement nommé aux rôles de confiance par la direction responsable de la sécurité.

i) L'Autorité d'horodatage ne doit pas nommer aux rôles de confiance ou de gestion toute personne connue pour avoir une condamnation pour un crime sérieux ou une autre infraction qui affecte son adéquation avec la position. Le personnel ne doit pas avoir accès aux fonctions de confiance avant que les contrôles nécessaires ne soient achevés.

VI.4. Exigences de sécurité techniques

VI.4.1. Exactitude temps

Si une unité d'horodatage fournit une exactitude différente de la seconde, alors cette exactitude doit être indiquée dans chaque contremarque de temps générée.

Nota - Ceci permet d'afficher une cohérence avec la politique [ETSI_PH], toutefois, il est possible d'indiquer dans la contremarque de temps l'exactitude de l'unité d'horodatage dans le cas ou celle-ci est d'une seconde.

VI.4.2. Génération de clé

L'Autorité d'horodatage doit garantir que toutes les clés cryptographiques sont produites dans des circonstances contrôlées. En particulier, la génération des clés de signature des unités d'horodatage doit être effectuée dans un module d'horodatage répondant aux exigences du chapitre IX ci-dessous.

VI.4.3. Certification des clés de l'unité d'horodatage

L'Autorité d'Horodatage doit s'assurer que la valeur de la clé publique et l'identifiant de l'algorithme de signature contenus dans la demande de certificat de l'Unité d'Horodatage sont égaux à ceux générés par l'Unité d'Horodatage.

L'Autorité d'Horodatage doit s'assurer qu'une demande de certificat d'Unité d'Horodatage auprès d'une Autorité de Certification contient, en plus des informations exigées dans la PC Type « cachet » pour la partie enregistrement, au moins les informations suivantes :

- Le nom (DN) de l'unité d'horodatage pour laquelle la demande de certificat est faite
- La valeur de la clé publique (et l'identifiant de l'algorithme) ;
- La durée d'utilisation souhaitée pour la clé privée.

L'Autorité d'Horodatage doit vérifier, lors de l'import du certificat de l'Unité d'Horodatage, qu'il provient bien de l'Autorité de Certification auprès de laquelle la demande de certificat a été effectuée.

L'Autorité d'Horodatage doit s'assurer que l'Unité d'Horodatage ne peut être opérationnelle qu'une fois ces exigences remplies.

VI.4.4. Protection des clés privées des unités d'horodatage

L'Autorité d'horodatage doit garantir que des clés privées des unités d'horodatage restent confidentielles et conservent leur intégrité. En particulier, les clés de signature des unités d'horodatage doivent être gardées et utilisées à l'intérieur d'un module d'horodatage répondant aux exigences du chapitre IX ci-dessous.

VI.4.5. Exigences de sauvegarde des clés des unités d'horodatage

Les clés privées des unités d'horodatage peuvent faire l'objet de copies de secours, soit dans un module d'horodatage conforme aux exigences du chapitre IX ci-dessous, soit hors d'un module d'horodatage mais dans ce cas sous forme chiffrée et avec un mécanisme de contrôle d'intégrité. Le chiffrement correspondant doit offrir un niveau de sécurité équivalent ou supérieur au stockage au sein du module d'horodatage et, notamment, s'appuyer sur un algorithme, une longueur de clé et un mode opératoire capables de résister aux attaques par cryptanalyse pendant au moins la durée de vie de la clé ainsi protégée. Les règles à respecter sont définies dans le document [RGS_B1].

Les opérations de chiffrement et de déchiffrement doivent être effectuées à l'intérieur du module d'horodatage de telle manière que les clés privées des unités d'horodatage ne soient à aucun moment en clair en dehors du module d'horodatage.

VI.4.6. Destruction des clés des unités d'horodatage

L'Autorité d'horodatage doit garantir que les clés de signature des unités d'horodatage sont détruites à la fin de leur cycle de vie.

VI.4.7. Algorithmes obligatoires

L'Autorité d'horodatage doit, dans la limite des algorithmes qu'elle reconnaît :

a) Accepter des valeurs de hachage générées par des clients et employant les algorithmes de hachage conformes aux exigences du chapitre VIII ci-dessous.

b) Générer des contremarques de temps signées selon les algorithmes et les longueurs de clé conformes aux exigences du chapitre VIII ci-dessous.

VI.4.8. Vérification des contremarques de temps

L'Autorité d'horodatage doit garantir que les utilisateurs de contremarques de temps peuvent avoir accès à l'information utilisable pour vérifier la signature numérique des contremarques de temps. En particulier :

a) Les certificats des unités d'horodatage doivent être disponibles, soit joints à la contremarque de temps, soit disponibles par d'autres moyens, par exemple un serveur.

b) Un ou plusieurs certificats utilisables pour valider une chaîne de certificats se terminant par un certificat d'unité d'horodatage doivent être disponibles.

VI.4.9. Durée de validité des certificats de clé publique des unités d'horodatage

La durée de validité des certificats des unités d'horodatage ne doit pas être plus longue que :

- La durée de vie cryptographique de la clé privée associée (cf [RGS_B_1]).
- Fin de validité du certificat d'AC qui l'a émis.

Il est à prendre en considération le fait que plus la durée de vie du certificat sera grande, plus la taille des enregistrements d'audit à conserver sera importante.

VI.4.10. Durée d'utilisation des clés privées des unités d'horodatage

La durée d'utilisation d'une clé privée sera au plus égale à la période de validité du certificat de clé publique correspondant. Toutefois elle sera en pratique réduite afin que la validité des contremarques de temps générées avec cette clé puisse être effectuée durant un laps de temps suffisant. La durée d'utilisation de la clé privée peut être définie soit au moment de l'initialisation du boîtier de l'unité d'horodatage, soit en définissant cette durée dans le certificat (PrivateKeyUsagePeriod).

VII. Annexe 1 : Documents cités en référence

VII.1. Réglementation

Renvoi	Document
[CNIL]	Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée
[ORDONNANCE]	Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électronique entre les usagers et les autorités administratives et entre les autorités administratives
[LOIDUPAYS]	Loi du pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices

VII. 2. Documents techniques

Renvoi	Document
[RGS]	Référentiel Général de Sécurité – version 1.0
[RGS_A_4]	RGS - Politiques de Certification Types - Profils de certificats, de LCR et OCSP et algorithmes cryptographiques – Version 2.3
[RGS_B_1]	Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI, Version 1.20
[ETSI_PH]	ETSI TS 102 023 V1.2.2 (2008-10) Policy requirements for Time-Stamping Authority
[ETSI_TSP]	ETSI TS 101 861 V1.2.1 (2002-03) Time Stamping Profile
[PP_HORO]	DCSSI - Profil de Protection - Systèmes d'horodatage EAL3+ DCSSI PP 2008/07
[RFC3161]	IETF - Internet X.509 Public Key Infrastructure - Time-Stamp Protocol -08/2001
[TF.460-5]	ITU-R Recommendation TF.460-5 (1997) «Standard-Frequency emissions».
[TF.536-1]	ITU-R Recommendation TF. TF.536-1(1998): «Time-Scale Notations». and Time-signal

VIII. Annexe 2 : Exigences sur les formats des contremarques de temps, des certificats et des LCR et sur les algorithmes cryptographiques

VIII.1. Contremarques de temps

Les contremarques de temps fournies par les AH respectant la présente PH Type doivent être une structure TimeStampToken conforme au [RFC3161].

Le tableau ci-dessous reprend l'ensemble des champs d'un TimeStampToken tels que définis dans le [RFC3161]. Une contremarque de temps conforme à cette PH Type doit respecter, de base, les exigences correspondantes du [RFC3161], moyennant les compléments et/ou modifications d'exigences définis dans ce tableau.

Champ	Exigences
messageImprint	Cf. chapitre VIII.3 ci-dessous sur les exigences concernant les fonctions de hachage.
accuracy	Si la synchronisation avec le temps UTC est différente de 1 seconde, ce champ doit être présent et doit préciser l'exactitude de la synchronisation. Si la synchronisation est de 1 seconde, il peut être omis.
ordering	Ce champ doit être absent ou bien contenir la valeur false.
tsa	Si ce champ est présent, il doit être identique au champ subject du certificat de l'UH ayant signé la contremarque de temps.
extensions	Des extensions peuvent être incluses par l'AH, mais aucune ne doit être marquée comme critique.

VIII.2. Certificats et LCR

Les gabarits des certificats d'UH doivent être conformes aux exigences des certificats de type « cachet » dont la clé privée associée est utilisée pour signer des jetons d'horodatage décrites dans le document [RGS_A_4]. Il est rappelé ici que :

- l'extension « Extended Key Usage » doit être présente, marquée critique, et ne contenir que l'identifiant id-kp-timeStamping à l'exclusion de toute autre.
- Le champ « DN Subject » doit identifier l'AH suivant les mêmes règles que l'identification des AC (cf. chapitre VII.1 de [RGS_A_4]) et l'identifiant propre à l'UH concernée, au sein de l'AH, doit être porté dans l'attribut commonName du DN de ce champ (au sein d'une AH, chaque UH doit avoir un identifiant unique).
- La durée de vie maximale est bornée selon le couple {durée de vie cryptographique de la clé ; fin de validité de la durée de vie de l'AC émettrice}.

Pour les LCR qui comportent des numéros de série correspondant à des certificats d'unité d'horodatage, il est obligatoire de supporter l'extension d'entrée LCR : reasonCode.

VIII.3. Algorithmes cryptographiques

Les algorithmes et fonctions cryptographiques (hachage, signature) mis en œuvre pour la génération des différents certificats, pour la génération des contremarques de temps ainsi que la valeur du champ messageImprint dans les contremarques de temps doivent respecter les exigences correspondantes de [RGS_A_4].

IX. Annexe 3 : Exigences de sécurité du module d'horodatage des UH

IX.1. Exigences sur les objectifs de sécurité

Le module d'horodatage, utilisé par l'AH pour générer et mettre en œuvre les clés de signature des UH et pour générer les contremarques de temps, doit répondre aux exigences de sécurité suivantes :

- Garantir que la génération des bi-clés des UH est réalisée exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique des bi-clés générées ;
- Assurer la confidentialité et l'intégrité des clés privées de signature des UH durant tout leur cycle de vie, et permettre leur destruction sûre en fin de vie ;
- Garantir l'authenticité et l'intégrité des clés publiques lors de leur export hors du module (à fins de certification par une AC) ;
- Lors de son importation dans le module, vérifier la correspondance entre le certificat importé et la clé publique de l'UH contenue dans le module ;
- Être capable d'identifier et d'authentifier ses utilisateurs ;
- Limiter l'accès à ses services en fonction de l'utilisateur et du rôle qui lui a été assigné ;
- Être capable de mener une série de tests, lors des phases d'initialisation, de personnalisation et d'opération, pour vérifier qu'il fonctionne correctement et entrer dans un état sûr s'il détecte une erreur ;
- Être capable de détecter les tentatives d'altérations physiques et d'entrer dans un état sûr quand une tentative d'altération est détectée ;
- Permettre de créer une signature numérique, pour signer les contremarques de temps générées par l'UH, qui ne révèle pas les clés privées de l'UH et qui ne peut pas être falsifiée sans la connaissance de ces clés privées ;
- Créer des enregistrements d'audit pour chaque modification concernant la sécurité ;
- Garantir la synchronisation de son horloge avec le temps UTC suivant la précision définie dans la DPH ;
- Fournir des contremarques de temps conformes aux requêtes reçues.

IX.2. Exigences complémentaires

Il est recommandé que le module d'horodatage utilisé par l'AH soit qualifié au niveau standard, attestant ainsi de sa conformité aux exigences de sécurité du chapitre IX.1 ci-dessus. Le profil de protection [PP_HORO] couvre ces exigences.

Lorsque le PSHE souhaite faire qualifier son offre d'horodatage, alors :

- Le module d'horodatage utilisé par l'AH doit être qualifié au niveau standard,
- Les fonctions cryptographiques telles que la génération des bi-clés des UH et la signature des contremarques de temps visées au chapitre IX.1 doivent être assurées par un module cryptographique évalué conformément aux exigences spécifiées aux alinéas 7.2.1.b et 7.2.2.a de la norme [ETSI_PH].

X. Annexe 4 - Vérification ou utilisation (informative)

Cette politique d'horodatage prévoit la vérification d'une contremarque de temps, pendant la période de validité du certificat de clé publique de l'unité d'horodatage qui l'a générée.

X.1. Empilement des contremarques de temps

S'il s'avère nécessaire de prolonger la durée de vie d'une contremarque de temps ou d'en conforter la robustesse, il est possible d'ajouter une contremarque de temps supplémentaire fournie par une autre unité d'horodatage.

Pour cela, il convient de pouvoir prouver que le certificat de l'unité d'horodatage référencé dans la contremarque de temps d'origine n'était pas révoqué au moment où la contremarque de temps supplémentaire a été ajoutée.

Après s'être assuré que l'unité d'horodatage qui a généré la première contremarque de temps n'est pas révoquée, une contremarque de temps supplémentaire sera apposée sur la contremarque précédente le demandeur de la nouvelle contremarque

Les LRC des AC en charge de l'unité d'horodatage devront être archivées afin de pouvoir démontrer que l'unité d'horodatage ayant généré la première contremarque de temps n'était pas révoquée à ce moment là.

Lors d'une vérification ultérieure, un utilisateur de contremarque de temps devra vérifier les deux contremarques de temps et s'assurer que l'unité d'horodatage ayant généré la première contremarque n'était pas révoquée à la date où la seconde contremarque de temps a été apposée. L'utilisateur de contremarque de temps devra en outre s'assurer que le certificat de l'unité d'horodatage ayant généré la seconde contremarque de temps n'est pas révoquée à l'instant de la vérification ultérieure.

X.2. Gestion de la révocation par les Autorités de Certification

La gestion de la révocation des certificats des unités d'horodatage doit être assurée comme pour toute AC.

Un service OCSP ferait l'affaire mais cela multiplierait les contraintes d'implémentation et dans le cas présent, étant donné que le risque de compromission d'une clé est minime, l'usage des LCR est tout à fait adapté.

Il est recommandé de mettre en place une AC spécifiquement en charge de la gestion des unités d'horodatage.

XI. Annexe 5 - Précision de la synchronisation de l'horloge

La précision de l'horloge a souvent été ressentie comme un paramètre essentiel. On peut très facilement obtenir des synchronisations par rapport à une horloge de référence UTC avec une précision de 10 microsecondes, mais cette précision n'a pas de sens dans le cadre de l'horodatage pour deux raisons :

- le temps de transit de la requête est largement supérieur à ce temps ;
- l'opération de signature de la contremarque de temps est largement supérieure à ce chiffre et se situe aujourd'hui au mieux dans l'échelle des 10 millisecondes.

Une précision d'une seconde est largement suffisante pour toutes les applications.

Des précisions meilleures peuvent cependant être utiles dans des contextes de liaisons particulières «courtes» (par exemple, réseaux locaux ou à l'intérieur d'un même système informatique). Cela n'a de sens que si elles sont commensurables avec le temps de propagation et de traitement de la demande. En l'état actuel de la technique, un horodatage bien meilleur que 10 millisecondes n'aurait pas grand sens.

Sans changer de politique, il est possible d'avoir une précision meilleure. Quand c'est le cas, cette précision est indiquée à l'intérieur de la contremarque de temps.

La précision est une propriété intrinsèque de l'unité d'horodatage. Certaines unités d'horodatage peuvent donc fournir des précisions meilleures. En s'adressant directement à une unité d'horodatage donnée, on peut donc obtenir une précision meilleure sans qu'il soit nécessaire de changer de politique d'horodatage et sans qu'il soit nécessaire d'utiliser de paramètre spécifique (le protocole défini dans le [RFC3161] ne comporte pas de paramètre spécifique pour ce faire).

XII. Annexe 6 - Protocole d'horodatage

Aucun protocole spécifique n'est requis, en dehors du format de la contremarque de temps (cf VIII.1.) Si la déclaration des pratiques d'horodatage déclare que le protocole d'horodatage est conforme au [RFC3161] ou au standard [ETSI_TSP], alors les sections suivantes s'appliquent.

XII.1. Conformité au RFC 3161

Cette section s'appuie sur le contenu du RFC 2026 (section 4.1.2) [RFC2026].

L'IETF n'a pas «des clauses de conformités». Au lieu de cela l'IETF stipule des tests d'interopérabilité.

Il est requis de démontrer l'interopérabilité avec au moins une mise en œuvre indépendante réalisée à partir d'un code de base différent.

L'Autorité d'horodatage doit pouvoir fournir une documentation au sujet des tests d'interopérabilité :

1. le test s'applique à toutes les options et les particularités de la spécification ;
2. la documentation doit inclure l'information concernant le support de chacune des options individuelles et des particularités.

XII.2. Conformité au standard ETSI TS 101 861

La norme [ETSI_TSP] inclut dans sa section 5 un profil pour le format de la réponse et dans sa section 6 un profil pour les protocoles de transport à supporter.

XIII. Annexe 7 - Compatibilité avec la politique d'horodatage de l'ETSI

La présente PH Type définie dans ce document est compatible sur la plupart des points avec la politique d'horodatage définie dans le document [ETSI_PH].

Cependant, les points suivants de la politique [ETSI_PH] ne sont pas repris dans cette politique :

TS 101 023 v1.2.1	**PH standard**	**Texte**	**Justificatif**
5.1		The present document defines requirements for a baseline time-stamp policy for TSAs issuing time-stamp tokens, supported by public key certificates, with an accuracy of 1 second or better.	Cette exigence, qui demande une précision d'au moins une seconde, n'a pas été reprise pour pouvoir prendre en compte des précisions moindres.
7.1.2 d)	7.	The TSA shall disclose to all subscribers and potential relying parties the terms and conditions regarding use of its time-stamping services. This statement shall at least specify for each time-stamp policy supported by the TSA: […] The expected life-time of the signature used to sign the time-stamp token (depends on the hashing algorithm being used, the signature algorithm being used and the private key length). (La durée de vie estimée de la signature utilisée pour signer la contremarque de temps (dépend de l'algorithme de hachage employé pour la signature, de l'algorithme de signature employé et de la longueur de la clé privée)	Cette exigence, sur l'estimation de la durée de vie de la clé de signature, n'a pas été reprise dans la présente politique du fait du caractère non garanti de l'information. De ce fait, l'estimation n'engage en rien l'AH.
7.2.1	/	The generation of TSU (s signing key(s) shall be undertaken in a physically secured environment (see clause 7.4.4) by personnel of trusted roles (see clause 7.4.3)	L'[ETSI_PH] impose le double contrôle de personnes possédant des rôles de confiance pour les actions sensibles sur les clés privées des unités d'horodatage (génération, sauvegarde…). Cette exigence n'est pas reprise dans l'annexe

		under, at least, dual control […].	A5.
7.2.2	3 et 9.1	Backup of TSU private keys is deprecated in order to minimize risk of key compromise.	L' [ETSI_PH] précise que la sauvegarde et l'import de clés privées dans le module cryptographique de l'unité d'horodatage sont des pratiques dépréciées. La sauvegarde et l'import des clés privées sont autorisés dans l'annexe A5 sans mentionner qu'il s'agit de pratiques dépréciées.
7.2.5.c	11.b	The TST generation system SHALL reject any attempt to issue TSTs if the signing private key has expired. (Le système de génération des contremarques de temps doit rejeter toute tentative de génération d'une contremarque de temps si la fin de la période d'utilisation de la clé privée de l'unité d'horodatage a été atteinte.)	L'obligation de destruction de la clé entraîne de facto l'impossibilité de générer de nouvelles contremarques de temps.

Cette politique d'horodatage a été réalisée dans l'optique de permettre à un opérateur, s'il le désire, de fournir un service compatible à la fois avec la présente PH et avec celle de l'ETSI. Il conviendra toutefois à l'AH de vérifier que les exigences des deux politiques sont respectées pour se prévaloir de cette compatibilité.

Si la conformité aux exigences de la PH de l'ETSI est réalisée, alors l'identifiant d'objet (OID) défini dans le document de l'ETSI peut donc aussi être utilisé :

{itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023) policy-identifiers(1) baseline-ts-policy(1)}.

Annexe B1

Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques

Historique des versions		
Date	**Version**	**Evolution du document**
xxx	1.0	Publication de la première version de l'annexe B1 du référentiel général de sécurité

Avant propos

Le présent référentiel est pris en application de l'article LP 20 de la loi du pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices, et de son arrêté d'application.

Le présent document et ses annexes sont une copie adaptée du RGS B1 – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, en vigueur en métropole, version 2.03 du 21 février 2014.

Le texte fait des renvois à des documents publiés par l'Agence nationale de la sécurité des systèmes d'information[94] (ANSSI) ou encore disponibles sur son site internet www.ssi.gouv.fr, en ce qu'ils reflètent l'état de l'art en matière de sécurité informatique.

Le référentiel et ses annexes sont disponibles en ligne sur le site internet www.lexpol.pf, et leur mise à jour est assurée par la Direction générale de l'économie numérique.

[94] L'ANSSI est un service à compétence nationale rattaché au Secrétaire général de la défense et de la sécurité nationale, l'autorité chargée d'assister le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale. Parmi ses nombreux objectifs, l'un d'eux consiste à promouvoir un espace de confiance pour les services en ligne. Elle y participe en ce sens notamment au travers de la règlementation (référentiels) et ses labels (certification des produits de sécurité et qualification des produits de sécurité et des prestataires de service de confiance).

1 Introduction

1.1 Objectif du document

La cryptographie moderne met à la disposition des concepteurs de systèmes d'information des outils permettant d'assurer, ou de contribuer à assurer, des fonctions de sécurité telles que la confidentialité, l'intégrité, l'authenticité et la non-répudiation. Ces outils sont souvent qualifiés d'algorithmes, de primitives ou encore de **mécanismes cryptographiques**.

Suite aux développements majeurs qui ont eut lieu au cours des trois dernières décennies, la science cryptographique, bien qu'encore jeune, semble avoir atteint un degré de maturité suffisant pour permettre de dégager des règles générales concernant le choix et le dimensionnement corrects des mécanismes. Ce document vise à expliciter ces règles ainsi que certaines recommandations.

1.2 Positionnement du document

Ce document traite des règles et recommandations concernant le choix et le dimensionnement de mécanismes cryptographiques. Il est complété par deux documents :

- Un premier document intitulé « Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques « traite plus spécifiquement des aspects liés à la création, la distribution et la manipulation de clés.
- Un second document intitulé « Authentification – Règles et recommandations concernant les mécanismes d'authentification « traite plus spécifiquement des aspects liés à l'utilisation de mots de passe, de cartes mémoire, de clés de déverrouillage pour accéder à un système d'information.

Ces différents aspects ne sont donc pas traités par le présent document. Ce document constitue l'annexe B1 du RGS.

1.3 Limites du champ d'application du document

Comme indiqué en section 1.2, les règles et recommandations concernant la gestion des clés cryptographiques et l'authentification sont traitées en détail dans deux documents complémentaires. Sont également explicitement exclus de ce document :

- La recommandation de mécanismes cryptographiques précis permettant d'atteindre les différents niveaux de robustesse cryptographique définis dans ce document, bien que certaines primitives très classiques soient mentionnées ;
- Les aspects liés à l'implantation des mécanismes et en particulier au choix du support ainsi qu'à la sécurité de l'implantation face aux attaques par canaux auxiliaires (timing attack, simple power analysis [**SPA**], differential power analysis [**DPA**], higher order differential power analysis [**HO-DPA**], electromagnetic power analysis [**EMA**]...) ou par injection de faute (differential fault analysis [**DFA**]) ;
- Les méthodes d'évaluation des mécanismes cryptographiques, qui reposent avant tout sur une connaissance précise de l'état de l'art en cryptographie ;
- Les méthodes d'analyse de menaces et de développement de produits cryptographiques menant à choisir les mécanismes cryptographiques permettant d'assurer les fonctions de sécurité identifiées ainsi que les niveaux de robustesse cryptographique nécessaires ;

- Les liens entre niveau de robustesse d'un mécanisme cryptographique et niveau de robustesse d'un produit tel que défini dans les processus de qualification ou d'évaluation selon une méthode normalisée telle que les Critères Communs ;
- Les fournitures nécessaires à l'évaluation de mécanismes cryptographiques, qui font l'objet d'un document séparé intitulé « Fournitures nécessaires à l'analyse de mécanismes cryptographiques »[95] ;
- Les mécanismes non cryptographiques assurant cependant des fonctions de sécurité tels que l'emploi de mots de passe, l'usage de la biométrie. . . Ces mécanismes sont exclus du champ d'application de ce document car ils ne peuvent être analysés au moyen de méthodes cryptographiques usuelles. Ceci ne remet cependant pas en cause leur intérêt éventuel dans certaines applications. De tels mécanismes sont traités dans le document « Authentification – Règles et recommandations concernant les mécanismes d'authentification ».

1.4 Définition des règles et recommandations

Les **règles** définissent des principes qui doivent *a priori* être suivis par tout mécanisme. L'observation de ces règles est une condition généralement nécessaire à la reconnaissance du bon niveau de sécurité du mécanisme. Cependant, le fait de suivre l'ensemble des règles, qui sont par nature très génériques, n'est pas suffisant pour garantir la robustesse du mécanisme cryptographique ; seule une analyse spécifique permet de s'en assurer.

En plus des règles, le présent document définit également des **recommandations**. Elles ont pour but de guider le choix de certaines primitives et d'inciter à certains dimensionnements permettant un gain considérable en termes de sécurité, pour un coût souvent modique. Il va de soi qu'en tant que recommandations, leur application peut être plus librement modulée en fonction d'autres impératifs tels que des contraintes de performance ou de coût.

Il importe de noter dès à présent que les règles et recommandations contenues dans ce document ne constituent pas un dogme imposé aux concepteurs de produits utilisant des mécanismes cryptographiques. L'objectif est de contribuer à une amélioration constante de la qualité des produits de sécurité. À ce titre, le suivi des règles énoncées dans ce document doit être considéré comme une démarche saine permettant de se prémunir contre de nombreuses erreurs de conception ainsi que contre d'éventuelles faiblesses non décelées lors de l'évaluation des mécanismes cryptographiques.

Dans un souci de transparence, les règles et recommandations contenues dans ce document sont le plus souvent accompagnées de justifications. Le but est de convaincre que les choix ne sont pas faits de manière arbitraire mais au contraire en tenant compte le plus rigoureusement possible de l'état de l'art actuel en cryptographie ainsi que des contraintes pratiques liées à sa mise en œuvre.

La définition des règles et des recommandations prend également en compte certaines hypothèses classiques telles que la loi de Moore sur l'évolution de la puissance de calcul disponible, ce qui permet de définir des règles et des recommandations de manière suffisamment objective et scientifique pour fixer un cadre acceptable par tout professionnel en sécurité des systèmes d'information. Il va cependant de soi qu'une telle

[95] Actuellement, version 1.2, n° 2336/SGDN/DCSSI/SDS du 6 novembre 2006.

analyse ne peut tenir compte d'éventuels événements « catastrophiques « tels qu'une cryptanalyse opérationnelle de l'**AES** ou la découverte d'une méthode de factorisation efficace sur de grands nombres.

Par ailleurs, l'estimation des niveaux de résistance qui seront nécessaires afin de garantir la sécurité à 10 ou 20 ans des informations est délicate. Elle est cependant requise par de nombreuses applications comme par exemple le maintien de la confidentialité de certaines informations ou la signature électronique qui nécessite souvent une validité à long terme. De plus, lors de la définition d'un produit, il est nécessaire d'avoir une vision dont le terme est dicté par la durée de vie envisagée. Il est bien entendu possible de résoudre certains problèmes par des moyens techniques (surchiffrement régulier d'informations devant être protégées à long terme, horodatage et signature régulière de documents notariés...) ; cette approche est parfois indispensable mais ne peut être généralisée à cause des contraintes qu'elle impose. Par conséquent, une analyse qui semble valable à plus de 15 ans a été développée. Les résultats présentés doivent cependant être pris avec précaution. Il suffit pour s'en convaincre de comparer l'état de l'art actuel à celui d'il y a quelques dizaines d'années ; aucun mécanisme utilisé aujourd'hui n'a plus de quarante ans, le plus ancien étant certainement le **DES**, standardisé en 1977.

1.5 Organisation du document

Ce document est organisé de la manière suivante :

- L'ensemble des règles et recommandations sont regroupées dans le chapitre 2 ; elles sont repérées selon la codification suivante : les premières lettres (**Règle** ou **Recom**) indiquent si l'on a affaire à une règle ou une recommandation, le domaine d'application est ensuite précisé et, finalement, un chiffre permet de distinguer les règles d'une même catégorie. Par exemple, **RègleFact-3** désigne la règle numéro **3** concernant le problème de la factorisation ;
- Un rappel non mathématique des principaux concepts cryptographiques nécessaires à la compréhension de ce document est proposé dans l'annexe A ;
- Des informations issues de publications du milieu académique sur le dimensionnement des mécanismes cryptographiques sont regroupées dans l'annexe B ;
- Les références bibliographiques apparaissent dans l'annexe C.

Ce document ne comporte volontairement aucun tableau récapitulatif des tailles minimales de paramètres requis. La concision a été privilégiée dans l'expression des règles et recommandations ; vouloir les résumer à une simple valeur numérique serait une grave source d'erreur et de confusion.

1.6 Mise à jour du document

Ce document ayant en particulier pour but de fixer des bornes numériques, par exemple en termes de tailles de clés, il convient de le maintenir à jour régulièrement. Une révision tous les deux ans semble à la fois réaliste et suffisante.

2 Règles et recommandations

Les règles et recommandations contenues dans ce document sont organisées de manière très comparable aux rappels cryptographiques proposés en annexe A. Elles s'adressent à un lecteur familier avec ces concepts, qui ne sont par conséquent pas systématiquement rappelés.

2.1 Cryptographie symétrique

2.1.1 Taille de clé symétrique

Dans cette section sont définies les propriétés attendues de clés utilisées par des mécanismes symétriques. Dans ce document, la taille d'une clé est le nombre de bits effectifs de cette clé, c'est-à-dire le nombre de bits réellement variables[96]. Par exemple le **DES** utilise des clés de 64 bits mais seuls 56 de ces bits peuvent être choisis aléatoirement, les 8 bits restants servant de contrôle de parité. C'est pourquoi on considère que les clés **DES** ont une taille de 56 bits.

Les tailles minimales définies ci-dessous n'ont de valeur que sous l'hypothèse que la meilleure attaque pratique permettant de mettre en défaut le mécanisme symétrique employé consiste à effectuer une recherche exhaustive sur l'espace des clés. Cette attaque étant générique, le respect des règles définies ci-dessous est une condition nécessaire qui ne peut être considérée comme suffisante. Une analyse cryptographique du mécanisme est en particulier indispensable.

REGLES ET RECOMMANDATIONS :

RègleCléSym-1. La taille minimale des clés symétriques utilisées jusqu'en 2020 est de 100 bits.

RègleCléSym-2. La taille minimale des clés symétriques devant être utilisées au-delà de 2020 est de 128 bits.

RecomCléSym-1. La taille minimale recommandée des clés symétriques est de 128 bits.

Justifications :

- L'estimation de la capacité de calcul que peut rassembler une organisation motivée fait l'objet de beaucoup de controverses. De nombreux indices (voir A.1.1, B.1.1 et B.2.1) indiquent cependant que l'emploi de clé de moins de 100 bits semble risqué. Les clés de 56 bits sont clairement insuffisantes et la capacité actuelle à attaquer des clés de 64 bits est aujourd'hui admise, même si un tel calcul n'est pas à la portée de n'importe qui. De telles attaques ont cependant déjà été menées concrètement dans le milieu public (voir B.1.1).
- Une recherche exhaustive sur des clés de 100 bits demeure difficilement concevable avant plusieurs dizaines d'années. L'emploi de clés de moins de 128 bits devrait cependant tendre à disparaître avec l'emploi d'algorithmes modernes tels que l'**AES**.

[96] Formellement, la taille de la clé est définie en fonction de l'espace des clés possibles et de la probabilité de choix de chacune des clés en utilisant le concept d'entropie. En pratique, une approche aussi complexe est généralement inutile, l'idée intuitive de « taille de clé effective » étant évidente.

Remarques :

- L'impact en termes de performances de l'emploi de clés d'au moins 128 bits est souvent faible, comme le montre l'exemple de l'**AES**.
- L'emploi de clés de 128 bits permet de s'assurer que les attaques génériques par recherche exhaustive seront inopérantes, y compris à assez long terme. Ceci ne veut bien entendu pas dire que tout mécanisme utilisant de telles clés est cryptographiquement sûr.
- L'emploi de clés de 112 bits, comme dans le cas du triple **DES**, ne pose pas de problème pratique de sécurité vis-à-vis d'attaques par recherche exhaustive. L'utilisation du triple **DES** peut cependant être déconseillée pour d'autres raisons, en particulier liées à la taille du bloc (64 bits) insuffisante pour assurer une sécurité pratique avec certains modes opératoires classiques.

2.1.2 Chiffrement symétrique

2.1.2.1 Chiffrement par bloc

Les deux caractéristiques les plus simples d'un mécanisme de chiffrement par bloc sont la taille effective de la clé ainsi que la taille des blocs traités (voir A.1.1). Les règles et recommandations concernant la taille effective de la clé ont été présentées au paragraphe précédent.

Taille de bloc.

REGLES ET RECOMMANDATIONS :

RègleBlocSym-1. La taille minimale des blocs de mécanismes de chiffrement par bloc utilisés jusqu'en 2020 est de 64 bits.

RègleBlocSym-2. Pour une utilisation au-delà de 2020, la taille minimale des blocs de mécanismes de chiffrement par bloc est de 128 bits.

RecomBlocSym-1. La taille recommandée des blocs de mécanismes de chiffrement par bloc est de 128 bits.

Justifications :

- L'emploi de blocs de taille trop petite rend des attaques élémentaires comme la constitution de dictionnaires plus efficaces en pratique que la recherche de la clé secrète. Il est communément admis que la taille d'un bloc doit être d'au moins 64 bits.
- Les mécanismes de chiffrement par bloc sont utilisés via des modes opératoires permettant de chiffrer des messages de taille quelconque ou bien de calculer des codes d'authentification de message. La taille du bloc intervient alors dans l'estimation de la sécurité de ces mécanismes. La principale menace est la découverte, fréquente, d'attaques dites « en racine carrée «, fondées sur le paradoxe des anniversaires (voir A.1) ; ceci signifie que certaines attaques deviennent opérationnelles dès que plus de $2^n/2$ blocs de message sont traités, où n désigne la taille en bits du bloc. Dans le cas de blocs de 64 bits, la limite de sécurité est donc seulement de quelques milliards de blocs, ce qui peut être très rapidement atteint pour certaines applications. Une manière simple de se prémunir en pratique contre de telles attaques est d'utiliser des blocs de 128 bits.
- L'emploi de blocs de moins de 128 bits devrait tendre à disparaître avec l'emploi d'algorithmes modernes tels que l'**AES**.

Choix de l'algorithme. Le choix d'un algorithme de chiffrement par bloc repose sur la prise en compte des règles et recommandations liées à la taille de la clé ainsi qu'à la taille du bloc. Au-delà de la simple considération de ces deux dimensions, il faut bien entendu prendre en compte la sécurité intrinsèque apportée par le mécanisme face à des attaques plus évoluées que la simple recherche exhaustive sur la clé (cryptanalyse linéaire, différentielle. . .).

Considérons une attaque sur un algorithme de chiffrement par bloc. Une telle attaque a un but et nécessite des moyens. Le but peut être de retrouver la clé ou, plus modestement, de distinguer le chiffrement par bloc d'une permutation aléatoire. Les moyens consistent par exemple à permettre à l'attaquant d'observer des chiffrés, les clairs correspondants étant connus ou pas, ou bien de lui permettre de faire chiffrer des messages de son choix, voire même de faire déchiffrer des chiffrés qu'il choisit.

Afin de simplifier, on considère généralement qu'une attaque est qualifiée par :

- le nombre N_{op} d'opérations de calcul nécessaires à l'attaque, une opération étant équivalente au chiffrement d'un bloc;
- le nombre N_{bloc} de blocs à faire chiffrer ou déchiffrer afin de réaliser l'attaque ;
- la quantité N_{mem} de mémoire nécessaire, par exemple pour stocker des précalculs.

REGLES ET RECOMMANDATIONS :

RègleAlgoBloc-1. Pour un algorithme de chiffrement ne devant pas être utilisé après 2020, aucune attaque nécessitant moins de $N_{op} = 2^{100}$ opérations de calcul ne doit être connue.

RègleAlgoBloc-2. Pour un algorithme de chiffrement dont l'utilisation au-delà de 2020 est envisagée, aucune attaque nécessitant moins de $N_{op} = 2^{128}$ opérations de calcul ne doit être connue.

RecomAlgoBloc-1. Il est recommandé d'employer des algorithmes de chiffrement par bloc largement éprouvés dans le milieu académique.

Remarque importante :

- Les règles ne font pas mention du nombre de blocs N_{bloc} à faire chiffrer ou déchiffrer afin de réaliser l'attaque, ni de la quantité de mémoire N_{mem} nécessaire. Ceci tient essentiellement à la volonté de ne pas trop compliquer l'énoncé de ces règles. Il conviendra, au cas par cas, de juger si l'un de ces deux paramètres est suffisamment important afin de justifier qu'un mécanisme de chiffrement par bloc est sûr même s'il ne vérifie pas les règles RègleAlgoBloc-1 et/ou RègleAlgoBloc-2.

Justifications :

- Les règles tentent de définir les attaques que l'on qualifie habituellement de pratiques, opérationnelles ou réalistes, bien que ces termes prennent souvent des sens très différents selon qui les emploie.
- L'aspect pratique des attaques est privilégié. Par contre, il va de soi que l'existence d'attaques plus « théoriques », même si elles ne mènent pas directement à des attaques opérationnelles, sont une preuve d'existence de faiblesses intrinsèques au mécanisme.
- L'emploi d'algorithmes largement étudiés par la communauté académique offre un gage de qualité très important.

Mécanisme conforme au référentiel :

- L'**AES**, tel qu'il est spécifié dans le **FIPS 197**, est un mécanisme de chiffrement par bloc conforme au référentiel.

Remarque :

- Le triple **DES**, c'est-à-dire l'utilisation du **DES** avec deux clés K_1 et K_2 en chiffrant avec K_1, déchiffrant avec K_2 et chiffrant de nouveau avec K_1, est un algorithme de chiffrement par bloc utilisant des clés de 112 bits et des blocs de 64 bits. Le triple **DES** respecte donc les règles RègleCléSym-1 et RègleBlocSym-1 imposant des tailles de clés et de bloc minimales lorsqu'une utilisation au-delà de 2020 n'est pas envisagée. Cependant, ce mécanisme utilise une taille de bloc inférieure à la taille préconisée dans la recommandation RecomBlocSym-1. Il convient donc d'être extrêmement prudent lorsqu'on utilise ce mécanisme avec un mode opératoire de chiffrement, d'intégrité ou bien dans des protocoles de transport de clé par exemple, en particulier à cause de la faible taille du bloc. De plus, le triple **DES** avec deux clés est vulnérable à une attaque à clair connu. La complexité de cette attaque est de 2^{80} pour 2^{40} couples clairs-chiffrés connus et de 2^{100} pour 2^{20} couples clairs-chiffrés connus. Selon le cadre d'emploi, l'utilisation du triple **DES** avec deux clés peut ne pas être conforme au référentiel. En particulier, le contexte d'emploi ne doit pas permettre le chiffrement avec une même clé de plus de 2^{20} blocs de message connus d'un attaquant.

Mode opératoire pour le chiffrement. Le mode opératoire pour le chiffrement permet d'assurer la confidentialité de messages de taille quelconque à partir d'une primitive de chiffrement par bloc. Comme expliqué en A.1.1, un simple mécanisme de chiffrement par bloc ne permet pas d'assurer une telle fonction, en particulier à cause de sa nature fondamentalement déterministe et de la taille imposée des blocs de données traités.

REGLES ET RECOMMANDATIONS :

Le choix d'un mode opératoire de chiffrement est très dépendant de la nature des données traitées et du modèle de sécurité envisagé pour ce mécanisme. Les règles et recommandations se veulent malgré tout relativement génériques.

RègleModeChiff-1. Au sein du modèle de sécurité correspondant à l'usage du mode de chiffrement, il ne doit exister aucune attaque de complexité inférieure à $2^{n/2}$ appels de la primitive où n est la taille en bits du bloc.

RecomModeChiff-1. L'emploi d'un mode opératoire de chiffrement non déterministe est recommandé.

RecomModeChiff-2. L'utilisation d'un mode opératoire de chiffrement se fera de préférence conjointement à l'utilisation d'un mécanisme d'intégrité. Un tel mécanisme pourra être indépendant du mode de chiffrement.

RecomModeChiff-3. On utilisera de préférence des modes opératoires disposant d'une preuve de sécurité.

Justifications :

- De nombreux modes, tels que le **CBC** (voir A.1.1), ne sont sûrs que si l'on traite au plus de l'ordre de $2^{n/2}$ blocs de messages clairs, où n désigne la taille en bits du bloc. Pour un mécanisme de chiffrement utilisant des blocs de 64 bits, cette limite peut être rapidement atteinte (32 Go).

- L'aspect pratique des attaques est privilégié. Par contre, il va de soi que l'existence d'attaques plus « théoriques «, même si elles ne conduisent pas directement à des attaques opérationnelles, sont une preuve d'existence de faiblesses intrinsèques au mécanisme. Pour garantir la confidentialité des informations, un mode opératoire de chiffrement ne doit pas être déterministe. Cela permet notamment d'éviter que le chiffrement d'un même message fournisse le même chiffré. L'emploi de « valeurs initiales « et d'un mode opératoire adapté (voir A.1.1) permet de résoudre ce problème.
- Il est important de prendre en considération les capacités d'un éventuel attaquant à observer des messages chiffrés mais également à obtenir les messages clairs correspondants, à faire chiffrer ou déchiffrer des messages de son choix. . . Le modèle de sécurité est ici fondamental ; se restreindre au scénario où l'attaquant peut seulement avoir connaissance de messages chiffrés est une grave erreur qui peut avoir de réelles conséquences pratiques sur la sécurité du mécanisme.
- Le besoin de confidentialité est souvent associé à un besoin d'intégrité, même si ce dernier semble parfois moins évident à première vue. Il est fondamental de prendre conscience du fait qu'un mécanisme de chiffrement peut apporter une protection de très haut niveau en termes de confidentialité sans pour autant garantir la moindre intégrité ! En particulier, aucun des modes opératoires classiques (**ECB**, **CBC**, **OFB**, **CFB**, **CTR**) n'apporte la moindre protection en intégrité.

Mécanisme conforme au référentiel :

- Le mode de chiffrement **CBC** utilisant une primitive de chiffrement conforme au référentiel comme l'**AES** et des valeurs initiales aléatoirement choisies pour chaque message et transmises en clair est un mécanisme de chiffrement symétrique conforme au référentiel. Ce mécanisme est rappelé en section A.1.1. Il est particulièrement important de garantir que les valeurs initiales sont générées dans le périmètre de sécurité du chiffrement – par exemple dans le composant sécurisé où le mode de chiffrement et la primitive sous-jacente sont implantés et non hors de ce composant – et avec un générateur d'aléa sûr. Elles ne doivent en aucun cas pouvoir être contrôlées ou prédites par un attaquant.

2.1.2.2 Chiffrement par flot

Les algorithmes de chiffrement par flot[97] constituent l'autre grande famille de mécanismes de chiffrement symétrique (voir A.1.1).

L'algorithme dit de « one-time pad », qui se résume à une addition bit à bit du message à chiffrer avec une clé de même taille, est à part dans la classification des algorithmes de chiffrement. Il ne peut en particulier pas être considéré comme un chiffrement par flot même si ces derniers en dérivent souvent. Cet algorithme dispose d'une sécurité parfaite. Ses contraintes d'emploi sont cependant telles que son utilisation est en pratique impossible, sauf dans des cas très particuliers. Rappelons que ce mécanisme nécessite en particulier d'employer une clé à usage unique aussi longue que le message à protéger, sans aucune possibilité d'une quelconque réutilisation de cette clé. En général, l'emploi du « one-time pad » repousse simplement le problème du chiffrement au niveau de la mise en accord de clé.

Choix de l'algorithme. Avant de définir des règles liées au choix d'algorithmes de chiffrement par flot, il

[97] « Stream cipher » en anglais.

convient de rappeler que ces derniers ne garantissent en général aucune forme d'intégrité des messages transmis (voir remarque ci-dessus pour les modes de chiffrement par bloc). Cependant, pour un algorithme de chiffrement par flot sans rebouclage, le déchiffrement d'un message chiffré non généré par l'algorithme de chiffrement n'apporte aucune information supplémentaire susceptible de favoriser une attaque. Le modèle de sécurité généralement retenu pour l'évaluation de tels mécanismes est la connaissance par l'adversaire du flot de sortie de l'algorithme.

Il convient par ailleurs de préciser qu'il est exclusivement question des algorithmes de chiffrement par flot « dédiés », en ce sens qu'ils ont été conçus spécialement pour cet usage. Les règles ne concernent pas les autres types de générateurs pseudo-aléatoires déterministes (mode flot de chiffrement par bloc, générateurs fondés sur des problèmes difficiles, générateurs informatiquement sûrs).

D'autre part, les règles et recommandations en termes de chiffrement par flot se fondent sur le constat qu'à ce jour la recherche académique dans ce domaine ne semble pas posséder la même maturité que dans le domaine des primitives de chiffrement par bloc. Ces règles sont cependant susceptibles d'être revues si des avancées théoriques importantes sont effectuées dans le domaine du chiffrement par flot.

REGLES ET RECOMMANDATIONS :

RègleChiffFlot-1. Pour un algorithme de chiffrement par flot ne devant pas être utilisé après 2020, aucune attaque nécessitant moins de 2^{100} opérations de calcul ne doit être connue.

RègleChiffFlot-2. Pour un algorithme de chiffrement par flot devant être utilisé après 2020, aucune attaque nécessitant moins de 2^{128} opérations de calcul ne doit être connue.

RecomChiffFlot-1. Il est recommandé d'employer des primitives de chiffrement par bloc et non des algorithmes de chiffrement par flot dédiés. Il est ainsi possible, si les propriétés du chiffrement par flot sont requises, d'utiliser un mode opératoire par flot de chiffrement par bloc conforme au référentiel et simulant un chiffrement par flot.

RecomChiffFlot-2. En cas d'utilisation d'un algorithme de chiffrement par flot, il est recommandé d'employer des algorithmes de chiffrement par flot largement éprouvés dans le milieu académique.

Remarque importante :

- Les règles ne font pas mention de la quantité de données à chiffrer ou à déchiffrer afin de réaliser l'attaque, ni de la quantité de mémoire nécessaire. Ceci tient essentiellement à la volonté de ne pas trop compliquer l'énoncé de ces règles. Il conviendra, au cas par cas, de juger si l'un de ces deux paramètres est suffisamment important afin de justifier qu'un mécanisme de chiffrement par flot est sûr même s'il ne vérifie pas les règles RègleChiffFlot-1 et/ou RègleChiffFlot-2.

Justifications :

- L'aspect pratique des attaques est privilégié. Par contre, il va de soi que l'existence d'attaques plus « théoriques », même si elles ne conduisent pas directement à des attaques opérationnelles, sont une preuve d'existence de faiblesses intrinsèques au mécanisme.
- L'emploi d'algorithmes largement étudiés par la communauté académique offre un gage de qualité très important.

- Les algorithmes de chiffrement par flot dédiés sont parfois préférés aux algorithmes de chiffrement par bloc pour leur efficacité. L'expérience montre cependant que la conception d'algorithmes de chiffrement par flot dédié est très difficile. De nombreuses propositions ont été cryptanalysées et le savoir-faire ne semble pas avoir atteint une maturité comparable à celle observée dans le domaine du chiffrement par bloc. Par conséquent, l'emploi de chiffrement par bloc, en combinaison avec des modes opératoires satisfaisants, est recommandé, de préférence à des algorithmes de chiffrement par flot.
- Lorsque les propriétés du chiffrement par flot sont néanmoins requises, il est recommandé, si la dégradation en termes de performance le permet, d'utiliser un mode opératoire par flot de chiffrement par bloc, tel que les modes classiques **OFB**, **CFB** ou **CTR**. Il est ainsi possible de tirer parti du savoir-faire acquis en chiffrement par bloc tout en bénéficiant d'un mécanisme de chiffrement par flot.

2.1.3 Authentification et intégrité de messages

Les règles sur les méthodes d'authentification et d'intégrité de messages sont très dépendantes du mécanisme choisi. Certaines règles générales peuvent cependant être émises.

REGLES ET RECOMMANDATIONS :

RègleIntegSym-1. Les méthodes symétriques d'intégrité les plus classiques se basent sur des mécanismes de chiffrement par bloc ou de hachage. De telles primitives doivent être conformes au référentiel.

RègleIntegSym-2. Il ne doit pas exister d'attaque sur le mécanisme d'intégrité utilisant moins de $2^{n/2}$ appels à la primitive sous-jacente où n est la taille de sortie de cette primitive.

RecomIntegSym-1. On utilisera de préférence des mécanismes disposant d'une preuve de sécurité.

Remarques :

- Par confusion avec les modes opératoires de chiffrement, l'emploi de « valeurs initiales » est parfois constaté pour des mécanismes d'intégrité tels que le **CBC-MAC**[98]; de graves failles de sécurité peuvent en découler.
- Il est important de prendre en considération les capacités d'un éventuel attaquant à observer des éléments d'intégrité mais également à en obtenir pour des messages de son choix, par exemple.
- De nombreux modes, tels que le **CBC-MAC**, ne sont sûrs que si l'on traite au plus de l'ordre de $2^{n/2}$ blocs de messages clairs, où n désigne la taille en bits du bloc. Pour un mécanisme de chiffrement utilisant des blocs de $n = 64$ bits, cette limite peut être rapidement atteinte.
- **L'emploi de clés de taille importante ne garantit pas nécessairement une sécurité en rapport avec cette taille. La plupart des variantes du CBC-MAC construites afin d'obtenir une sécurité**

[98] Pour des raisons de simplification, **CBC-MAC** désigne le mode avec surchiffrement également connu sous le nom de **CBC-MAC** « retail ». (voir section A.1.1)

comparable à celle du triple DES ont ainsi été cryptanalysées au sens où leur sécurité est plus comparable à celle du DES que du triple DES (c'est le cas de l'exemple de la section A.1.1 si l'on utilise le **DES** comme algorithme de chiffrement par bloc, même si la taille de la clé est au total de 112 bits).

- Un mécanisme d'intégrité vient souvent en complément d'un mécanisme assurant la confidentialité. La composition de deux mécanismes cryptographiques n'est jamais simple et doit être réalisée avec soin. À titre d'exemple, il est possible en associant un très bon chiffrement avec un très bon algorithme d'intégrité d'obtenir un mécanisme n'assurant plus le service de confidentialité.

Mécanismes conformes au référentiel :

- Le mode d'intégrité **CBC-MAC** « retail « utilisant l'**AES** comme mécanisme de chiffrement par bloc et deux clés distinctes (une pour la chaîne **CBC** et l'autre pour le surchiffrement dit « retail ») est conforme au référentiel (à condition, bien entendu, de ne pas utiliser de valeur initiale). Ce mécanisme est rappelé section A.1.1. Il est à noter que le mode **CBC-MAC** sans surchiffrement n'est sûr que lorsqu'il est utilisé pour des messages de taille fixe.
- Le mode d'intégrité **HMAC** utilisant **SHA-2** comme fonction de hachage est conforme au référentiel.

*Mécanisme **non conforme** au référentiel :*

- Le mode d'intégrité **CBC-MAC** « retail « recommandé ci-dessus n'est pas conforme au référentiel s'il est utilisé avec le **DES** comme mécanisme de chiffrement par bloc, et ce même s'il emploie deux clés distinctes. En effet, bien qu'utilisant alors 112 bits de clé, l'observation de 2^{32} **MACs** valides permet ensuite de retrouver ces 112 bits de clé en effectuant « seulement » de l'ordre de 2^{56} calculs de **DES**.

2.2 Cryptographie asymétrique

Les mécanismes de cryptographie asymétrique reposent tous sur des problèmes mathématiques difficiles, généralement issus de la théorie des nombres (voir 2.2.2). L'emploi de tels types de problèmes, difficiles à résoudre pour un attaquant, est par conséquent primordial en termes de sécurité.

2.2.1 Problèmes mathématiques asymétriques

2.2.1.1 Factorisation

Le problème de la factorisation consiste à retrouver la décomposition en facteurs premiers d'un entier donné, obtenu de manière secrète par multiplication de deux nombres premiers, généralement de taille comparable. Un tel nombre composé est classiquement appelé « module ».

Le problème de la factorisation est principalement utilisé par le cryptosystème **RSA**. Les calculs de chiffrement et de déchiffrement **RSA** font intervenir deux autres données que le module, appelées « exposant public » et « exposant secret ».

REGLES ET RECOMMANDATIONS :

RègleFact-1. La taille minimale du module est de 2048 bits, pour une utilisation ne devant pas dépasser l'année 2030.

RègleFact-2. Pour une utilisation au-delà de 2030, la taille minimale du module est de 3072 bits.

RègleFact-3. Les exposants secrets doivent être de même taille que le module.

RègleFact-4. Pour les applications de chiffrement, les exposants publics doivent être strictement supérieurs à $2^{16} = 65536$.

RecomFact-1. Il est recommandé d'employer des modules d'au moins 3072 bits, même pour une utilisation ne devant pas dépasser 2030.

RecomFact-2. Il est recommandé, pour toute application, d'employer des exposants publics strictement supérieurs à $2^{16} = 65536$.

RecomFact-3. Il est recommandé que les deux nombres premiers *p* et *q* constitutifs du module soient de même taille et choisis aléatoirement uniformément.

Justifications :

- La taille des modules **RSA** est un sujet souvent très polémique. L'usage courant fait que l'utilisation de modules de 1024 bits est en général considéré comme suffisant pour garantir une sécurité pratique, même si les analyses effectuées par les plus grands spécialistes du domaine s'accordent sur l'idée que de tels modules n'apportent pas une sécurité suffisante, ou tout du moins comparable à celle que l'on exige des autres mécanismes cryptographiques. L'application d'un paradigme fondamental de la cryptographie, qui consiste à dimensionner les systèmes non pas en se plaçant juste à la limite des capacités d'attaquants connus (voir B.2.1) mais en s'imposant une marge de sécurité, milite pour l'emploi de modules d'au moins 2048 bits, même si aucun module de 1024 bits n'a été officiellement factorisé à ce jour[99]. Par conséquent, l'emploi de modules de 1024 bits est considéré comme une prise de risque incompatible avec des critères de sécurité raisonnables.
- Les paragraphes B.2.1 et B.2.2 fournissent des informations complémentaires sur les analyses liées au problème de la factorisation.
- L'emploi d'exposants secrets particuliers (comme des exposants secrets petits par exemple) afin d'améliorer les performances est à proscrire étant donné les attaques pratiques publiées à ce sujet.
- L'emploi d'exposants publics très petits, tels que l'exposant 3, est également à proscrire dans le cas du chiffrement à cause des attaques existantes. Plus généralement, pour toute application, l'emploi de tels exposants est déconseillé pour des raisons de sécurité.
- L'emploi de nombres premiers *p* et *q* trop proches ou de tailles trop différentes peut compromettre la sécurité du système. Il faut également éviter des valeurs possédant des propriétés particulières comme l'absence d'un grand facteur premier dans la décomposition de *p*-1 ou *q*-1. Pour éviter ces problèmes, il est recommandé de choisir *p* et *q* aléatoirement uniformément parmi les nombres premiers de taille égale à la moitié de la taille du module.

2.2.1.2 Logarithme discret

Le problème dit « du logarithme discret » est fondé sur la difficulté d'inverser l'opération d'exponentiation dans un groupe. Ce problème peut être instancié dans différentes structures et nous donnons ici des règles et

[99] Un résultat de 2007 annonce la factorisation d'un nombre de 1039 bits. Cependant ce nombre n'est pas de type module **RSA**.

recommandations sur les choix de paramètres à utiliser pour trois d'entre elles :

- Les corps finis **GF**(*p*) à p éléments où p est un nombre premier ;
- Les groupes des points de courbes elliptiques définies sur **GF**(*p*) où p est un nombre premier ;
- Les groupes des points de courbes elliptiques définies sur **GF**(2^n).

Bien qu'il soit possible d'instancier ce problème dans d'autres structures, nombre d'entre elles sont à proscrire : tel est notamment le cas des corps finis de petite caractéristique, et en particulier de **GF**(2^n). Certaines de ces autres structures ne présentent toutefois pas de faiblesses connues, mais leur sécurité doit être étudiée au cas par cas et leur emploi doit être soumis à l'avis de l'ANSSI.

Logarithme discret dans GF(*p*) Le problème dit « du logarithme discret dans **GF**(*p*) » est fondé sur des calculs effectués dans le corps fini à *p* éléments, où *p* est un nombre premier également appelé « module ».

REGLES ET RECOMMANDATIONS :

RègleLogp-1. La taille minimale de modules premiers est de 2048 bits pour une utilisation ne devant pas dépasser l'année 2030.

RègleLogp-2. Pour une utilisation au delà de 2030, la taille minimale de modules premiers est de 3072 bits.

RègleLogp-3. On emploiera des sous-groupes dont l'ordre est multiple d'un nombre premier d'au moins 200 bits.

RecomLogp-1. Il est recommandé d'employer des modules premiers d'au moins 3072 bits, même pour une utilisation ne devant pas dépasser 2030.

RecomLogp-2. Il est recommandé d'employer des sous-groupes dont l'ordre est premier (au lieu d'être multiple d'un nombre premier).

Justifications :

- Le problème du logarithme discret dans **GF**(*p*) semble avoir une complexité comparable à celle de la factorisation. Des méthodes similaires s'appliquent à la résolution des deux problèmes et il est raisonnable de penser qu'une avancée majeure dans la résolution du problème de la factorisation s'accompagnera d'une avancée semblable dans celui du logarithme discret. Il est par conséquent naturel d'appliquer des règles identiques pour les deux problèmes.
- Le problème du logarithme discret semble cependant légèrement plus difficile en pratique, certaines phases de calcul étant plus délicates que pour la factorisation, les records de calcul (voir B.2.1) mettent en évidence un décalage compris entre 100 et 200 bits mais on peut se demander si une telle différence ne provient pas en partie du plus grand prestige promis à un record en matière de factorisation.
- La raison de recommander un sous-groupe d'ordre premier est que, si l'ordre d'un sous-groupe n'est pas premier mais possède un petit facteur premier (dans le pire cas, 2), le problème Diffie–Hellman décisionnel dans ce sous-groupe peut être résolu avec une probabilité non négligeable. Ceci peut être très problématique, notamment dans des procédures de chiffrement de type **ElGamal**.

Logarithme discret dans les courbes elliptiques définies sur GF(*p*). Il est également possible de définir un problème de logarithme discret dans des structures plus complexes pour lesquelles aucun algorithme plus

efficace que les méthodes génériques de calcul de logarithme discret n'est connu. C'est en particulier aujourd'hui le cas des courbes elliptiques qui sont définies sur un corps de base pouvant être, en pratique, premier (**GF**(*p*)) ou binaire (**GF**(2^n)).

REGLES ET RECOMMANDATIONS :

RègleECp-1. Pour une utilisation ne devant pas dépasser 2020, on emploiera des sous-groupes dont l'ordre est multiple d'un nombre premier d'au moins 200 bits.

RègleECp-2. Pour une utilisation au-delà de 2020, on emploiera des sous-groupes dont l'ordre est multiple d'un nombre premier d'au moins 256 bits.

RègleECp-3. En cas d'utilisation de courbes particulières faisant reposer la sécurité sur un problème mathématique plus facile que le problème générique de calcul de logarithme discret sur courbe elliptique définie sur **GF**(p), ce problème devra vérifier les règles correspondantes.

RecomECp-1. Il est recommandé d'employer des sous-groupes dont l'ordre est premier (au lieu d'être multiple d'un nombre premier)

Justifications :

- Le problème du logarithme discret sur courbe elliptique semble aujourd'hui un problème très difficile. Il permet d'obtenir, pour des tailles de paramètres réduites, une sécurité comparable à celle exigée pour des primitives symétriques.
- En cas d'utilisation de courbes généralement qualifiées de « particulières «, la sécurité peut être sérieusement dégradée. Le problème mathématique sous-jacent peut notamment être ramené à un problème de calcul de logarithme discret dans un corps fini et non plus sur une courbe elliptique. Dans ce cas, les règles relatives à ce problème s'appliquent bien évidemment. Par exemple, dans le cadre d'un cryptosystème utilisant les couplages — pour lequel l'utilisation de courbes « particulières « est nécessaire — le choix desdites courbes devra être fait avec soin. En particulier, les préconisations de la partie 2.2.1.2 concernant la difficulté du logarithme discret devront être prises en compte pour le choix du groupe multiplicatif dans lequel le couplage prend ses valeurs.
- La raison de recommander un sous-groupe d'ordre premier est encore une fois que si l'ordre d'un sous-groupe n'est pas premier mais petit multiple (dans le pire cas, 2) d'un grand premier, le problème Diffie–Hellman décisionnel dans ce sous-groupe peut être résolu avec une probabilité non-négligeable.

Mécanisme conforme au référentiel :

- L'emploi de la courbe **FRP256v1** – définie dans le journal officiel n° 241 du 16/10/2011 et dont les paramètres, validés l'ANSSI, peuvent librement être intégrés dans tous les produits de sécurité – est conforme au référentiel. Il en est de même de l'emploi des courbes P-256, **P-384** et **P-521** définies dans le **FIPS 186-2** du 27/01/2000.

Logarithme discret dans les courbes elliptiques définies sur GF(2^n)

REGLES ET RECOMMANDATIONS :

RègleEC2-1. Pour une utilisation ne devant pas dépasser 2020, on emploiera des sous-groupes dont l'ordre est multiple d'un nombre premier d'au moins 200 bits.

RègleEC2-2. Pour une utilisation au-delà de 2020, on emploiera des sous-groupes dont l'ordre est multiple d'un nombre premier d'au moins 256 bits.

RègleEC2-3. Le paramètre n doit être un nombre premier.

RègleEC2-4. En cas d'utilisation de courbes particulières faisant reposer la sécurité sur un problème mathématique plus facile que le problème générique de calcul de logarithme discret sur courbe elliptique définie sur **GF**(2^n), ce problème devra vérifier les règles correspondantes.

RecomEC2-1. Il est recommandé d'employer des sous-groupes dont l'ordre est premier (au lieu d'être multiple d'un nombre premier).

Justifications :

- L'emploi de *n* composé réduit considérablement la difficulté du calcul de logarithme discret et affaiblit donc le mécanisme correspondant.
- Les courbes elliptiques définies sur **GF**(*p*) ne sont pas différenciées de celles définies sur **GF**(2^n).

Mécanisme conforme au référentiel :

- L'emploi des courbes **B-283**, **B-409** et **B-571** définies dans le **FIPS** 186-2 du 27/01/2000 est conforme au référentiel.

2.2.1.3 Autres problèmes

Plusieurs autres problèmes ont été proposés dans le milieu académique afin de fournir des alternatives aux problèmes cités précédemment. C'est notamment le cas de la résolution de systèmes d'équations multivariées, de la recherche de plus courts ou plus proches vecteurs dans des réseaux euclidiens ou encore du décodage de codes correcteurs d'erreurs. Ces problèmes n'étant que peu utilisés aujourd'hui en pratique, leur sécurité est à traiter au cas par cas.

2.2.2 Chiffrement asymétrique

Toute méthode de chiffrement asymétrique s'appuie sur un problème difficile de base. Ce dernier doit donc être en accord avec le niveau de robustesse recherché. Il est de plus possible pour certains mécanismes de chiffrement de faire la preuve, éventuellement sous certaines hypothèses, que la sécurité est équivalente à celle du problème de base et pas uniquement reliée de manière heuristique. Cette approche moderne de la cryptographie permet d'atteindre un niveau d'assurance meilleur que la simple approche qui consiste à constater l'absence d'attaques connues.

REGLES ET RECOMMANDATIONS :

RecomChiffAsym-1. Il est recommandé d'employer des mécanismes de chiffrement asymétrique disposant d'une preuve de sécurité.

Justification :

- L'existence d'une preuve de sécurité apporte des garanties importantes sur la résistance du mécanisme.

Mécanisme conforme au référentiel :

- Le mécanisme de chiffrement asymétrique **RSAES-OAEP** défini dans le document **PKCS#**1v2.1 est conforme au référentiel à condition de respecter les règles RègleFact-1, RègleFact-2, RègleFact-3 et RègleFact-4.

Mécanisme non conforme au référentiel :

- Le mécanisme de chiffrement asymétrique **RSAES**, mis en œuvre selon le document **PKCS#**1 v1.5 n'est pas conforme au référentiel dans un contexte où il est possible d'invoquer un oracle de vérification de padding. En effet, Bleichenbacher a mis en évidence en 1998 une attaque (attaque à messages chiffrés choisis adaptative) exploitant judicieusement un tel oracle pour retrouver le message clair correspondant à un chiffré donné [Ble98].

2.2.3 Signature asymétrique

Toute méthode de signature asymétrique s'appuie sur un problème difficile de base. Ce dernier doit donc être en accord avec le niveau de robustesse recherché. Il est de plus possible pour certains mécanismes de signature de faire la preuve, éventuellement sous certaines hypothèses, que la sécurité est équivalente à celle du problème de base et pas uniquement reliée de manière heuristique.

Les schémas de signature utilisent de plus en général des fonctions de hachage dont le niveau de robustesse (voir 2.3) doit bien entendu être en accord avec le niveau de robustesse souhaité pour le mécanisme de signature.

REGLES ET RECOMMANDATIONS :

RecomSignAsym-1. Il est recommandé d'employer des mécanismes de signature asymétrique disposant d'une preuve de sécurité.

Mécanismes conformes au référentiel :

- Le mécanisme de signature asymétrique **RSA-SSA-PSS**[100] défini dans le document **PKCS#1 v2.1** est conforme au référentiel à condition de respecter les règles RègleFact-1, RègleFact-2, RègleFact-3 et RègleFact-4.
- Le mécanisme de signature asymétrique **ECDSA** défini dans le **FIPS 186-2**, ainsi que le mécanisme de signature asymétrique **ECKCDSA**, sont conformes au référentiel lorsqu'ils utilisent la courbe **FRP256 v1** – définie dans le journal officiel de la République française n° 241 du 16/10/2011 et dont les paramètres, validés par l'ANSSI, peuvent librement être intégrés dans tous les produits de sécurité – ou lorsqu'ils utilisent l'une des courbes **P-256**, **P-384**, **P-521**, **B-283**, **B-409** et **B-57**1 définies dans le **FIPS 186-2**.

Mécanisme non conforme au référentiel :

- Le mécanisme de signature asymétrique **RSASSA**, mis en œuvre selon le document **PKCS#1 v1.5** n'est pas conforme au référentiel lorsque l'exposant public *e* est petit et pour un mauvais choix

[100] **RSA-SSA-PSS** : "RSA Signature Scheme with Appendix – Provably Secure encoding method for digital Signatures".

d'implantation des vérifications liées au padding. En effet, Bleichenbacher a mis en évidence en 2006 une attaque permettant de forger des signatures dans ce cas [Ble06].

2.2.4 Authentification d'entités et établissement de clé

Comme il est rappelé en A.2.3, les mécanismes interactifs d'authentification d'entités et d'établissement de clé reposent en général au moins partiellement sur des mécanismes de génération d'aléa, de hachage et de chiffrement ou de signature à clé publique. Les règles et recommandations énoncées dans les sections 2.2.2, 2.2.3, 2.3 et 2.4 s'appliquent alors directement. Ces mécanismes peuvent également faire appel à des primitives asymétriques spécifiques, telles que les schémas d'authentification « à divulgation nulle de connaissance » ou le schéma d'établissement de clé de Diffie-Hellman; les règles et recommandations énoncées dans la section 2.2.1 s'appliquent alors aux problèmes mathématiques sur lesquels ces primitives reposent. Bien entendu, l'évaluation du niveau de robustesse global du mécanisme doit être effectuée avec soin, même si des primitives conformes au référentiel sont employées. Une attention particulière devra notamment être portée à la résistance des mécanismes d'établissement de clé aux attaques par le milieu. L'utilisation conjointe de mécanismes d'établissement de clé et d'authentification d'entité convenablement liés l'un à l'autre peut permettre de se prémunir contre des attaques de ce type. Il est également souhaitable qu'un mécanisme d'établissement de clé assure la confidentialité dans le futur ou **PFS** (de l'anglais *perfect forward privacy*) des clés symétriques temporaires (ou *clés de session*) qu'il permet d'établir. On peut définir informellement la propriété de **PFS** comme l'impossibilité d'obtenir quelque information que ce soit sur une clé de session pour un attaquant capable (1) d'observer et/ou perturber les échanges d'établissement de clé au cours de laquelle cette clé de session a été établie entre deux entités et (2) d'accéder, postérieurement à la période de validité de cette clé de session, à l'ensemble des secrets d'une de ces deux entités. Une condition nécessaire pour assurer cette propriété de **PFS** est de recourir, pour l'établissement des clés symétriques temporaires, à un schéma reposant sur l'emploi par les deux entités de secrets éphémères effacés après utilisation. Bien entendu, les clés symétriques temporaires doivent elles-mêmes être effacées par les deux entités à l'échéance de leur période de validité (fin de session).

Les mécanismes utilisant des mots de passe sous une forme quelconque (pass-phrase, code d'identification personnel...) ainsi que les mécanismes s'appuyant sur des procédés biométriques ne sont pas de nature cryptographique et par conséquent ne sont pas traités dans le cadre de ce document. Bien entendu, ceci ne signifie pas qu'ils ne présentent aucun intérêt pour la sécurisation d'un système d'information.

Le document intitulé « Authentification – Règles et recommandations concernant les mécanismes d'authentification »aborde plus spécifiquement cette question. Rappelons cependant quelques remarques élémentaires liées à l'utilisation de mots de passe :

- Si l'on souhaite dériver des clés secrètes à partir de mots de passe, ces derniers doivent être suffisamment longs et « non devinables » pour offrir une sécurité compatible avec les règles relatives aux tailles de clés. À titre d'exemple, des mots de passe de 8 caractères alphanumériques (chiffres et lettres majuscules ou minuscules) ne permettent pas de générer des clés de plus de 47 bits, et encore sous l'hypothèse très optimiste que ces mots de passe sont choisis aléatoirement.
- Il convient, lorsqu'on étudie la sécurité d'un mécanisme d'authentification, de distinguer les calculs qui peuvent être effectués « off-line », c'est-à-dire sans accès à une ressource telle qu'un serveur, et les opérations qui doivent être réalisées « on-line ». Ainsi un protocole d'authentification par mot de passe ne doit pas permettre de tests de vérifications off-line efficaces. Il faut également prendre en compte le nombre de ressources susceptibles d'être attaquées.

- Notons enfin que des attaques fondées sur le paradoxe des anniversaires peuvent également s'appliquer, par exemple si une liste d'empreintes de mots de passe d'accès à un système est disponible.

2.3 Fonctions de hachage

Les fonctions de hachage cryptographiques doivent avoir plusieurs propriétés telles que la résistance à la recherche de « collisions » (voir A.3). De telles collisions peuvent cependant toujours être trouvées au moyen d'attaques génériques fondées sur le « paradoxe des anniversaires ». Un des buts lors de la conception d'une fonction de hachage est par conséquent de faire en sorte qu'il n'existe pas de meilleure attaque. En pratique, afin de contrer les attaques fondées sur le paradoxe des anniversaires, une empreinte doit être deux fois plus longue qu'une clé symétrique pour atteindre le même niveau de robustesse.

D'autre part, les fonctions de hachage itératives sont construites autour de fonctions plus élémentaires appelées fonctions de compression. L'existence d'attaques sur ces constituants, attaques qualifiées de « partielles « ci-dessous, n'implique pas nécessairement la possibilité d'attaquer la fonction de hachage en elle-même mais trahit des défauts de conception majeurs.

REGLES ET RECOMMANDATIONS :

RègleHash-1. Pour une utilisation ne devant pas dépasser 2020, la taille minimale des empreintes générées par une fonction de hachage est de 200 bits.

RègleHash-2. Pour une utilisation au-delà de 2020, la taille minimale des empreintes générées par une fonction de hachage est de 256 bits.

RègleHash-3. La meilleure attaque connue permettant de trouver des collisions doit nécessiter de l'ordre de $2^{h/2}$ calculs d'empreintes, où *h* désigne la taille en bits des empreintes.

RecomHash-1. L'emploi de fonctions de hachage pour lesquelles des « attaques partielles » sont connues est déconseillé.

Justifications :

- Les règles en termes de taille d'empreinte sont directement déduites de celles appliquées en cryptographie symétrique.
- Il faut insister sur le fait que l'existence d'attaques partielles, même si elles ne conduisent pas à une attaque sur la fonction de hachage, trahit de graves défauts de conception.
- Le critère de sécurité employé pour juger de la qualité d'une fonction de hachage est l'absence de collisions connues. Dans certaines applications, cette propriété semble trop forte car seul le calcul de « pré-image » doit être irréalisable. Il est cependant considéré ici qu'indépendamment de son contexte d'utilisation, une fonction de hachage ne peut être reconnue conforme au référentiel que si elle présente une résistance suffisante à la recherche de collision. Ceci n'est pas contradictoire avec la possibilité qu'un mécanisme employant une fonction de hachage non conforme au référentiel puisse tout de même être jugé, dans sa globalité, comme atteignant un niveau de sécurité suffisant.

Mécanisme conforme au référentiel :

- Le mécanisme de hachage **SHA-256** défini dans le **FIPS 180-2** est conforme au référentiel.

Mécanisme non conforme au référentiel :

- Le mécanisme de hachage **SHA-1** défini dans le **FIPS 180-2** a récemment fait l'objet d'une attaque en recherche de collision. La complexité de cette attaque est estimée à 2^{63}, c'est à dire inférieure à 2^{80}. Même si cette attaque n'a pas conduit, au moment de la rédaction de ce document, au calcul d'une collision explicite, sa seule existence montre une faille sérieuse dans la sécurité de cette fonction. Le mécanisme de hachage **SHA-1** n'est donc pas conforme au référentiel. Il ne respecte ni RègleHash-1, ni RègleHash-3.

2.4 Génération d'aléa cryptographique

Comme expliqué au paragraphe A.4, la qualité de l'aléa est un élément crucial pour la sécurité d'un système, que ce soit pour la génération des clés ou pour le bon fonctionnement des primitives cryptographiques.

Dans cette partie sont énoncées les règles et les recommandations applicables à un générateur d'aléa destiné à alimenter un système cryptographique de manière durable.

Un tel générateur consiste généralement en la combinaison de différentes sources d'aléa et d'une couche de retraitement algorithmique.

Plus précisément, une **source d'aléa** désignera un dispositif susceptible de fournir en entrée du retraitement des éléments au moins partiellement aléatoires. Une source d'aléa est :

- **physique** s'il s'agit d'un **générateur physique** d'aléa, c'est-à-dire d'un dispositif physique spécialement conçu pour produire des bits aléatoires en quantité (théoriquement) illimitée ;
- **systémique** si elle correspond à une accumulation d'événements partiellement imprévisibles provenant du système (par exemple le procédé d'accumulation d'aléa de /**dev/random** sous Linux) ;
- **importée** s'il s'agit de données secrètes parfaitement aléatoires spécialement fournies par le reste du système d'information ;
- **manuelle** s'il s'agit de données aléatoires secrètes obtenues par action intentionnelle d'un utilisateur (par exemple : frappes au clavier, mouvements de la souris. . .).

On note que selon les cas les sources d'aléa peuvent être disponibles de manière régulière ou, au contraire, ponctuelle.

Dans le cas d'un ordinateur personnel, l'exemple le plus simple de source manuelle consiste à demander à l'utilisateur d'entrer au clavier une suite suffisamment longue de caractères « aléatoires », puis à en extraire une valeur secrète courte par hachage. Toutefois, de manière générale, il est préférable que l'interaction de l'utilisateur ne soit pas facilement reproductible et fasse intervenir également des valeurs comme les instants de frappe au clavier ou les positions successives de la souris.

Un **retraitement algorithmique** est un mécanisme de nature cryptographique destiné à combiner différentes sources d'aléa et à garantir dans la durée la qualité de l'aléa produit.

Un **état interne** est une donnée secrète dédiée au retraitement, destinée généralement à accumuler l'entropie des sources d'aléa. Les éventuelles clés secrètes utilisées par les mécanismes cryptographiques employés par le retraitement font également partie de l'état interne.

En l'absence de source d'aléa régulière, c'est-à-dire si les sources d'aléa disponibles sont ponctuelles, on note que le retraitement s'apparente à un **générateur pseudo-aléatoire**. Il possède nécessairement un état interne et une source d'aléa ponctuelle pour l'initialiser.

Dans le cas des systèmes pouvant être mis hors tension (cas considéré par défaut dans ce qui suit), un élément

de sécurité important consiste en l'utilisation d'une **mémoire non volatile**, protégée en confidentialité et en intégrité, pour stocker des données qui seront utilisées lors de l'initialisation suivante. Ces données peuvent par exemple être mises à jour par les fonctions d'initialisation et/ou d'avancement. En particulier, de telles dispositions permettent de se protéger des attaques par rejeu et de fournir suffisamment d'entropie à l'algorithme de retraitement lors de l'initialisation.

Finalement, les différents éléments constituant un générateur d'aléa cryptographique peuvent être représentés de la manière suivante (figure 1), étant entendu que tous les composants ne sont pas forcément nécessaires et que le détail des fonctionnalités représentées peut varier d'un système à un autre.

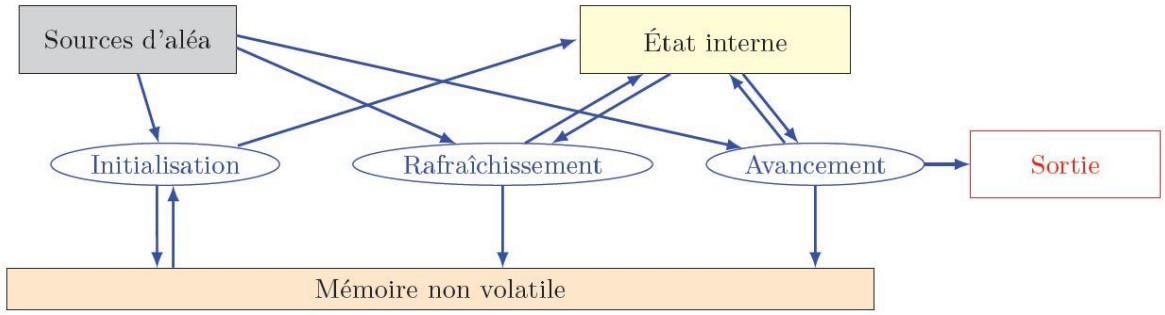


FIGURE 1 – Architecture générique pour la génération d'aléa cryptographique

Les règles et recommandations applicables aux générateurs d'aléa se fondent sur le constat qu'il est aujourd'hui très difficile de fournir une preuve convaincante concernant la qualité de l'aléa issu d'un générateur physique, alors qu'il est relativement aisé de se convaincre de la qualité d'un bon retraitement. Ces règles sont cependant susceptibles d'être revues si des avancées théoriques importantes sont effectuées dans le domaine des générateurs physiques d'aléa.

2.4.1 Architecture d'un générateur d'aléa

REGLES ET RECOMMANDATIONS :

RègleArchiGDA-1. Un retraitement algorithmique disposant d'un état interne doit être employé.

RègleArchiGDA-2. En l'absence de générateur physique d'aléa, le retraitement algorithmique doit disposer d'une mémoire non volatile.

RègleArchiGDA-3. L'état interne doit être au minimum de 128 bits. En l'absence d'un rafraîchissement suffisamment fréquent par un générateur physique d'aléa, cette limite inférieure est portée à 160 bits.

RègleArchiGDA-4. La qualité des sources d'aléa ponctuelles ou régulières utilisées pour initialiser l'état interne doit être suffisante pour assurer à la valeur initiale de cet état une entropie voisine de sa longueur, ou tout au moins supérieure au seuil défini dans la règle RègleArchiGDA-3 si un raisonnement permet d'établir qu'aucune faiblesse n'en résulte.

RecomArchiGDA-1. Il est recommandé d'utiliser un retraitement avec un état interne d'au moins 256 bits, une mémoire non volatile et une source d'aléa rafraîchissant régulièrement l'état interne du

générateur.

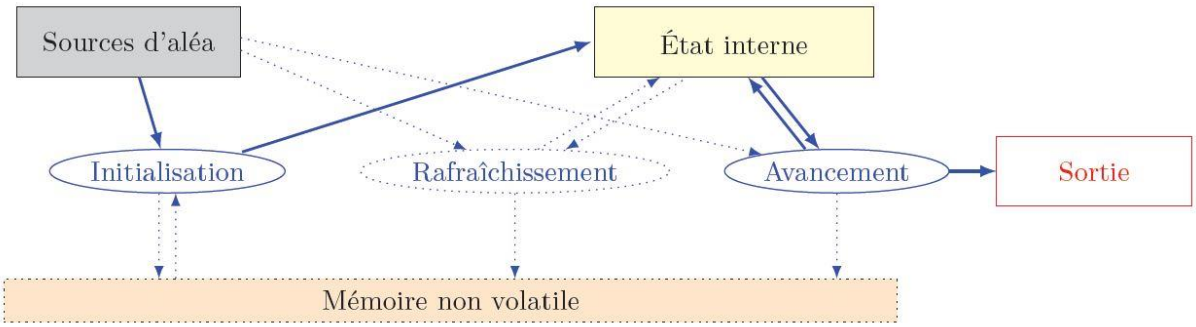


FIGURE 2 – Architecture minimale pour la génération d'aléa (Les pointillés figurent les éléments recommandés.)

Justifications :

- L'emploi d'un générateur physique non retraité est exclu. De même, l'emploi de retraitements élémentaires (« lissages »), ou dont l'état interne est trop petit est jugé insuffisant.
- Un retraitement algorithmique est, par nature, très différent d'un générateur physique d'aléa. En effet, le retraitement est un algorithme déterministe qui ne « génère « pas d'aléa mais uniquement des suites de bits indistinguables de suites réellement aléatoires en partant d'une graine aléatoire de petite taille.
- Le bon fonctionnement du retraitement algorithmique peut facilement être contrôlé, à l'instar de tout autre mécanisme déterministe cryptographique. Il y a là une différence majeure avec les générateurs physiques d'aléa pour lesquels il est tout juste possible de contrôler qu'ils ne sont pas dans un état de panne évident au moyen de tests statistiques. En particulier, utiliser des tests statistiques de panne à la sortie du retraitement algorithmique est non seulement inutile mais peut même s'avérer dangereux pour la sécurité. Par ailleurs, il convient d'appliquer les mêmes règles d'implantation aux algorithmes de retraitement que pour tout autre mécanisme cryptographique.

Remarques :

- Par **rafraîchissement** de l'état interne, on entend le calcul d'un nouvel état interne combinant l'ancien état et des données aléatoires externes. (Il ne s'agit donc pas d'une simple réinitialisation.) En cas de source continue d'aléa, le rafraîchissement est souvent combiné à l'avancement.
- Dans le cas où le retraitement utiliserait des clés secrètes, celles-ci sont considérées comme faisant partie de l'état interne, en particulier pour le calcul de sa taille.

2.4.2 Générateur physique d'aléa

Le générateur physique d'aléa est conçu pour générer de l'aléa tout au long de la vie du système. Il importe donc de garantir autant que possible la qualité et la fiabilité de cet aléa.

REGLES ET RECOMMANDATIONS :

RègleArchiGVA-1. Le générateur physique d'aléa doit disposer d'une description fonctionnelle. Celle-ci doit notamment indiquer les principes concourant à la génération de vrai aléa.

RègleArchiGVA-2. Des tests statistiques en sortie du générateur physique ne doivent pas faire apparaître de défauts significatifs dans l'aléa généré.

RecomArchiGVA-1. Il est souhaitable qu'un raisonnement permette de justifier la qualité de l'aléa produit par le générateur physique.

Justifications :

- La conception d'un générateur physique ne repose pas simplement sur la juxtaposition de composants physiques, en espérant que l'assemblage obtenu fournisse un aléa satisfaisant. Une certaine réflexion doit guider le concepteur dans ses choix. Ces choix de conception et la réflexion qui les a guidés doivent donc apparaître dans un document. Il s'agit, entre autres, de décrire les sources physiques utilisées et le traitement appliqué à ces sources.
- Il est souvent recommandé de surveiller la qualité de l'aléa issu d'une source physique au moyen de tests statistiques élémentaires afin de détecter d'éventuels blocages. Ces tests doivent bien entendu être réalisés avant tout retraitement. Il convient également de spécifier très précisément la conduite à tenir en cas de détection de panne par ces tests.
- L'étape suivante, qui est une simple recommandation, est de justifier les choix faits par un raisonnement, qu'il soit heuristique ou rigoureux, qualitatif ou quantifié. La forme et le type de raisonnement sont laissés libres. Son but est de convaincre à la fois les concepteurs et les utilisateurs que le générateur d'aléa produit bien de l'aléa vrai.
- Force est de constater aujourd'hui qu'il est très difficile de fournir une preuve convaincante concernant la qualité de l'aléa issu d'un générateur physique. Il est donc nécessaire de pratiquer des tests statistiques sur un échantillon représentatif issu directement du générateur physique. Ces tests servent de validation a posteriori des choix de conception. On pourra par exemple utiliser les tests préconisés par le **NIST** (**FIPS 140-2** et **SP 800-22**), mais tout test paraissant pertinent peut être utilisé.

Remarque :

- Les tests statistiques concernés par la règle RègleArchiGVA-2 sont des tests d'usine ou des tests ponctuels. Il ne s'agit pas d'éventuels tests de panne pouvant être réalisés en fonctionnement, au cours de l'utilisation du générateur physique.

2.4.3 Retraitement algorithmique

Les propriétés attendues du retraitement algorithmique pour la génération d'aléa sont maintenant énoncées.

REGLES ET RECOMMANDATIONS :

RègleAlgoGDA-1. Les primitives cryptographiques employées par le retraitement algorithmique doivent être conformes au référentiel.

RègleAlgoGDA-2. Dans l'hypothèse où *l'état interne* est fiable, même en cas de défaillance des sources d'aléa présentes, les sorties successives du retraitement doivent être parfaitement aléatoires du point de vue de l'attaquant. De plus, la connaissance de ces sorties ne doit pas mettre en danger la confidentialité des états internes ni des sources d'aléa (fiables).

RègleAlgoGDA-3. En cas de compromission « simple » affectant ou bien l'état interne ou bien les sources d'aléa éventuellement présentes mais n'affectant pas simultanément ces deux types d'éléments, la sortie courante ne doit donner à l'attaquant aucune information exploitable sur les sorties passées.

Justifications :

- Le mécanisme de retraitement employé se doit d'utiliser des primitives cryptographiques (fonction de hachage, chiffrement par bloc...) conformes au référentiel.
- Le but du retraitement est de garantir la qualité cryptographique de l'aléa généré. De plus, comme la détection des pannes physiques est délicate, on souhaite limiter leur impact sur la sécurité du générateur final.

2.5 Gestion de clés

La gestion des clés est un problème à part entière, qui se révèle parfois aussi complexe que la détermination des procédés de chiffrement et d'intégrité. Ce problème est donc traité dans un document qui lui est spécifiquement consacré. Ce document s'intitule « Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques ». Afin de donner un premier aperçu du problème de la gestion des clés, quelques règles sont énoncées dans la suite de cette section. Ces règles ne sont pas exhaustives et le lecteur est invité à se reporter au document spécialisé pour connaître l'étendue des règles régissant la gestion de clés.

Avant de traiter des règles et recommandations relatives à la gestion des clés, rappelons que le recouvrement de clé est un mécanisme à part entière dont le niveau de robustesse doit, à ce titre, être estimé en utilisant les mêmes règles que pour tout autre mécanisme cryptographique. Ce problème est également traité dans le document « Gestion des clés cryptographiques ».

2.5.1 Clés secrètes symétriques

Les deux principaux risques généraux dans l'emploi de clés secrètes sont, d'une part, l'usage d'une clé pour plusieurs emplois (en confidentialité et intégrité par exemple), et d'autre part l'emploi de clés partagées par un nombre important d'utilisateurs ou d'équipements (voir A.5). De telles clés sont désignées par le terme de « **clés communes** » au sens où elles sont détenues par de nombreux acteurs de même niveau hiérarchique au sein d'un système. Ces clés sont également appelées « **clés de réseau** » dans certaines applications.

Les clés communes ne doivent pas être confondues avec les « **clés maîtres »** utilisées afin de générer des « **clés dérivées »**. Dans ce cas, seules les clés dérivées sont présentes dans les produits et pas les clés maîtres ayant permis leur génération. Ceci est à distinguer du cas des « **clés différenciées »** qui sont générées localement à partir d'une même clé secrète pour être utilisées par des mécanismes distincts.

REGLES ET RECOMMANDATIONS :

RègleGestSym-1. L'emploi d'une même clé pour plus d'un usage est exclu[101].

RègleGestSym-2. Les éventuelles clés différenciées utilisées avec un mécanisme conforme au référentiel doivent être générées en utilisant un mécanisme de diversification conforme au référentiel.

RègleGestSym-3. Les éventuelles clés dérivées doivent être générées en utilisant un mécanisme de diversification conforme au référentiel.

[101] Afin de ne pas freiner la mise en place de solutions sécurisées dans les systèmes d'information de l'administration, il est possible que le corps du RGS, ainsi que ses annexes A, définissent des exceptions ponctuelles à cette règle.

RecomGestSym-1. L'emploi de clés communes est déconseillé.

Justifications :

- L'emploi d'une même clé à plus d'un usage, par exemple pour chiffrer avec un mécanisme de confidentialité et assurer l'intégrité avec un mécanisme différent, est source de nombreuses erreurs. Ceci n'interdit cependant pas de différencier localement deux clés à partir d'une même clé secrète, à condition que le mécanisme de diversification soit conforme au référentiel.
- La règle RègleGestSym-3 indique la nécessité de dimensionner le système de manière à ce que les cibles privilégiées d'attaque comme les clés maîtres soient suffisamment protégées.
- L'emploi de clés communes est déconseillé car de telles clés sont des cibles privilégiées d'attaque.

2.5.2 Bi-clés asymétriques

Une infrastructure de gestion de clés est en général construite de manière hiérarchique, chaque clé publique étant certifiée par une clé de rang immédiatement supérieur jusqu'à arriver à une clé racine.

REGLES ET RECOMMANDATIONS :

RègleGestAsym-1. L'emploi d'une même bi-clé à plus d'un usage est exclu[102].

RègleGestAsym-2. Les clés hiérarchiquement importantes, telles que les clés racine, doivent être générées et utilisées par des mécanismes conformes au référentiel.

Justifications :

- L'emploi d'une même bi-clé à plus d'un usage, par exemple pour chiffrer et signer, est une source d'erreurs graves.
- La règle RègleGestAsym-2 indique la nécessité de dimensionner le système de manière à ce que des cibles privilégiées d'attaque comme les clés racine soient suffisamment robustes.

[102] Afin de ne pas freiner la mise en place de solutions sécurisées dans les systèmes d'information de l'administration, il est possible que le corps du RGS, ainsi que ses annexes A, définissent des exceptions ponctuelles à cette règle.

Annexe A Définitions et concepts

L'objet de cette annexe est de rappeler certaines définitions et certains concepts essentiels en cryptographie dans le but de faciliter la compréhension des règles et des recommandations de ce document. Ces rappels couvrent le strict minimum et sont énoncés volontairement de façon non mathématique. Pour plus de détails, on pourra par exemple consulter les ouvrages de référence suivants : [MvV97], [Sti01], [Vau06] et [CFA+06]. On pourra également trouver de nombreux éléments de réponse dans [Ste98] et [Sch01]. Une approche plus historique est présentée dans [Sin99].

Des compléments permettant de préciser certaines notions mais pouvant être passés en première lecture sont proposés en petits caractères, dans le style de ce paragraphe.

La **cryptologie**, discipline à la frontière entre mathématiques et informatique, est traditionnellement définie comme la « science du secret «. Longtemps concentrée sur la problématique de la confidentialité, à des fins essentiellement militaires ou diplomatiques, la cryptologie a bénéficié d'un essor scientifique important suite au développement de la société de l'information jusqu'à devenir un outil incontournable pour sécuriser les systèmes d'information.

La cryptologie traite de la conception, de la sécurité et de l'emploi de mécanismes cryptographiques, le terme générique de **mécanisme** englobant ici à la fois les **primitives** (fonction de hachage, chiffrement par bloc. . .), les **modes opératoires** et les **protocoles** cryptographiques.

On divise traditionnellement la cryptologie en deux branches selon que l'on se place du point de vue du concepteur ou de celui de l'attaquant. La **cryptographie** étudie la conception de mécanismes permettant d'assurer des propriétés de sécurité variées comme la confidentialité, l'intégrité ou l'authenticité de l'information. La **cryptanalyse** s'intéresse à ces mêmes primitives en tentant d'analyser leur sécurité, voire de la mettre en défaut. Il va de soi qu'il n'y a pas de cryptographie sans cryptanalyse et inversement.

Par ailleurs, sur un plan technique, on distingue habituellement la cryptographie **symétrique**, encore qualifiée de **conventionnelle** ou de cryptographie à **clé secrète**, de la cryptographie **asymétrique**, ou encore cryptographie à **clé publique**. Cette séparation est issue de l'article fondateur de W. Diffie et M. Hellman [DH76] qui, en 1976, a donné naissance à la cryptographie asymétrique en suggérant que pour chiffrer un message à l'attention d'un destinataire donné il n'est pas nécessaire de partager au préalable un secret avec lui. Dans la suite de ce chapitre, les primitives symétriques et asymétriques sont abordées de manière séparée.

Une seconde dimension de classification des primitives cryptographiques concerne l'objectif de sécurité visé. Traditionnellement on distingue les besoins de confidentialité et/ou d'intégrité des données, d'authentification de données ou d'entités ainsi que les besoins de non-répudiation. D'autres fonctions sont bien entendues envisageables mais celles qui viennent d'être citées sont, de loin, les principales traitées par des moyens cryptographiques.

Le but de la **confidentialité** est de s'assurer que des informations transmises ou stockées ne sont accessibles qu'aux personnes autorisées à en prendre connaissance. Cet objectif de sécurité est classiquement assuré par le chiffrement mais peut bien entendu également l'être par tout autre moyen approprié, à commencer par des mesures organisationnelles non cryptographiques.

Assurer l'**intégrité** de données consiste à empêcher, ou tout du moins à détecter, toute altération non autorisée de données. Par altération, on entend toute modification, suppression partielle ou insertion d'information. L'intégrité des données est classiquement assurée en cryptographie par des codes d'authentification de message ou des mécanismes de signature numérique.

L'authentification de données vise à s'assurer qu'elles proviennent bien d'un interlocuteur particulier. Une

telle authentification implique l'intégrité de ces informations et est assurée par les mécanismes cités ci-dessus. **L'authentification d'entités**, encore désignée sous le terme **d'identification,** vise pour sa part à s'assurer qu'un correspondant est bien celui qu'il prétend être. Elle peut être réalisée de diverses manières, symétriques ou asymétriques.

La **non-répudiation** est un service visant à éviter qu'une entité puisse nier avoir effectué une certaine action. Le principal mécanisme de non-répudiation est la signature à clé publique, une signature sur un message devant en général rester valide, même si le signataire change ensuite d'avis.

Les principales primitives offertes par la cryptographie moderne peuvent maintenant être abordées. Le tableau 1 permet de les répartir en fonction de leur nature symétrique ou asymétrique et de leur objectif de sécurité. Bien entendu, d'autres primitives très intéressantes peuvent être citées mais elles ne s'inscrivent pas naturellement dans un tel tableau. La suite de ce chapitre décrit sommairement ces primitives et rappelle les points essentiels, nécessaires à la compréhension du reste de ce document.

TABLE 1 – Primitives cryptographiques offrant un service donné

<table>
<tr><th colspan="2">Service</th><th>Cryptographie symétrique</th><th>Cryptographie asymétrique</th></tr>
<tr><td colspan="2" rowspan="2">Confidentialité</td><td rowspan="2">Chiffrement conventionnel par bloc (A.1.1.1)
ou par flot (A.1.1.2)</td><td>Chiffrement à clé publique (A.2.1)</td></tr>
<tr><td>Échange de clé (A.2.3)</td></tr>
<tr><td colspan="2">Intégrité</td><td rowspan="2">Code d'authentification de message (A.1.3)</td><td rowspan="4">Signature numérique (A.2.2)</td></tr>
<tr><td rowspan="2">Authentification</td><td>de données</td></tr>
<tr><td>d'entités</td><td>Défi-réponse (A.1.4)</td></tr>
<tr><td colspan="2">Non-répudiation</td><td>Aucune primitive</td></tr>
</table>

A.1 Cryptographie symétrique

Les primitives cryptographiques symétriques se caractérisent par le fait qu'elles utilisent des clés cryptographiques partagées par plusieurs personnes ou entités. Une **clé secrète symétrique** est donc simplement un élément secret. La sécurité d'un système utilisant de telles clés repose donc notamment sur la protection de ces secrets.

Une clé secrète est généralement une suite quelconque de bits, c'est-à-dire de 0 et de 1, de taille fixée. Cette taille de clé, notée n ci-après, est déterminante pour la sécurité du système car on peut former exactement 2^n clés de longueur n. Les systèmes symétriques sont en général susceptibles d'être attaqués de manière générique au moyen d'une énumération de toutes les clés possibles. Une telle attaque, dite par « recherche exhaustive «, ne peut cependant aboutir que si le nombre de calculs est réalisable par des moyens informatiques raisonnables. La capacité à effectuer 2^n opérations fournit donc une borne inférieure au dimensionnement des systèmes symétriques.

Afin de fixer les idées sur les ordres de grandeur manipulés, et surtout de bien prendre conscience que 2^n est un nombre très rapidement gigantesque lorsque n croît, quelques exemples numériques concrets sont rassemblés dans le tableau 2.

Ces chiffres montrent simplement que la fonction 2^n croît extrêmement rapidement avec n. La capacité, même en disposant de moyens très importants, de réaliser de l'ordre de 2^{128} calculs apparaît donc très peu plausible de nos jours. Pour ceux qui ont encore des doutes, il apparaît en tout état de cause qu'effectuer 2^{256} calculs est parfaitement impossible et ne le sera jamais. C'est une des rares certitudes que l'on peut avoir en

cryptographie. Ceci va en particulier à l'encontre de l'idée reçue selon laquelle tout cryptosystème peut nécessairement être cassé par recherche exhaustive à condition d'y mettre les moyens.

n	2^n	Ordre de grandeur
32	2^{32}	Nombre d'hommes sur Terre
46	2^{46}	Distance Terre–Soleil en millimètres
46	2^{46}	Nombre d'opérations effectuées en une journée à raison d'un milliard d'opérations par seconde (1GHz)
55	2^{55}	Nombre d'opérations effectuées en une année à raison d'un milliard d'opérations par seconde (1GHz)
82	2^{82}	Masse de la Terre en kilogrammes
90	2^{90}	Nombre d'opérations effectuées en 15 milliards d'années (âge de l'univers) à raison d'un milliard d'opérations par seconde (1GHz)
155	2^{155}	Nombre de molécules d'eau sur Terre
256	2^{256}	Nombre d'électrons dans l'univers

TABLE 2 – Ordre de grandeur de la valeur de 2n

A.1.1 Chiffrement symétrique

Les primitives symétriques les plus connues sont les algorithmes de chiffrement. Ceux-ci permettent, au moyen de clés secrètes connues des seuls émetteurs et récepteurs d'informations, de protéger la confidentialité de ces dernières, même si le canal de communication employé est écouté. Il doit cependant être d'ores et déjà bien clair que ceci laisse ouvert le problème majeur de l'échange initial de la clé secrète entre les correspondants.

Il faut noter que le seul terme admis en français est celui de chiffrement. On entend cependant souvent parler de « cryptage « qui est un anglicisme, voire de « chiffrage », mais ces mots sont incorrects. L'opération inverse du chiffrement est le déchiffrement. On désigne par « décryptage », ou « décryptement », l'opération qui consiste à retrouver le clair correspondant à un chiffré donné sans connaître la clé secrète, après avoir trouvé une faille dans l'algorithme de chiffrement.

Les algorithmes de chiffrement symétrique permettent également de sécuriser le stockage d'informations, sans intention de les transmettre. On peut ainsi protéger la confidentialité d'informations enregistrées sur des supports potentiellement vulnérables.

La protection en confidentialité d'informations permet cependant uniquement de s'assurer que le contenu de ces informations est inaccessible à un attaquant. Par contre, nulle garantie d'intégrité ou d'authenticité n'est

a priori fournie par les méthodes de chiffrement et rien ne permet d'exclure des possibilités d'attaques actives visant à modifier les informations transmises ou stockées. On peut ainsi facilement concevoir des scénarios d'attaques au cours desquels un attaquant peut modifier des communications protégées en confidentialité sans avoir à comprendre précisément ce qui est transmis. Un exemple de cette attaque est détaillé en section A.1.1.2.

Les méthodes de chiffrement symétrique, encore appelé chiffrement conventionnel ou chiffrement à clé secrète, se divisent naturellement en deux familles, le **chiffrement par bloc** (« block cipher ») et le **chiffrement par flot** (« stream cipher »), décrites ci-dessous.

A.1.1.1 Chiffrement par bloc

Une primitive de chiffrement par bloc est un algorithme traitant les données à chiffrer par blocs de taille fixée. On notera *k* le nombre de bits de ces blocs de données ; typiquement, cette taille vaut 64 ou 128 bits en pratique. Un tel mécanisme permet donc uniquement de combiner une suite de *k* bits de données avec une clé de *n* bits afin d'obtenir un bloc de données chiffrées de même taille *k* que le bloc de données claires.

L'une des principales propriétés attendues d'un mécanisme de chiffrement par bloc est d'être facilement inversible si l'on dispose de la clé secrète de chiffrement. On veut également que, sans informations sur la clé secrète, il soit impossible en pratique de retrouver de l'information sur le message d'origine. Seuls les détenteurs de la clé secrète doivent être capables de transformer des données claires en données chiffrées et, inversement, des données chiffrées en données claires.

L'un des exemples les plus connus d'algorithme de chiffrement par bloc est le **DES** (Data Encryption Standard) défini en 1977 par le NIST, institut de normalisation américain, comme standard de chiffrement à usage commercial. Il traite des blocs de k = 64 bits au moyen de clés de *n* = 56 bits. La sécurité du **DES** a fait couler depuis lors beaucoup d'encre. Cet algorithme peut cependant être considéré comme particulièrement bien conçu, la meilleure attaque pratique connue étant la recherche exhaustive sur les clés. La taille de ces clés est cependant sous-dimensionnée, ce qui rend aujourd'hui cette attaque réalisable, au moyen d'une machine dédiée, en quelques heures seulement.

On utilise cependant toujours couramment le **DES** mais sous la forme du « triple **DES** », une variante utilisant des clés de 112 bits, inattaquable par recherche exhaustive. L'objectif à moyen terme est cependant de le remplacer par l'**AES** (Advanced Encryption Standard), sélectionné par le NIST au terme d'une compétition internationale. L'**AES** est conçu pour traiter des blocs de 128 bits au moyen de clés de 128, 192 ou 256 bits.

Plus généralement, un algorithme de chiffrement par bloc combine des opérations de **substitution**, visant à remplacer des symboles par d'autres afin d'en cacher le sens, avec des opérations de **permutation** échangeant la position des symboles. Ces deux principes sont historiquement très anciens mais demeurent encore valables aujourd'hui, toute primitive de chiffrement par bloc pouvant être vue comme une combinaison intelligente de ces deux opérations.

À ce niveau, il convient de comprendre précisément ce que permet de faire un algorithme de chiffrement par bloc, et surtout ce qu'il ne permet pas. Tout d'abord, un tel algorithme permet uniquement de traiter des blocs de taille fixe, relativement petite. Par conséquent, afin de chiffrer des messages de taille quelconque, il convient de définir comment le message doit être codé en une suite de blocs de taille fixe. Ceci implique de définir très précisément comment répartir l'information de tels messages en une suite de bits de longueur exactement un multiple de la taille *k* du bloc élémentaire. On appelle cette opération le « padding » ou le « bourrage ».

De plus, un algorithme de chiffrement par bloc est fondamentalement déterministe : à partir d'un bloc de

données et d'une clé secrète, il produit toujours le même bloc de chiffré. Ainsi, un attaquant passif observant deux blocs de chiffré identiques peut immédiatement en déduire que les blocs de message clair correspondants sont identiques, sans pour autant apprendre la moindre information sur ce clair. Dans certaines circonstances, une telle information est cependant suffisante pour attaquer un système.

À titre d'exemple, imaginons un système bancaire où, afin de vérifier la validité d'un **PIN** code (« Personal Identification Number ») à quatre chiffres de carte de crédit, ce code est chiffré et envoyé à un central bancaire. Si l'on utilise un simple chiffrement par bloc avec une clé bancaire fixe, à chaque **PIN** code va correspondre un unique chiffré. On peut dès lors imaginer par exemple qu'un attaquant observant les communications apprendra immédiatement qui a le même **PIN** code que lui.

Afin de traiter des messages de taille quelconque et d'assurer la confidentialité globale de ces messages, et pas uniquement une confidentialité « par bloc «, il convient donc de définir un **mode opératoire** précisant comment convertir le message en une suite de blocs ainsi que le mode de chiffrement de ces blocs afin d'obtenir finalement le message chiffré. Notons que la définition d'un tel mode opératoire n'a nul besoin de tenir compte des détails de l'algorithme de chiffrement par bloc employé ; seule la taille *k* des blocs est réellement nécessaire. Notons encore qu'afin de rompre le caractère déterministe du chiffrement, il est nécessaire de « randomiser » le processus, c'est-à-dire d'introduire une valeur aléatoire.

Le mode opératoire le plus connu est le **CBC** (« cipher-block chaining »). Une des nombreuses variantes fonctionne de la manière suivante : afin de chiffrer un message formé d'une suite de bits, on commence par ajouter à droite un bit valant 1 et autant de 0 que nécessaire afin d'obtenir un nombre total de bits multiple de la taille du bloc. Notons $x_1, x_2, \ldots, xt$ les *t* blocs de message clair ainsi obtenus. On choisit ensuite un bloc aléatoire, noté **IV** pour « initial vector «, indépendant du message et des précédents chiffrements. Si l'on note **E***K*(*x*) le résultat du chiffrement du bloc x avec la clé K, le chiffré (« $c_0, c_1, c_2, \ldots, ct$) du message est obtenu en posant c_0 = IV et en calculant successivement c*i* = E*K*(c_i-1 ⊕ x_i) pour *i* allant de 1 à *t* (l'opérateur « ou-exclusif » noté « ⊕ » représente l'addition bit à bit, sans retenue). Graphiquement, on obtient la représentation symbolique de la figure 3.

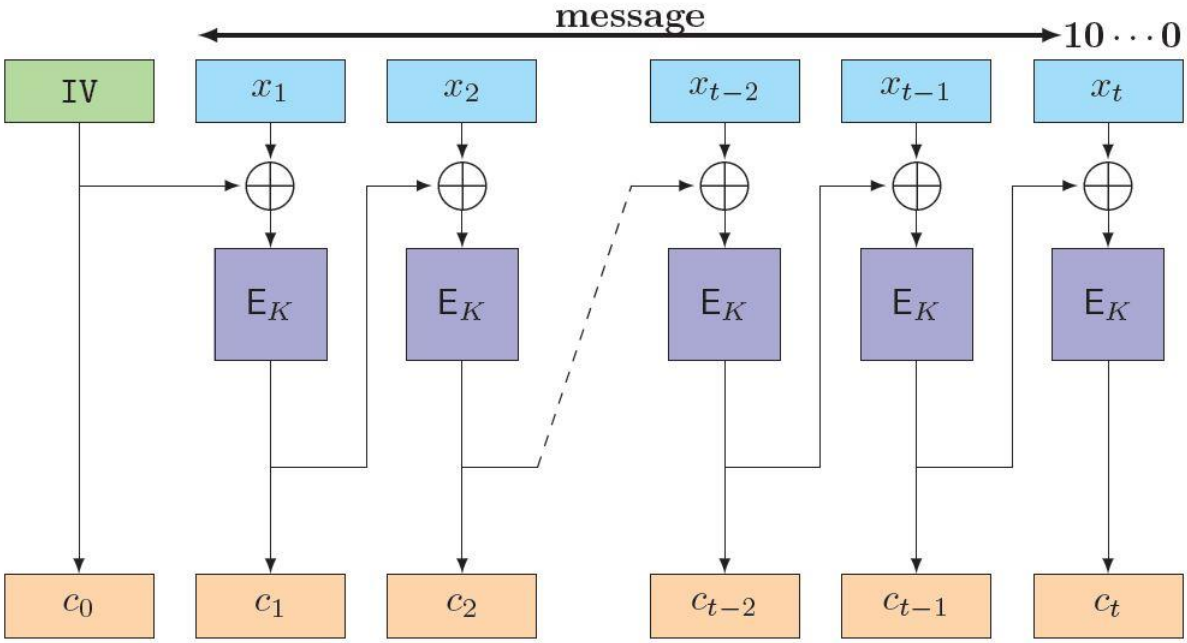


FIGURE 3 – Mode opératoire CBC

Cet exemple de mode opératoire illustre la phase initiale de padding, consistant à compléter le message par un bit valant 1 suivi de bits nuls. Il montre également que l'emploi de données aléatoires, via l'**IV**, permet de rendre le chiffrement non déterministe. Ainsi, le chiffrement du même message deux fois de suite n'a qu'une chance infime d'utiliser le même **IV** et par conséquent l'ensemble du chiffré va différer à cause du mécanisme de rebouclage faisant intervenir le bloc de chiffré ci - 1 lors du chiffrement du bloc de message clair xi. Notons encore que dans cette variante du mode **CBC**, l'**IV** est transmis en clair, sans avoir besoin d'être chiffré.

Afin de déchiffrer un message (c_0,c_1,c_2,...,c_t), il suffit de calculer xi = c_{i-1} $\oplus$ $\mathbf{D}_K(c_i)$ pour i allant de 1 à t, $\mathbf{D}_K(c)$ désignant le déchiffré du bloc c avec la clé secrète **K**. Il est facile de vérifier que le message ainsi obtenu est bien le message initial. Notons enfin que ce mode a naturellement une propriété d'auto-synchronisation; si des blocs de chiffré sont perdus en cours de transmission, il suffit d'obtenir deux blocs successifs intacts afin de pouvoir reprendre correctement le déchiffrement.

A.1.1.2 Chiffrement par flot

Les primitives de chiffrement par flot utilisent une approche différente du chiffrement par bloc au sens où elles considèrent généralement le message à chiffrer comme une suite de bits qui sont combinés de manière simple (généralement un « ou-exclusif bit à bit ») avec une séquence de bits dérivée de la clé secrète (et dans la plupart des cas également d'un vecteur d'initialisation).

Les algorithmes de chiffrement par flot s'inspirent du chiffrement de Vernam qui est à la fois très simple, très sûr et inutilisable en pratique. Si l'on considère un message représenté sous la forme d'une suite de bits m_1, m_2, m_3, ... ainsi qu'une clé également vue comme une suite de bits k_1, k_2, k_3, . .., le chiffré du message est alors très simplement obtenu au moyen de l'opération de « ou-exclusif bit à bit « (appelée le **XOR**), où le i-ème bit de chiffré ci s'obtient par addition (sans retenue) du i-ème bit de message avec le i-ème bit de clé, soit $c_i = m_i \oplus k_i$. Ainsi $0 \oplus 0 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$ et $1 \oplus 1 = 0$, le dernier cas étant le seul où l'opération **XOR** diffère de l'addition classique.

Afin de déchiffrer, il suffit d'appliquer la même opération de ou-exclusif bit à bit du chiffré avec la clé secrète car $c_i \oplus k_i = (m_i \oplus k_i) \oplus k_i = m_i \oplus (k_i \oplus k_i) = m_i \oplus 0 = m_i$, en remarquant que, quelle que soit la valeur k_i de chaque bit de clé, $k_i \oplus k_i$ vaut toujours 0.

Il est facile de démontrer que le chiffrement de Vernam est parfaitement sûr, en termes de confidentialité, si la clé est au moins de même taille que le message à chiffrer et n'est utilisée qu'une seule fois. Ceci restreint évidemment considérablement les applications envisageables à cause de la taille de la clé à partager entre émetteur et destinataire ; dans la plupart des cas, cette mise en accord de clé secrète pose un problème similaire à la transmission sécurisée du message lui-même.

Claude Shannon a démontré en 1949 l'impossibilité de réaliser des primitives cryptographiques parfaites reposant sur des clés de taille strictement inférieure à celle du message à chiffrer et par conséquent l'impossibilité de réaliser des primitives parfaites utilisables en pratique. L'approche moderne ne viole pas cette idée mais admet une sécurité imparfaite ; tout l'art du cryptographe est d'estimer ce degré d'imperfection et de concevoir des primitives pour lesquelles il peut être rendu négligeable. On ne cherche donc pas à se protéger contre un adversaire disposant d'une puissance de calcul infinie mais plutôt d'une puissance de calcul pour laquelle on sait estimer une borne supérieure.

L'idée maîtresse du chiffrement par flot est d'utiliser des clés de petite taille, typiquement de l'ordre de 128 bits, et d'en dériver de manière déterministe, et par conséquent parfaitement reproductible, des suites d'allure

aléatoire pouvant être utilisées comme des clés de même longueur que le message avec l'algorithme de chiffrement de Vernam[103]. Le déchiffrement agit ensuite de même, en générant la même suite à partir de la clé secrète.

En écho à la mise en garde de l'introduction de la section A.1.1, le chiffrement par flot dérivé de l'algorithme de Vernam fournit un exemple simple et particulièrement éloquent du fait qu'assurer la confidentialité, même de manière parfaite, n'entraîne pas automatiquement une protection en intégrité du message transmis. En effet, si un attaquant désire inverser un bit de message clair, c'est-à-dire transformer un 0 en 1 ou inversement, il lui suffit d'ajouter 1 au bit de chiffré ci et donc de transmettre $c'_i = c_i \oplus 1$. Lors du déchiffrement, le destinataire va calculer $c'_i \oplus k_i = c_i \oplus 1 \oplus k_i = m_i \oplus 1$; si m_i vaut 0 le résultat obtenu est un 1 et, inversement, si m_i vaut 1 le résultat est $1 \oplus 1 = 0$. Par conséquent, même si l'attaquant n'a aucune idée de la valeur du bit modifié, il peut à coup sûr et sans effort l'inverser. À titre d'exemple d'application, on peut par exemple imaginer le chiffrement du montant d'une transaction financière ; le positionnement du montant à payer dans le message se situe en général à une position fixe, facile à connaître. On peut alors inverser un bit de cette somme et ainsi facilement transformer un faible montant en une somme très importante, comme si l'on transformait, en notation décimale, 0000017 euro en 1000017 euro.

La confusion classique entre confidentialité et intégrité est souvent renforcée par des images un peu trop simplistes du mécanisme d'action des primitives cryptographiques. On présente ainsi souvent le chiffrement comme la version électronique d'une enveloppe opaque ou, pire, d'un coffre-fort. Comme on imagine mal pouvoir modifier des informations contenues dans un coffre sans pouvoir en prendre connaissance, on peut à tort s'imaginer que le chiffrement protège totalement les données, tant en confidentialité qu'en intégrité. L'exemple précédent montre cependant qu'employé seul, le chiffrement peut se révéler parfaitement inefficace face à certaines menaces. Si l'on désire réaliser des « coffres-forts numériques «, il faut donc au minimum, en plus de la confidentialité, assurer l'intégrité des données. Ceci peut se faire en combinant deux mécanismes séparés ou bien au moyen d'un mécanisme conçu pour assurer simultanément la confidentialité et l'intégrité. Une telle mise en place de mécanisme doit cependant être réalisée avec le plus grand soin.

On parle de chiffrement par flot **synchrone** lorsque la suite chiffrante est calculée à partir de la clé secrète, indépendamment du message à chiffrer. Inversement, les algorithmes de chiffrement par flot **asynchrones**, ou **auto-synchronisants** utilisent des suites chiffrantes dépendant de la clé secrète mais également d'un certain nombre de bits de texte chiffré. L'intérêt avancé pour une telle approche est de permettre une sorte de resynchronisation automatique du déchiffrement, même si des portions de message chiffré sont perdues lors de la transmission.

Notons qu'une telle propriété tient plus de la correction d'erreurs de transmission que d'une quelconque protection de nature cryptographique des données. On peut dès lors s'interroger sur l'adéquation de telles techniques ainsi que sur la menace réelle qu'elle vise à éviter. Notons également que certains modes opératoires de chiffrement par bloc, tel que le mode **CBC** vu précédemment, possèdent aussi cette propriété d'auto-synchronisation à condition que des blocs entiers soient perdus.

[103] Plus précisément, cette approche conduit à une classe particulière d'algorithmes de chiffrement par flot appelés « binary additive stream ciphers ».

A.1.2 Sécurité du chiffrement

Au-delà de la description des primitives de chiffrement, il convient de définir précisément ce que l'on attend comme propriétés de sécurité de leur part. L'idée intuitive selon laquelle aucune information sur le message clair ne doit pouvoir être déduite du chiffré par un attaquant est délicate à définir précisément et nécessite beaucoup de soin. La cryptographie moderne a cependant développé des **modèles de sécurité** très précis afin d'expliciter sans ambiguïté ce que l'on attend des primitives de chiffrement.

Afin de préciser la difficulté d'une définition précise de ce que l'on attend du chiffrement, reprenons l'exemple de la randomisation vue section A.1.1.1. Une propriété naturellement attendue d'un algorithme de chiffrement est d'être non-inversible par quelqu'un qui ne dispose pas de la clé secrète. En l'absence de toute attaque connue, cette propriété semble vérifiée par l'**AES** ou le triple **DES**. Il a cependant déjà été remarqué qu'un chiffrement déterministe (c'est le cas de l'**AES** ou du triple **DES**), aussi bon soit-il, entraîne que deux chiffrements du même message génèrent des chiffrés identiques et qu'une part d'information est ainsi dévoilée. La propriété de non-inversibilité est donc insuffisante et doit être raffinée.

L'idée selon laquelle la connaissance de messages chiffrés ne doit révéler aucune information sur les messages clairs associés est classiquement formalisée par la notion de « sécurité sémantique ». Une telle définition est complexe mais peut se résumer à l'intuition suivante : si un mécanisme de chiffrement est tel qu'en proposant deux messages différents de son choix (mais de même taille), notés M_0 et M_1, et en obtenant le chiffré C de l'un des deux, on est incapable de savoir lequel des deux messages a été chiffré, ceci signifie que la vue d'un chiffré ne contient aucune information exploitable sur le clair associé, quels que soient les messages traités.

Il est de plus possible de renforcer encore ce modèle en tenant compte de capacités éventuellement très évoluées d'un attaquant. On peut par exemple reprendre l'expérience précédente en permettant à celui qui propose les deux messages M_0 et M_1 d'obtenir en plus le chiffré de n'importe quel autre message de son choix ainsi que le déchiffré de n'importe quel chiffré, évidemment différent de C. S'il est encore impossible de deviner si C est le chiffré de M_0 ou M_1, il est clair que le mécanisme de chiffrement sera résistant dans un grand nombre de scénarios d'attaque.

Les modèles de sécurité les plus forts sont obtenus par la combinaison d'un objectif de sécurité exigeant (par exemple la sécurité sémantique) et d'un attaquant disposant de ressources puissantes (par exemple, des oracles de chiffrement et/ou de déchiffrement). Ces modèles offrent donc les meilleures garanties. Le niveau de sécurité le plus élevé correspond au modèle de « l'indistinguabilité face aux attaques à chiffrés choisis adaptatives », désigné par l'acronyme **IND-CCA2**.

Les modèles de sécurité utilisés en cryptographie moderne peuvent parfois paraître trop généreux pour les attaquants, mais ils sont justifiés par le fait que dans certaines circonstances, les attaquants contre lesquels on veut se prémunir ont une grande marge de manœuvre. Évaluer la sécurité d'une primitive dans de tels modèles de sécurité permet également de minimiser les risques de faille de sécurité lors de leur composition[104] avec d'autres mécanismes afin de concevoir des systèmes complets. De plus, utiliser des primitives sûres face à des attaquants très puissants est un important gage de qualité. Enfin, la cryptographie moderne propose des primitives permettant d'atteindre de tels niveaux de sécurité sans réduire fortement les

[104] C'est-à-dire utilisation conjointe.

performances ; il serait par conséquent dommage de se priver de l'emploi de ces mécanismes.

A.1.3 Authentification et intégrité de messages

Des techniques cryptographiques symétriques permettent également de garantir l'intégrité de données transmises, qu'elles soient déjà protégées en confidentialité ou non. De tels mécanismes visent à garantir qu'aucune altération des données n'a eu lieu au cours de leur transmission. L'inadéquation des mécanismes de chiffrement pour garantir une telle intégrité des données a déjà été mentionnée. Notons par ailleurs que les méthodes cryptographiques visent en général à se prémunir face à des attaques volontaires, potentiellement intelligentes, par opposition aux techniques de codage et aux protocoles de transmission visant à détecter ou à corriger des erreurs aléatoires et involontaires.

Plus précisément, la principale technique permettant d'assurer l'intégrité des données consiste à calculer un **code d'authentification de message** (souvent appelé **MAC** pour « message authentication code ») à partir des données à protéger et d'une clé secrète partagée avec celui à qui le message est destiné. Ce code d'authentification, typiquement long de 128 bits, est ensuite ajouté au message et transmis. Après réception, le code d'authentification est recalculé à l'aide de la clé secrète et du message reçu, potentiellement corrompu. Le résultat obtenu est comparé au **MAC** reçu; s'ils sont identiques, il est extrêmement probable que les données sont intègres et proviennent donc de la bonne personne.

Il faut insister sur la différence conceptuelle fondamentale existant entre chiffrement et calcul de code d'authentification de message. Par contre, à un niveau plus technique, de nombreuses similarités peuvent réapparaître. L'algorithme le plus connu de calcul de **MAC** est le **CBC-MAC**. Le code d'authentification est alors simplement calculé en appliquant le mode de chiffrement **CBC** (décrit figure 3) au message, sans utiliser de vecteur d'initialisation (**IV**), et en ne conservant comme valeur de **MAC** que le dernier bloc de chiffré, surchiffré avec une clé *K*', différente de celle utilisée dans la chaîne **CBC**. Graphiquement, on obtient la représentation symbolique de la figure 4. On voit clairement que toute modification, même minime, du message à protéger engendre un résultat totalement différent comme **MAC**. Il faut cependant se garder de penser qu'un tel mécanisme est sûr, dans un sens général, sur cette simple impression initiale, car une telle analyse ne constitue pas une preuve de sécurité.

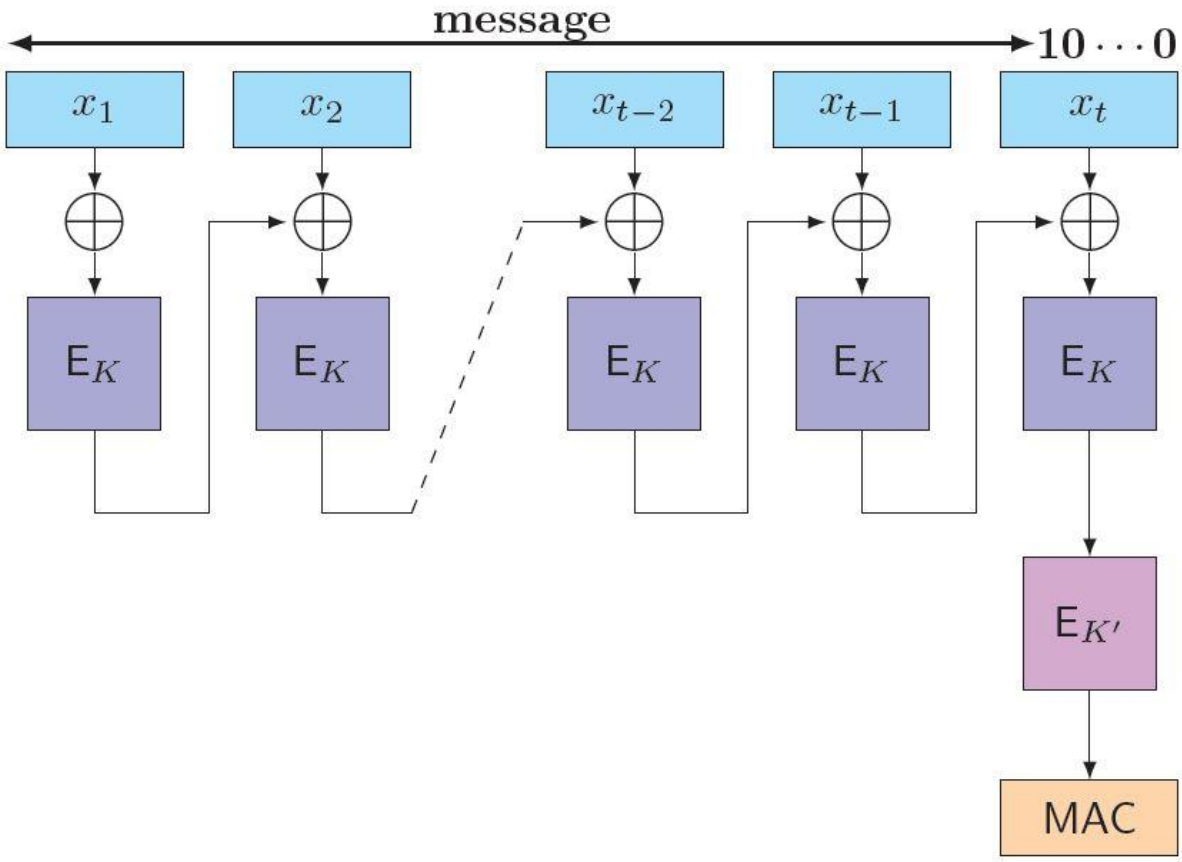


FIGURE4 – Mode opératoire CBC-MAC

La protection de l'intégrité d'un message garantit également, vis-à-vis du destinataire, son authenticité car la connaissance de la clé secrète est nécessaire pour générer des **MAC** corrects. Par contre, cette authentification n'a pas de valeur vis-à-vis d'un tiers car rien ne permet de savoir par quel détenteur de la clé secrète un **MAC** est réellement généré. De plus, toute vérification par un tiers nécessite de lui révéler la clé secrète utilisée. Ceci est intrinsèquement lié à la nature symétrique du mécanisme.

On désigne parfois les codes d'authentification de message sous le terme de **signature symétrique** mais il doit être bien entendu que ce qualificatif de signature est impropre pour la simple raison que la propriété de non-répudiation n'est pas assurée. Actuellement, seuls les mécanismes asymétriques, qui évitent justement que la connaissance de la clé secrète ne soit nécessaire pour vérifier la validité d'une signature, peuvent réellement rendre de tels services de sécurité.

Notons enfin qu'un code d'authentification de message valide ne permet que de garantir l'authenticité de ce message. Si l'on souhaite assurer l'intégrité et l'authenticité d'un ensemble de messages formant une communication, et éviter par exemple le rejeu ou la suppression de certains messages accompagnés de **MAC**s valides, il convient de soigner les méthodes de chaînage employées.

A.1.4 Authentification d'entités

À partir des primitives de chiffrement et de calcul de **MAC** qui viennent d'être décrites, il est facile de dériver des mécanismes permettant d'authentifier des entités, ce terme étant pris au sens large. La principale différence entre l'authentification d'entités et celle de messages est le caractère **interactif** de la première

alors que la seconde doit pouvoir être effectuée en une seule transmission, comme par exemple dans des applications de messagerie sécurisée.

La méthode symétrique la plus utilisée afin de s'assurer de l'identité d'un correspondant est de partager avec lui une clé secrète. Afin de s'assurer ensuite que quelqu'un se présentant sous son identité est bien la bonne personne, l'authentification va consister à s'assurer que ce dernier possède bien la clé secrète. La technique la plus simple, s'apparentant directement aux techniques de mot de passe, consiste à transmettre le secret. Les inconvénients sont cependant multiples, à commencer par le risque qu'un simple attaquant passif intercepte le secret et l'utilise ensuite. Par conséquent, une bien meilleure méthode est celle dite par « challenge-response », que l'on peut traduire par « question-réponse » ou « défi-réponse ». L'idée est d'envoyer à celui que l'on souhaite authentifier un message quelconque, de lui demander de le chiffrer en utilisant la clé secrète partagée, puis de renvoyer le résultat obtenu. Si la réponse reçue se déchiffre correctement et aboutit à la question posée, il y a une forte probabilité pour que la personne qui a calculé le chiffré possède effectivement la clé secrète et, par conséquent, qu'elle soit la personne qu'elle prétend être. Notons cependant que ceci n'est vrai que si aucune question déjà posée n'est réutilisée lors des authentifications suivantes.

Le problème de la non-réutilisation des questions est très sensible mais peut facilement être résolu si l'on dispose d'une source de données aléatoires, sans avoir à mémoriser les questions déjà posées. En effet, il est possible de calculer la probabilité qu'une même question de n bits soit obtenue deux fois si les questions sont tirées au hasard. Par application du fameux « paradoxe des anniversaires », on montre que la première collision apparaît en moyenne après environ $2^{n/2}$ tirages. Par conséquent, si le nombre maximal d'authentifications avec une même clé est nettement inférieur à $2^{n/2}$, l'emploi de challenges aléatoires de n bits est suffisant, le risque de poser deux fois la même question étant négligeable. À titre d'application, des questions de 64 bits sont parfaitement adaptées jusqu'à plusieurs millions d'authentifications et des challenges de 128 bits potentiellement utilisables sans limite atteignable en pratique.

Le problème majeur de telles authentifications symétriques réside, comme dans le cas du chiffrement et de l'intégrité de messages, dans la nécessité de partager une clé secrète entre personne identifiante et personne identifiée. Ceci implique de plus l'impossibilité de distinguer ces deux personnes. On peut ainsi se demander s'il est vraiment nécessaire que celui qui vérifie l'identité connaisse nécessairement le secret associé à l'identité d'un individu. Une fois de plus, la réponse à ce problème est apportée par la cryptographie asymétrique dont les bases vont maintenant être décrites.

A.2 Cryptographie asymétrique

L'idée majeure de la cryptographie asymétrique est que les opérations publiques (le chiffrement, la vérification de signature. . .) n'ont pas nécessairement besoin d'utiliser les mêmes clés que les opérations privées (le déchiffrement, la signature. . .). Ainsi, la cryptographie asymétrique, telle que décrite par W. Diffie et M. Hellman [DH76], utilise des « clés privées », que seul un utilisateur possède et peut utiliser pour les opérations privées, et des « clés publiques », que tout le monde connaît et peut utiliser pour les opérations publiques. Les clés publiques et privées sont reliées par des équations mathématiques, ces équations étant la base de problèmes que l'on croit difficiles à résoudre. Pour illustrer la notion de difficulté en pratique, une image simple est la suivante : à partir d'un pot de peinture jaune et d'un pot de peinture bleue, il est facile par simple mélange d'obtenir un pot de peinture verte. Par contre, l'opération inverse consistant à séparer les pigments jaunes des pigments bleus, sans être théoriquement infaisable, l'est en pratique. Dans cet exemple, le vert fait office d'élément public, et le bleu et le jaune sont privés : tout le monde sait que le but est de diviser le vert en bleu et jaune pour retrouver la clé privée, mais l'opération est considérée comme très difficile. De même, dans le monde mathématique, il existe de telles opérations inversibles mais asymétriques

dans leur difficulté. On les appelle souvent problèmes difficiles ou asymétriques.

La plus connue de ces opérations asymétriques est la multiplication de grands nombres premiers[105]. L'opération inverse, consistant à retrouver ces nombres à partir du résultat, est appelée factorisation ou encore décomposition en produit de facteurs premiers. Choisir deux nombres premiers de taille fixée et les multiplier est une opération facile mais, dès que la taille des entiers manipulés est suffisamment grande, aucune méthode efficace permettant de retrouver ces facteurs premiers à partir de la simple valeur de leur produit n'est connue à ce jour. Insistons sur le fait qu'une telle factorisation n'est pas impossible ; elle est mathématiquement parfaitement définie et l'on connaît des algorithmes fort simples permettant de la retrouver. Le problème réside dans la complexité temporelle, c'est-à-dire dans le temps de calcul nécessaire à ces méthodes pour trouver le résultat. De plus, rien ne permet de dire qu'il n'existe pas de méthode efficace. On peut tout juste affirmer qu'aucune méthode efficace de factorisation utilisant une technologie disponible n'a été rendue publique à ce jour.

Parmi les problèmes asymétriques, comme celui de la factorisation, on distingue les problèmes asymétriques dits « à trappe ». Ils se fondent sur une opération facile à réaliser mais difficile à inverser à moins de disposer d'un élément supplémentaire appelé la « trappe ». L'exemple le plus connu, mais également le plus utilisé dans les produits actuels, est l'opération sur laquelle repose le fameux cryptosystème **RSA**. Cette opération est directement liée au problème de la factorisation, la connaissance des facteurs premiers constituant la trappe permettant d'inverser facilement le calcul.

En termes de comparaison avec le monde physique, on peut par exemple penser au mélange de limaille de fer et de limaille de cuivre. Comme dans le cas des pots de peinture de couleurs primaires différentes, l'opération de mélange est aisée mais l'opération inverse est très complexe, à moins de disposer d'un aimant qui constitue en quelque sorte la trappe.

Les recherches en cryptographie de ces 30 dernières années ont permis de disposer de quelques problèmes mathématiques asymétriques utilisables à des fins cryptographiques. Ils ne sont cependant pas nombreux et reposent presque tous sur des problèmes issus de la théorie des nombres : factorisation et calculs de « logarithmes discrets » dans des structures mathématiques variées, dont les « courbes elliptiques » sont des exemples particulièrement intéressants.

L'idée de base des problèmes de logarithme discret consiste à utiliser une structure mathématique contenant un nombre fini d'éléments que l'on peut combiner au moyen d'une opération possédant des propriétés semblables à celles de l'addition ou de la multiplication sur les entiers classiques. Une telle structure est appelée « groupe » en algèbre, le groupe étant dit additif si l'opération est notée +, ou multiplicatif si l'opération est notée ×. On peut ensuite définir une version itérée de l'opération agissant sur les éléments du groupe. Si l'on note multiplicativement l'opération et si x désigne un élément du groupe alors le produit de n copies de x se note « x à la puissance n », soit x^n. Le calcul de x^n est facile, même pour de très grandes valeurs de l'entier n. Par contre, dans certains groupes, l'opération inverse consistant, à partir de x et de x^n, à retrouver l'entier n est très difficile, bien que mathématiquement parfaitement définie. On parle de calcul de « logarithme discret », n étant appelé « logarithme de x^n en base x ». Comme dans le cas de la factorisation, il doit être clair que le calcul de logarithme n'est pas impossible en théorie ; il suffit par exemple de tester

[105] Les nombres premiers étant les nombres divisibles uniquement par 1 et par eux-mêmes. Par exemple, 2, 3, 5, 7 sont premiers, mais 6 — qui est divisible par 1, 2, 3 et 6 — ne l'est pas.

toutes les valeurs possibles de *n*, même s'il existe de bien meilleures méthodes. Cependant, pour des dimensionnements suffisants, aucune méthode efficace permettant d'effectuer de tels calculs en temps raisonnable dans les groupes utilisés en cryptographie n'est connue. Les « courbes elliptiques «, si leurs paramètres sont choisis avec soin, sont de tels exemples de groupes dans lesquels on suppose que le calcul de logarithme discret est particulièrement difficile.

Aucun détail nécessitant de lourds rappels mathématiques ne sera donné ici. Il suffira de noter simplement que ces problèmes ne deviennent réellement difficiles, et donc cryptographiquement intéressants, que pour des tailles suffisantes de certains paramètres. Ce sont ces tailles qui déterminent la sécurité intrinsèquement apportée par le problème de base à l'ensemble du cryptosystème. La sécurité d'un système asymétrique s'évalue donc en fonction de la difficulté à résoudre numériquement un certain problème mathématique et non pas en fonction de la taille de l'espace des clés. Ainsi, par exemple, lorsque l'on parle de **RSA-2048**, ceci signifie que l'on utilise **RSA** avec un paramètre, appelé module, long de 2048 bits et obtenu par multiplication de deux nombres premiers de 1024 bits chacun. Il ne faut par conséquent pas s'étonner de voir apparaître en cryptographie asymétrique des paramètres ou des clés de 2048 bits ou plus alors qu'en cryptographie symétrique les clés dépassent rarement 128 bits, voire 256 bits pour les plus longues. Les tailles de clés symétriques et asymétriques ne sont donc pas comparables[106].

Notons enfin que l'emploi d'un problème réellement difficile et correctement dimensionné est une condition nécessaire afin d'obtenir un niveau de sécurité recherché. Bien entendu, ceci est très loin d'être suffisant car bien d'autres sources de failles de sécurité existent, que ce soit dans l'emploi du problème, dans les modes opératoires, dans la gestion des clés, dans les problèmes de conception ou d'implantation des protocoles, etc.

A.2.1 Chiffrement asymétrique

L'idée essentielle du **chiffrement asymétrique**, encore souvent appelé chiffrement à clé publique, est que rien n'impose à l'émetteur d'un message chiffré d'être capable de déchiffrer les messages qu'il envoie. Dit autrement, aussi naturelle qu'elle puisse paraître, l'intuition selon laquelle la même clé doit être utilisée à la fois pour le chiffrement et le déchiffrement n'est pas fondamentalement justifiée.

Dans le cadre du chiffrement, l'idée est d'utiliser des paires de clés, ou bi-clés, composées d'une **clé privée**[107] et d'une clé publique associée. Afin de chiffrer un message à l'attention d'un correspondant, on utilise la clé publique de ce dernier. Après transmission, l'opération inverse de déchiffrement est effectuée en utilisant la clé privée. Les propriétés du mécanisme sont telles que la connaissance de la clé publique ne permet pas de retrouver la clé privée. Par conséquent, la clé publique peut, comme son nom l'indique, être largement diffusée. Par contre, la clé privée doit être gardée confidentielle.

Une image classique consiste à imaginer une boîte aux lettres (physique). L'équivalent de la clé publique est la boîte à l'adresse du destinataire, adresse consultable par tous, dans un annuaire par exemple. L'équivalent de la clé privée est la clé de la boîte dont ne dispose, normalement, que le propriétaire de la boîte. Afin de

[106] Ainsi, si 256 bits de clés sont largement suffisants pour la cryptographie symétrique, un module RSA de 256 bits peut être factorisé sur un simple PC en moins d'une heure.

[107] L'usage veut que l'on réserve le terme de clé secrète aux applications symétriques et le terme de clé privée aux applications asymétriques. Une clé publique est donc en général naturellement associée à une clé privée, alors qu'une telle association n'a aucun sens pour une clé secrète.

transmettre un document, il « suffit » de prendre connaissance de l'adresse du destinataire et de le lui envoyer sous pli scellé. Lors de la réception, seul le destinataire peut prendre connaissance du document à la condition que lui seul possède la clé. Cette image permet en outre de comprendre le problème posé par l'authentification de la boîte du destinataire puisqu'il faut savoir relier de manière fiable le destinataire à sa boîte pour s'assurer que la bonne personne recevra le document. Pour le destinataire des documents si aucun mécanisme n'est prévu pour authentifier l'émetteur, il ne peut davantage s'assurer de l'intégrité de ce qu'il reçoit.

Il est important de noter que, contrairement au cas des mécanismes symétriques, il n'est pas ici nécessaire que les deux correspondants partagent, au préalable, une clé secrète. Ceci permet théoriquement de résoudre très élégamment les problèmes de mise en accord de clé inhérents à la cryptographie symétrique. Il se pose cependant le problème de la certification des clés publiques visant à s'assurer qu'une clé publique utilisée pour chiffrer appartient bien au correspondant à qui l'on destine le message.

Le problème apparaît plus clairement formalisé sous le diptyque confidentialité/authentification. En effet s'il est facile de comprendre que l'échange d'un secret nécessite de la confidentialité, on aurait tendance à oublier que l'authentification de l'origine du secret (c'est-à-dire à la fois la garantie de son intégrité et de l'émetteur) est cruciale. Si la cryptographie asymétrique lève le problème de la confidentialité, le problème de l'authentification reste quant à lui entier. Il est résolu par des mécanismes de certification comme cela est indiqué plus loin.

Comme dans le cas du chiffrement par bloc, l'utilisation de chiffrement à clé publique avec des messages de taille quelconque doit être très précisément spécifiée. Ceci implique d'être capable de formater et de compléter les messages afin d'appliquer l'algorithme de chiffrement; on parle de « padding » ou « bourrage ». L'utilisation de données aléatoires est également nécessaire afin de « randomiser » le chiffrement et par conséquent d'éviter que le chiffrement du même message à deux reprises produise des chiffrés identiques. Ceci est fondamental pour des applications où l'espace des messages, c'est-à-dire l'ensemble des messages, est restreint à un petit sous-ensemble des messages possibles. Cette problématique est d'ailleurs similaire à celle rencontrée dans le cas symétrique et exposée en section A.1.1.1.

Notons enfin que pour des raisons d'efficacité il est inutile de chiffrer de grands messages au moyen d'un mécanisme asymétrique. Une méthode bien plus efficace, désignée sous le terme de « chiffrement hybride », consiste à choisir une clé de session pour un mécanisme de chiffrement symétrique et à ne chiffrer avec le mécanisme à clé publique que cette clé de session, le message étant lui chiffré en symétrique avec la clé de session. On peut ainsi transmettre la clé de session de manière sécurisée à son interlocuteur, et un long message peut être chiffré de manière conventionnelle et très efficace.

A.2.2 Signature cryptographique asymétrique

La **signature cryptographique** permet de garantir l'intégrité d'un message sans utiliser de clé secrète partagée entre l'émetteur et le destinataire. Elle permet également d'assurer une authentification forte de l'émetteur du message en empêchant ce dernier de nier par la suite avoir envoyé le message ; on parle de propriété de non-répudiation.

La signature est un mécanisme asymétrique qui peut donner l'impression d'avoir de nombreuses similitudes avec le chiffrement à clé publique. Signature et chiffrement ne doivent cependant surtout pas être confondus. Le principal point commun est l'emploi de bi-clés formées d'une clé privée et d'une clé publique associée.

La clé privée permet de générer la signature d'un message sous la forme d'une donnée qui lui est accolée[108], à la manière des **MACs** vus au chapitre A.1.1. Afin de vérifier la validité d'une signature, il suffit de disposer de la clé publique. Par conséquent, tout le monde peut potentiellement s'assurer de l'authenticité d'un message puisque la clé publique peut être librement rendue disponible. Ceci réalise donc une version électronique de la signature manuscrite classique, certains diront même en mieux. Notons cependant qu'ici encore la certification de la clé publique est un problème crucial qui est abordé rapidement ci-dessous dans le chapitre A.5 consacré à la gestion de clé, et qui est repris plus en détail dans le référentiel intitulé « Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques », spécifiquement consacré à cette problématique.

Comme pour le chiffrement, la mise en forme à appliquer au message avant signature est très importante en termes de sécurité. Elle utilise souvent une fonction de hachage transformant un message de longueur quelconque en une empreinte de taille fixe et petite.

On a souvent tendance à présenter la signature numérique comme une sorte de réciproque du chiffrement asymétrique. Ceci provient du fait que dans le cas de **RSA**, souvent présenté comme illustration, chiffrement et signature sont en effet très proches, la signature d'un message s'apparentant fortement à l'opération de déchiffrement. Ce cas est cependant exceptionnel. La grande majorité des schémas de signature ne peuvent être utilisés à des fins de chiffrement.

A.2.3 Authentification asymétrique d'entités et établissement de clé

Les idées permettant une authentification interactive d'entités vues au chapitre A.1.1 peuvent bien entendu s'étendre aux primitives asymétriques. Afin d'authentifier quelqu'un dont on connaît avec certitude la clé publique, il suffit par exemple de chiffrer à son attention un message quelconque suffisamment long et de lui demander de retourner ce message clair. De même, on peut lui demander de signer un tel message et ensuite vérifier la validité de cette signature.

Il existe cependant des mécanismes spécifiquement conçus pour le cadre interactif. Ces primitives dites « à divulgation nulle de connaissance « ou « zero-knowledge », bien qu'encore peu utilisées en pratique, sont à la source de la plupart des schémas de signature numérique. On citera par exemple le standard de signature américain **DSA** (« digital signature algorithm »), qui présente une certaine parenté avec le protocole d'authentification de Schnorr.

La cryptographie asymétrique permet également de résoudre le problème de la confidentialité dans l'établissement de clé, qui consiste pour deux entités ne partageant initialement aucun secret commun à se mettre d'accord sur une valeur de clé secrète[109]. La sécurité de l'établissement de clé est un problème délicat, car celui-ci doit se faire à l'aide d'un canal non sécurisé, c'est à dire potentiellement écouté voire entièrement contrôlé par un attaquant. L'article fondateur de W. Diffie et M. Hellman [DH76] décrivait d'ailleurs principalement une solution au problème d'établissement de clé ; le protocole résultant est ce que l'on appelle encore aujourd'hui l'» échange de clé de Diffie-Hellman ».

[108] Plus exactement, le mécanisme consistant à calculer une signature et à l'ajouter au message est appelé « signature avec appendice ». D'autres techniques permettant d'économiser un peu de place sont envisageables avec des mécanismes tel que **RSA** utilisant une permutation à trappe. Ceci n'a cependant que peu d'importance en première approche.

[109] Cette clé secrète pouvant par exemple par la suite être utilisée pour chiffrer des messages.

Techniquement, la remarque fondamentale de W. Diffie et M. Hellman est que, lorsque l'on utilise une structure mathématique dans laquelle le calcul de logarithme discret est difficile, on peut facilement choisir un grand entier secret *a* et publier x^a sans que *a* ne puisse être retrouvé par quiconque. Ainsi, afin que deux interlocuteurs notés A et B se mettent d'accord sur un secret commun *K*, il suffit que A choisisse un entier *a* et transmette $y = x^a$, que B choisisse un entier *b* et transmette $z = x^b$. A peut alors calculer $K = z^a = (x^b)^a = x^{ab}$ et B peut faire de même en calculant la même valeur $K = y^b$. Par contre, un attaquant qui écoute passivement la communication ne peut apprendre que *y* et *z* ; à ce jour l'on ne connaît pas de méthode plus efficace que le calcul de logarithme discret pour retrouver les secrets a et b afin d'en déduire le secret partagé *K*.

Notons cependant que ce protocole élémentaire ne permet pas de garantir la sécurité face à des attaquants actifs pouvant modifier les communications. Il ne garantit également aucune forme d'authentification des interlocuteurs. Une attaque connue sous le nom d'attaque par le milieu permet en effet à un attaquant actif de mettre en défaut la sécurité de l'échange de clé de Diffie-Hellman.

En pratique, les mécanismes d'authentification et d'établissement de clé sont généralement utilisés de concert en pratique car, d'une part, établir une clé avec une personne dont on ignore l'identité a peu d'intérêt et, d'autre part, une simple authentification apporte peu. Le lien entre authentification et établissement de clé doit cependant être réalisé avec soin : il est nécessaire que les deux mécanismes soient imbriqués si l'on souhaite éviter des scénarios tels que l'attaque par le milieu. Un schéma d'authentification totalement décorrélé de l'établissement de clé ne protégerait pas le système contre les attaques par le milieu, que l'authentification soit mise en œuvre avant l'établissement de clé ou bien après l'établissement de clé — sur un canal chiffré à l'aide des clés établies au moyen de ce dernier[110].

A.2.4 Sécurité des primitives asymétriques

La cryptographie moderne a développé des techniques de preuve de nature mathématique afin de tenter de prouver la sécurité des primitives, notamment asymétriques. Ces preuves n'ont pas un caractère absolu mais reposent avant tout sur un modèle de sécurité formalisant les propriétés attendues de la primitive ainsi que les capacités supposées de l'attaquant contre lequel on veut se prémunir.

Ces preuves sont dites « par réduction « au sens où elles vont ramener la sécurité globale d'une primitive à une hypothèse bien identifiée telle que « factoriser des modules **RSA** de 2048 bits n'est pas possible[111] ». Les preuves en clé publique n'assurent ainsi jamais une « sécurité inconditionnelle » — c'est-à-dire face à un attaquant de puissance infinie[112]. Elles offrent au contraire le plus souvent une « sécurité calculatoire », c'est-à-dire l'assurance qu'il est impossible d'attaquer une certaine propriété du schéma sans résoudre un certain problème mathématique.

Afin d'illustrer l'importance mais également la difficulté de définition d'un modèle de sécurité, prenons l'exemple de la signature. On peut tout d'abord considérer divers types d'attaques, selon les capacités de

[110] Dans le premier cas, il suffirait en effet à un attaquant d'attendre le succès de la phase d'authentification pour mettre en oeuvre une attaque par le milieu. Dans le second cas, il lui suffirait de réaliser une attaque par le milieu contre le schéma d'établissement de clé, puis de relayer sur les canaux chiffrés ainsi établis les messages du protocole d'authentification entre ces entités.

[111] En un temps raisonnable.

[112] La puissance étant ici la mémoire et la puissance de calcul.

l'attaquant, qui peuvent aller de la simple connaissance de la clé publique de vérification de signature à la capacité d'obtenir la signature de n'importe quel message de son choix. On peut également s'interroger sur la définition même de ce que l'on entend par succès d'une attaque. Cela peut aller de la simple « contrefaçon existentielle «, consistant à réussir à générer une signature valide d'un message non maîtrisé, à un « cassage total », consistant à retrouver la clé privée de signature.

Il existe deux types de sécurité, comme mis en avant la première fois par M. Bellare et Ph. Rogaway [BR94] : la sécurité « asymptotique » et la sécurité « exacte ». Quand la première se contente d'assurer que le schéma est sûr pour des paramètres « assez grands «, la seconde énonce clairement des estimations de la difficulté de l'attaque en fonction de la difficulté du problème. Ainsi, il est très important de prendre en compte les résultats qu'apportent la preuve, et de ne pas s'arrêter au fait que le schéma est sûr pour des paramètres assez grands. Pour être plus précis, la sécurité exacte conduit à ce que l'on appelle des réductions fines (dans lesquels la difficulté du cassage du schéma est de l'ordre de la difficulté du problème mathématiques) et des réductions lâches (dans lesquels il est plus facile — d'un ordre de grandeur non négligeable — de casser le schéma que de résoudre le problème). On voit ainsi que les schémas à préférer sont ceux apportant les réductions les plus fines possibles, car les autres schémas nécessitent de plus grandes clés et paramètres pour une même garantie de sécurité. De même, s'il n'est pas possible de sélectionner un schéma avec une réduction fine, il faut en ce cas utiliser les coefficients de finesse donnés par la preuve pour en déduire les tailles de paramètres et de clés adéquats. Ceci permet de conserver une signification à la garantie de sécurité offerte par la preuve.

Il est clair qu'une primitive asymétrique prouvée sûre, relativement à une hypothèse bien identifiée et raisonnable, est d'autant plus intéressante que l'on a pris en compte des attaquants puissants et des définitions de succès d'attaque modestes dans la preuve. Tout comme pour la sécurité du chiffrement symétrique, vue au chapitre A.1.1, les modèles de sécurité utilisés en cryptographie moderne peuvent paraître excessifs mais l'expérience montre que c'est loin d'être le cas et qu'il est important de se placer dans ce cadre contraignant afin d'évaluer correctement les primitives.

A.3 Fonctions de hachage

Un certain nombre de primitives cryptographiques, ou directement utilisées en cryptographie, ne sont pas paramétrées par des clés. La classification usuelle basée sur la nécessité ou l'absence de nécessité de partager un secret commun ne s'applique pas. Ces primitives sont néanmoins souvent classées parmi les primitives symétriques dans la mesure où leurs caractéristiques principales empruntent beaucoup aux primitives à clé secrète ou que le cadre de leur utilisation nécessite qu'émetteur et récepteur réalisent les mêmes opérations (de manière symétrique, donc).

La plus importante de ces primitives est la fonction de hachage dont le but est de transformer, de manière déterministe, une suite de bits de longueur quelconque, en un **condensat**, encore appelé **empreinte** ou **haché**, de taille fixée. On demande de plus à une fonction de hachage cryptographique d'être en pratique non inversible, c'est-à-dire qu'il ne soit pas possible étant donné un condensat de trouver un message dont l'image par la fonction de hachage est égale à ce condensat : on dit que le calcul d'un antécédent est difficile. On demande en outre qu'il ne soit pas possible de trouver deux messages distincts ayant même condensat. On dit alors que la fonction de hachage est **sans collision**.

Bien entendu, une fonction de hachage étant une fonction d'un ensemble de taille potentiellement infinie vers un ensemble de taille finie, il existe une infinité de telles collisions. On demande cependant qu'il ne soit pas possible de calculer pratiquement, en temps raisonnable, une telle collision.

Une fois encore le paradoxe des anniversaires peut s'appliquer ; si l'on note n le nombre de bits du condensat

et si la fonction de hachage peut être considérée comme ayant un comportement relativement aléatoire malgré le fait qu'elle soit parfaitement définie en tous points[113], alors, pour trouver une collision, il suffit de calculer de l'ordre de $2^{n/2}$ hachés de messages aléatoires avant que deux de ces messages ne fournissent le même condensat. Ceci fournit une borne inférieure à la taille nécessaire des sorties des fonctions de hachage cryptographiques.

Une des nombreuses applications des fonctions de hachage apparaît dans les schémas de signature numérique afin de réduire le message de longueur quelconque à un simple condensat de taille fixée et petite. Elles sont également utilisées afin de réaliser certains codes d'authentification de message (par exemple **HMAC**).

Suite aux publications consécutives à l'annonce d'attaques sur les principales familles de fonctions de hachage en août 2004, le panel des fonctions de hachage considérées comme sûres s'est beaucoup réduit puisque n'y apparaissent plus ni **MD5** (définitivement cassé) ni **SHA-1** (qui n'est plus conforme au référentiel). Dans l'attente de la publication de nouveaux standards, dont par exemple **SHA-3**, et de leur mise à l'épreuve, la famille **SHA-2** reste utilisable.

A.4 Génération d'aléa cryptographique

La cryptographie fait un usage intensif de données aléatoires, typiquement afin de générer des clés mais également pour bien d'autres applications comme dans les opérations de formatage de messages avant chiffrement ou signature. La qualité des données aléatoires utilisées est parfois critique en termes de sécurité et nécessite de disposer de données aléatoires « de qualité ».

À titre d'exemple particulièrement frappant de la nécessité de disposer de bon aléa pour certaines applications, citons le standard de signature américain **DSA**. En utilisant cet algorithme, la signature d'un message nécessite l'emploi d'un nombre aléatoire de 160 bits, gardé secret par le signataire. Pour chaque signature, il est nécessaire de disposer d'un nouveau nombre aléatoire indépendant des précédents et donc à usage unique.

Sans que cela ne remette en cause la sécurité de **DSA**, on connaît aujourd'hui une attaque qui permet de retrouver la clé privée à condition de disposer de signatures pour lesquelles seulement 2 bits du nombre aléatoire à usage unique sont connus. Cette attaque fonctionne donc très efficacement même si les 158 bits restants sont parfaitement aléatoires et inconnus de l'attaquant. Cet exemple montre que, pour certaines applications, il est impossible de se contenter de nombres partiellement aléatoires.

La génération de bits réellement aléatoires, c'est-à-dire valant 0 ou 1 avec même probabilité et, surtout, indépendants les uns des autres, est particulièrement délicate sur une plate-forme fondamentalement déterministe comme un ordinateur ou un microprocesseur de carte à puce. Il existe cependant des dispositifs physiques spécifiques tirant parti de phénomènes supposés imprévisibles comme le bruit thermique ou le temps s'écoulant entre deux désintégrations d'une source radioactive. On parle alors de générateur **d'aléa vrai** ou **d'aléa physique**.

Il est également possible de générer du **pseudo-aléa**, c'est-à-dire des suites de bits indistinguables de suites réellement aléatoires mais issues d'un mécanisme déterministe initialisé avec un germe ou graine, de petite taille mais réellement aléatoire pour sa part. La plupart des mécanismes de chiffrement par flot sont d'ailleurs

[113] C'est-à-dire que, avant d'avoir fait le calcul, la valeur du hachage en un point est aléatoire pour un utilisateur. Une bonne fonction de hachage a ce comportement aléatoire, alors qu'une simple fonction de troncature par exemple n'est pas du tout aléatoire.

construits autour de tels générateurs pseudo-aléatoires.

Notons enfin que, par définition, il est en pratique impossible de distinguer du pseudo-aléa correctement généré de véritables bits aléatoires. Malgré l'existence de notions théoriques bien définies issues de la théorie de l'information, comme celle d'entropie, la seule manière de tester des bits ainsi générés est d'appliquer des tests statistiques visant à détecter des biais statistiques dont la probabilité d'apparition est négligeable dans des séquences de bits issues de sources d'aléa vrai. L'efficacité de ces tests, aussi élaborés soient-ils, demeure cependant très limitée en pratique. Une suite déterministe aussi simple que la succession des décimales de π suffit en effet à tromper la plupart des tests statistiques.

A.5 Gestion de clés

A.5.1 Clés secrètes symétriques

La gestion des clés peut être plus ou moins simple selon les applications. Dans le contexte de mécanismes symétriques, la principale difficulté réside dans la distribution, ou mise en accord, des clés afin de permettre aux correspondants de partager les mêmes secrets initiaux sans que des attaquants potentiels ne les aient interceptés. Ceci peut être réalisé au moyen de techniques asymétriques modernes mais peut également l'être via des méthodes non cryptographiques de nature organisationnelle.

En outre, une durée de vie maximale, appelée **crypto-période**, est en général associée à chaque clé. Une telle durée de vie peut être représentée par une date limite d'emploi ou par un compteur du nombre d'utilisations qui ne doit pas dépasser une certaine limite. Une telle limitation de l'usage des clés vise en général à réduire l'effet d'une éventuelle compromission des clés. Elle peut cependant également s'avérer nécessaire si les primitives cryptographiques sont sous-dimensionnées par rapport au niveau de sécurité visé. Il est cependant important de bien comprendre que dans un système cryptographiquement bien conçu il ne doit pas y avoir de phénomène « d'usure » des clés limitant leur emploi.

Afin de protéger les clés lors de leur stockage, celles-ci peuvent être elles-mêmes chiffrées avec une autre clé qui n'a généralement pas à être partagée. On désigne en général sous le terme de **clé noire** une clé ainsi chiffrée, par opposition aux **clés rouges** qui sont en clair. Il va de soi que l'ensemble des clés d'un système en fonctionnement ne peuvent toutes être noires simultanément.

Notons enfin un cas particulier d'architecture, encore assez courant, utilisant un secret largement partagé entre un grand nombre d'utilisateurs. La divulgation de telles clés a en général des conséquences dramatiques en termes de sécurité, ce qui est contradictoire avec leur large diffusion. Dans certaines applications, l'usage exclusif de primitives symétriques rend nécessaire l'emploi de telles architectures ; ceci milite fortement en faveur d'une utilisation d'architectures asymétriques permettant de s'en passer.

À titre d'exemple, imaginons un groupe important de n individus souhaitant pouvoir s'authentifier mutuellement. En utilisant des techniques symétriques, on peut soit prévoir une clé secrète par paire d'individu, ce qui implique que chacun mémorise au moins n - 1 clés, soit donner la même clé à tout le monde. Si l'on souhaite de plus pouvoir ajouter de nouveaux membres facilement, cette dernière solution devient le seul possible. Cependant, quelle confiance peut-on avoir dans un tel système, même si la clé est stockée dans une enceinte protégée telle une carte à puce ?

Une manière simple de résoudre ce problème avec une technique asymétrique est de faire choisir à chaque membre du groupe une bi-clé dont la clé publique est certifiée par une autorité. Chaque membre doit donc uniquement mémoriser sa bi-clé et la clé publique de l'autorité. On peut ensuite utiliser une des techniques d'identification évoquées au chapitre A.2.1.

A.5.2 Bi-clés asymétriques

La gestion des bi-clés en cryptographie asymétrique est à la fois plus simple et plus complexe que dans le cas symétrique. Plus simple, et également plus sûre, car il n'y a plus besoin de partager des secrets à plusieurs. Ainsi, la clé privée n'a besoin d'être connue que de son seul détenteur et certainement pas divulguée à d'autres. Par conséquent, il n'y a en théorie nul besoin de faire générer de telles clés par un tiers. On peut par exemple tout à fait concevoir qu'une clé privée soit générée par une carte à puce et qu'à aucun moment de la vie du système cette clé n'ait à quitter l'enceinte supposée sécurisée de la carte.

Le problème majeur qui se pose réside cependant dans la nécessité d'associer une clé publique à l'identité de son détenteur légitime. Une telle certification de clé publique peut être effectuée au moyen de la signature d'un certificat par une autorité qui certifie de ce fait que telle clé publique appartient bien à tel individu ou entité. Il se pose alors le problème de la vérification de cette signature qui va à son tour nécessiter la connaissance de la clé publique de l'autorité. Afin de certifier cette clé, on peut concevoir qu'une autorité supérieure génère un nouveau certificat, et ainsi de suite. On construit ainsi un chemin de confiance menant à une clé racine en laquelle il faut bien finir par avoir confiance, sans que cette confiance soit garantie par un mécanisme cryptographique. De telles constructions sont désignées sous le terme **d'infrastructure à clé publique** (**ICP** ou **PKI** pour « public key infrastructure »). La notion **d'Infrastructure de gestion de clé** (**IGC** ou **KMI** pour « key management infrastructure ») recouvre quant à elle toutes les opérations d'enregistrement ou d'affectation d'une clé dans un système en y incluant aussi la vérification de l'identité de son possesseur, la gestion de ses équipements, des révocations, etc.

Notons enfin que dans de nombreuses applications pratiques, il est nécessaire de disposer d'une sorte de voie de secours permettant par exemple d'accéder à des données chiffrées sans être pour autant destinataire de ces informations. Les motivations de tels **mécanismes de recouvrement** peuvent être multiples mais il est important d'insister sur le fait qu'elles peuvent être parfaitement légales et légitimes. La méthode la plus simple est le séquestre de clés consistant à mettre sous scellés les clés privées ou secrètes tout en contrôlant les conditions d'accès à ces informations.

Des travaux cryptographiques modernes proposent cependant de nombreuses autres solutions bien plus souples, sûres et efficaces.

Annexe B Éléments académiques de dimensionnement cryptographique

Cette annexe présente quelques informations issues d'annonces et de publications académiques permettant de contribuer à la justification de certains dimensionnements cryptographiques.

B.1 Records de calculs cryptographiques

Les records de calculs cryptographiques permettent de donner une borne inférieure à la difficulté pratique de certains problèmes. Ils concernent essentiellement le « cassage » de clés symétriques par énumération de l'ensemble des clés possibles (recherche dite exhaustive) ainsi que la résolution de problèmes mathématiques issus de la théorie des nombres (factorisation et logarithme discret dans des structures variées).

B.1.1 Records de calculs en cryptographie symétrique

Les principaux records de calcul rendus publics ont utilisé le réseau Internet et le bénévolat d'internautes acceptant d'effectuer des calculs sur leur ordinateur personnel en « tâche de fond ». Les principaux résultats sont d'une part le cassage de clés **DES** de 56 bits :

- 17 juin 1997, **96 jours** de calcul distribué sur Internet ;
- 23 février 1998, **41 jours** de calcul distribué sur Internet[114] ;
- 17 juillet 1998, **56 heures** de calcul sur une machine spécifique[115] dont le coût a été estimé à 250 000 dollars ;
- 19 janvier 1999, **22 heures** de calcul en combinant la machine précédemment citée et des calculs sur Internet.

D'autre part le cassage de clés de chiffrement **RC5** :

- 19 octobre 1997, version **56 bits** cassée après 250 jours de calcul sur Internet ;
- 14 juillet 2002, version **64 bits** cassée après 1757 jours de calcul sur Internet.

Il va de soi que ces « records » ne tiennent pas compte des capacités de calcul de services gouvernementaux spécialisés qui ne recherchent bien évidemment pas la publicité. Ceci ne doit cependant pas engendrer de paranoïa excessive, comme expliqué au paragraphe A.1.1.

B.1.2 Records de calculs de factorisation

Les principaux records successifs en termes de calcul de factorisation de modules produits de deux nombres premiers de taille comparable sont :

- 9 juin 1993, Denny, Dodson, Lenstra et Manasse, **397** bits (120 chiffres décimaux) ;
- 2 avril 1994, Atkins, Graff, Lenstra et Leyland, **426** bits (129 chiffres décimaux) ;
- 10 avril 1996, Lenstra et al., **432** bits (130 chiffres décimaux) ;

[114] Voir http://www.distributed.net.

[115] Voir http://www.eff.org/Privacy/Crypto/Crypto_misc/DESCracker.

- 2 février 1999, te Riele et al., **466** bits (140 chiffres décimaux) ;
- 22 août 1999, te Riele et al., **512** bits (155 chiffres décimaux) ;
- 18 janvier 2002, Bahr, Franke et Kleinjung, **524** bits (158 chiffres décimaux) ;
- 1er avril 2003, Bahr, Franke, Kleinjung, Lochter et Boehm, **530** bits (160 chiffres décimaux) ;
- 3 décembre 2003, Franke et Kleinjung, **576** bits (174 chiffres décimaux) ;
- 9 mai 2005, Bahr, Boehm, Franke et Kleinjung, **663** bits (200 chiffres décimaux) ;
- 12 décembre 2009, Kleinjung et al., **768** bits (232 chiffres décimaux).

Les deux premiers records ont utilisé l'algorithme du crible quadratique et les suivants l'algorithme du crible algébrique, le plus efficace connu à ce jour pour factoriser de grands entiers quelconques. La plupart de ces challenges ont été proposés par la société **RSA**[116].

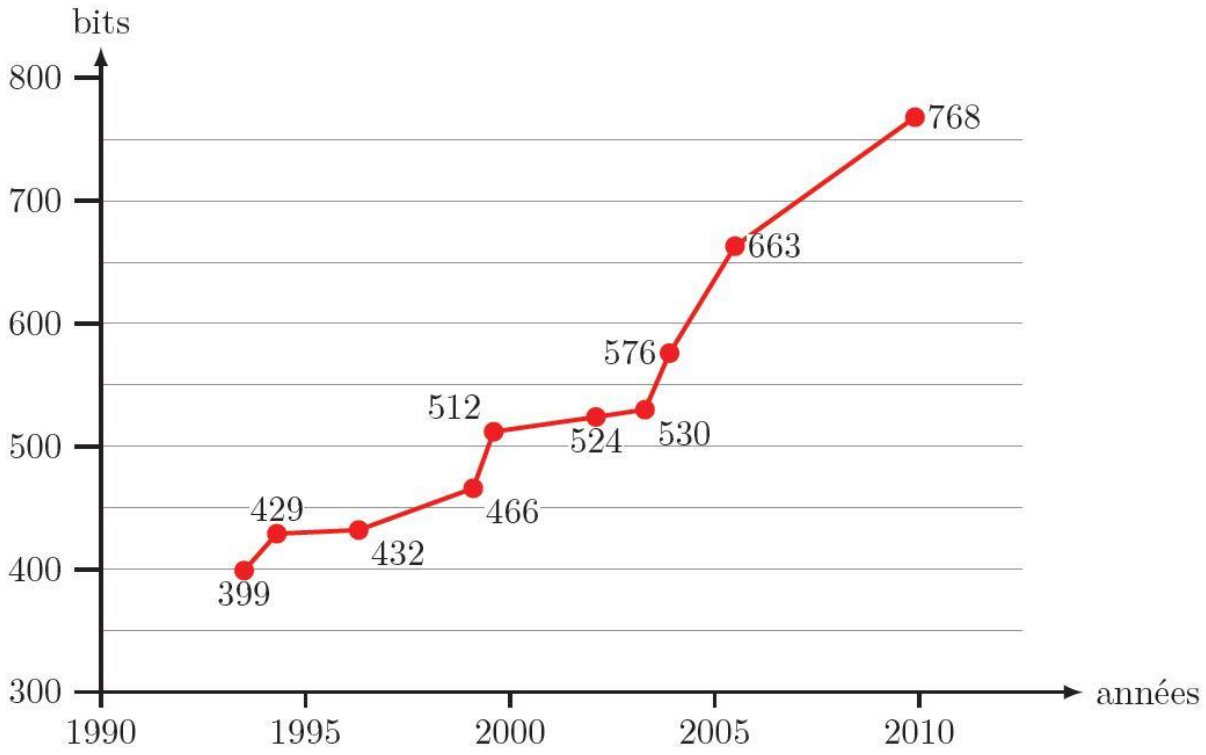


FIGURE 5 – Records de factorisation

B.1.2.1 Factorisation par des machines dédiées

De même qu'il est possible de concevoir des machines dédiées conçues exclusivement à des fins de calculs

[116] Les challenges de la société RSA étaient disponibles sur http://www.rsasecurity.com/rsalabs/ challenges, mais ont été retirés en 2007.

exhaustifs sur des clés de chiffrement symétrique, il est aujourd'hui sérieusement envisagé de concevoir de telles machines afin de factoriser de grands modules **RSA**. Le projet le plus abouti a été présenté par Adi Shamir et Eran Tromer en août 2003. Les estimations de coût indiquent qu'il semblerait possible de réaliser pour quelques dizaines de millions d'euros une machine capable de factoriser des modules de 1024 bits en moins d'un an. À ce jour aucune annonce de conception concrète n'a cependant été faite.

B.1.2.2 Autres records de factorisation

Notons enfin que dans certains cas il est possible d'employer des algorithmes de factorisation particuliers, plus efficaces que les algorithmes généraux mais ne s'appliquant pas à tous les entiers (et en particulier, à ce jour, ne s'appliquant pas aux modules **RSA**).

L'algorithme SNFS (crible algébrique dit « spécial ») a ainsi permis de factoriser le nombre de Mersenne $2^{809} - 1$ de **809** bits (244 chiffres décimaux) début 2003, puis le nombre de Mersenne $2^{1039} - 1$ de **1039** bits (313 chiffres décimaux) en 2007, un nombre qui est donc plus grand qu'un module **RSA** de 1024 bits.

B.1.3 Records de calcul de logarithme discret dans GF(*p*)

Les principaux records successifs en termes de calcul de logarithme discret dans un corps fini premier à *p* éléments **GF**(*p*) sont les suivants. Pour chaque record, la taille — exprimée en bits et en chiffres décimaux — du nombre premier p est indiquée :

- 25 novembre 1996, Weber, Denny et Zayer, **281** bits (85 chiffres décimaux) ;
- 26 mai 1998, Joux et Lercier, **298** bits (90 chiffres décimaux) ;
- novembre 1999, Joux et Lercier, **331** bits (100 chiffres décimaux) ;
- 19 janvier 2001, Joux et Lercier, **364** bits (110 chiffres décimaux) ;
- 17 avril 2001, Joux et Lercier, **397** bits (120 chiffres décimaux) ;
- 18 juin 2005, Joux et Lercier, **431** bits (130 chiffres décimaux) ;
- 5 février 2007, Bahr, Franke et Kleinjung, **530** bits (160 chiffres décimaux).

B.1.4 Records de calcul de logarithme discret dans GF(2^n)

Les principaux records successifs en termes de calcul de logarithme discret dans un corps fini à 2^n éléments **GF**(2^n) avec n un nombre premier sont :

- 1992, Gordon et McCurley, **GF**(2^{401}) soit **401** bits (121 chiffres décimaux) ;
- 25 septembre 2001, Joux et Lercier, **GF**(2^{521}) soit **521** bits (157 chiffres décimaux) ;
- 23 février 2002, Thomé, **GF**(2^{607}) soit **607** bits (183 chiffres décimaux) ;
- 22 septembre 2005, Joux et Lercier, **GF**(2^{613}) soit **613** bits (185 chiffres décimaux) ;
- 10 avril 2013, Barbulescu et al., **GF**(2^{809}) soit **809** bits (183 chiffres décimaux).

Les principaux records successifs en termes de calcul de logarithme discret dans un corps fini à 2^n éléments **GF**(2^n) avec n un nombre composé sont :

- 11 février 2013, Joux, **GF**(2^{1778}) soit **1778** bits (536 chiffres décimaux) ;

- 19 février 2013, Gologlu, Granger, McGuire et Zumbragel, **GF**(2^{1971}) soit **1971** bits (594 chiffres décimaux) ;
- 22 mars 2013, Joux, **GF**(2^{4080}) soit **4080** bits (1229 chiffres décimaux) ;
- 11 mai 2013, Granger, Granger, McGuire et Zumbragel, **GF**(2^{6120}) soit **6120** bits (1843 chiffres décimaux) ;
- 21 mai 2013, Joux, **GF**(2^{6168}) soit **6168** bits (1857 chiffres décimaux) ;
- 31 janvier 2014, Granger, Kleinjung et Zumbragel, GF(2^{9234}) soit **9234** bits (2780 chiffres décimaux).

On notera en particulier qu'à taille de corps équivalente, le calcul de logarithme discret est bien plus facile dans **GF**(2^n) que dans **GF**(p).

B.1.5 Records de calcul de logarithme discret dans GF(p^n)

Les principaux records en termes de calcul de logarithme discret dans un corps fini à p^n éléments **GF**(p^n), pour p égal à 3, sont les suivants :

- 19 février 2010, Hayashi et al., **GF**(3^{426}) soit **676** bits (204 chiffres décimaux) ;
- 17 juin 2012, Hayashi, Shimoyama, Shinohara et Takagi, **GF**(3^{582}) soit **923** bits (278 chiffres décimaux) ;
- 28 janvier 2014, Adj, Menezes, Oliveira et Rodriuez-Henriquez, **GF**(3^{822}) soit **1303** bits (393 chiffres décimaux).

Les principaux records en termes de calcul de logarithme discret dans un corps fini à p^n éléments **GF(**p^n), pour p supérieur à 3, sont les suivants :

- 28 juin 2005, Lercier et Vercauteren, **GF**(370801^{18}) soit **334** bits (101 chiffres décimaux) ;
- 24 octobre 2005, Joux et Lercier, **GF**(65537^{25}) soit **401** bits (121 chiffres décimaux) ;
- 9 novembre 2005, Joux et Lercier, **GF**(370801^{30}) soit **556** bits (168 chiffres décimaux) ;
- Août 2006, Joux, Lercier, Smart et Vercauteren, **GF**(p^3), où p est un nombre premier de 132 bits (40 chiffres décimaux), soit **394** bits (119 chiffres décimaux) ;
- 24 décembre 2012, Joux, GF(33553771^{47}) soit **1175** bits (354 chiffres décimaux) ;
- 6 janvier 2013, Joux, **GF**(33341353^{57}) soit **1425** bits (429 chiffres décimaux).

On notera en particulier qu'à taille de corps équivalente, le calcul de logarithme discret pour p et n de taille moyenne est plus facile que dans **GF**(p).

B.1.6 Calcul de logarithme discret sur courbe elliptique

La société Certicom a publié le 6 novembre 1997 une liste de challenges[117] concernant le problème du

[117] Voir http://www.certicom.com.

logarithme discret sur courbe elliptique. Les challenges sont de trois types : courbe elliptique « quelconque » définie sur **GF**(*p*), courbe elliptique « quelconque » définie sur **GF**(2^n), et courbe de Koblitz également définie sur **GF**(2^n). Ces challenges sont respectivement désignés par les codes **ECCp-***x*, **ECC2-***x* et **ECC2K-***x*, où x désigne la taille en bits de l'ordre premier du sous-groupe dans lequel sont définies les opérations.

TABLE 3 – Challenges Certicom

Challenge	Date d'annonce	Nombre d'opérations
ECCp-79	06/12/1997	2^{40}
ECCp-89	12/01/1998	2^{44}
ECCp-97	18/03/1998	2^{47}
ECCp-109	06/11/2002	2^{54}
ECCp-131	Non résolu	
ECC2-79	16/12/1997	2^{40}
ECC2-89	09/02/1998	2^{44}
ECC2-97	22/09/1999	2^{47}
ECC2-109	15/04/2004	2^{54}
ECC2-131	Non résolu	
ECC2K-95	21/05/1998	2^{44}
ECC2K-108	04/04/2000	2^{51}
ECC2K-130	Non résolu	

Le tableau 3 reproduit les résultats annoncés jusqu'à aujourd'hui ainsi que les prochains challenges non-résolus et le nombre d'opérations qui ont été nécessaires.

Le 8 juillet 2009, Bos, Kaihara, Kleinjung, Lenstra et Montgomery ont résolu une instance du problème du logarithme discret sur une courbe elliptique définie sur **GF**(*p*) où *p* est un nombre premier de **112** bits.

B.2 Étude de la taille des clés d'après l'article de Lenstra [Len04]

A. Lenstra a publié en 2004 un article visant à comparer les niveaux de robustesse des divers problèmes employés en cryptographie. Ce travail académique doit bien entendu être considéré avec beaucoup de prudence ; il a cependant le mérite de proposer des modèles à la fois motivés et raisonnables.

Mise en garde : ce travail est mentionné dans ce document car il est le plus complet réalisé à ce jour dans ce domaine par des chercheurs du milieu académique. Il est, de plus, souvent référencé, ainsi que sa version antérieure, datant de 2001. Le fait de le citer et d'en mentionner certains des résultats dans cette partie ne constitue cependant pas une caution de l'article pris dans son intégralité. En particulier, la responsabilité

de certaines affirmations est laissée à leurs auteurs.

B.2.1 Évolution des tailles de clés symétriques

Il est facile d'estimer l'évolution des tailles de clés symétriques nécessaires sous l'hypothèse d'une loi de Moore selon laquelle la quantité de mémoire et la puissance de calcul disponibles pour un prix donné doublent tous les 18 mois. Le graphique de la figure 6 indique l'évolution des tailles de clés nécessaires afin de maintenir un niveau de sécurité équivalent à celle du **DES** (56 bits) en 1982 : en vertu de ce qui précède, la longueur de clé nécessaire augmente d'un bit tous les 18 mois. Le graphique se lit donc de la façon suivante. L'année est donnée en abscisse. L'ordonnée indique la taille de clé en bits offrant une sécurité équivalente à la sécurité du **DES** en 1982. À titre de comparaison, on a représenté en pointillés ce que donnerait l'extrapolation basée sur une loi de Moore plus optimiste (doublement tous les 15 mois) ou plus pessimiste (doublement tous les 24 mois).

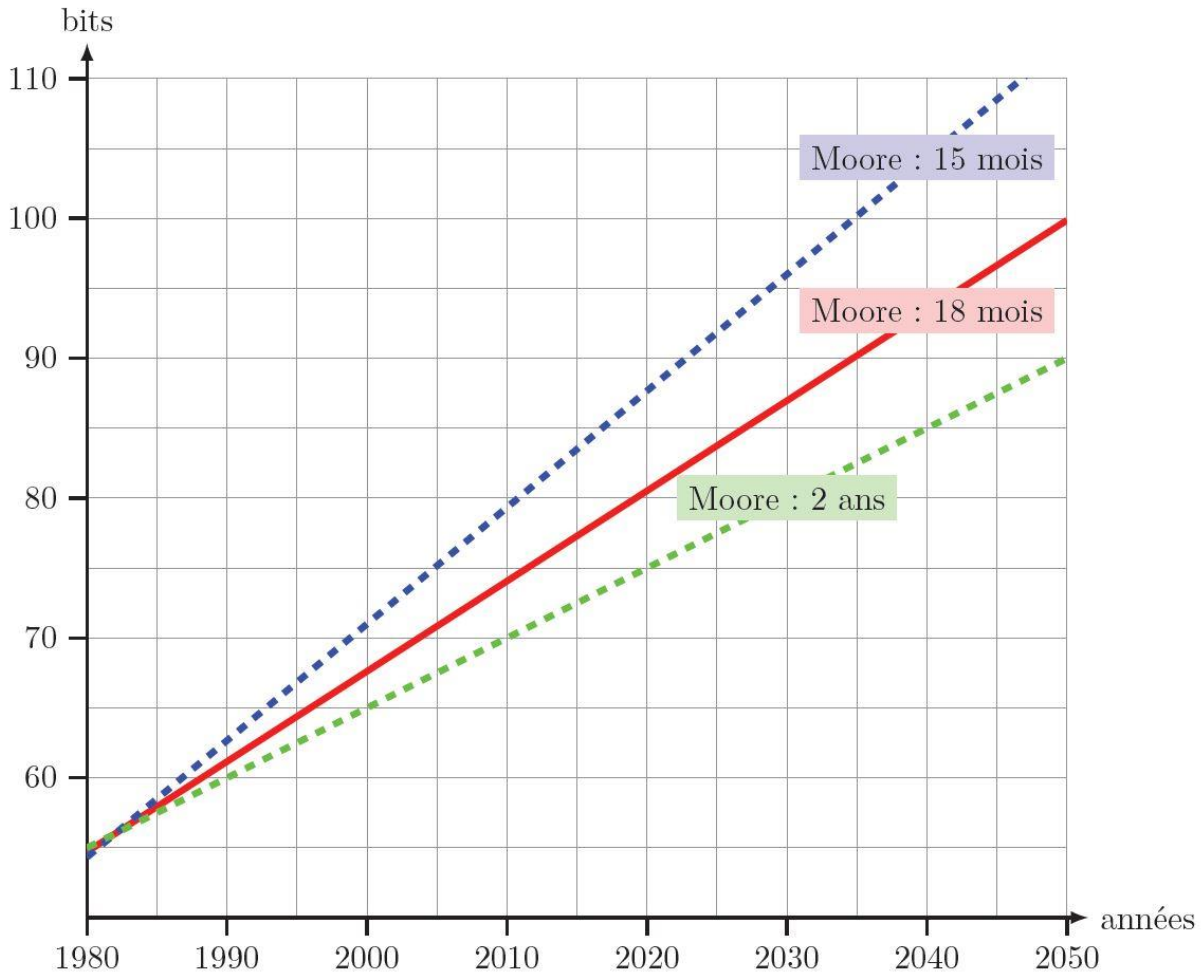


FIGURE 6 – Taille de clé symétrique offrant une sécurité équivalente à celle du **DES** en 1982

Remarques :

- Des clés de 128 bits apportent un très haut niveau de sécurité face à une attaque par recherche exhaustive.
- Des clés de 256 bits offrent une sécurité démesurée face aux attaques par recherche exhaustive.

- En conclusion, on peut se protéger efficacement contre les attaques par recherche exhaustive, même à un horizon très lointain.

B.2.2 Évolution des tailles de modules en cryptographie asymétrique

Le même genre d'évaluation peut être réalisé pour des modules asymétriques.

Le graphique de la figure 7 se lit de la façon suivante. L'année est donnée en abscisse. L'ordonnée indique la taille de module en bits offrant une sécurité équivalente à la sécurité du **DES** en 1982. En poursuivant le raisonnement de l'article de Lenstra [Len04], on adopte les hypothèses suivantes : tout d'abord les records publiés laissent à penser que les implantations matérielles conduisent à un meilleur rapport performances/coût; de fait la loi de Moore d'un doublement de puissance du matériel tous les 18 mois est applicable ; par ailleurs, les améliorations dans l'implantation des algorithmes de factorisation sont également à prendre en compte : l'expérience montre qu'elles correspondent assez bien à une progression de type loi de Moore. L'article de Lenstra fait l'hypothèse que les deux facteurs de progrès (améliorations du matériel et avancées algorithmiques) sont indépendants, et peuvent donc s'accumuler ; en l'occurrence, on obtient une division par deux de la difficulté de factoriser un module de taille donnée au bout de 9 mois.

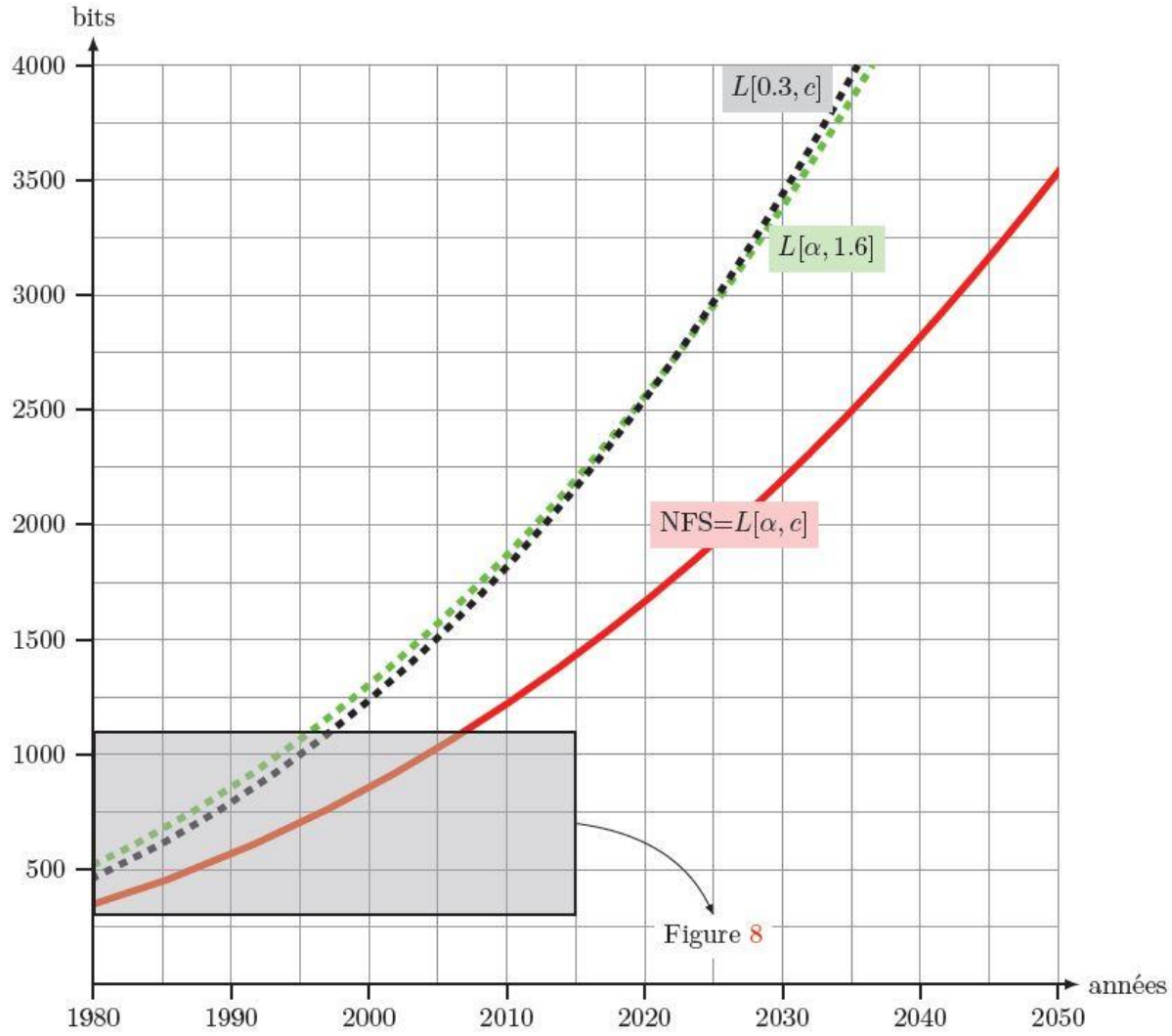


FIGURE 7 - Taille de module offrant une sécurité équivalente à celle du DES en 1982. Influence de la constante (en vert) et de l'exposant (en noir) du crible algébrique (NFS). Les paramètres actuels de l'algorithme **NFS** sont $\alpha = 1/3$ et $c = \sqrt[3]{64/9} \approx 1.92$.

Sur la figure 7, la courbe rouge en trait plein représente l'évolution des tailles de module en se basant sur les hypothèses précédentes. Par ailleurs, les éventuels progrès algorithmiques, en factorisation d'entiers comme en calcul de logarithmes discrets, peuvent avoir une influence considérable sur le choix des tailles de paramètres. Le meilleur algorithme de factorisation connu aujourd'hui, le crible algébrique ou **NFS**, a une complexité notée $L[\alpha,c]$ qui dépend de deux facteurs : une « constante » c et un « exposant » a. La courbe verte en pointillé représente les tailles de module offrant une sécurité équivalente au **DES** en 1982, en supposant que l'on dispose d'un algorithme pour lequel la constante c vaut 1.60 au lieu de 1.92 (avec un exposant inchangé et une loi de Moore basée sur 9 mois). La courbe noire en pointillé représente le même phénomène en supposant que l'on dispose d'un algorithme pour lequel l'exposant a vaut 0.30 au lieu de 1/3 (Les autres paramètres étant pris, là encore, identiques à ceux de la courbe rouge). On notera que ces deux courbes s'intersectent.

Remarques :

- La croissance est nettement non linéaire à cause de l'existence d'algorithmes dits « sous-exponentiels « tels que les cribles quadratiques et algébriques.
- À moyen terme, l'emploi de modules de grande taille s'impose.
- Aucune distinction n'est faite ici entre problème de factorisation et de logarithme discret dans **GF**(p) car cette distinction aurait peu de sens en pratique. On considère cependant que le problème du logarithme discret est légèrement plus difficile que celui de la factorisation ; en pratique, dans les gammes de tailles envisagées, 100 à 200 bits les séparent, cette approximation étant très imprécise.

Une comparaison de cette courbe et des records annoncés publiquement est nécessaire. Les courbes de la figure 7 ont vocation à guider les choix de paramètres pour éviter le cassage d'un système, alors que les records ne traduisent que le savoir-faire académique en matière de cassage. Ces records ne rendent pas compte des réalisations non publiées.

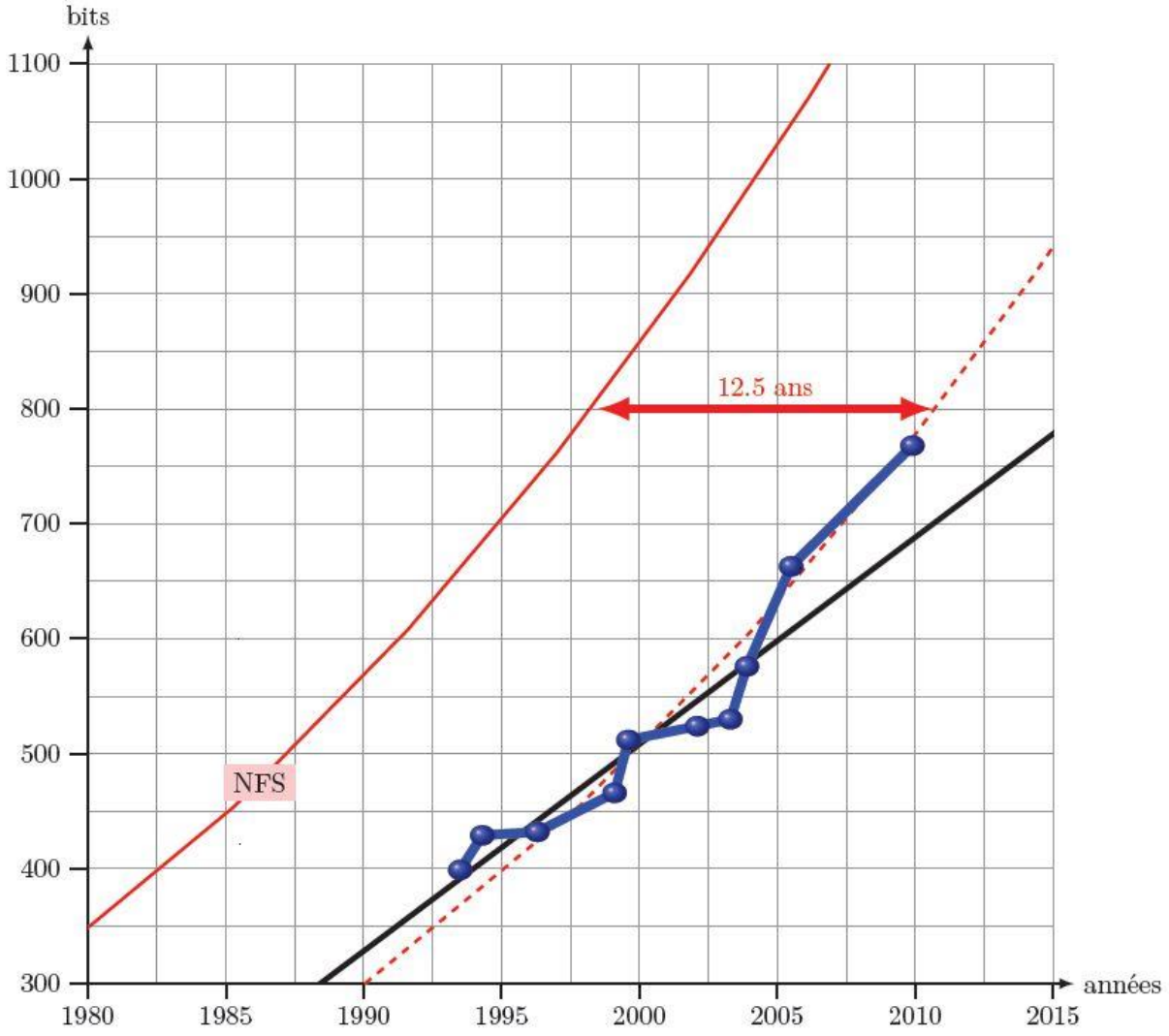


FIGURE 8 - Comparaison entre les records de factorisation et les tailles théoriques nécessaires pour une sécurité équivalente à celle du **DES** en 1982

Ces précautions étant prises, observons les records publiés et comparons-les aux courbes précédentes. Dans la figure 8 :

- Les 10 records de factorisation sont indiqués par les billes bleues. La droite noire et épaisse est une interpolation linéaire de ces records.
- La courbe rouge continue correspond à la courbe rouge de la figure 7 : meilleur algorithme connu (crible algébrique NFS), soutenu par une loi de Moore de doublement tous les 9 mois.
- La courbe rouge en pointillé représente le même scénario décalé de 12,5 ans.

Que peut-on conclure de ce graphe ? Il est tout d'abord évident que les points expérimentaux sont peu nombreux et donc certainement peu significatifs. De plus, on n'a pas tenu compte de l'effort de calcul qui a été nécessaire pour obtenir chacun de ces records. On constate cependant que l'hypothèse faite sur la loi de Moore (progrès conjoints du matériel et de la qualité d'implantation des algorithmes) correspond assez bien à une avance de 12 ans sur les records (ou sur leur interpolation). Dans tous les cas, il convient de rester

extrêmement prudent quant à l'interprétation de ces résultats : les courbes obtenues ici sont basées sur des hypothèses qui, tout en étant réalistes, sont avant tout arbitraires. De plus ces courbes sont extrêmement proches les unes des autres et semblent très sensibles à une petite variation des paramètres.

En conclusion, des principes cryptographiques élémentaires poussent à tenir compte de toutes les hypothèses disponibles permettant de dimensionner correctement un système afin de se mettre à l'abri des attaquants les plus puissants. C'est le parti pris dans l'article de Lenstra et également par la plupart des experts du domaine. Les observations qui viennent d'être faites peuvent cependant pousser certains concepteurs à assumer le risque d'employer des modules plus petits afin de gagner en performance tout en maintenant une sécurité « apparemment suffisante ». Le débat peut bien entendu se prolonger à l'infini car il est impossible de le trancher objectivement avec des arguments indiscutables.

B.2.3 Évolution des tailles de courbes elliptiques

Le même travail est réalisé dans le cas de courbes elliptiques. La figure 9 résume les différentes situations, et se lit de la façon suivante. L'année est donnée en abscisse. L'ordonnée indique la taille de module en bits offrant une sécurité équivalente à la sécurité du **DES** en 1982. La courbe rouge correspond au scénario actuel, en se basant sur une loi de Moore offrant un doublement de la puissance de calcul tous les 18 mois (autrement dit, la même hypothèse que les courbes rouges continues des figures précédentes). Une loi de Moore très optimiste d'un doublement tous les ans mène à la courbe en bleu et en pointillé. Enfin en tenant compte d'hypothétiques progrès algorithmiques (algorithmes en $O(q^{0.4})$ au lieu de $O(q^{0.5})$ où q désigne le nombre de points de la courbe), on obtient la courbe en noir et en pointillé.

B.2.4 Équivalence de sécurité entre tailles de module asymétrique et de clé symétrique

Afin de comparer clés symétriques et asymétriques, on peut reprendre les données précédentes et tracer les équivalences, indépendamment du temps. On obtient les courbes de la figure 10 comparant les clés symétriques et les modules asymétriques. Le graphique se lit de la façon suivante. Le nombre de bits des clés symétriques est donné en abscisse. L'ordonnée indique la taille en bits du module asymétrique offrant une sécurité équivalente. La courbe en rouge résulte de l'interprétation de la formule de complexité du meilleur algorithme connu (crible algébrique ou **NFS**). La courbe verte en pointillé représente le scénario où un progrès algorithmique permet un gain de 25% sur la constante c, soit une valeur c = 1.44. La courbe noire et en pointillé représente le scénario où un progrès de 25% est fait sur la valeur de l'exposant a, soit une valeur $\alpha = 1/4$.

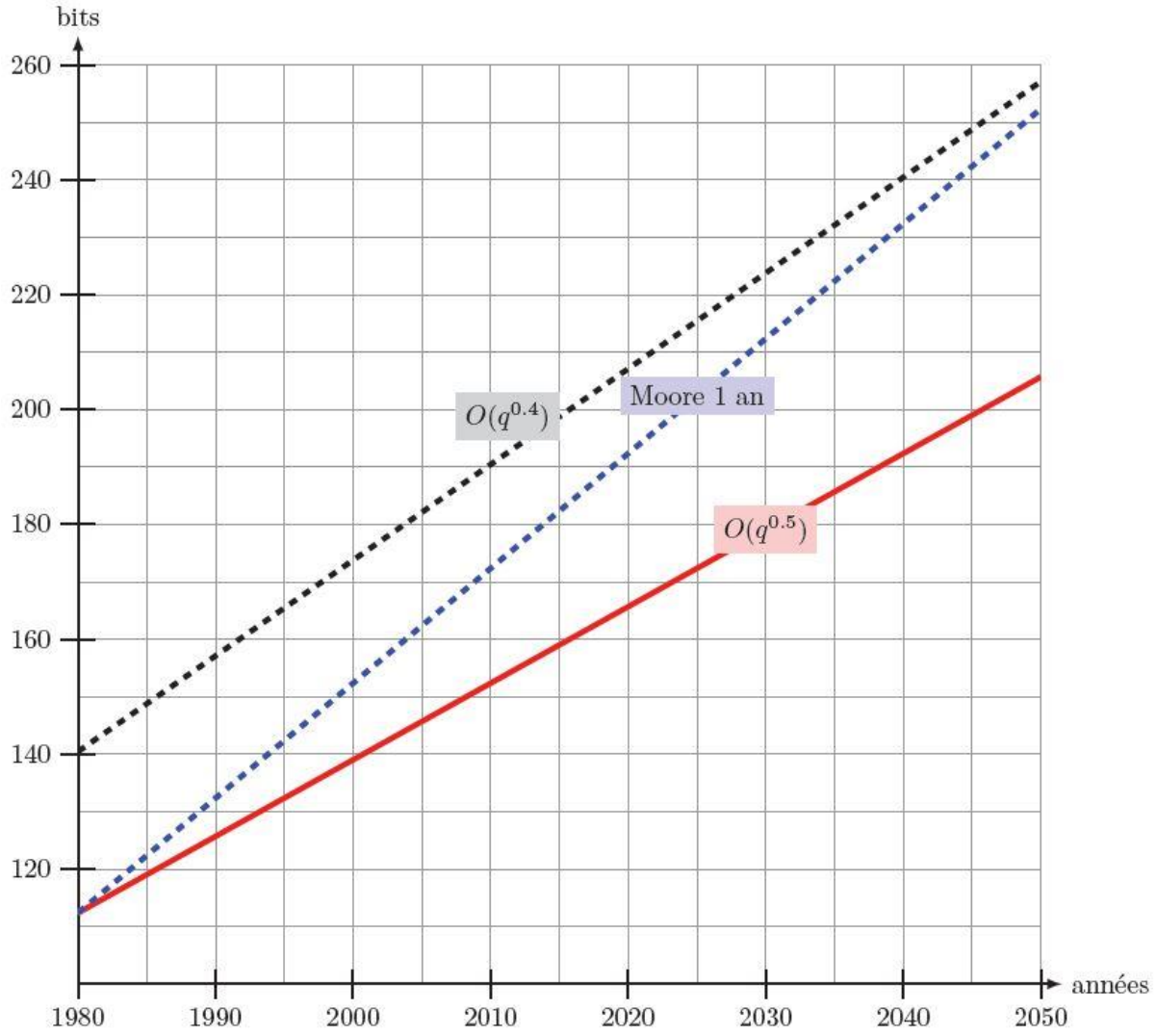


FIGURE9 – Taille de courbes elliptiques offrant une sécurité équivalente à celle du **DES** en 1982, et influence des potentiels progrès algorithmiques (en noir).

Remarques :

- Rechercher une sécurité équivalente en cryptographie asymétrique basée sur le problème de la factorisation ou sur celui sur logarithme discret à celle apportée en cryptographie symétrique par une clé secrète de plus de 128 bits mène à des tailles de clé très importantes, peu utilisables en pratique.
- Il est absurde de chercher à utiliser des modules d'une sécurité comparable à celle d'une clé symétrique de 256 bits.
- Il est courant de chercher à comparer la taille des clés symétriques et celle des clés asymétriques en estimant le « nombre de bits asymétriques » équivalent, en termes de sécurité, à un « bit symétrique ». En d'autres termes, ceci n'est rien d'autre que la pente de la courbe de la Figure 10. On peut par conséquent énoncer en termes courants que : « pour des clés longues d'environ 1024 bits, un bit

symétrique équivaut à 51 bits asymétriques », « pour des clés longues d'environ 2048 bits, un bit symétrique équivaut à 77 bits asymétriques ».

- On peut également reformuler ces affirmations sous la forme suivante : « pour doubler l'effort nécessaire afin de factoriser un module de 1024 bits, il convient d'utiliser un module de 1024+51=1075 bits ».

B.2.5 Équivalence de sécurité entre tailles de courbe elliptique et de clé symétrique

Le même procédé peut être appliqué pour comparer les clés symétriques et les cryptosystèmes à base de courbes elliptiques. On obtient les courbes de la figure 11. Le graphique se lit de la façon suivante. Le nombre de bits des clés symétriques est donné en abscisse. L'ordonnée indique la taille en bits de la courbe elliptique offrant une sécurité équivalente. La courbe en rouge résulte de l'interprétation de la formule de complexité du meilleur algorithme connu (en $O(q^{0.5})$). La courbe noire en pointillé représente le scénario où un progrès algorithmique permet d'avoir une complexité en $O(q^{0.4})$.

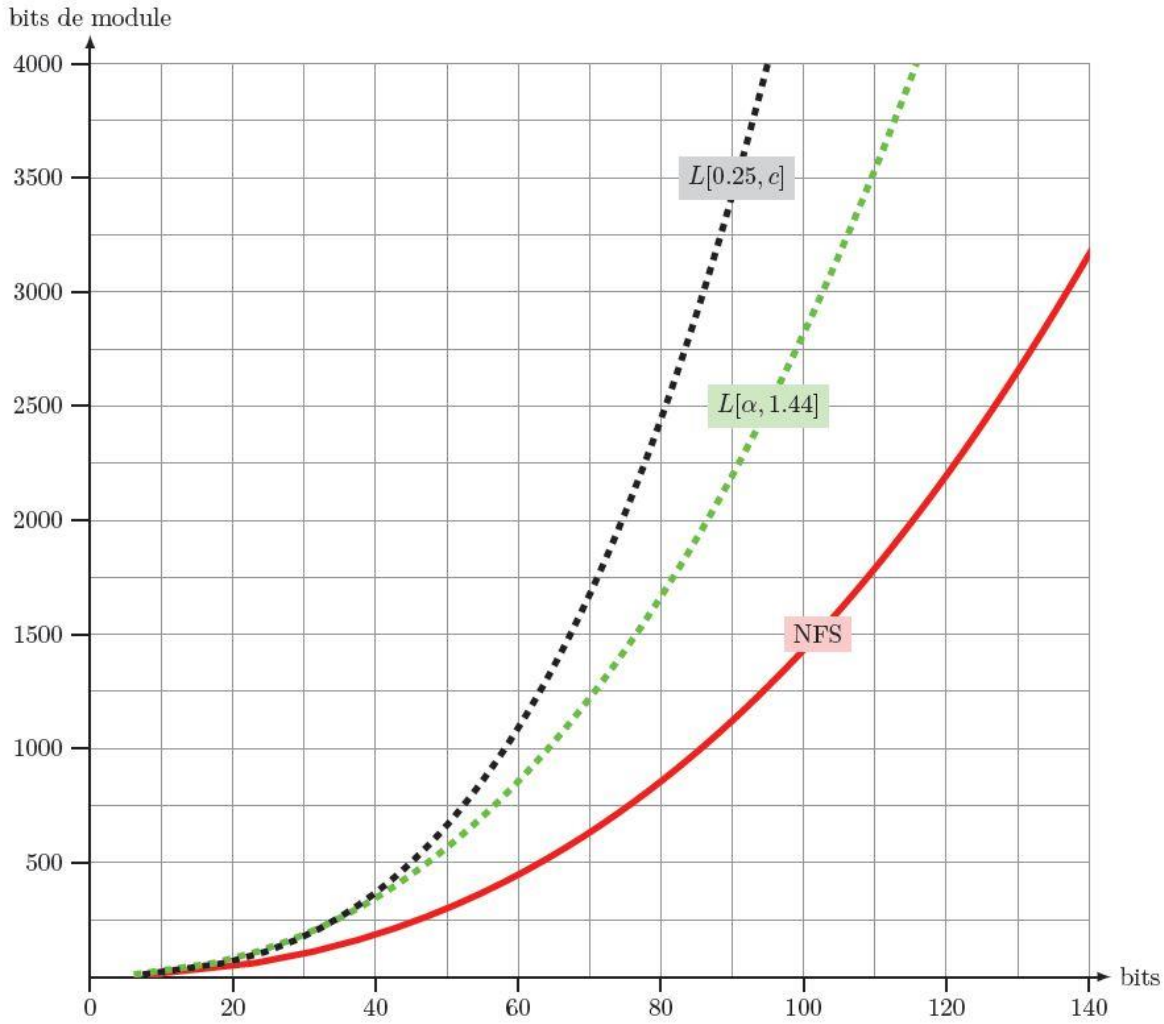


FIGURE 10 – Équivalence entre taille de module asymétrique et taille de clé symétrique. Influence des progrès algorithmiques (gain de 25%) sur la constante (courbe verte) ou

l’exposant (courbe noire) du crible algébrique.

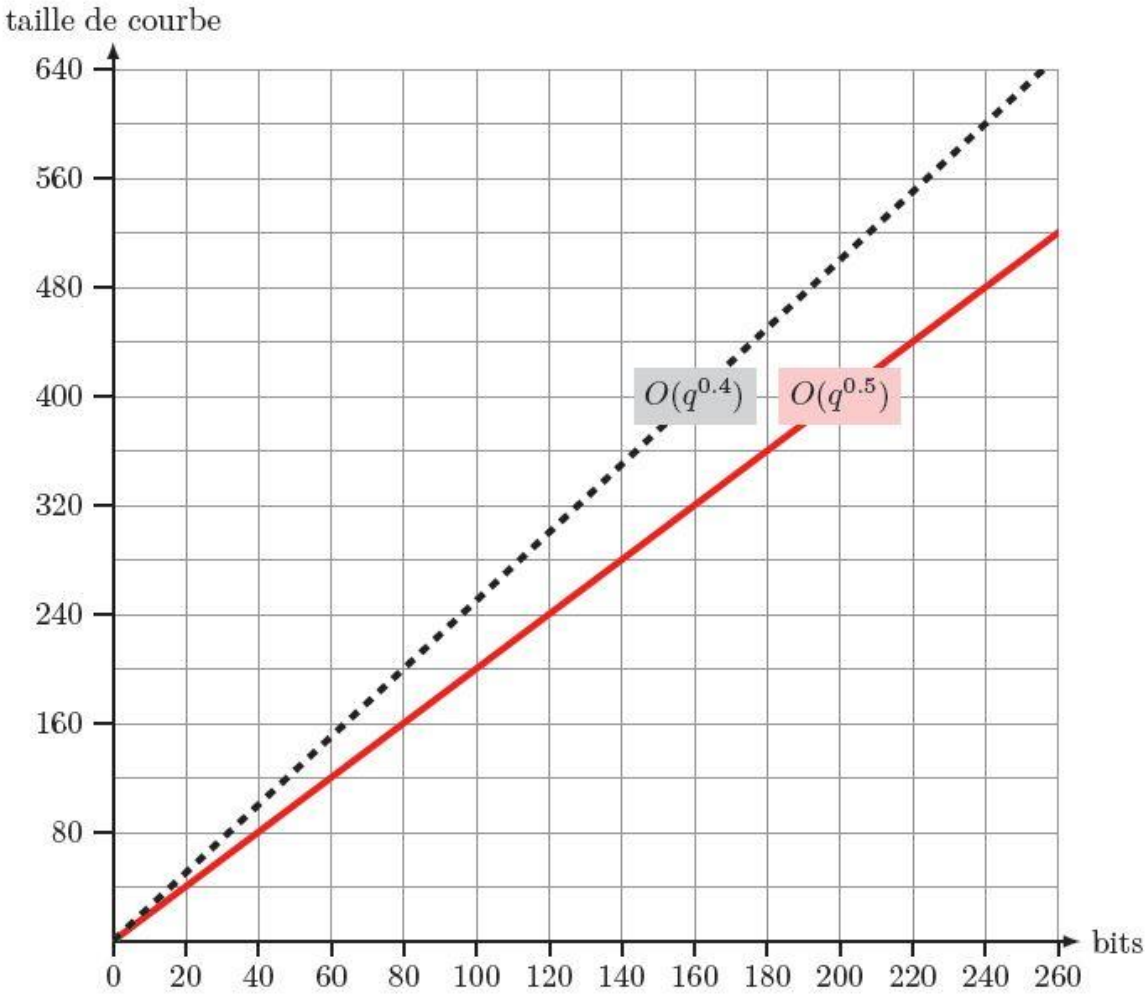


FIGURE11 – Équivalence entre dimensionnement de cryptosystème à base de courbe elliptique et taille de clé symétrique

Annexe C Bibliographie

Ble98. Daniel Bleichenbacher. Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS #1. In Proceedings of Crypto 1998, volume 1462 of LNCS, pages 1–12, 1998.

Ble06. Daniel Bleichenbacher. Crypto Rump Session, 2006.

BR94. Mihir Bellare and Philipp Rogaway. Optimal asymmetric encryption. In Proceedings of Eurocrypt 1994, volume 839 of LNCS, pages 92–111. Springer-Verlag, 1994.

CFA+06. Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren, editors. Handbook of elliptic and hyperelliptic curve cryptography. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2006.

DH76. Whitfield Diffie and Martin Hellman. New directions in cryptography. IEEE Transactions on Information Theory, 22(6) :644–654, 1976.

Len04. Arjen Lenstra. Handbook of Information Security, volume 2, chapter Key Lengths. Wiley, 2004.

MvV97. Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. Handbook of Applied Cryptography. CRC Press, 1997. http://www.cacr.math.uwaterloo.ca/hac.

Sch01. Bruce Schneier. Cryptographie appliquée. Vuibert, 2001.

Sin99. Simon Singh. Histoire des codes secrets. JC Lattès, 1999.

Ste98. Jacques Stern. La science du secret. Éditions Odile Jacob, 1998.

Sti01. Douglas Stinson. Cryptographie, théorie et pratique. Vuibert, 2001.

Vau06. Serge Vaudenay. A Classical Introduction to Cryptography : Applications for Communications Security. Springer, 2006.

Annexe D Liste des tableaux

Annexe E Table des figures

Annexe F Index des termes et des acronymes utilisés

Annexe G Index des règles et des recommandations

Recom -SignAsym-1, 23

Annexe B2

Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques

Historique des versions		
Date	**Version**	**Evolution du document**
xxx	1.0	Publication de la première version de l'annexe B2 du référentiel général de sécurité

Avant propos

Le présent référentiel est pris en application de l'article LP 20 de la loi du pays n° 2017 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices, et de son arrêté d'application.

Le présent document et ses annexes sont une copie adaptée du RGS B2 – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, en vigueur en métropole, version 2.0 du 8 juin 2012.

Le texte fait des renvois à des documents publiés par l'Agence nationale de la sécurité des systèmes d'information[118] (ANSSI) ou encore disponibles sur son site internet www.ssi.gouv.fr, en ce qu'ils reflètent l'état de l'art en matière de sécurité informatique.

Le référentiel et ses annexes sont disponibles en ligne sur le site internet www.dgen. pf, et leur mise à jour est assurée par la Direction générale de l'économie numérique.

[118] L'ANSSI est un service à compétence nationale rattaché au Secrétaire général de la défense et de la sécurité nationale, l'autorité chargée d'assister le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale. Parmi ses nombreux objectifs, l'un d'eux consiste à promouvoir un espace de confiance pour les services en ligne. Elle y participe en ce sens notamment au travers de la règlementation (référentiels) et ses labels (certification des produits de sécurité et qualification des produits de sécurité et des prestataires de service de confiance).

1 Introduction

1.1 Contexte

1.1.1 Objectif du document

La sécurité de la plupart des systèmes d'information repose pour partie sur l'utilisation de fonctions cryptographiques. Ces fonctions ont une sécurité de nature essentiellement mathématique qui repose sur des hypothèses importantes quant aux clés cryptographiques utilisées. Ces hypothèses peuvent être formalisées par des objectifs de sécurité qui doivent impérativement être respectés pour que les fonctions cryptographiques puissent remplir leur rôle. Pour que les fonctions cryptographiques remplissent effectivement leur rôle, il est indispensable que leur gestion soit sûre au niveau du système d'information. L'objectif de ce document est de présenter le cycle de vie d'une clé cryptographique et différentes architectures de gestion de clés possibles. Il vise aussi à aider à l'élaboration d'un système de gestion de clés.

1.1.2 Positionnement du document

Ce document traite des règles et recommandations concernant la gestion des clés utilisées dans les mécanismes cryptographiques. Il complète le document « Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques » qui constitue l'annexe B1 du RGS, notamment ses paragraphes « 2.5 Gestion de clés » et « A.5 Gestion de clés ».

Ce document constitue l'annexe B2 du RGS.

1.1.3 Définition des règles et recommandations

Les **règles** définissent des principes qui doivent a priori être suivis par tout mécanisme. L'observation de ces règles est une condition généralement nécessaire à la reconnaissance du bon niveau de sécurité du mécanisme. Cependant, le fait de suivre l'ensemble des règles, qui sont par nature très génériques, n'est pas suffisant pour garantir la robustesse du mécanisme cryptographique ; seule une analyse spécifique permet de s'en assurer.

En plus des règles, le présent document définit également des **recommandations**. Elles ont pour but de guider le choix de certaines architectures de gestion de clés permettant un gain considérable en termes de sécurité, pour un coût souvent modique. Il va de soi qu'en tant que recommandations, leur application peut être plus librement modulée en fonction d'autres impératifs tels que des contraintes de performance ou de coût.

Il importe de noter dès à présent que les règles et recommandations contenues dans ce document ne constituent pas un dogme imposé aux concepteurs de produits utilisant des mécanismes cryptographiques. L'objectif est de contribuer à une amélioration constante de la qualité des produits de sécurité. À ce titre, le suivi des règles énoncées dans ce document doit être considéré comme une démarche saine permettant de se prémunir contre de nombreuses erreurs de conception ainsi que contre d'éventuelles faiblesses non décelées lors de l'évaluation des mécanismes cryptographiques.

Dans un souci de transparence, les règles et recommandations contenues dans ce document sont le plus souvent accompagnées de justifications. Le but est de convaincre que les choix ne sont pas faits de manière arbitraire mais au contraire en tenant compte le plus rigoureusement possible de l'état de l'art actuel en cryptographie ainsi que des contraintes pratiques liées à sa mise en œuvre.

Le lecteur est invité à se référer également à l'annexe B1 du RGS « Mécanismes cryptographiques – Règles

et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques », notamment pour les différentes limitations décrites qui s'appliquent aussi au présent document. Ainsi, il convient de rappeler que les notions, règles et recommandations contenues dans ce document s'adressent à un lecteur familier des concepts de gestion de clés.

1.1.4 Organisation du document

L'organisation de ce document est dans certains aspects similaire à celle du document « Mécanismes crptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques » :

- Les concepts généraux relatifs à la gestion des clés cryptographiques sont présentés en section 1.2 ;
- Le cycle de vie d'une clé est défini en section 1.3, ainsi que les différents types d'architectures fonctionnelles associées à la gestion des clés ;
- L'ensemble des règles et recommandations s'appliquant aux différentes étapes du cycle de vie sont ensuite regroupées au chapitre 2;
- Les règles et recommandations sont repérées selon la codification suivante : les premières lettres (**Règle** ou **Recom**) indiquent si l'on à affaire à une règle ou une recommandation, le domaine d'application est ensuite précisé et, finalement, un chiffre permet de distinguer les règles d'un même domaine d'application.

Ce document ne comporte volontairement aucun tableau récapitulatif. Les différentes règles et recommandations ne peuvent en effet être assimilées à une recette décrivant comment réaliser une architecture de gestion de clés, ce qui serait une grave source d'erreurs et de confusions.

1.1.5 Mise à jour du document

Comme pour le document « Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques », ce document a vocation à être révisé régulièrement pour tenir compte des évolutions constantes des menaces et des possibilités technologiques.

1.2 La gestion de clés cryptographiques

1.2.1 Définitions et concepts

L'objet de ce chapitre est de rappeler les définitions et concepts essentiels en matière de gestion de clés cryptographiques afin de bien comprendre les règles et recommandations émises dans ce document. Ces rappels couvrent le strict minimum. Ils sont bien évidemment sommaires et volontairement non mathématiques.

1.2.1.1 Clés secrètes symétriques

La gestion des clés peut être plus ou moins simple selon les applications. Dans le contexte de mécanismes symétriques, la principale difficulté réside dans la distribution, ou mise en accord, des clés afin de permettre aux correspondants de partager les mêmes secrets initiaux sans que des attaquants potentiels ne les aient interceptés. Ceci peut être réalisé au moyen de techniques asymétriques modernes mais peut également l'être via des méthodes non cryptographiques de nature organisationnelle.

Une durée de vie maximale, appelée crypto-période, est de plus en général associée à chaque clé. Une telle durée de vie peut être représentée par une date limite d'emploi ou par un compteur du nombre d'utilisations

qui ne doit pas dépasser une certaine limite. Une telle limitation de la durée de vie des clés vise en général à réduire l'effet d'une éventuelle compromission des clés. Il est important de bien comprendre que dans un système cryptographiquement bien conçu il ne doit pas y avoir de phénomène « d'usure » des clés limitant leur durée d'utilisation.

Afin de protéger les clés lors de leur stockage, elles peuvent être elles-mêmes chiffrées avec une autre clé qui n'a généralement pas à être partagée. On désigne en général sous le terme de clé noire une clé ainsi chiffrée, par opposition aux **clés rouges** qui sont en clair. Dans l'acception courante, une **clé noire** est toutefois protégée avec un niveau de sécurité au moins identique à celui des données qu'elle protège. Or dans certains cas, la protection réalisée sur la clé n'atteint pas ce niveau cryptographique. Par exemple, si la clé est chiffrée à l'aide d'un mot de passe dont l'entropie est faible. On pourrait dans ce cas parler de **clé camouflée** pour distinguer ce type de cas de figure, même si cette terminologie n'est pas établie.

Notons enfin un cas particulier d'architecture, encore assez courant, utilisant un secret largement partagé entre un grand nombre d'utilisateurs. La divulgation de telles clés a en général des conséquences dramatiques en termes de sécurité, ce qui est contradictoire avec leur large diffusion. Dans certaines applications, l'usage exclusif de primitives symétriques rend nécessaire l'emploi de telles architectures ; ceci milite fortement en faveur d'une utilisation d'architectures asymétriques permettant de s'en passer.

A titre d'exemple, imaginons un groupe important de N individus souhaitant pouvoir s'authentifier mutuellement. En utilisant des techniques symétriques, on peut soit prévoir une clé secrète par paire d'individus, ce qui implique que chacun mémorise au moins N - 1 clés, soit donner la même clé à tout le monde. Si l'on souhaite de plus pouvoir ajouter de nouveaux membres facilement, cette dernière solution devient le seul possible. Cependant, même si la clé est a priori protégée, sa large diffusion augmente le risque de compromission.

Une manière simple de résoudre ce problème avec une technique asymétrique est de faire choisir à chaque membre du groupe une bi-clé dont la partie publique est certifiée par une autorité. Chaque membre doit alors uniquement mémoriser sa bi-clé et la clé publique de l'autorité.

1.2.1.2 Bi-clés asymétriques

La gestion des clés en cryptographie asymétrique est à la fois plus simple et plus complexe que dans le cas symétrique. Plus simple, mais également plus sûre, car il n'y a plus besoin de partager des secrets à plusieurs. Ainsi, la clé privée n'a besoin d'être connue que de son seul détenteur et certainement pas divulguée à d'autres. Par conséquent, il n'y a en théorie nul besoin de faire générer de telles clés par un tiers. On peut par exemple tout à fait concevoir qu'une clé privée soit générée par une carte à puce et qu'à aucun moment de la vie du système cette clé n'ait à quitter l'enceinte supposée sécurisée de la carte.

Le problème majeur qui se pose réside cependant dans la nécessité d'associer une clé publique à l'identité de son détenteur légitime. Une telle certification de clé publique peut être effectuée au moyen de la signature d'un certificat par une autorité qui certifie de ce fait que telle clé publique appartient bien à tel individu ou entité. Il se pose alors le problème de la vérification de cette signature qui va à son tour nécessiter la connaissance de la clé publique de l'autorité. Afin de certifier cette clé, on peut concevoir qu'une autorité supérieure génère un nouveau certificat, et ainsi de suite. On construit ainsi un chemin de confiance menant à une clé racine en laquelle il faut bien finir par avoir confiance. De telles constructions sont désignées sous le terme d'infrastructure de gestion de clés (IGC).

Notons enfin que dans de nombreuses applications pratiques, il est nécessaire de disposer d'une sorte de voie de secours permettant par exemple d'accéder à des données chiffrées sans être pour autant destinataire de ces informations. Les motivations de tels mécanismes de recouvrement peuvent être multiples mais il est

important d'insister sur le fait qu'elles peuvent être parfaitement légales et légitimes. La méthode la plus simple est le séquestre de clé consistant à mettre sous scellé les clés privées ou secrètes tout en contrôlant les conditions d'accès à ces informations. Des travaux cryptographiques modernes proposent cependant de nombreuses autres solutions bien plus souples, sûres et efficaces.

1.2.2 Objectifs de sécurité minimaux

1.2.2.1 Définitions

Authenticité Une clé cryptographique n'est qu'une valeur numérique. Le remplacement d'une clé par une autre peut permettre, s'il est possible, de contourner un mécanisme cryptographique. Les attaques dites « par le milieu « utilisent ce principe en usurpant l'identité du possesseur de la clé. Mais il peut aussi être très dangereux de pouvoir faire employer une clé par un algorithme cryptographique ou pour un usage pour lequel elle n'a pas été prévue. Il est donc important que les clés utilisées soient non seulement intègres, c'est-à-dire non modifiées, mais encore correctement associées à une entité du système, un algorithme cryptographique et un usage. L'objectif de sécurité correspondant est appelé **authenticité** de la clé.

Clé secrète vs. privée De façon systématique une « clé secrète » désigne dans la suite de ce document une clé cryptographique utilisée dans un système symétrique, une « clé privée » la partie qui doit rester secrète d'une bi-clé asymétrique et une « clé publique » la partie qui est diffusée dans un système asymétrique.

Environnement de confiance Par définition, un **environnement de confiance** désigne l'environnement dans lequel est exploitée une clé d'un système cryptographique.

- La notion d'environnement de confiance définie ici est volontairement très générale. Une application cryptographique va forcément disposer au moins d'un environnement de confiance, de même que les différentes entités d'un système de gestion de clés. La forme physique de ces environnements peut être quelconque.
- Il est naturel d'imaginer que l'environnement de confiance est sécurisé. Toutefois, il peut exister des systèmes où l'environnement de confiance n'est pas sécurisé techniquement. Inversement, un équipement peut être sécurisé sans être de confiance. Le fait d'utiliser des clés cryptographiques implique obligatoirement que pour le niveau de sécurité visé, l'environnement d'utilisation est « suffisamment » de confiance, car cet environnement ayant accès aux clés cryptographiques peut les exploiter.
- Même si ne sont exploitées que des clés publiques, l'environnement qui les utilise doit être de confiance. En effet, si on prend l'exemple d'un outil de vérification de certificats de clés publiques, il ne va utiliser que des clés publiques permettant la vérification de la chaîne de certificats. Pour autant, il est indispensable pour la sécurité du système que cet outil de vérification soit de confiance et que le stockage des clés publiques qu'il utilise protège ces dernières en authenticité et en intégrité.

Tiers de confiance Par définition, un **tiers de confiance** désignera toute entité qui effectue pour le compte d'utilisateurs finaux des opérations critiques pour la sécurité des clés. Dans ce document, un tiers de confiance est typiquement une autorité de certification d'une IGC. La confiance dans cette autorité est en effet indispensable à la sécurité.

1.2.2.2 Cryptographie symétrique

La sécurité des systèmes de cryptographie symétriques repose sur la confidentialité, l'authenticité et l'intégrité d'une ou plusieurs clés secrètes partagées entre deux ou plusieurs entités. Toute atteinte à ces objectifs de sécurité est une atteinte directe à une ou plusieurs des fonctions de sécurité utilisant le système

cryptographique.

1.2.2.3 Cryptographie asymétrique

La sécurité des systèmes de cryptographie asymétriques repose :

- Sur la confidentialité, l'authenticité et l'intégrité d'une ou plusieurs clés privées ;
- Sur l'authenticité et l'intégrité des clés publiques utilisées.

Toute atteinte à ces objectifs de sécurité est une atteinte directe à une ou plusieurs des fonctions de sécurité utilisant le système cryptographique.

Disons tout de suite que les objectifs d'authenticité et d'intégrité des clés publiques sont tout aussi importants et difficiles à réaliser que l'objectif de confidentialité d'une clé privée ou secrète.

1.2.2.4 Disponibilité

Outre ces objectifs liés à la nature cryptographique des mécanismes utilisés, le bon fonctionnement du système nécessite avant toute chose la disponibilité des clés. Ce point peut s'avérer déterminant dans beaucoup d'aspects de la conception d'une architecture de gestion de clés.

1.3 Typologie des architectures de gestion de clés

1.3.1 Cycle de vie des clés cryptographiques

1.3.1.1 Demande de clé

Avant tout, une clé cryptographique n'est générée que suite à une demande, implicite ou explicite, qui permet d'identifier le début du cycle de vie d'une clé. Cette demande peut, dans certains cas, donner lieu à une formalisation utile au suivi de la clé dans son cycle de vie.

1.3.1.2 Génération

L'opération de génération de clés dépend des algorithmes cryptographiques utilisés. Dans tous les cas, une expertise cryptographique est indispensable à la validation de ce processus, crucial pour remplir les objectifs de sécurité énoncés ci-dessus. Les règles de l'état de l'art en matière de génération de clés pour un algorithme donné et de génération d'aléa ne sont toutefois pas l'objet de ce document.

Génération centralisée La génération de clés peut être effectuée de façon centralisée. Dans ce cas, l'utilisateur final fait confiance à un tiers pour la génération de ses éléments secrets et privés. Dans certains contextes, la génération de clés fait aussi apparaître la fabrication ou la personnalisation d'éléments matériels. Dans la suite deux cas seront distingués :

- La génération centralisée de clé aléatoire consiste à utiliser un générateur d'aléa pour fabriquer selon un procédé cryptographique les clés secrètes ou privées ;
- La dérivation de clé à partir d'une clé maître consiste à utiliser un procédé cryptographique pour obtenir à partir d'une clé dite maître et d'éléments publics d'identification de l'utilisateur final une clé secrète ou privée.

Génération locale La génération de clé peut aussi être effectuée de façon privative lorsque la génération intervient localement au niveau de l'utilisateur final. La génération peut être effectuée directement au sein de l'environnement de confiance. Il peut aussi y avoir injection de clé sous le contrôle de l'utilisateur local. Dans ce dernier cas, la génération de clé est supposée contrôlée par l'utilisateur local et sort du périmètre de

ce document. Dans la suite trois cas seront distingués :

- La génération locale de clé aléatoire consiste à utiliser localement un générateur d'aléa pour fabriquer selon un procédé cryptographique les clés secrètes ou privées ;
- La différentiation locale de clé consiste à utiliser un procédé cryptographique pour obtenir à partir d'une clé privée ou secrète locale et d'éléments de différenciation une autre clé secrète ou privée, généralement destinée à un usage différent ;
- L'échange de clé consiste, lors de l'ouverture d'une session entre deux ou plusieurs intervenants, à utiliser un protocole cryptographique dédié pour élaborer une clé secrète commune aux intervenants.

1.3.1.3 Affectation

Une fois une clé cryptographique générée, son admission dans le système d'information est une opération cruciale en termes de sécurité. C'est cette opération qui associe à une valeur numérique l'identité de l'utilisateur, de l'entité, du flux d'information, etc. auquel elle est affectée ainsi que l'usage qui lui est dévolu (signature, chiffrement, échange de clé, etc.). Cette opération existe que la cryptographie utilisée soit asymétrique ou non ; elle prend toutefois selon les systèmes des formes différentes. On peut définir cette opération comme celle qui fait passer une valeur numérique du statut de donnée brute au statut de clé cryptographique dans un système.

Il ne faut pas confondre l'affectation avec l'injection d'une clé dans un équipement. Cette dernière opération est associée dans ce document à l'étape d'introduction de la clé affectée dans le système applicatif (cf. section 1.3.1.4).

L'opération d'affectation prend en outre un aspect encore plus crucial lorsqu'il s'agit de la première admission dans le système. Pour distinguer ce cas de figure, on parlera dans ce document du **premier enrôlement** d'un utilisateur ou d'un équipement dans un système. En effet, dans ce cas, la sécurité de l'opération ne peut résulter que de procédés non cryptographiques, de nature physique et organisationnels. C'est lors de ce premier enrôlement que seront affectés à l'utilisateur ou à l'équipement les premiers éléments cryptographiques permettant ultérieurement de le reconnaître de façon sûre et de lui affecter de nouvelles clés.

1.3.1.4 Introduction

Un autre aspect de la gestion d'une clé consiste à l'introduire physiquement ou logiquement dans l'ensemble du système applicatif une fois que son rôle a été correctement défini. Cet aspect recouvre la distribution et le transport de la clé jusqu'à l'utilisateur ou à l'équipement, puis son injection éventuelle dans l'environnement de confiance de l'utilisateur ou de l'équipement.

L'introduction est l'opération qui fait passer la clé affectée du système de gestion de clés proprement dit au système applicatif qui va l'utiliser.

1.3.1.5 Utilisation

De par leur nature même, les éléments privés ou secrets ne peuvent être employés que dans un environnement de confiance. Cet environnement est en effet responsable du stockage des clés et de leur bonne gestion pendant la durée où elles sont utilisées. Il peut en découler notamment des exigences quant à la protection de l'environnement de confiance applicatif.

1.3.1.6 Fin de vie

La fin de vie d'une clé cryptographique donne lieu à une révocation, un retrait, voire une destruction. Ces

opérations existent que la cryptographie utilisée soit asymétrique ou non.

Révoquer une clé n'est pas synonyme de retrait en ce sens qu'une clé peut avoir été révoquée et continuer d'être utilisée pour des opérations de vérification ou de compatibilité ascendante. De même le retrait ne signifie pas forcément que la clé ne sera plus jamais utilisée : elle peut être archivée pour permettre, par exemple, de mener une enquête postérieurement à son retrait.

1.3.1.7 Renouvellement

Le renouvellement d'une clé cryptographique est un processus à prévoir dès la conception d'un système d'information. Là encore cette opération existe que la cryptographie utilisée soit asymétrique ou non. Ce renouvellement peut intervenir de façon normale ou provoquée par des événements fortuits comme une compromission.

1.3.1.8 Recouvrement

Le recouvrement de clé est une opération qui peut avoir pour objectif d'assurer la disponibilité d'un service ou de répondre à des exigences légales. Ce type de fonctionnalité est d'autant plus difficile à mettre en œuvre que ses objectifs sont par nature contraires aux objectifs de sécurité visés par ailleurs. La définition précise de la fonctionnalité visée est indispensable de même qu'une expertise cryptographique globale.

L'expertise cryptographique est indispensable car dans certains cas, un simple archivage des clés ne répond pas à l'objectif de recouvrement opérationnel du fait des propriétés des protocoles cryptographiques. Par exemple, dans un protocole d'échange de clé de type Diffie–Hellman aléatoire, l'ensemble des données échangées dans le protocole sont publiques et le secret utilisé lors de la session est à usage unique et n'est pas conservé au-delà de son temps d'utilisation. La connaissance de l'ensemble des échanges et des clés privées n'est d'aucune utilité pour retrouver le secret aléatoire choisi.

1.3.2 Architectures fonctionnelles des systèmes utilisateurs

1.3.2.1 Architecture répartie

Dans une architecture répartie (voir figure 1), chaque utilisateur final est susceptible d'entrer en relation de façon cryptographiquement sécurisée avec tous les autres utilisateurs finaux du système d'information. Potentiellement, si le système comprend *N* utilisateurs, alors il existe *N(N - 1)/2* flux d'information à protéger.

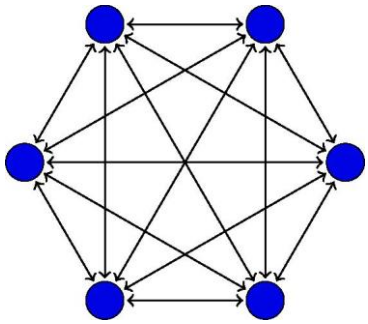


Figure 1 – Architecture fonctionnelle répartie

1.3.2.2 Architecture centralisée

Dans une architecture centralisée (voir figure 2), les utilisateurs finaux sont susceptibles de n'entrer en relation qu'avec un ou plusieurs utilisateurs centraux identifiés. Si le système d'information comprend *n* utilisateurs centraux et *N* utilisateurs, alors il existe *nN* flux d'information potentiels à protéger. En règle générale, *n* est très inférieur à *N*.

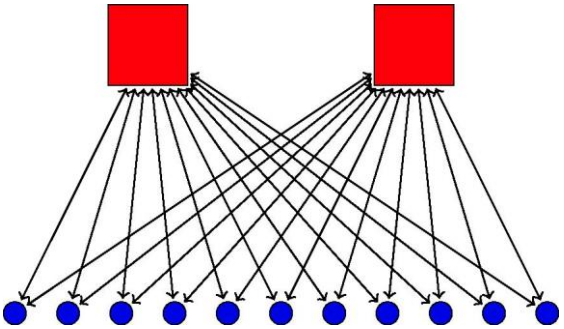


Figure 2 – Architecture fonctionnelle centralisée

1.3.3 Exemples illustratifs

1.3.3.1 Exemples d'architectures fonctionnelles

Un exemple typique d'architecture répartie est la messagerie sécurisée de bout en bout. Dans ce cas, chaque utilisateur du système peut envoyer un message à chacun des utilisateurs. Mais on observe ce même type d'architecture lorsque deux téléphones chiffrants ou deux chiffreurs IP sont amenés à communiquer.

Un exemple caractéristique d'architecture centralisée est la gestion de moyens de paiement. Dans ce cas, l'utilisateur final n'interagit qu'avec sa banque et n'a pas d'échanges directs avec un autre utilisateur final.

Bien entendu, les systèmes réels offrent souvent des situations intermédiaires entre ces deux architectures.

Il convient en outre de ne pas confondre ici une architecture fonctionnelle centralisée avec une génération de clés centralisées. En toute rigueur, ces deux problématiques sont indépendantes, même si dans la pratique, on utilisera souvent une génération de clés centralisée dans une architecture fonctionnelle centralisée. La réciproque n'est pas vraie. On trouve très souvent, notamment dans les infrastructures de gestion de clés, des générations de clés centralisées utilisées, par exemple, dans une messagerie typique des architectures fonctionnelles réparties.

1.3.3.2 Exemples de cycles de vie possibles

Les exemples ci-dessous se veulent purement illustratifs des notions définies ci-dessus. Ils ne présentent qu'une instanciation possible parmi la multitude des cycles de vie possibles dans chaque cas. Ils ne constituent en aucun cas une recommandation de réalisation.

Infrastructure de gestion de clés Une infrastructure de gestion de clés offre principalement un service à une application cliente qui a besoin de clés cryptographiques pour fonctionner. En oubliant les clés propres aux services de l'IGC, le cycle de vie d'une clé d'utilisateur de l'application cliente pourrait être par exemple le suivant :

1. La demande de clé intervient auprès d'une autorité d'enregistrement.
2. La génération de la clé peut être locale, par exemple réalisée par un butineur ou une carte à puce.
3. Le premier enrôlement se fait auprès d'une autorité d'enregistrement.
4. Les affectations de clés ultérieures peuvent être effectuées en ligne. Comme la génération est supposée locale dans notre exemple, l'introduction de la clé dans le système consiste uniquement en la certification de la clé.
5. Si l'application cliente est un contrôle d'accès, alors la clé est utilisée à chaque établissement d'une session sécurisée.

6. L'expiration du certificat, ou sa révocation à la demande de l'utilisateur ou sur compromission sont autant de cas de fin de vie de la clé.
7. La demande de renouvellement intervient à nouveau auprès de l'autorité d'enregistrement.
8. Enfin, le séquestre de clé peut être un service de recouvrement offert à l'utilisateur.

Système de paiement Dans un système applicatif de paiement, le cycle de vie d'une clé du porteur de moyen de paiement peut être décrit par exemple comme suit :

1. La demande de clé se fait généralement sous la forme d'une demande de support électronique de paiement auprès de son guichet bancaire.
2. La génération de la clé intervient au moment de la personnalisation de la carte bancaire, de façon centralisée.
3. L'affectation de la clé intervient au même moment.
4. L'introduction de la clé dans le système se fait lors de la délivrance de la carte ou à l'aide d'un mécanisme d'activation téléphonique si l'organisme bancaire n'a pas de guichet.
5. L'utilisation de la clé est effective à chaque transaction financière.
6. La date de fin de validité de la carte ne constitue pas la fin de vie de la clé. Celle-ci peut ou non être reconduite dans la carte renouvelée. Par ailleurs, une carte volée est listée pour éviter sa possible utilisation frauduleuse, ce qui constitue un autre cas de fin de vie.
7. En cas de perte de carte, la clé est renouvelée lors du changement de carte.
8. Il n'y a pas à proprement parler de fonctionnalité de recouvrement.

Sécurité locale d'un poste de travail. Pour la sécurisation locale d'un poste de travail, le cycle de vie de la clé de sécurisation du poste peut par exemple être décrit succinctement de la façon suivante :

1. La demande de clé est effectuée par un administrateur qui souhaite donner des droits d'accès à un utilisateur.
2. La génération est locale au poste de travail et ne sert qu'à la protection de celui-ci.
3. L'affectation se fait localement en liaison avec la définition des droits d'accès du poste.
4. L'introduction de la clé intervient, par exemple, au moment du chiffrement du disque dur.
5. L'utilisation de la clé est permanente au cours de l'utilisation du poste de travail.
6. La fin de vie de la clé correspond à un reformatage ou à un transchiffrement du disque dur.
7. Lors du changement d'utilisateur, la clé de chiffrement est changée pour garantir que le nouvel utilisateur d'un matériel n'a pas accès aux données de son prédécesseur.
8. Il est enfin généralement fortement souhaitable que la clé de chiffrement du disque soit sauvegardée et accessible à un administrateur désigné pour pallier la perte de la clé utilisateur, mais la procédure d'accès à cette clé peut aussi être interdite à l'administrateur informatique et réservée à un rôle particulier.

2 Règles et recommandations

Dans toute la suite, des règles et recommandations minimales sont définies pour des systèmes de gestion de clés. Par raccourci, le terme de clé conforme au référentiel sera employé lorsque ceci ne prêtera pas à confusion.

2.1 Règles et recommandations générales

L'utilisation d'une clé cryptographique doit obligatoirement se faire dans un environnement de confiance. Que la clé soit publique, privée ou secrète, les objectifs de sécurité sur l'utilisation de celle-ci sont tels que toute atteinte à ces objectifs de sécurité remet en cause les fonctions de sécurité remplies par l'usage de la cryptographie. Ces objectifs ont été rappelés en section 1.2.2.

L'impact d'une clé doit dans tous les cas être étudié. Il s'agit, pour un système donné, de mesurer l'impact de l'atteinte à l'un des objectifs de sécurité ci-dessus. Ceci ne doit pas se confondre avec l'analyse du risque de compromission. Il s'agit bien d'estimer, sous l'hypothèse que la compromission ou l'atteinte à l'intégrité de la clé a eu lieu, les conséquences pour le système cryptographique. C'est sur cette étude d'impact que l'analyse de risque peut ensuite s'appuyer pour estimer la robustesse du système.

Dans beaucoup de systèmes cryptographiques, notamment ceux faisant intervenir des tiers de confiance, il existe une ou plusieurs clés dont la compromission ou l'atteinte à l'intégrité peut entraîner des atteintes aux objectifs de sécurité de tout ou d'une grande partie des acteurs du système. Il s'agit par exemple des clés maîtres d'un système de dérivation de clé, d'une clé de réseau ou de la clé privée d'une autorité de certification. Une telle clé sera qualifiée de clé présentant un risque d'impact systémique ou de façon plus concise de clé à *risque systémique*.

RÈGLES ET RECOMMANDATIONS :

RègleImpact-1. Dans une architecture de gestion de clés l'impact de chaque clé du système doit être évalué.

Justification :

- L'expérience prouve qu'une étude systématique de l'impact de chaque clé apporte beaucoup pour l'amélioration de la robustesse du système.

RègleDurée-1. Dans une architecture de gestion de clés l'étude d'impact d'une clé doit prendre en compte les différentes durées associées à celle-ci.

Justifications :

- Les différentes durées d'une clé ont une grande importance en terme d'analyse de risque :
  - Durée d'utilisation de la clé : c'est la période pendant laquelle la clé est active.
  - Crypto-période : c'est la durée au-delà de laquelle la clé est renouvelée.
  - Durée d'impact de la clé : c'est la période pendant laquelle une compromission de la clé a un impact sur le système.
  - Durée d'archivage : pour certaines clés, notamment de confidentialité, c'est la période durant laquelle la clé doit être archivée pour une utilisation ponctuelle ultérieure.
- Généralement la durée d'impact d'une clé est supérieure à sa durée d'utilisation, elle-même

supérieure à sa crypto-période. L'estimation de ces différentes durées est l'un des éléments fondamentaux de l'étude d'impact.

- L'archivage des clés est dans un grand nombre de cas un besoin opérationnel, légal ou réglementaire. Les exigences quant à cet archivage dépendent fortement de l'étude d'impact.

RègleImpactSystémique-1. Dans une architecture de gestion de clés les procédures de récupération du système en cas d'atteinte à la confidentialité à l'intégrité ou à l'authenticité d'une clé présentant un risque d'impact systémique doivent être étudiées et documentées.

Justifications :

- Cette règle vise à sensibiliser les concepteurs au risque qu'il y aurait à faire reposer l'ensemble d'un système cryptographique sur une clé à risque systémique sans prévoir le cas où les objectifs de sécurité sur cette clé seraient remis en cause.
- Aucun dispositif purement technique n'est à même de protéger de façon satisfaisante une clé présentant un risque systémique.
- L'expérience prouve qu'une étude systématique de l'impact de chaque clé apporte beaucoup pour l'amélioration de la robustesse du système, notamment en identifiant justement les clés présentant un impact systémique.

RecomImpactSystémique-1. Dans une architecture de gestion de clés il est recommandé d'éviter d'avoir recours à des clés présentant un risque systémique.

Justifications :

- L'analyse d'impact peut conduire à proposer des solutions pour limiter l'impact de certaines clés ou organiser leur renouvellement de façon à éviter l'existence même de clés à risque systémique.
- Ceci n'est pas toujours possible : une clé racine dans une IGC par exemple présente toujours des risques systémiques.

2.2 Demande de clé

La demande de clé ne fait pas l'objet de règle ou de recommandation particulière. En effet, cette étape du cycle de vie est fortement tributaire du contexte opérationnel. On s'attachera toutefois à bien identifier cette étape et les procédures afférentes car c'est par leur correcte définition que pourront être satisfaites certaines des règles et des recommandations liées à l'affectation ultérieure des clés et relatives au contrôle de l'authenticité et de l'intégrité des clés.

2.3 Génération de clé

2.3.1 Génération locale de clé

2.3.1.1 Génération locale de clé aléatoire

RÈGLES ET RECOMMANDATIONS :

RègleAléaLocal-1. La génération locale d'une clé cryptographique aléatoire doit faire appel à un générateur d'aléa conforme au référentiel.

Justification :

- La génération d'aléa utilisée pour générer des clés cryptographiques doit avoir un niveau de qualité cohérent avec le niveau de sécurité recherché. Le document « Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques « édité par l'ANSSI contient d'ores et déjà un certain nombre de règles et de recommandations sur la génération d'aléa, notamment en matière de retraitement algorithmique.

2.3.1.2 Différentiation locale de clé

RÈGLES ET RECOMMANDATIONS :

RègleDifférentiation-1. La différentiation locale d'une clé cryptographique doit faire appel à un mécanisme cryptographique conforme au référentiel.

Justification :

- Le procédé cryptographique utilisé pour différencier localement une clé cryptographique doit avoir un niveau de qualité cohérent avec le niveau de sécurité recherché. Le document « Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques » édité par l'ANSSI contient d'ores et déjà un certain nombre de règles et de recommandations applicables.

2.3.1.3 Échange de clés

RÈGLES ET RECOMMANDATIONS :

RègleÉchangeClés-1. L'échange d'une clé cryptographique avec une entité homologue distante doit faire appel à un mécanisme cryptographique conforme au référentiel.

Justification :

- Le protocole cryptographique d'échange de clé utilisé doit avoir un niveau de qualité cohérent avec le niveau de sécurité recherché. Le document « Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques » édité par l'ANSSI contient d'ores et déjà un certain nombre de règles et de recommandations applicables.

2.3.2 Génération centralisée de clé

2.3.2.1 Génération centralisée de clé aléatoire

RÈGLES ET RECOMMANDATIONS :

RègleAléaCentral-1. La génération centralisée d'une clé cryptographique aléatoire doit faire appel à un générateur d'aléa conforme au référentiel.

Justification :

- La génération d'aléa utilisée pour générer des clés cryptographiques doit avoir un niveau de qualité cohérent avec le niveau de sécurité recherché.

RecomAléaCentral-1. Il est recommandé que la génération centralisée d'une clé cryptographique aléatoire fasse appel à un générateur d'aléa conforme au référentiel et respectant de plus l'ensemble des recommandations associées.

Justification :

- Le caractère centralisé de cette opération rend celle-ci d'autant plus cruciale car une attaque sur le générateur d'aléa pourrait permettre de remonter à l'intégralité des clés générées. Il convient donc de chercher à élever le niveau d'exigence au niveau de la génération centralisée.

RègleGénérationCentralisée-1. La génération centralisée d'une clé cryptographique aléatoire doit intervenir dans un environnement de confiance conforme au référentiel.

Justification :

- La qualité intrinsèque du générateur d'aléa ne suffit pas à elle seule à garantir la sécurité de la génération. L'ensemble du dispositif technique et organisationnel qui intègre le générateur d'aléa doit être analysé.

RecomGénérationCentralisée-1. Il est recommandé que la génération centralisée d'une clé cryptographique aléatoire intervienne dans un environnement de confiance conforme au référentiel et respectant de plus l'ensemble des recommandations associées.

Justification :

- Si une vulnérabilité intervient au niveau de la génération centralisée des clés, c'est l'ensemble du système applicatif qui peut être compromis. Il est donc naturel d'attacher un soin plus grand aux règles de sécurité relatives à cette génération centralisée.

2.3.2.2 Dérivation de clés

Un mécanisme de dérivation de clé vise à remplacer un mécanisme de génération de clé purement aléatoire par un procédé déterministe dépendant de l'identité de l'utilisateur final.

Ce type de procédé peut présenter des avantages, notamment dans une architecture applicative centralisée utilisant des mécanismes cryptographiques symétriques. Il permet dans ce cas de réduire le besoin de stockage sécurisé des n utilisateurs centraux qui, pour s'adresser à leurs *N* utilisateurs rattachés, n'ont à mémoriser qu'un secret maître au lieu de *N* secrets individuels d'utilisateurs.

Il permet aussi de faciliter l'organisation d'un service de recouvrement de clés, ce qui peut constituer un besoin opérationnel et fonctionnel.

Par contre, la compromission d'une clé maître, qui permet à un attaquant potentiel de retrouver l'ensemble des clés dérivées à partir de cette clé, constitue un risque majeur pour ce type de procédé.

RÈGLES ET RECOMMANDATIONS :

RègleDérivation-1. La clé maître d'un mécanisme de dérivation de clé doit être exploitée dans un environnement de confiance conforme au référentiel.

RecomDérivation-1. Il est recommandé que la clé maître d'un mécanisme de dérivation de clé soit exploitée dans un environnement de confiance conforme au référentiel et respectant de plus l'ensemble des recommandations associées.

RecomDérivation-2. Les mécanismes de dérivation de clé ne devraient être utilisés que dans des architectures applicatives centralisées.

Justifications :

- Comme pour la génération de clé aléatoire centralisée les mécanismes de dérivation de clé présentent un risque systémique. La règle et la recommandation sont donc cohérentes avec celles de la génération centralisée.
- L'utilisation d'un mécanisme de dérivation de clés apporte un risque supplémentaire lié à sa cryptanalyse possible. Il est donc recommandé de n'utiliser ce type de mécanisme que si les objectifs de sécurité visés ne sont pas facilement atteignables par d'autres moyens. Dans le cas d'architectures applicatives réparties, il semble au contraire beaucoup plus aisé d'éviter le recours à des mécanismes de dérivation.

2.3.3 Génération de clé de signature

L'usage de signature implique le souhait d'assurer un objectif de non-répudiation directement au niveau cryptographique. Cet objectif est délicat à atteindre par des moyens purement techniques. On pourra donc avoir intérêt à viser un simple objectif d'authenticité et à le compléter par des mesures opérationnelles ou contractuelles.

Les règles et recommandations ci-dessous concernent la génération d'une clé destinée à un usage de signature. Elles complètent les règles et recommandations génériques proposées ci-dessus.

RÈGLES ET RECOMMANDATIONS :

RègleDérivationSignature-1. La génération d'une clé de signature ne doit pas faire intervenir de mécanisme de dérivation de clé.

Justification :

- La clé privée de signature doit être parfaitement maîtrisée par l'utilisateur pour que l'objectif de non répudiation puisse être atteint. Il ne doit pas être fait usage d'un mécanisme de dérivation de clé puisque la connaissance de la clé maître permet d'usurper l'identité de tout utilisateur.

RecomGénérationAléatoireSignature-1. Il est recommandé que la génération d'une clé de signature aléatoire soit effectuée directement par l'utilisateur final dans son environnement de confiance.

RecomGénérationAléatoireSignature-2. Il est recommandé que la génération d'une clé de signature aléatoire fasse intervenir de l'aléa provenant d'une source maîtrisée par l'utilisateur final.

Justifications :

- Il est naturel que la génération d'une clé de signature soit locale. Toutefois, il peut être acceptable de générer cette clé de façon centralisée par un tiers de confiance.
- L'utilisation dans le processus de génération de l'aléa d'éléments fournis par l'utilisateur (mouvements de souris, frappes clavier, etc.) réduit les risques de possibilité de répudiation liés à une faiblesse éventuelle de la qualité de l'aléa utilisé.
- L'utilisation d'un dispositif technique évalué fournissant de l'aléa est envisageable. Toutefois, s'agissant d'une clé de signature, le fait d'y ajouter des éléments provenant de l'utilisateur contredit l'argument consistant à prétendre que le générateur d'aléa utilisé pourrait avoir reproduit la clé générée dans un autre contexte.

2.4 Affectation d'une clé

L'affectation d'une clé cryptographique dans un système applicatif est une opération qui est souvent mal comprise dans ses impacts en matière de sécurité. C'est cette opération qui occasionne le plus de problèmes notamment en termes d'initialisation. En effet, la problématique de premier enrôlement conduit souvent à un problème de « poule et d'œuf » : comment m'enrôler dans un système de façon sûre, alors que ce système ne me connaît pas.

L'affectation vise à garantir, pour les autres utilisateurs du système applicatif, que la clé générée est :

- D'une part bien définie dans son rôle à l'égard du système ;
- D'autre part bien associée à l'identité de son utilisateur final, qu'il soit personne ou entité automatique du système.

L'opération varie notablement en fonction de l'existence ou non d'un tiers de confiance.

2.4.1 Usage d'une clé cryptographique

La cryptographie peut être employée pour réaliser beaucoup de fonctions de sécurité de natures différentes. Dans ce document les usages de clés suivants seront distingués :

- Chiffrement : c'est l'usage le plus connu des algorithmes cryptographiques, visant à répondre à un objectif de confidentialité (par exemple **AES** en mode **CBC**) ;
- Intégrité : c'est un usage spécifique de la cryptographie symétrique visant à garantir qu'un message n'a pas été modifié (par exemple **CBC-MAC** surchiffré) ;
- Authentification : c'est un usage visant à garantir l'identité d'une personne ou d'un équipement par un mécanisme cryptographique insensible au rejeu ;
- Signature : c'est un usage spécifique de la cryptographie asymétrique visant à répondre à un triple objectif d'intégrité d'un message, d'authentification de son émetteur et garantissant la non-répudiation (par exemple **ECDSA** et **ECKCDSA**) ;
- Transfert de clé : c'est un usage visant à transmettre de façon confidentielle une clé cryptographique utilisée dans un autre contexte, mais sans que l'authenticité soit nécessaire (par exemple chiffrement **CBC** par une clé secrète de chiffrement de clé) ;
- Échange de clé : c'est un usage visant à s'accorder de façon confidentielle sur une clé cryptographique utilisée dans un autre contexte, sans que l'authenticité soit nécessaire (par exemple Diffie–Hellman) ;
- Dérivation de clé : c'est un usage visant à obtenir pour un ensemble d'utilisateurs, à partir d'une clé maître et d'un élément d'identité d'un utilisateur, une clé privée ou secrète spécifique de ce dernier ;
- Différentiation locale de clé : c'est un usage visant à obtenir, à partir d'une clé privée ou secrète et d'éléments complémentaires, une ou plusieurs clés privées ou secrètes destinées à des usages différents ;
- Source d'aléa : c'est l'usage consistant à introduire dans un générateur pseudo-aléatoire, une quantité d'information secrète aléatoire permettant de différencier ce générateur pour chaque équipement et de l'utiliser, bien qu'il reste purement déterministe, comme un générateur d'aléa.

L'usage d'une clé peut parfois être difficile à caractériser. Il semble toutefois, que l'on peut toujours se ramener aux cas ci-dessus. Il convient toutefois de ne pas confondre l'usage des clés et les services de sécurité

qu'elles rendent.

Par exemple, dans un défi Diffie–Hellman signé par une clé **RSA** le service rendu est un échange de clé authentifié. On peut toutefois distinguer l'élément d'aléa dont découle le challenge (qui est rarement désigné comme clé mais qui reste un élément secret) dont l'usage est de type *transfert de clé* et la clé **RSA** dont l'usage est de type *signature*.

RÈGLES ET RECOMMANDATIONS :

RègleUsage-1. L'usage d'une clé doit être unique[119].

Justifications :

- L'emploi d'une même clé à plus d'un usage, par exemple pour chiffrer avec un mécanisme de confidentialité et assurer l'intégrité avec un mécanisme différent, est source de nombreuses erreurs. Ceci n'interdit cependant pas de dériver deux clés à partir d'une même clé source à condition que le mécanisme de dérivation soit conforme au référentiel, ni de mettre en place un mécanisme de chiffrement authentifié où chiffrement et authentification sont assurés par un unique mécanisme qui a été spécialement conçu pour une telle utilisation et non par deux mécanismes distincts.
- L'emploi d'une même bi-clé à plus d'un usage, par exemple pour chiffrer et signer, est aussi une grave source d'erreurs.

2.4.2 Objectifs de sécurité de l'affectation

L'objectif intrinsèque à l'affectation d'une clé cryptographique à un utilisateur ou à un équipement est celui d'authenticité qui se décline en deux aspects :

- Garantir à l'utilisateur ou à l'équipement l'authenticité de la clé qui lui est proposée ;
- Garantir pour le système, la possession effective de la clé par l'utilisateur ou l'équipement auquel elle est affectée.

RÈGLES ET RECOMMANDATIONS :

RègleAffectation-1. Les mécanismes cryptographiques utilisés lors de l'affectation d'une clé cryptographique à un utilisateur ou à un équipement donné doivent être conformes au référentiel. Ces mécanismes doivent garantir la confidentialité, l'intégrité et l'authenticité de la clé.

Justifications :

- Cette règle n'est applicable que pour les affectations postérieures au premier enrôlement effectué.
- Au cours du premier enrôlement, la (les) clé(s) affectées(s) lors de cette étape d'initialisation devra(ont) ensuite servir conformément à son (leurs) usage(s) identifié(s) pour garantir dans les affectations ultérieures de nouvelles clés les objectifs de sécurité requis.

[119] Afin de ne pas freiner la mise en place de solutions sécurisées dans les systèmes d'information de l'administration, il est possible que le corps du RGS, ainsi que ses annexes A, définissent des exceptions ponctuelles à cette règle.

- Il est naturel que les mécanismes cryptographiques utilisés soient conformes au référentiel tout comme les clés qu'ils protègent.

RecomAffectation-1. Il est recommandé que les mécanismes cryptographiques utilisés lors de l'affectation d'une clé cryptographique à un utilisateur ou à un équipement donné garantissent la possession de la clé par l'utilisateur ou l'équipement auquel elle est affectée.

Justifications :

- Il est considéré que l'objectif de confidentialité sur la clé peut constituer un élément de preuve implicite de possession puisque seul l'utilisateur ou l'équipement destinataire est susceptible de disposer de la clé. Toutefois, il est préférable de disposer d'une preuve explicite de cette possession avant de considérer la clé comme affectée.
- Ne pas vérifier la possession de la clé lors de l'affectation présente des risques car dès que la clé est affectée, les autres entités du système peuvent commencer à l'utiliser. Il peut donc y avoir des atteintes à la disponibilité, par exemple si le message envoyé n'est pas déchiffrable par le destinataire. Il peut aussi y avoir des atteintes en confidentialité, par exemple si un attaquant empêche l'acheminement d'une nouvelle clé pour obliger un utilisateur ou un équipement à continuer d'utiliser une clé qu'il s'est procuré.

2.4.3 Objectifs sur le premier enrôlement

Seul le premier enrôlement d'un utilisateur ou d'un équipement dans le système est maintenant considéré. Une fois cet enrôlement réalisé, il est considéré que les utilisateurs ou équipements finaux disposent des moyens cryptographiques permettant d'effectuer des affectations de clés ultérieures.

Les objectifs du premier enrôlement restent identiques et visent à garantir :

- L'authenticité de la clé proposée ;
- La possession de la clé par l'utilisateur.

Ces objectifs ne peuvent toutefois être remplis que par des mesures largement organisationnelles puisque les équipements en présence ne sont pas à la clé.

Techniquement, ce premier enrôlement va donc, par exemple, consister en l'introduction d'une clé de base dans un équipement. Cette clé d'initialisation cryptographique servira ensuite à protéger les échanges liés à l'affectation d'autres clés dans le système. C'est la raison pour laquelle le premier enrôlement revêt une importance cruciale, car c'est le seul qui ne peut pas reposer sur des moyens cryptographiques de protection et c'est pourtant celui sur lequel reposera dans beaucoup de cas la sécurité des affectations ultérieures.

Mais il peut aussi ne pas y avoir d'affectation ultérieure : dans l'exemple de système de paiement de la section 1.3.3.2, la personnalisation est effectuée une fois pour la durée de vie de la carte et ce sont des mesures organisationnelles qui garantissent que c'est le bon usager qui reçoit sa carte et donc sa clé.

Remarque :

- Les règles et recommandations relatives à ce premier enrôlement dépendent du mode de génération de la clé affectée. Pour alléger la rédaction il sera par exemple question de *premier enrôlement d'une clé générée localement* pour désigner *l'affectation d'une clé générée localement lors du premier enrôlement de l'utilisateur ou de l'équipement auquel elle est affectée.*

2.4.3.1 Premier enrôlement d'une clé générée localement

Premier enrôlement d'une clé générée localement sans tiers de confiance

RÈGLES ET RECOMMANDATIONS :

RègleEnrôlementPrivatif-1. Lors de son premier enrôlement, l'utilisateur final d'un système doit proposer à ses interlocuteurs un moyen de contrôler son identité, l'authenticité de la clé qu'il cherche à s'affecter et le fait qu'il possède bien cette clé.

Justification :

- Dans le cadre d'un premier enrôlement sans tiers de confiance, il est indispensable que les interlocuteurs échangent des moyens de contrôle de leurs identités respectives et de l'association de ces identités avec les clés échangées. Il est aussi nécessaire de s'assurer de la possession de la clé.

Remarques :

- À titre d'exemple, pour un premier enrôlement de clés de messagerie via l'internet, on peut imaginer utiliser le haché (souvent appelé empreinte) d'une clé publique et utiliser l'un des moyens suivants :
  - Le publier sur son site personnel ;
  - L'envoyer par SMS (l'authentification découlant alors de la connaissance ou non du numéro de téléphone de l'appelant) ;
  - L'envoyer par courrier signé (l'authentification résultant de la signature manuscrite).
- La signature de la clé publique par la clé privée (auto-signature) ne constitue un élément de preuve de la possession de la clé que si la donnée signée dépend bien de l'interlocuteur. Dans le cas contraire, le rejeu est toujours possible.

RecomContrôleIndépendant-1. Dans un système, il est recommandé que le moyen de contrôle proposé par l'utilisateur final lors de son premier enrôlement soit véhiculé de façon indépendante de sa clé.

Justification :

- Il n'est pas souhaitable d'interdire l'enrôlement à distance dans un système. Sur l'exemple ci-dessus, des trois moyens proposés, seuls les deux derniers peuvent être considérés comme indépendants.

Premier enrôlement d'une clé générée localement auprès d'un tiers de confiance Il convient tout d'abord de noter que cette situation n'a de sens que dans le cas d'une infrastructure de gestion de clés (IGC), c'est-à-dire d'un système cryptographique asymétrique. En effet, dans un tel système la clé privée de l'utilisateur n'a pas besoin d'être communiquée au tiers de confiance et ne sort donc pas de l'environnement de confiance de l'utilisateur. Au contraire, pour un système symétrique, générer une clé de façon locale et l'affecter à un usage et une identité auprès d'un tiers de confiance va consister à l'acheminer vers ce dernier. On obtiendra au final une situation similaire à celle d'une génération de clé symétrique centralisée après acheminement de la clé vers son utilisateur final puisque les deux parties auront un secret partagé. Cette situation finale similaire aurait toutefois été obtenue de façon aberrante par une génération de la clé symétrique au niveau local.

L'utilisateur final qui a généré sa clé localement dans son environnement de confiance doit, préalablement à l'affectation de sa clé par le tiers de confiance, prouver à ce dernier :

- L'authenticité de la clé publique qu'il propose ;

- Qu'il est bien en possession de la clé privée correspondante.

Pour cela, il est nécessaire que l'identité de l'utilisateur soit déjà connue du tiers de confiance.

RÈGLES ET RECOMMANDATIONS :

RègleEnrôlementIGC-1. Dans un système avec tiers de confiance, pour assurer le premier enrôlement d'une clé générée localement, le tiers de confiance doit disposer d'un moyen de contrôler l'identité de l'utilisateur final, l'authenticité de sa clé et le fait qu'il possède bien cette clé. L'utilisateur final doit disposer de même d'un moyen de contrôler l'authenticité des éléments publics de l'IGC.

Justifications :

- Cette règle est similaire à celle de l'enrôlement privatif. Toutefois, l'introduction d'un tiers de confiance rend la relation entre les deux parties dissymétriques au contraire de celle d'un enrôlement privatif où les deux parties sont des utilisateurs finaux.
- Un mécanisme de contrôle de l'identité annoncée par l'utilisateur doit être présent. Comme il s'agit du premier enrôlement, ce mécanisme est de nature non cryptographique. Par exemple, on peut utiliser un précédent enrôlement dans un autre système connu du tiers de confiance (numéro de téléphone, numéro GSM, etc.) pour acheminer l'empreinte de la clé affectée à un usage et une identité donnée. L'objectif de sécurité est là encore d'éviter les attaques par le milieu sur le processus d'enrôlement à distance.
- De même, l'utilisateur final doit être en mesure de contrôler l'authenticité du tiers de confiance. En l'occurrence, comme il s'agit d'une infrastructure de gestion de clés, il convient généralement d'être en mesure de contrôler par un moyen indépendant l'authenticité de la clé publique de l'autorité de certification racine. Ceci peut se faire, par exemple, par la publication de l'empreinte de cette clé par un moyen indépendant.

Remarque :

- Il est important notamment de ne pas reposer sur le seul mécanisme d'auto-signature du certificat de l'autorité racine. En effet, dans ce cas particulier, le fait que la clé soit auto-signée n'est pas une preuve d'authenticité mais un élément de preuve de possession de la clé privée. En effet, le certificat étant daté et signé, il n'est pas possible à un tiers de modifier la date du certificat ou les éléments de publication des listes de révocation sans invalider le certificat. Le mécanisme d'auto-signature est aussi important pour garantir l'intégrité de la donnée.

RecomContrôleIndépendant-1. Il est recommandé que le premier enrôlement auprès d'un tiers de confiance d'un utilisateur final générant localement sa clé utilise un moyen d'acheminement indépendant du processus d'enregistrement pour tous les éléments de contrôle de l'identité de l'utilisateur, de l'authenticité de la clé et de celle des éléments publics de l'IGC.

Justifications :

- Il n'est pas souhaitable d'interdire l'enrôlement à distance dans un système qui ne disposerait pas de moyen d'acheminement indépendant pour les éléments de contrôle de l'identité de l'utilisateur et de l'authenticité de la clé.
- Il convient toutefois de noter que dans le cas d'un processus d'enrôlement automatisé auprès d'un tiers de confiance, l'application de cette recommandation est fortement recommandée pour contrer la

menace d'attaque par le milieu.

2.4.3.2 Premier enrôlement d'une clé générée de façon centralisée

Premier enrôlement d'une clé générée de façon centralisée sans tiers de confiance Cette situation n'a pas de sens car le centre de génération de clés est de facto un tiers de confiance.

Premier enrôlement d'une clé générée de façon centralisée avec tiers de confiance

RÈGLES ET RECOMMANDATIONS :

RègleEnrôlementCentralSécuritéPhysique-1. Dans un système avec tiers de confiance, le premier enrôlement d'une clé générée de façon centralisée doit être réalisé dans un environnement de confiance et par un lien physique de confiance.

Justifications :

- La problématique du premier enrôlement d'une clé générée de façon centralisée est aussi celle de son acheminement. En effet, comme il s'agit du premier enrôlement, l'utilisateur final ne dispose pas de moyens cryptographiques lui permettant de déchiffrer cette première clé qui doit lui être envoyée.
- Par voie de conséquence, l'environnement de confiance de l'utilisateur final doit être au plus près d'une entité de confiance contrôlée par le tiers de confiance. On peut penser par exemple aux autorités d'enregistrement d'une IGC ou à un centre de personnalisation. L'injection de l'élément secret doit se faire par un lien physique de confiance. On notera que ceci implique un enrôlement en vis-à-vis avec l'entité de confiance qui émane du tiers de confiance.
- Cette règle vise à assurer le même niveau de sécurité que lors d'une génération locale de clé. Rappelons qu'il s'agit ici de réaliser le premier enrôlement, c'est-à-dire de fournir à l'utilisateur final les premiers éléments cryptographiques qui vont asseoir ultérieurement toute la sécurité du système de gestion de clés. Il est donc naturel de prendre à ce moment toutes les précautions nécessaires.

RègleEnrôlementCentral-1. Dans un système avec tiers de confiance, lors d'un premier enrôlement, le tiers de confiance doit disposer d'un moyen de contrôler l'identité de l'utilisateur final et l'utilisateur final doit avoir un moyen de vérifier l'authenticité de sa clé générée de façon centralisée par le tiers de confiance.

Justification :

- La sécurité physique de l'enrôlement ne diminue pas la nécessité de contrôle de l'identité de l'utilisateur et de l'authenticité de sa clé mais cette fois-ci c'est l'utilisateur final qui doit être en mesure de contrôler sa clé. Ce dernier point n'implique pas forcément des mesures techniques. En effet, la relation de confiance entre l'utilisateur final et son tiers de confiance, la procédure d'enrôlement en vis-à-vis, la mise à disposition d'un moyen cryptographique comme environnement de confiance sont autant de moyens pour l'utilisateur final de s'assurer de l'authenticité de son vis-à-vis.

Premier enrôlement d'une clé dérivée

RÈGLES ET RECOMMANDATIONS :

RègleEnrôlementDérivationSécuritéPhysique-1. Le premier enrôlement d'une clé générée par un processus de dérivation à partir d'une clé maître doit être réalisé dans un environnement de confiance et

par un lien physique de confiance.

Justifications :

- La problématique du premier enrôlement d'une clé dérivée est la même que celle d'une clé générée de façon centralisée. En effet, l'objet de la dérivation de clé n'est pas d'introduire dans l'environnement de confiance de l'utilisateur la clé maître de la dérivation, mais bien sa clé dérivée.
- Comme il s'agit du premier enrôlement, l'utilisateur final ne dispose pas de moyens cryptographiques lui permettant de déchiffrer cette première clé. Cette dernière doit donc être introduite au plus près d'une entité de confiance contrôlée par le tiers de confiance, ce qui implique un enrôlement en vis-à-vis avec cette entité.
- Cette règle vise à assurer le même niveau de sécurité que lors d'une génération locale de clé. Rappelons qu'il s'agit ici de réaliser le premier enrôlement, c'est-à- dire de fournir à l'utilisateur final les premiers éléments cryptographiques qui vont asseoir ultérieurement toute la sécurité du système de gestion de clés. Il est donc naturel de prendre à ce moment toutes les précautions nécessaires.

RègleEnrôlementDérivation-1. Lors d'un premier enrôlement, le tiers de confiance doit disposer d'un moyen de contrôler l'identité de l'utilisateur final et l'utilisateur final doit avoir un moyen de vérifier l'authenticité de sa clé générée par dérivation d'une clé maître contrôlée par le tiers de confiance.

Justification :

- La problématique du premier enrôlement d'une clé dérivée est la même que celle d'une clé générée de façon centralisée.

2.5 Introduction d'une clé

2.5.1 Acheminement de clé

La problématique d'acheminement d'une clé intervient par exemple lors d'une génération centralisée ou d'une génération par un procédé de dérivation à partir d'une clé maître.

L'acheminement des éléments de premier enrôlement pour lesquels la protection ne peut s'appuyer sur des mécanismes cryptographiques n'est pas envisagé ici. Cette opération de premier enrôlement a été envisagée en section 2.4.3.

L'acheminement de clé peut aussi intervenir dans un processus de génération locale d'une clé secrète, par exemple au cours d'un processus d'échange de clé. Il est considéré dans ce cas que le processus d'échange de clé est du niveau applicatif et ne fait pas partie de la gestion des clés. Il n'en demeure pas moins que les objectifs de sécurité sur ce mécanisme sont tout à fait similaires à ceux de l'acheminement d'une clé aléatoire générée de façon centralisée.

2.5.1.1 Acheminement de clé aléatoire générée de façon centralisée

RÈGLES ET RECOMMANDATIONS :

RègleAcheminemementCléCentral-1. L'acheminement jusqu'à l'utilisateur final d'une clé cryptographique générée aléatoirement de façon centralisée doit bénéficier de moyens de protection conformes au référentiel. Ces moyens doivent garantir l'authenticité, l'intégrité et la confidentialité de la clé acheminée.

Justification :

- Lorsqu'une clé est générée de façon centralisée, il faut, une fois la clé générée, pouvoir l'acheminer de façon protégée jusqu'à l'utilisateur final. Ceci suppose, soit des moyens organisationnels, soit la présence dans le système d'un mécanisme spécifique ayant ses propres clés et mécanismes cryptographiques et destiné à protéger cet acheminement. Ce dernier doit avoir un niveau de sécurité cohérent avec celui recherché pour la clé.

RecomAcheminementNoirCentralBout-en-bout-1. Il est recommandé que l'acheminement jusqu'à l'utilisateur final d'une clé cryptographique générée aléatoirement de façon centralisée soit protégé cryptographiquement de bout en bout en authenticité, intégrité et confidentialité par des mécanismes de protection conformes au référentiel.

Justification :

- Il est recommandé que cet acheminement soit protégé de bout en bout, de façon cryptographique, c'est-à-dire que le système de génération de clé protège la clé générée de façon telle que seul le destinataire final, à l'exclusion de tout intermédiaire, puisse y avoir accès. On retrouve là le concept classique de clé noire de bout en bout. La clé cryptographique opérationnelle *rouge* ne devrait exister qu'au niveau de sa génération et de son utilisation. Cette recommandation ne s'applique pas, bien entendu, aux éléments de premier enrôlement pour lesquels la protection ne peut s'appuyer sur un mécanisme cryptographique.

2.5.1.2 Acheminement de clé générée par dérivation

RÈGLES ET RECOMMANDATIONS :

RègleAcheminememementCléDérivée-1. L'acheminement jusqu'à l'utilisateur final d'une clé cryptographique générée par un procédé de dérivation à partir d'une clé maître doit bénéficier de moyens de protection conformes au référentiels. Ces moyens doivent garantir l'authenticité, l'intégrité et la confidentialité de la clé acheminée.

RecomAcheminementNoirDérivéeBout-en-bout-1. Il est recommandé que l'acheminement jusqu'à l'utilisateur final d'une clé cryptographique générée par un procédé de dérivation à partir d'une clé maître soit protégé cryptographiquement de bout en bout en authenticité, intégrité et confidentialité par des mécanismes de protection conformes au référentiel.

Justification :

- La problématique d'acheminement est la même que la clé soit générée aléatoirement de façon centralisée ou dérivée à partir d'une clé maître. Cette recommandation ne s'applique pas, bien entendu, aux éléments de premier enrôlement pour lesquels la protection ne peut s'appuyer sur un mécanisme cryptographique.

2.5.2 Injection de clé

2.5.2.1 Injection de clé générée localement

Il peut sembler curieux d'envisager l'injection d'une clé générée localement. Toutefois, dans certains cas, la génération d'une clé peut être effectuée par l'utilisateur dans un environnement de confiance distinct de l'environnement de confiance applicatif.

Par exemple, un utilisateur averti pourrait employer un logiciel autonome pour générer sa clé privée de signature et vouloir ensuite l'injecter dans un logiciel de messagerie. Dans ce cas, la génération est locale mais l'environnement de confiance de l'utilisateur est scindé en deux parties relatives à la génération et à l'utilisation des clés.

RÈGLES ET RECOMMANDATIONS :

RecomInjectionCléLocale-1. Il est recommandé que la génération locale d'une clé cryptographique ne donne pas lieu à un processus d'injection.

Justification :

- La génération locale de clé a pour principal objectif de donner une plus grande maîtrise à l'utilisateur final dans l'injection de ses clés. Toutefois, ceci ne doit pas se faire au prix des objectifs de sécurité premiers de protection des clés. Il semble difficile de séparer au niveau local l'environnement de confiance de l'utilisateur en deux.

RègleInjectionCléLocale-1. L'injection d'une clé cryptographique générée localement doit bénéficier de moyens de protection conformes au référentiel. Ces moyens doivent garantir l'authenticité, l'intégrité et la confidentialité de la clé injectée.

Justification :

- Comme il n'est pas souhaitable d'interdire de séparer la génération locale de l'utilisation des clés, il convient de prévoir les mesures techniques permettant de garantir le respect des objectifs de sécurité sur la clé générée. Les moyens requis peuvent être par exemple de prévoir la possibilité pour l'utilisateur de contrôler une empreinte cryptographique de la clé qu'il a introduite dans son environnement de confiance d'utilisation. En matière de confidentialité, la définition du périmètre exact de l'environnement de confiance peut notablement s'élargir si la génération locale est effectuée de façon indépendante de l'application utilisatrice.

2.5.2.2 Injection de clé générée de façon centralisée Injection de clé aléatoire générée de façon centralisée

RÈGLES ET RECOMMANDATIONS :

RègleInjectionCléCentral-1. L'injection dans l'environnement de confiance de l'utilisateur final d'une clé cryptographique générée aléatoirement de façon centralisée doit bénéficier de moyens de protection conformes au référentiel. Ces moyens doivent garantir l'authenticité, l'intégrité et la confidentialité de la clé injectée.

Justifications :

- Cette règle est en cohérence avec celle liée à l'acheminement de cette même clé. Il s'agit ici d'attirer l'attention des concepteurs sur la sécurité de l'étape d'injection qui peut nécessiter d'être opérée par des mécanismes distincts de ceux utilisés lors de l'acheminement de la clé.

RecomInjectionCléCentral-1. Il est recommandé que l'injection dans l'environnement de confiance de l'utilisateur final d'une clé cryptographique générée aléatoirement de façon centralisée soit effectuée à partir d'une donnée protégée dès la génération en confidentialité, authenticité et intégrité par des mécanismes cryptographiques conformes au référentiel.

Justification :

- Il est recommandé que l'acheminement soit protégé de bout en bout de façon cryptographique. Cette recommandation est donc cohérente avec celle de l'acheminement.

Remarque :

- Cette recommandation ne s'applique pas, bien entendu, aux éléments de premier enrôlement pour lesquels la protection ne peut s'appuyer sur un mécanisme cryptographique.

Injection de clé générée par dérivation

RÈGLES ET RECOMMANDATIONS :

RègleInjectionCléDérivée-1. L'injection dans l'environnement de confiance de l'utilisateur final d'une clé cryptographique générée par un processus de dérivation à partir d'une clé maître doit bénéficier de moyens de protection conformes au référentiel. Ces moyens doivent garantir l'authenticité, l'intégrité et la confidentialité de la clé injectée.

RecomInjectionCléDérivée-1. Il est recommandé que l'injection dans l'environnement de confiance de l'utilisateur final d'une clé cryptographique générée par un processus de dérivation à partir d'une clé maître soit effectuée à partir d'une donnée protégée dès la génération en confidentialité, authenticité et intégrité par des mécanismes cryptographiques conformes au référentiel.

Justification :

- La problématique d'acheminement est la même que la clé soit générée aléatoirement de façon centralisée ou dérivée à partir d'une clé maître. Cette recommandation ne s'applique pas, bien entendu, aux éléments de premier enrôlement pour lesquels la protection ne peut s'appuyer sur un mécanisme cryptographique.

2.6 Utilisation d'une clé

2.6.1 Diffusion d'une clé

La diffusion d'une clé dans un système est le nombre d'environnements de confiance qui sont susceptibles d'y accéder en clair. La diffusion augmente le risque de compromission d'une clé. La diffusion minimale d'une clé est :

- Pour une clé privée limitée à un seul environnement de confiance ;
- Pour une clé secrète limitée à deux environnements de confiance.

Il existe d'un point de vue théorique des moyens de partager un secret entre plusieurs entités de telle façon que des calculs puissent être effectués à partir de ce secret sans le révéler. Ces méthodes mathématiques peuvent être utilisées mais ne sont pas envisagées ici. Elles vont plus loin que le simple partage de secret, qui permet, à partir de parts de secret distinctes, de reconstituer un secret dans un environnement de confiance et de l'utiliser.

RÈGLES ET RECOMMANDATIONS :

RecomDiffusion-1. Il est recommandé que la diffusion d'une clé privée ou secrète soit limitée aux seuls environnements de confiance qui l'utilisent vraiment.

Justifications :

- La limitation de la diffusion d'une clé est un moyen simple de réduire le risque de compromission.
- Toutefois, l'objectif de confidentialité sur la clé peut être assuré par des moyens techniques ou physiques. L'analyse de risque peut dans ce cas aboutir à la conclusion que le risque de compromission est acceptable, même si la diffusion de la clé est large. Il n'est donc pas nécessaire, d'édicter en règle cette recommandation.
- Ceci est en cohérence avec la recommandation d'acheminement protégé en confidentialité de bout en bout.

2.6.2 Utilisation applicative d'une clé

RÈGLES ET RECOMMANDATIONS :

RègleEnvironnementConfiance-1. L'utilisation d'une clé cryptographique dans un système applicatif doit obligatoirement se faire dans un environnement de confiance ayant un niveau de sécurité conforme au référentiel.

Justification :

- Que la clé soit publique, privée ou secrète, les objectifs de sécurité sur l'utilisation de celle-ci sont tels que toute atteinte à ces objectifs de sécurité remet en cause les fonctions de sécurité qui nécessitent l'emploi de la cryptographie.

RègleVérificationAuthenticité-1. Avant toute utilisation d'une clé dans un système applicatif, son authenticité et son intégrité doivent être vérifiées par un mécanisme de sécurité conforme au référentiel.

Justifications :

- La vérification d'authenticité avant utilisation est une mesure simple qui bloque un grand nombre de chemins d'attaque cryptographique.
- Il convient de noter que cette vérification n'est pas forcément de nature cryptographique ; elle peut découler du processus d'enrôlement ou s'appuyer sur l'environnement de confiance.

RègleVérificationUtilisabilité-1. Avant toute utilisation d'une clé dans un système applicatif, il doit être vérifié par un mécanisme de sécurité conforme au référentiel que la clé est toujours utilisable.

Justifications :

- La fin de vie d'une clé est une opération qui doit être prévue par une architecture de gestion de clés pour gérer, notamment, les cas de compromissions.
- Pour être efficace, il convient que les informations de retrait ou de révocation soient exploitées.

2.7 Fin de vie d'une clé

RÈGLES ET RECOMMANDATIONS :

RègleFinUtilisation-1. Une architecture de gestion de clés doit prévoir la fin de vie de l'ensemble des clés qu'elle gère ou utilise.

Justifications :

- La fin de vie d'une clé, le dés-enrôlement d'un utilisateur ou la compromission d'une clé sont, par exemple, des événements tout à fait prévisibles qui doivent donner lieu à une procédure de révocation.
- Ces événements doivent être étudiés pour toutes les clés, y compris les éventuelles clés maîtres, clés racines, etc. dont la fin de vie a des impacts sur le système différents de la fin de vie d'une clé utilisateur.

RecomCauseFinUtilisation-1. Il est recommandé qu'une architecture de gestion de clés traite les différentes causes de fin de vie d'une clé de façon distincte.

Justifications :

- Les procédures de révocation de clé prévues pour gérer une crypto-période peuvent s'avérer non adaptées si la cause de la révocation est une compromission. Il convient donc de bien identifier les causes de révocation et de s'assurer que les procédures de révocation et éventuellement de renouvellement des clés sont adaptées à chaque cas de figure.
- Les cas qui ne sont pas nominaux comme la compromission d'une clé peuvent être traités par des mesures non techniques.

RègleEffacement-1. Une clé dont la durée d'utilisation est dépassée doit être effacée des environnements de confiance où elle était utilisée par un moyen technique conforme au référentiel.

Justifications :

- Si la durée d'utilisation de la clé est dépassée, alors, hormis un éventuel archivage, aucun environnement de confiance de l'architecture de gestion de clés n'a besoin de conserver cette clé.
- Les règles et recommandations sur le procédé d'effacement feront l'objet d'un document séparé.

2.8 Renouvellement d'une clé

RÈGLES ET RECOMMANDATIONS :

RègleRenouvellement-1. Une architecture de gestion de clés doit prévoir le renouvellement de l'ensemble des clés qu'elle gère ou utilise.

Justifications :

- Au même titre que la fin de vie, le renouvellement de chaque clé du système doit être étudié.
- L'étude des procédures de renouvellement d'une clé permet d'affiner l'étude d'impact de chaque clé, notamment en identifiant celles qui présentent un risque systémique du fait de leur diffusion et/ou de la difficulté de leur renouvellement.

RègleRenouvellementEnrôlement-1. Une architecture de gestion de clés doit assurer que le renouvellement d'une clé ne puisse se faire qu'après vérification de l'authenticité de la nouvelle clé et de la possession de celle-ci par l'utilisateur. Les mécanismes utilisés pour cette vérification doivent être conformes au référentiel.

Justification :

- Cette règle est en cohérence avec celles relatives à l'enrôlement.

2.9 Recouvrement d'une clé

RÈGLES ET RECOMMANDATIONS :

RègleRecouvrement-1. Une architecture de gestion de clés qui prévoit des fonctions de recouvrement de clés doit mettre en place des contrôles d'accès à cette fonctionnalité conformes au référentiel et respectant de plus l'ensemble des recommandations associées.

Justification :

- Le contrôle de la fonction de recouvrement est primordial pour éviter toute atteinte intempestive aux objectifs de sécurité principaux d'une architecture de gestion de clés.

Annexe A Table des figures

Annexe B Index des règles et des recommandations

Annexe B3

Règles et recommandations concernant les mécanismes d’authentification

Historique des versions		
Date	**Version**	**Evolution du document**
xxx	1.0	Publication de la première version de l'annexe B3 du référentiel général de sécurité

Avant propos

Le présent référentiel est pris en application de l'article LP 20 de la loi du pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices, et de son arrêté d'application.

Le présent document et ses annexes sont une copie adaptée du RGS B3 – Règles et recommandations concernant les mécanismes d'authentification, en vigueur en métropole, version 1.0 du 13 janvier 2010.

Le texte fait des renvois à des documents publiés par l'Agence nationale de la sécurité des systèmes d'information[120] (ANSSI) ou encore disponibles sur son site internet www.ssi.gouv.fr, en ce qu'ils reflètent l'état de l'art en matière de sécurité informatique.

Le référentiel et ses annexes sont disponibles en ligne sur le site internet www.lexpol.pf, et leur mise à jour est assurée par la Direction générale de l'économie numérique.

[120] L'ANSSI est un service à compétence nationale rattaché au Secrétaire général de la défense et de la sécurité nationale, l'autorité chargée d'assister le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale. Parmi ses nombreux objectifs, l'un d'eux consiste à promouvoir un espace de confiance pour les services en ligne. Elle y participe en ce sens notamment au travers de la règlementation (référentiels) et ses labels (certification des produits de sécurité et qualification des produits de sécurité et des prestataires de service de confiance).

A. Introduction

A.1. Contexte

A.1.a. Objectif du document

L'objectif de ce document est de présenter une modélisation permettant de décrire ou d'évaluer les mécanismes d'authentification et de conseiller sur les « meilleures pratiques » à suivre en matière d'authentification lors de l'élaboration d'un système d'information.

Ce document est principalement destiné aux développeurs de produits de sécurité utilisant des fonctions d'authentification pour les aider à réaliser ces fonctions de sécurité.

La lecture de ce document présuppose que le lecteur est familier avec les concepts utilisés en cryptographie et particulièrement, ceux exposés dans « règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques ».

A.1.b. Rôle de l'authentification

L'authentification a pour but de vérifier l'identité dont une entité (personne ou machine) se réclame. L'authentification est toujours précédée ou combinée avec une identification qui permet à cette entité de se faire reconnaître du système par un élément dont on l'a doté : un identifiant. En résumé, s'identifier c'est communiquer un identifiant présumé, s'authentifier c'est apporter la preuve que l'entité s'est vue attribuer cet identifiant.

Ce document ne traite que la fonction d'authentification. L'identification est considérée comme acquise et nous supposons donc l'identité connue par le biais d'un identifiant préalablement enregistré. De même, ce document ne traite pas des méthodes d'identification consistant à reconnaître dans un ensemble d'identifiants connus, celui qui correspond à une entité donnée.

L'authentification vise :

- Soit à contrôler l'accès à des informations, des locaux, plus généralement des biens d'un système d'information, en étant dans ce cas associé à une fonction d'attribution de privilèges particuliers liés à l'identité de l'entité ;
- Soit à garantir une imputabilité avec vérification forte de l'identité affichée, par exemple pour la journalisation d'actions, la facturation de communications, l'authentification de données, etc. ;
- Soit à assurer une combinaison de ces fonctions d'attribution de privilèges et d'imputation.

Dans tous les cas, l'utilisation de mécanismes d'authentification sûrs est nécessaire à la réalisation de ces objectifs, mais la sécurité globale de l'authentification doit évidemment reposer également sur d'autres mesures relatives au système d'information dans sa globalité (sécurité physique, intégrité des logiciels, qualité des développements applicatifs, etc.) qui ne sont pas l'objet du présent document.

A.1.c. Typologie des fonctions d'authentification

Le replacement de la fonction « authentification » dans son contexte permet en particulier d'introduire la question de l'intégration de cette fonction dans son environnement dans le cadre de l'objectif recherché, à savoir l'attribution (pour autorisation ou imputation) d'une action à son auteur réel ou, dit autrement, que l'entité qui agit est bien celle que l'on a authentifiée.

On distingue deux grands types de solutions :

- L'acte signé pour lequel le lien entre l'authentification et l'action est direct et intemporel ;

- La session authentifiée, pour laquelle l'authentification intervient ponctuellement en début de session, avant la première action, et qui nécessite par là même une traçabilité entre l'ouverture et le déroulement de la session pendant toute sa durée.

Notons tout de suite que **la problématique liée à la signature électronique n'est pas l'objet de ce document**. Toutefois, comme dans le cas de la signature, le fait même que l'authentification puisse conduire à imputer des actions à une personne identifiée nécessite que cette fonction soit correctement implantée et que l'utilisateur qui s'authentifie ne la considère pas comme une opération anodine.

A.1.d. Positionnement du document

Ce document complète le document « règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques » édité par l'ANSSI, en particulier son paragraphe « 2.2.4 authentification d'entités ».

Par ailleurs, l'enregistrement éventuel de l'utilisateur dans le système d'authentification et la mise à disposition des éléments cryptographiques nécessaires ne sont pas couverts dans ce document. Cette problématique générale est traitée dans le document « règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques ».

Nous décrivons dans ce document des règles et des recommandations relatives aux mécanismes d'authentification.

- Les **règles** définissent des principes qui doivent a priori être suivis par tout mécanisme. L'observation de ces règles est une condition généralement nécessaire, mais non suffisante, à la reconnaissance du bon niveau de sécurité du mécanisme. Inversement, le fait de suivre l'ensemble des règles, qui sont par nature très génériques, ne garantit pas la robustesse ; seule une analyse spécifique permet de s'en assurer.
- En plus des règles, nous définissons également des **recommandations**. Elles ont pour but de guider dans le choix de certains mécanismes d'authentification permettant un gain important en termes de sécurité. Il va de soi qu'en tant que recommandations, leur application peut être plus librement modulée en fonction d'autres impératifs tels que des contraintes de performance, d'ergonomie ou de coût.

Il importe de noter dès à présent que les règles et recommandations contenues dans ce document ne constituent pas un dogme imposé aux concepteurs de produits utilisant des mécanismes d'authentification. L'objectif est de contribuer à une amélioration constante de la qualité des produits de sécurité. A ce titre, le suivi des règles énoncées dans ce document doit être considéré comme une démarche saine permettant de se prémunir contre de nombreuses erreurs de conception ainsi que contre d'éventuelles faiblesses non décelées lors de l'évaluation des mécanismes d'authentification.

Dans la mesure du possible, chaque règle et recommandation contenue dans ce document fait l'objet d'une justification qui tient compte le plus rigoureusement possible de l'état de l'art ainsi que des contraintes pratiques liées à la mise en œuvre.

Le lecteur est invité à se référer également à l'annexe du document « règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques », notamment pour les différentes limitations décrites qui s'appliquent aussi au présent document.

A.1.e. Organisation du document

L'organisation de ce document est dans certains aspects similaires à celle du document « règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques » :

- Les concepts généraux de modélisation de l'authentification sont présentés au paragraphe A.2 ;
- L'ensemble des règles et recommandations s'appliquant aux différentes étapes du cycle de vie sont ensuite regroupées dans le chapitre B, à partir de la page 15;
- Les règles et recommandations sont repérées selon la codification suivante : les premières lettres (**Règle** ou *Recom*) indiquent si l'on à affaire à une règle ou une recommandation, le domaine d'application est ensuite précisé et, finalement, un chiffre permet de distinguer les règles d'un même domaine d'application.

Ce document ne comporte volontairement aucun tableau récapitulatif. Les différentes règles et recommandations ne peuvent en effet être assimilées à une recette décrivant comment réaliser un mécanisme d'authentification, ce qui serait une source d'erreurs et de confusions.

A.1.f. Mise à jour du document

Ce document a vocation à être révisé régulièrement pour tenir compte des évolutions constantes des menaces et des possibilités technologiques.

A.2. Modèle de la fonction d'authentification

A.2.a. Préambule

Il est habituel de faire reposer l'authentification sur un ou plusieurs éléments parmi :

- Ce que l'on sait (par exemple, un mot de passe) ;
- Ce que l'on a (par exemple, une carte à puce) ;
- Ce que l'on est (par exemple, une empreinte digitale) ;
- Ce que l'on sait faire (par exemple, une signature manuscrite).

Notons tout de suite que ces deux derniers éléments d'authentification sont clairement anthropomorphes et ne s'appliquent pas à des dispositifs automatiques. Nous distinguerons donc deux modèles selon que l'authentification aura lieu entre machines ou s'il s'agit de l'authentification d'une personne vis-à-vis d'une machine.

Nous supposons également que l'authentification ne peut s'effectuer qu'après une installation préalable de clés cryptographiques ou d'informations partagées entre les acteurs concernés du système d'information. En d'autres termes, nous ne nous intéressons pas au processus d'enregistrement d'un utilisateur dans une entité organisatrice, mais aux moyens techniques et cryptographiques à mettre en place suite à cet enregistrement, pour que l'utilisateur puisse ensuite être authentifié correctement lors de son utilisation du système d'information.

A.2.b. Modèle général du processus d'authentification

A.2.b.1. Définition des notions

Nous définissons ci-dessous notre modèle. Sont indiquées en gras et soulignées, lors de leur définition, les différentes notions utilisées par le modèle. Celles-ci sont ensuite mentionnées en italique pour rappeler qu'il s'agit de notions définies dans le modèle.

La réalisation des fonctions contrôle d'accès et imputation fait intervenir :

- Un **demandeur**, qui souhaite effectuer des **actions** et doit pour cela prouver son **identité**,
- Un **receveur**, qui peut permettre les *actions*, en devant au préalable vérifier l'*identité* de leur auteur.

La suite des actions circule sur un **canal** reliant le *demandeur* au *receveur*. L'**authentification** permet de relier de façon fiable, pour le *receveur*, les *actions* circulant sur ce *canal* à l'*identité* du *demandeur*.

Le temps d'exploitation du *canal* par le *demandeur* constitue une **session authentifiée** Cette *session* peut se terminer :

- À l'initiative du *demandeur* ou
- À l'initiative du *receveur*, s'il estime qu'il n'est plus en mesure de garantir le lien entre les *actions* véhiculées sur le *canal* et l'*identité* du *demandeur*.
- Il s'agit bien d'une possibilité. Le modèle n'interdit pas que la session authentifiée soit de durée infinie.
- S'agissant d'un modèle, il convient de ne pas confondre le canal avec le vecteur de transmission de données utilisé. Les données d'authentification échangées entre le demandeur et le receveur peuvent par exemple emprunter un chemin différent de celui des actions.

A.2.b.2. Etats constitutifs d'une authentification

On distingue donc :

- Un état initial, non authentifié, dans lequel le *receveur* interdit les *actions* ;
- Une phase de **connexion**, c'est-à-dire d'ouverture du *canal*, qui constitue le contrôle de l'*identité* du *demandeur* par le *receveur*;
- Un état authentifié d'une certaine durée, constituant la *session authentifiée* pendant laquelle les *actions* sont autorisées par le *receveur* ;
- Une phase de **déconnexion** permettant le retour à l'état initial.

Tous les états peuvent potentiellement engendrer une erreur qui peut générer une alarme. Les transitions entre états, quant à elles, dépendent du contexte. Les états successifs constitutifs de *l'authentification* sont présentés dans la figure 1.

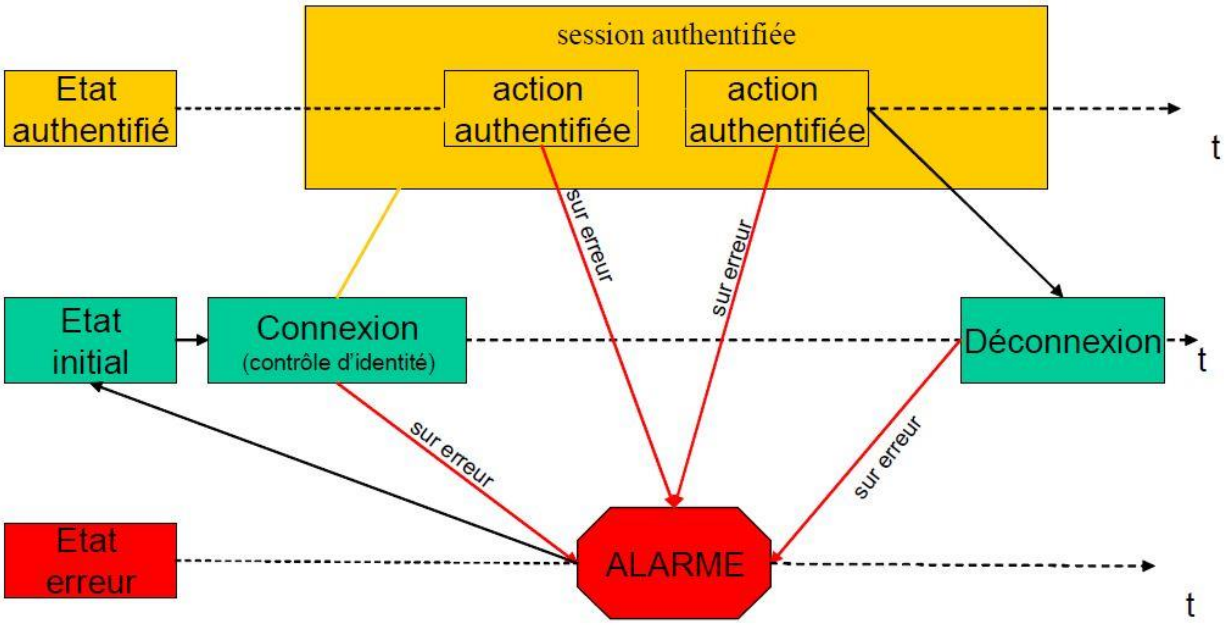


Figure 1 États constitutifs d'une authentification

- Dans beaucoup de cas, l'authentification nécessite de sécuriser le *canal* par un échange de clés cryptographiques au moment de la *connexion*. L'ensemble de la *session* utilise alors ces clés pour se protéger en intégrité et si besoin en confidentialité.
- Même si les termes employés sont effectivement inspirés de modes de communication connectés car ils correspondent à beaucoup des applications visées, rappelons encore une fois que le *canal* ne doit pas être confondu avec les vecteurs utilisés pour transporter les données. L'opération de *connexion* du présent modèle est donc une opération virtuelle qui correspond dans un cas concret à une ou plusieurs opérations physiques ou mathématiques impliquant le *demandeur*, qui peut lui même être constitué de plusieurs entités (personnes ou machines).
- De même, en toute généralité, *la session authentifiée* peut être excessivement courte et les processus de *connexion* et de *déconnexion* peuvent ne pas correspondre à des opérations cryptographiques.

A.2.c. Applications du modèle général

L'un des objectifs recherchés par la présente proposition de modélisation est d'encourager à bien identifier dans un système d'information quelles sont les opérations constitutives de l'authentification. En effet, déterminer dans le système d'information qui joue le rôle de demandeur ou de receveur, quelles sont les opérations liées à la connexion, quelles sont les actions véhiculées par quel canal, etc. permet de mieux discerner les objectifs de sécurité associés à la fonction globale d'authentification. Il devient ensuite possible de vérifier que les objectifs de sécurité sont bien couverts par des mécanismes de sécurité dont la robustesse peut être évaluée.

Partant de ce principe, nous allons préciser maintenant des modèles plus proches de réalités concrètes d'implantation pour pouvoir proposer des recommandations sur les mécanismes de sécurité à mettre en place.

A.2.c.1. Authentification de machines

A.2.c.1.1. Modèle d'authentification de machines

Nous allons distinguer dans la suite trois entités :

- L'environnement de confiance local,
- le SI distant,
- le SI d'authentification de confiance.

L'environnement de confiance local est le *demandeur*, à savoir la machine qui s'authentifie auprès du SI distant, le *receveur*.

Ce terme « environnement de confiance » est choisi en cohérence avec le document « règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques ».

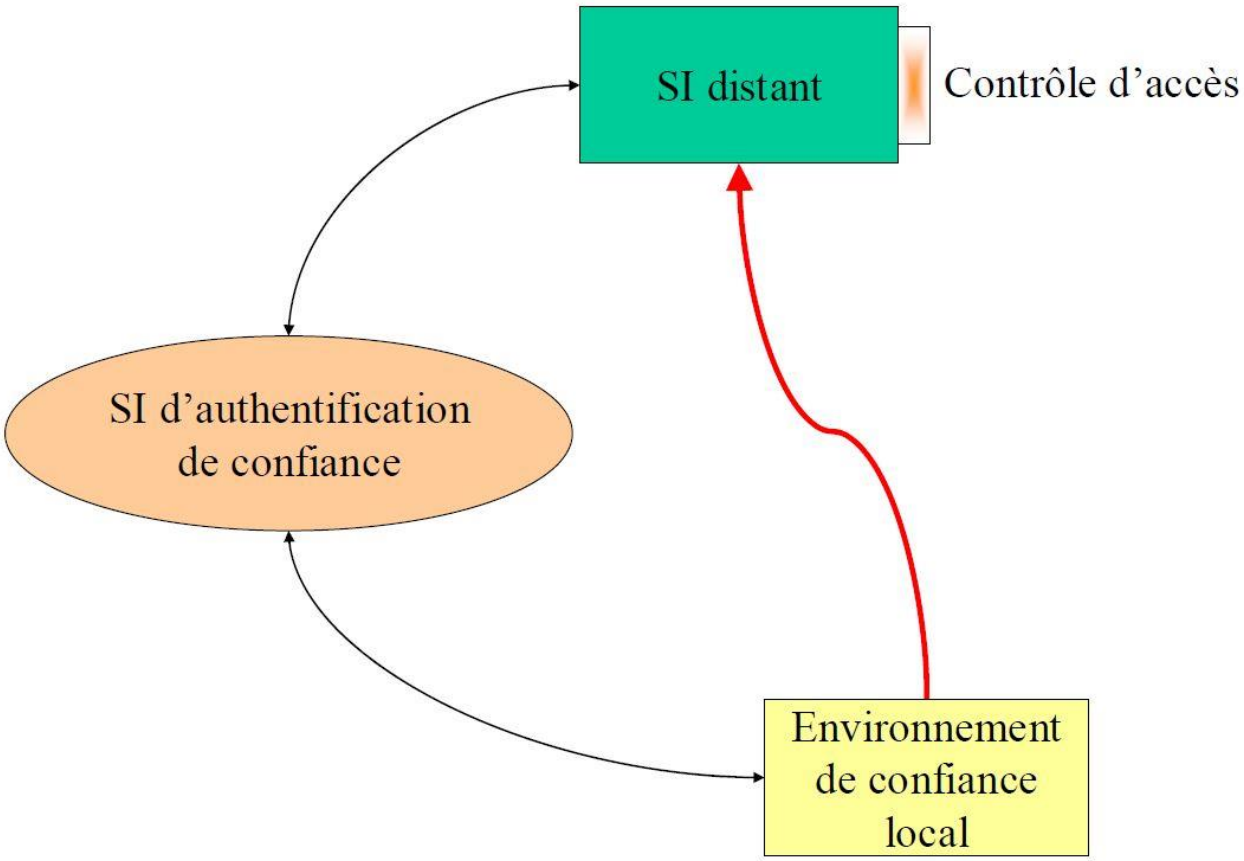


Figure 2 Modèle d'authentification de machines

Le modèle de la figure 2 introduit aussi un SI d'authentification de confiance avec lequel les deux systèmes d'information sont en interaction. L'existence de ce système n'est pas obligatoire. S'il est présent, alors :

- Le SI distant doit faire confiance au SI d'authentification de confiance pour authentifier l'environnement de confiance local.
- L'environnement de confiance local fait confiance au SI d'authentification de confiance pour la protection des éléments d'authentification qu'il lui transmet.
- Il peut s'agir, par exemple, d'un portail d'authentification (single-sign-on) qui authentifierait l'environnement de confiance local pour le compte du SI distant et dont la réponse serait elle-même authentifiée par le SI distant.

Dans cette représentation, les différentes flèches représentent les *canaux* authentifiés possibles entre les entités. Le *canal* d'authentification principal (flèche rouge) relie le *demandeur* au *receveur*. Les autres *canaux* nécessitent dans la plupart des cas d'être authentifiés pour garantir la sécurité de l'*authentification* du *canal* principal. Ces interactions peuvent être des communications, mais aussi des relations de confiance établies, par exemple, par un enrôlement. Ces interactions ne sont pas obligatoires.

- À titre d'exemple on peut chercher à appliquer ce modèle à un client et un serveur de fichiers reliés par une liaison IPSEC configurée manuellement à l'aide d'un secret partagé. Le serveur joue le rôle de SI distant contrôlant l'accès aux fichiers, tandis que le client est l'environnement de confiance local. La configuration étant manuelle, il n'y a pas de SI d'authentification de confiance.
- De même, on peut appliquer le modèle à une situation similaire impliquant un client et un serveur de fichiers reliés en IPSEC, mais cette fois-ci utilisant une infrastructure de clés publiques et un protocole

d'échange de clés Diffie-Hellman signé. Le modèle comprend alors en plus l'infrastructure de clés publiques qui joue le rôle de SI d'authentification de confiance. Elle participe à l'authentification mutuelle par la certification du client et du serveur.

- Pour vérifier le caractère général du modèle, on peut aussi envisager un exemple totalement différent de système de contrôle d'accès physique utilisant un badge sans contact. On y trouve :
  - Un environnement de confiance local, le badge sans contact, demandeur,
  - un SI distant, le dispositif de verrouillage de la porte, receveur,
  - un SI d'authentification, le serveur qui gère les droits d'accès en fonction de l'identité annoncée par le badge.

On voit bien sur cet exemple qu'il n'y a pas authentification du porteur du badge. C'est uniquement ce dispositif qui est authentifié. En outre, on pourrait imaginer plusieurs scénarios de contrôle d'accès, par exemple :

- Le badge s'authentifie auprès du SI d'authentification qui vérifie les droits d'accès et donne un signal au SI distant pour ouvrir la porte. Ce signal est dans ce cas « authentifié » soit par un mécanisme cryptographique soit par la sécurité physique de la connexion entre le SI d'authentification et le SI distant.
- Le badge s'authentifie auprès du SI distant qui demande ensuite au SI d'authentification si l'identité annoncée est autorisée ou pas. Là encore, la sécurité de la transmission entre le SI distant et le SI d'authentification peut être assurée par divers mécanismes.

Un autre exemple que l'on peut considérer est celui de la télévision à péage dont la problématique est un peu différente. Le décodeur du téléspectateur doit recevoir du diffuseur, par voie hertzienne, les informations lui permettant de calculer une clé de décodage. Pour éviter la fraude, le décodeur n'accepte ces informations que si le diffuseur est bien authentifié. Dans cette application, l'environnement de confiance local est (paradoxalement) le diffuseur qui demande l'accès au SI distant, le décodeur de l'utilisateur, pour lui introduire une clé. L'opération de connexion se fait sur détection par le décodeur de la trame contenant les informations de décodage. L'action immédiate est la vérification de l'authenticité de la trame et, si certaines autres informations sont remplies, le calcul de la clé de décodage. La déconnexion est implicite du fait que chaque trame d'informations est authentifiée séparément. La seule différence avec la signature électronique réside dans le fait qu'une fois vérifiée l'authenticité de l'action, celle-ci n'a plus d'importance : le système n'a pas besoin de conserver la signature de l'information.

A.2.c.1.2. Règles et recommandations applicables à l'authentification de machines

Les règles et recommandations concernant l'application de ce modèle font l'objet du paragraphe B.1. Elles s'appliquent au *canal* de transmission entre l'environnement de confiance local et le SI distant qui est réputé non sûr, c'est-à-dire que la flèche rouge de la figure 2 est soumise à des menaces d'interception, d'altération, d'écoute, de rejeu, etc. Il est évident que toute réalisation pratique peut, par une analyse de risque, estimer que ce *canal* est sûr et dans ce cas aboutir à la conclusion qu'il n'est pas nécessaire de mettre en œuvre ces recommandations. Le retour d'expérience observé sur certains cas concrets laisse toutefois à penser que même dans le cas de canaux de transmission réputés sûrs, il est largement préférable pour la sécurité d'adopter une stratégie de défense en profondeur en mettant en œuvre les mécanismes proposés. En effet, la simple imputabilité des actions qui en découle est de nature à améliorer la sécurité globale.

Les flèches noires de la figure 2 correspondent à l'utilisation d'un tiers de confiance. Ce cas est traité au paragraphe B.1.c.1.2.

Le caractère authentique de ces flux est indispensable à l'authentification du flux principal. Par conséquent, de façon indirecte, si ces flux sont véhiculés par des canaux de transmission non sûrs, les règles et

recommandations du flux principal vont également leur être applicables.

A.2.c.2. Authentification d'une personne vis-à-vis d'une machine

A.2.c.2.1. Modèle d'authentification d'une personne vis-à-vis d'une machine

L'authentification d'une personne vis-à-vis d'un système d'information est délicate à réaliser de façon directe. En effet, du point de vue de la machine, seul un procédé de nature cryptographique s'avère sûr, tandis que la personne, quant à elle, ne peut directement employer un tel mécanisme.

Les procédés « d'authentification « directe d'une personne se caractérisent tous par la possibilité de rejeu. Il est rare qu'une personne change systématiquement de mot de passe à chaque utilisation[121] et les procédés de nature biométrique ou comportementale utilisent tous, au contraire, le rejeu pour fonctionner. Il n'y a pas, à notre connaissance, de mécanisme humainement exploitable permettant une authentification sans rejeu[122].

Pour bien les distinguer, nous qualifierons ces procédés de **déverrouillage.** En effet, ces procédés permettent dans la plupart des cas d'accéder à des ressources soumises, là encore, à un contrôle d'accès.

Comme exemple de procédés de déverrouillage, caractérisés par la possibilité de rejeu, on peut citer :

- La saisie d'un mot de passe, qui déverrouille un ordinateur,
- la présentation d'un badge personnel, qui « déverrouille » ce dernier en le rendant accessible aux opérations de vérification,
- l'insertion d'un support amovible, qui donne l'accès aux données qu'il contient,
- la saisie d'un PIN code, qui active des fonctionnalités d'une carte à puce,
- la reconnaissance d'une caractéristique biométrique,
- etc.

Le modèle que nous emploierons complète le précédent en faisant apparaître l'utilisateur (voir figure 3).

[121] En tout cas tant qu'elle n'est pas assistée par un dispositif technique.

[122] Les procédés de type calculette délivrant un mot de passe à usage unique sont typiquement des systèmes d'information réalisant pour le compte de l'utilisateur une opération cryptographique.

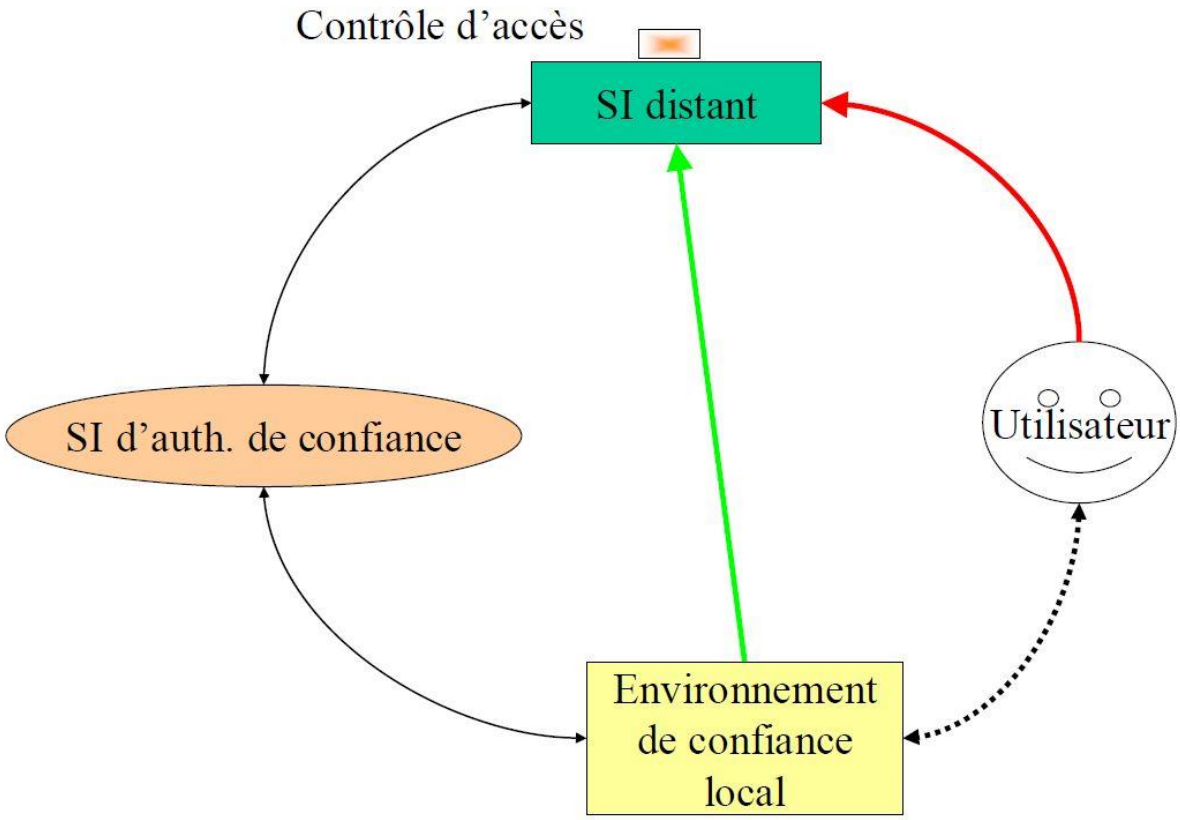


Figure 3 Modèle d'authentification de personne

Dans ce modèle, c'est l'utilisateur qui s'authentifie, mais les droits d'accès qui seront ainsi ouverts le seront vis-à-vis du SI distant pour l'environnement de confiance local, lequel effectuera les actions au bénéfice de l'utilisateur. L'authentification s'effectue donc de machine à machine entre l'environnement de confiance local et le SI distant, mais grâce à un déverrouillage de l'environnement de confiance local par l'utilisateur.

- Dans un premier exemple nous reprenons celui de l'accès d'un client local à un serveur de fichiers en introduisant l'utilisateur de la machine locale. Celui-ci va déverrouiller localement la machine avec un mot de passe, ce qui permet l'utilisation des informations secrètes stockées sur la machine locale dont le verrouillage est contrôlé par le système d'exploitation local. On voit que la machine locale joue le rôle d'environnement de confiance local. Elle héberge également les informations secrètes de l'utilisateur qui constituent le support d'authentification de l'utilisateur. Par la suite, l'environnement de confiance local utilisera ces données pour authentifier l'utilisateur auprès du SI distant (le serveur) et lui permettre d'accéder aux fichiers.
- Comme deuxième exemple, reprenons l'exemple du contrôle d'accès physique, mais en faisant cette fois-ci apparaître l'utilisateur. C'est en effet lui qui est demandeur de l'ouverture d'un canal authentifié : la porte. Pour cela, il utilise un support, le badge, qui va obtenir pour lui l'ouverture du loquet de la porte. Le receveur, le SI distant, est par définition chargé de garantir l'authenticité des actions transitant par le canal « porte ». C'est la raison pour laquelle, il peut, par exemple, commander la fermeture du loquet au bout de quelques secondes s'il estime qu'il n'a plus de garantie d'authenticité entre l'identité authentifiée au départ et la personne qui a effectivement la possibilité de traverser la porte.

Dans cet exemple, plusieurs mécanismes de déverrouillage sont possibles :

- La simple présentation du badge est un mécanisme de déverrouillage, puisqu'elle met le badge en

situation d'activité ;

- Si le badge dispose d'un code PIN, la saisie du code est une opération de déverrouillage ;
- De même, une caractéristique biométrique peut être utilisée pour déverrouiller le badge ;
- On pourrait aussi considérer un système de mots de passe à usage unique générés par le badge et, dans ce cas, c'est l'activation du mécanisme de génération et/ou la saisie du mot de passe généré qui constituent le déverrouillage.

On voit toutefois sur cet exemple que tous les mécanismes de déverrouillage n'ont pas la même robustesse, notamment par rapport à la menace de perte ou de vol du badge.

- Dans un troisième exemple, nous pouvons revenir sur l'accès d'un client local à un serveur de fichiers en imaginant un support de clés de type clé USB de stockage de masse, sans capacité de calcul. Dans ce cas, les données secrètes ne peuvent être accédées de l'environnement de confiance local que si le support est présent, ce qui constitue le déverrouillage de l'environnement de confiance local. Ce mécanisme peut être amélioré en chiffrant les données sur la clé à l'aide d'un mot de passe. Dans ce cas, le déverrouillage consiste à introduire le support ET à saisir un mot de passe.
- Poursuivons sur l'accès d'un client local à un serveur de fichiers. Si le support est une carte à microprocesseur, alors on peut laisser la ressource effectuer les calculs cryptographiques. L'environnement de confiance local n'a dans ce cas jamais accès aux clés qui lui permettent d'obtenir l'ouverture du canal. Le mécanisme de déverrouillage reste dans ce cas la présentation du support. Il peut être amélioré si la carte contrôle elle-même un code PIN. On peut également demander à ce que ce code PIN ne soit pas accessible à l'environnement de confiance local, par exemple par l'emploi d'un lecteur sécurisé. Certains systèmes vont même jusqu'à un tryptique poste local, lecteur intelligent, support carte à mémoire. Le déverrouillage de l'environnement de confiance local est alors plus complexe : il implique une authentification de machines entre le lecteur et la carte, qui est elle-même déverrouillée par un code PIN.
- Un autre exemple d'application du modèle est celui de l'accès distant à un serveur par un système à mot de passe unique. Dans ce cas, l'utilisateur dispose d'une calculette qui lui fournit son mot de passe. Ce dernier est saisi par l'utilisateur sur l'interface d'accès du serveur distant. Le mot de passe calculé peut résulter, par exemple, de l'application d'une fonction cryptographique à un challenge généré par le serveur, ou de la synchronisation antérieure d'un générateur de pseudo-aléa entre le serveur et la calculette. Dans ce cas, l'environnement de confiance local est constitué du poste d'accès ET de la calculette. Le déverrouillage de l'utilisateur consiste à assembler ces deux composants par la saisie croisée du challenge sur la calculette et du mot de passe à usage unique sur le poste d'accès.

A.2.c.2.2. Règles et recommandations applicables à l'authentification d'une personne vis-à-vis d'une machine

Les règles et recommandations concernant l'application de ce modèle font l'objet du paragraphe B.2. Elles s'appliquent au canal de transmission entre l'environnement de confiance local et l'utilisateur, c'est-à-dire la flèche en pointillés noirs de la figure 3. La flèche verte de la figure 3 est évidemment supposée soumise à des menaces d'interception, d'altération, d'écoute, de rejeu, etc. Les règles et recommandations du paragraphe B.1 lui seront donc applicables.

L'authentification de l'utilisateur vis-à-vis du système distant (flèche rouge de la figure 3) résulte de ces différentes règles et des procédures d'enregistrement et de gestion des clés de l'utilisateur dans le système qui ne sont pas l'objet du document (cf. § A.1.d).

A.2.c.3. Authentification de personnes de bout-en-bout

L'authentification de bout-en-bout de deux personnes ne nécessite pas de règle supplémentaire. Elle peut en

effet être modélisée en symétrisant le modèle précédent (voir figure 4). L'authentification mutuelle des utilisateurs distants (flèche rouge de la figure 4) résulte de la double authentification des utilisateurs vis-à-vis des SI (flèches orange de la figure 4) et de la confiance de chaque utilisateur dans son propre SI du fait des mécanismes de déverrouillage utilisés (flèches en pointillés noirs de la figure 4).

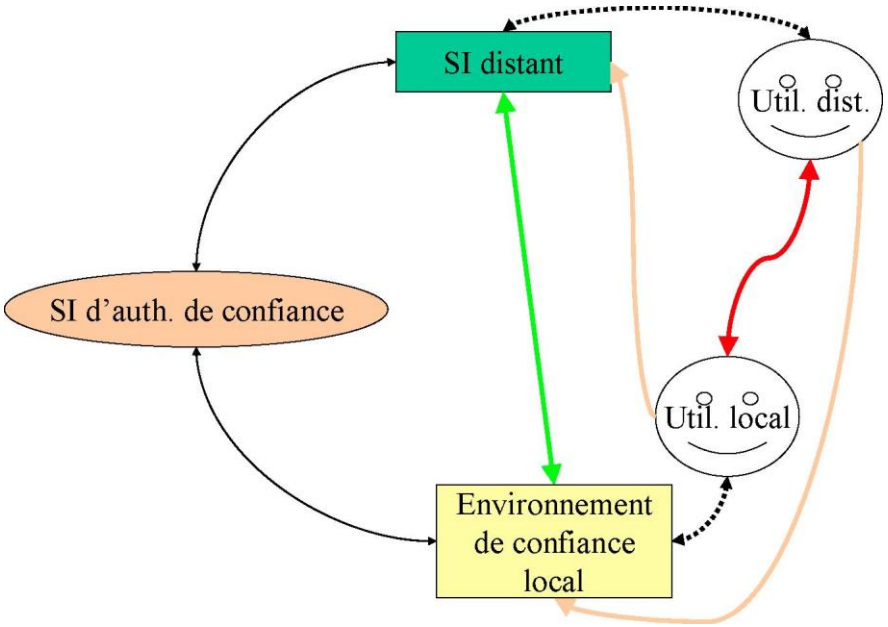


Figure 4 Modèle d'authentification de bout-en-bout

B. Règles et recommandations

B.1. Authentification de machines

B.1.a. Mécanismes cryptographiques

L'utilisation de mécanismes cryptographiques robustes est indispensable pour espérer atteindre une bonne authentification en évitant, par exemple, l'usurpation d'identité ou le rejeu d'une authentification. Ils mettent en œuvre une preuve de possession d'un élément secret (clé cryptographique) par l'intermédiaire d'un protocole d'authentification garantissant la confidentialité de l'élément secret.

Une autre propriété recherchée pour un protocole d'authentification est qu'il doit être impossible pour un attaquant, même s'il récupère les données secrètes d'authentification, de déchiffrer ou de modifier les communications d'une session qu'il n'a pas ouverte.

- Les mécanismes utilisant des mots de passe sous une forme quelconque (pass-phrase, code d'identification personnel…) ainsi que les mécanismes s'appuyant sur des procédés biométriques ne sont pas de nature cryptographique. Bien entendu, ceci ne signifie pas qu'ils ne présentent aucun intérêt dans un processus d'authentification, mais nous les distinguons dans ce document en parlant de mécanisme de déverrouillage.
- Le simple chiffrement des données transmises n'est pas suffisant pour empêcher le rejeu. Par exemple, pour un système d'authentification par mot de passe, si le haché du mot de passe est simplement transmis, alors il est possible de simuler le comportement de l'environnement de confiance local sans disposer du mot de passe originel.

Nous ne reprendrons pas ici les « règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques ». Rappelons simplement que les mécanismes interactifs d'authentification d'entités reposent en général sur des mécanismes symétriques ou asymétriques de génération d'aléa, de hachage, de chiffrement ou de signature ; les règles énoncées par ailleurs pour ces mécanismes s'appliquent donc directement.

Bien entendu, l'évaluation du niveau de robustesse du mécanisme global d'authentification doit être effectuée avec soin, même si des primitives de niveau compatible sont employées.

RègleProtocole. L'authentification entre deux machines doit faire intervenir un protocole cryptographique interactif d'authentification conforme au référentiel général de sécurité.

Justification :

- L'authentification de deux machines est un processus automatique qui doit s'appuyer sur un protocole interactif pour être sûr. Entre deux machines, seul un procédé cryptographique permet d'éviter l'usurpation d'identité. Tout autre procédé ne peut être considéré comme un procédé d'authentification dans ce cas. La simple présentation d'un élément, même si son intégrité est garantie par une signature, ne saurait constituer un mécanisme d'authentification robuste du fait des possibilités de rejeu. Dans ce document, nous parlons dans ce cas de déverrouillage.

B.1.b. Gestion de clés

À partir du moment où un mécanisme cryptographique est nécessaire pour l'authentification, une gestion des clés cryptographiques doit être mise en place. Cette gestion peut faire intervenir des outils techniques, des mesures organisationnelles ou des combinaisons de ces moyens. En matière d'authentification, la gestion des clefs doit permettre d'interdire à un environnement de confiance local corrompu de se connecter sans pour autant perturber le fonctionnement du SI distant.

Nous ne reprendrons pas ici les « règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques » ; elles s'appliquent directement aux mécanismes cryptographiques employés dans les protocoles d'authentification interactifs du paragraphe B.1.a ci-dessus.

RègleGestionClés. L'authentification entre deux machines doit faire intervenir une architecture de gestion des clés du protocole cryptographique utilisé conforme au référentiel général de sécurité.

Justification :

- Comme un procédé cryptographique est indispensable, la gestion de ses clés est nécessaire et doit viser un niveau de sécurité cohérent.

B.1.c. Etats du processus d'authentification

B.1.c.1. Connexion

B.1.c.1.1. Authentification intrinsèque

Il est préférable, lorsque c'est possible, que l'authentification soit intrinsèquement requise plutôt qu'artificiellement imposée, c'est-à-dire qu'un mécanisme de contrôle d'accès défaillant ne puisse donner l'accès en l'absence d'authentification.

RecomAuthIntrinsèque. Il est recommandé que dans un système d'authentification entre deux machines, la défaillance du SI distant ou sa prise de contrôle par un adversaire malfaisant ne permette pas l'accès direct aux actions contrôlées.

Justification :

- Cette recommandation vise à réduire, voire supprimer le caractère potentiellement névralgique du SI distant.
- Par exemple, si on cherche à protéger l'accès à des fichiers, on peut chiffrer ces derniers à l'aide d'une clé contenue dans le dispositif d'authentification. Dans ce cas, le SI distant n'a pas lui-même accès aux données, même s'il contrôle le canal authentifié.
- Il faut toutefois faire attention à ne pas utiliser, par exemple, une clé de chiffrement à des fins d'authentification. On pourrait en effet, dans l'exemple ci-dessus, se heurter au principe d'unicité d'usage d'une clé.

B.1.c.1.2. Tiers de confiance

Il faut, dans la mesure du possible, éviter l'authentification « transitive « (je m'authentifie auprès de A, qui s'authentifie auprès de B, etc.) qui cumule les sources de vulnérabilités.

Toutefois, ce type d'authentification présente également des intérêts en termes d'administration de la sécurité. Par exemple, le modèle des « web services » prévoit une administration des identités par une portion du système et une administration des droits d'accès par les applications. Dans ce modèle, l'application fait confiance au tiers pour authentifier l'environnement de confiance local. Elle n'a à gérer que ses propres droits, associés à l'identité de l'environnement de confiance local.

RègleTiersDeConfiance-1. Si un tiers de confiance est utilisé de façon directe pour une authentification entre deux machines, alors les mécanismes d'authentification du système local vis-à-vis de ce tiers de confiance doivent être conformes au référentiel général de sécurité.

RègleTiersDeConfiance-2. Si un tiers de confiance est utilisé de façon directe pour une authentification entre deux machines, alors les mécanismes d'authentification du système distant vis-à-vis de ce tiers de confiance doivent être conformes au référentiel général de sécurité.

RecomTiersDeConfiance. Si un tiers de confiance est utilisé de façon directe pour une authentification entre deux machines, alors il est recommandé que les mécanismes d'authentification du système distant vis-à-vis de ce tiers de confiance respectent de plus l'ensemble des recommandations du référentiel général de sécurité.

Justification :

- Si le mécanisme utilisé pour l'authentification consiste à demander à un tiers de confiance de réaliser l'authentification pour son compte, alors l'authentification de l'environnement de confiance local vis-à-vis du tiers de confiance doit être de niveau similaire.
- En outre, la réponse du tiers de confiance doit aussi être authentifiée et il est crucial que cette authentification soit d'un niveau de sécurité supérieur car le tiers de confiance, s'il est usurpé, donne la possibilité d'usurper toute identité.
- Rappelons qu'il convient de ne pas confondre ce tiers de confiance avec celui d'une architecture de gestion de clés qui peut être par ailleurs indispensable.

B.1.c.2. Session authentifiée

Si l'authentification sert à établir un accès à des données confidentielles, le canal ouvert doit être protégé en intégrité et en confidentialité. On fera en particulier attention à la suppression ou au rejeu des échanges en protégeant l'intégrité de l'intégralité des communications. De plus, le lien entre l'authentification et l'échange de clés qui va permettre de sécuriser les communications doit être effectué avec précaution.

RecomConfidentialité. Si une authentification est utilisée pour contrôler l'accès à des données confidentielles, alors il est recommandé que la session authentifiée permette la mise en place d'un mécanisme cryptographique conforme au référentiel général de sécurité, assurant la confidentialité et l'intégrité de ces données.

Justification :

- L'authentification nécessitant l'emploi d'un protocole cryptographique, il y a un réel avantage à en profiter pour chiffrer les données dont l'accès est contrôlé. Toutefois, ceci n'est qu'une recommandation car d'autres mesures peuvent suffire à protéger la confidentialité des données, l'authentification n'intervenant alors que pour garantir le cloisonnement du besoin d'en connaître.
- Par exemple, si un tunnel chiffrant est établi par ailleurs ou que l'authentification est interne à un réseau local, la confidentialité des données peut être considérée comme acquise.

B.1.c.3. Déconnexion

B.1.c.3.1. Effacement

La sécurité du processus d'authentification repose souvent sur la confidentialité des éléments temporaires échangés au cours du protocole d'authentification. Il est donc important que les développeurs soient attentifs à l'effacement de ces données dès lors qu'elles ne sont plus utilisées.

RègleEffacement. À la déconnexion d'une session authentifiée, si des éléments secrets ont été échangés lors de la phase d'authentification, ils doivent être effacés.

Justification :

- Il convient de bien insister sur la nécessité d'un effacement physique : les donnée correspondantes ne doivent plus être présentes pour garantir la sécurité du protocole d'authentification.
- La suppression des moyens d'accéder à ces données (pointeurs) n'est pas suffisante pour respecter cette règle. On prendra soin, par exemple, de mettre l'ensemble des mémoires correspondantes à zéro

et de vider les éventuels tampons intermédiaires avant de supprimer les références aux valeurs sensibles.
- Une passe d'écriture à zéro de l'ensemble des mémoires ayant contenu des données sensibles constitue un effacement conforme à la présente règle.

RecomMémoireVolatile. Il est recommandé que les éléments secrets échangés lors de la connexion d'une session authentifiée soient uniquement stockés en mémoire volatile et jamais sur un support magnétique.

Justification :

- L'effacement de données stockées sur un support magnétique est très délicat à mettre en œuvre. Il est donc largement préférable de s'assurer que les données correspondantes ne sont jamais stockées sur un tel support.
- L'utilisation d'une mémoire volatile garantit dans une certaine mesure que si le processus d'authentification est interrompu par une panne, les éléments sensibles ne seront pas compromis.
- Sur un ordinateur, cette recommandation vise à éviter que les pages mémoire utilisées pour stocker les éléments sensibles d'authentification puissent être stockées sur le disque de l'ordinateur par les mécanismes habituels de mémoire virtuelle ou zone d'échanges (swap). Le fait qu'il ne soit pas toujours possible de garantir que le système d'exploitation ne recopie pas une page mémoire dans une zone virtuelle stockée sur disque justifie le fait que cette mesure ne soit que recommandée.

B.1.c.3.2. Inactivité

Dans une session authentifiée, il est souhaitable d'incorporer un dispositif de déconnexion automatique en cas d'inactivité.

RecomInactivité. Au cours d'une session authentifiée, il est recommandé d'incorporer un dispositif de déconnexion automatique en cas d'inactivité.

Justification :

- ll'inactivité d'une session authentifiée est la première étape de scénarios d'attaque classique d'usurpation de session. Il est donc important de réduire ce risque en prévoyant un tel dispositif.
- Ceci n'apparaît que comme une recommandation pour tenir compte des cas où la détection de l'inactivité pourrait être délicate à réaliser.
- Il est important de noter que nous nous plaçons ici dans le cas de l'authentification de machines. Cette recommandation n'implique donc pas une action d'un utilisateur.

B.1.d. Audit

Pour détecter une utilisation frauduleuse il est nécessaire que puissent être consultées les traces des authentifications réussies. En outre, tous les états d'une session authentifiée peuvent potentiellement engendrer une erreur qui peut révéler un comportement anormal, voire une tentative d'usurpation d'identité. De même, les transitions entre états, quant à elles, dépendent du contexte et peuvent aussi être le révélateur d'anomalies.

RègleAudit. Toute erreur survenant au cours d'une session authentifiée doit générer une trace d'alarme ne pouvant être modifiée ni effacée.

RecomAudit. Il est recommandé que toute transition d'état survenant au cours d'une session authentifiée génère une trace d'alarme ne pouvant être modifiée ni effacée.

Justification :

- Le minimum requis est de pouvoir tracer des tentatives d'authentification ayant conduit à des anomalies.
- Toutefois, en cas d'enquête, il peut être tout aussi utile de disposer des traces d'authentification réussie et plus généralement des événements marquants de la session authentifiée, à savoir les transitions d'état.

B.2. Authentification de personnes

Rappelons encore une fois ici que les règles et recommandations ci-dessous ne s'appliquent pas à la problématique de la signature électronique qui répond à des enjeux différents. En effet, nous cherchons ici à définir les mécanismes de sécurité applicables à la protection d'une session authentifiée qui, par nature, est limitée dans le temps, alors que la signature électronique doit protéger l'intégrité et l'authenticité d'une donnée dans la durée.

B.2.a. Utilisation d'un environnement de confiance local

RègleAuthentification. L'authentification d'un utilisateur auprès d'un SI distant doit faire intervenir un environnement de confiance local déverrouillé par l'utilisateur et réalisant, pour son compte, une authentification de machine à machine conforme au référentiel général de sécurité.

Justification :

- Comme indiqué en préambule, la simple utilisation à distance d'un mécanisme de déverrouillage ne saurait constituer un dispositif d'authentification.
- Le simple chiffrement des données transmises n'est pas suffisant pour empêcher le rejeu. Par exemple, pour un système d'authentification par mot de passe, si le haché du mot de passe est simplement transmis, alors il est possible de simuler le comportement de l'environnement de confiance local sans disposer du mot de passe originel.
- La faiblesse intrinsèque d'un mécanisme de déverrouillage réside dans le fait que l'utilisateur ne peut, de façon ergonomique, que répéter une même opération (saisie de mot de passe, empreinte biométrique, etc.) à chaque nouvelle occurrence. Dans une authentification à distance, ceci ouvre des possibilités de fraude d'ores et déjà largement employées dans le hameçonnage, qui visent à récupérer les informations rejouées par l'utilisateur à chaque nouvelle authentification.
- Il existe aussi des attaques « en paradoxe des anniversaires » qui peuvent s'appliquer, par exemple si une liste d'empreintes de mots de passe d'accès à un système distant est disponible.
- L'utilisation d'un environnement de confiance local paraît largement envisageable dès lors que l'utilisateur dispose forcément d'un système d'information pour réaliser les actions que le SI distant va lui autoriser.

La notion d'environnement de confiance définie dans le document « règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques » est cohérente avec cette règle. En effet, d'une part l'authentification de machines réalisée peut faire intervenir des clés cryptographiques, d'autre part le mécanisme de déverrouillage ne peut être utilisé que dans un environnement de confiance, puisqu'il est intrinsèquement vulnérable au rejeu.

- Pour réaliser l'authentification de machine entre l'environnement de confiance local et le SI distant, on pourrait souhaiter dériver des clés secrètes à partir de mots de passe, ces derniers doivent être suffisamment longs et « non devinables » pour offrir une sécurité compatible avec les règles relatives aux tailles de clé. À titre d'exemple, des mots de passe de 8 caractères alphanumériques (chiffres et lettres majuscules ou minuscules) ne permettent pas de générer des clés de plus de 47 bits, et encore, sous l'hypothèse très optimiste que ces mots de passe sont choisis aléatoirement… De tels mots de passe ne permettent donc pas d'atteindre un niveau conforme au référentiel. Même en allongeant la

taille des mots de passe, ce type de procédé resterait vulnérable aux attaques en hameçonnage évoquées ci-dessus. Il est donc encore préférable que l'authentification réalisée exploite aussi l'identité de l'environnement de confiance local employé.

RecomPérimètre. Dans une authentification distante d'un utilisateur, il est recommandé que le périmètre physique de l'environnement de confiance local utilisé pour réaliser l'authentification de machine avec le SI distant reste sous le contrôle de l'utilisateur.

Justification :

- L'environnement de confiance local accède par définition aux informations de déverrouillage propres à l'utilisateur. Il est fortement souhaitable que ces informations n'aient pas à être validées ou exploitées en dehors d'un périmètre dont l'utilisateur a conscience.
- Les informations de déverrouillage doivent être considérées comme des données personnelles. Les exploiter en dehors d'un périmètre physique sur lequel l'utilisateur peut exercer un certain contrôle entraîne des objectifs de sécurité importants sur ce périmètre.
- À titre d'exemple, on peut considérer le cas concret d'une base de données biométriques. L'authentification d'une personne peut être envisagée par comparaison au niveau d'un serveur des données acquises. Dans ce cas, l'environnement de confiance « local » s'étend par définition jusqu'au serveur qui réalise cette opération de comparaison. Il est possible de réaliser un tel mode de fonctionnement, mais il est évident que le serveur doit dans ce cas garantir la protection des données rejouables qu'il exploite. C'est la raison pour laquelle nous ne souhaitons pas interdire un tel mode de fonctionnement, mais nous recommandons une architecture pour laquelle les objectifs de sécurité peuvent être moins exigeants.

RecomCloisonnement. Dans une authentification distante d'un utilisateur, il est recommandé que les fonctions employées par l'environnement de confiance local pour réaliser l'authentification de machine avec le SI distant soit cloisonnées des autres fonctions de l'environnement de confiance local.

Justification :

- L'authentification de personnes repose sur des mécanismes de déverrouillage qui permettent le rejeu. L'obtention des informations correspondantes constitue donc une cible de choix pour un attaquant, d'autant que ces informations sont faiblement modifiables. Les différents mots de passe utilisés sont souvent des variations les uns des autres et les caractères biométriques sont intrinsèques à la personne. Plus que toute autre fonction, celles de l'environnement de confiance local qui gèrent ces informations doivent donc être protégées. Les autres fonctions de l'environnement de confiance local doivent être empêchées d'accéder aux informations traitées dans le cadre de l'authentification de personne. Les vulnérabilités éventuelles de ces autres fonctions ne doivent pas compromettre les informations sensibles que l'utilisateur emploie dans son authentification distante.
- L'utilisation courante de systèmes non totalement maîtrisés justifie que cette mesure ne soit qu'une recommandation.

RecomCloisonnementPhysique. Dans une authentification distante d'un utilisateur, il est recommandé que l'utilisation d'un support physique amovible soit indispensable à l'environnement de confiance local pour utiliser les clés cryptographiques nécessaires à l'authentification de machines avec le SI distant.

Justification :

- S'agissant d'une authentification de personne, il est raisonnable que l'utilisateur ait le moyen de conserver sous son contrôle physique les éléments déterminants de l'authentification de son identité.

RecomInterdictionAccèsClés. Dans une authentification distante d'un utilisateur, il est recommandé que les clés cryptographiques employées par l'environnement de confiance local pour réaliser l'authentification de machine avec le SI distant ne puissent être extraites par l'utilisateur.

Justification :

- La connaissance du secret de déverrouillage ne doit pas permettre d'activer des fonctions d'accès aux éléments secrets d'authentification. Cela signifie en particulier que l'utilisateur légitime ne doit pas pouvoir retrouver ses éléments secrets d'authentification. En effet, l'existence de ces fonctions est inutile à l'authentification proprement dite et peut offrir des opportunités d'attaques.
- Ce type de fonction peut toutefois être implanté dans le souci de pouvoir sauvegarder les éléments d'authentification. L'objectif de cette recommandation est dans ce cas d'attirer l'attention des concepteurs sur les dangers intrinsèques liés à ces fonctionnalités et les objectifs de sécurité correspondants à prévoir.

B.2.b. Mécanismes de déverrouillage

RègleDéverrouillage. L'environnement de confiance local intervenant dans l'authentification d'un utilisateur auprès d'un SI distant doit nécessiter un déverrouillage par l'utilisateur avant de pouvoir réaliser, pour son compte, une authentification de machine à machine conforme au référentiel général de sécurité.

Justification :

- L'environnement de confiance local doit être protégé par un dispositif de verrouillage afin qu'il ne puisse pas être utilisé à l'insu de l'utilisateur.

RecomDéverrouillageLocal. Il est recommandé que l'environnement de confiance local intervenant dans l'authentification d'un utilisateur auprès d'un SI distant gère de façon autonome son mécanisme de déverrouillage.

Justification :

- L'autonomie de l'environnement de confiance local doit être recherchée au niveau du dispositif de verrouillage car la mise en œuvre de tiers est très délicate à envisager s'agissant d'un mécanisme intrinsèquement vulnérable au rejeu.
- L'utilisation d'un serveur d'authentification peut permettre de déverrouiller la session d'un utilisateur. Ce type d'architecture est possible et correspond à des architectures de systèmes d'information largement utilisées (Kerberos, Radius, SRP, etc…). La mise en œuvre de ce type d'architecture est toutefois délicate à gérer du fait de l'authentification à réaliser entre le serveur tiers et l'environnement de confiance local. Elle peut donc présenter des vulnérabilités dans l'implantation rendant le mécanisme global non conforme.

RègleDéverrouillagePersonnel. L'activation de l'environnement de confiance local intervenant dans l'authentification d'un utilisateur auprès d'un SI distant nécessite la présentation d'un élément personnel à l'utilisateur légitime.

Justification :

- Pour que le mécanisme de verrouillage protège effectivement l'utilisation de l'environnement de confiance local à l'insu de l'utilisateur légitime, il est nécessaire que ce mécanisme mette en œuvre un élément caractéristique de la personne authentifiée.

RecomDéverrouillagePersonnel. Il est recommandé que l'activation de l'environnement de confiance local intervenant dans une authentification d'un utilisateur auprès d'un SI distant nécessite la présentation de deux éléments personnels à l'utilisateur légitime.

Justification :

- Cette recommandation est en cohérence avec la notion traditionnelle « d'authentification forte », qui préconise de combiner deux mécanismes parmi ce que l'on sait, ce que l'on a, ce que l'on est ou ce que l'on sait faire.
- Nous considérons toutefois que les applications doivent définir leur besoin éventuel « d'authentification forte » des utilisateurs. C'est la raison pour laquelle ce type d'authentification n'est pas une règle.

RecomSecretDéverrouillage. Il est recommandé que l'activation de l'environnement de confiance local intervenant dans l'authentification d'un utilisateur auprès d'un SI distant nécessite la présentation d'un secret connu uniquement de l'utilisateur légitime.

Justification :

- L'un des moyens simples de respecter cette règle est de faire intervenir un secret (mot de passe, code PIN, etc.) sans que ceci soit le seul moyen possible.
- La simple présentation d'un badge personnel peut être un mécanisme de déverrouillage conforme.
- Le contrôle d'une caractéristique biométrique peut être un mécanisme de déverrouillage conforme. Il est toutefois recommandé que le contrôle de cette caractéristique soit effectué par l'environnement de confiance local.

RecomTauxFausseAcceptation. Il est recommandé que le mécanisme de déverrouillage de l'environnement de confiance local intervenant dans l'authentification d'un utilisateur auprès d'un SI distant ne puisse pas être contourné par quiconque avec une probabilité de succès supérieure à une chance sur 2^{11}.

Justification :

- Cette probabilité est relativement faible. Elle correspond à environ une chance sur deux mille. S'agissant du déverrouillage d'un environnement de confiance local, cette probabilité semble suffisante et correspondre à l'état de l'art actuel.
- Cette recommandation ne doit pas être comprise uniquement vis-à-vis d'un potentiel attaquant extérieur. L'authentification vise à garantir l'identité d'une personne. La notion d'administrateur est donc très délicate à gérer dans ce contexte. Le fait qu'un administrateur dispose de droits d'accès lui permettant d'usurper l'identité d'un utilisateur peut dans certains cas conduire à des conséquences non négligeables.
- Cette probabilité s'entend comme une mesure de la sécurité intrinsèque du mécanisme et non des dispositifs de protection éventuels de celui-ci.
- Si des serveurs d'authentification distants sont mis en œuvre, alors la mesure d'une telle probabilité est insuffisante à estimer la solidité du mécanisme de déverrouillage contre des attaques en force brute parallélisées sur plusieurs comptes. L'analyse de risque devra alors être affinée.
- Un code porteur de 4 chiffres présente une entropie de $4.\log_2(10) \approx 13{,}29$ bits. Si trois codes peuvent être présentés avant blocage de l'environnement de confiance local, alors la probabilité de fausse acceptation est de 3 sur $2^{13.29}$ soit un sur $2^{13.29-\log_2(3)} \approx 2^{11.7}$. Un tel mécanisme est conforme à la recommandation.
- Un mot de passe de 6 caractères pris dans un alphabet de 32 symboles présente une entropie de 30 bits. De façon locale, un tel mot de passe répond bien à la recommandation dès lors qu'il y a une

limitation du nombre de tentatives, mais si ce mot de passe peut être présenté dix fois à un serveur distant qui héberge cent mille sites, alors la probabilité de fausse acceptation est théoriquement d'environ $2^{30} - 19 \cdot 9 \cdot 3 = 210.07$. En outre, dans la pratique, l'attaque peut très bien consister à ne présenter chaque jour que cinq mots de passe en comptant que l'utilisateur légitime va régulièrement réactiver son compte. Ce faisant, la possibilité d'une recherche exhaustive devient envisageable avec dans ce cas une quasi-certitude de pouvoir contourner le mécanisme de déverrouillage d'un utilisateur.

RecomCheminSûr. Il est recommandé que les informations dont dépend l'activation de l'environnement de confiance local intervenant dans l'authentification d'un utilisateur auprès d'un SI distant soient directement introduites au niveau des fonctions de l'environnement de confiance local qui les exploitent sans possibilité d'écoute ni de perturbation.

Justification :

- Par voie de conséquence, il est recommandé que l'environnement de confiance local dispose d'un accès direct au(x) dispositifs) d'acquisition des éléments sensibles d'activation.
- Si un support amovible est employé, les objectifs de confidentialité sur les éléments sensibles d'activation pourraient sembler couverts par un chiffrement de la liaison entre le dispositif d'acquisition et le support. Toutefois, la faible entropie du secret nécessite de limiter au maximum les risques d'interception, même si la communication est chiffrée. En outre, la perturbation de cette liaison pourrait nuire à la disponibilité. C'est la raison pour laquelle il est recommandé de disposer d'un chemin de confiance direct pour l'activation de l'environnement de confiance local par l'utilisateur.
- L'exemple typique d'application est celui de la carte à puce avec mot de passe utilisable sur un poste de travail. Le mot de déverrouillage de cette carte peut soit être saisi sur le clavier du poste, soit être introduit directement au niveau du lecteur par l'utilisation d'un clavier intégré. La deuxième solution est évidemment plus sûre que la première. Toutefois, l'authentification ainsi réalisée vise entre autres à permettre d'utiliser le poste de travail tout en offrant un contrôle d'accès plus sécurisé aux données qu'il va manipuler. Le poste de travail est donc de confiance, indépendamment du processus d'authentification. C'est la raison pour laquelle l'utilisation d'un chemin sûr ne fait l'objet que d'une recommandation.

B.2.c. Audit

Outre les mécanismes d'audit de l'authentification de machine réalisée vis-à-vis du SI distant par l'environnement de confiance local pour le compte de l'utilisateur, il convient de prévoir, dans le cas de l'authentification de personnes, des mécanismes complémentaires permettant à l'utilisateur lui même d'être en mesure de contrôler que son identité n'est pas usurpée.

RecomAuditPersonnel. Il est recommandé que dans une authentification distante d'un utilisateur, ce dernier soit en mesure de consulter de manière sécurisée les audits de ses authentifications, mais sans pouvoir ni les modifier, ni les effacer.

Justification :

- L'authentification distante peut mettre en œuvre un support physique amovible. C'est l'exploitation de ce support qu'il peut être intéressant d'auditer pour vérifier, par exemple, qu'il n'a pas été utilisé à l'occasion d'une perte momentanée.
- Ce mécanisme relève du principe de précaution au cas où les mécanismes d'audit de l'authentification de machines seraient contournés.

C. Guide d'interprétation dans certains cas particuliers

C.1. Mot de passe à usage unique

C.1.a. Préambule

Parmi tous les mécanismes de déverrouillage, l'utilisation d'un secret connu de l'utilisateur est de loin le plus répandu. Ceci est lié au fait que ce mécanisme est d'une part facile à mettre en œuvre par l'utilisateur et d'autre part qu'il ne nécessite pas de dispositif coûteux, la présence d'un clavier étant dans la plupart des cas nécessaire au-delà du simple processus d'authentification.

Ainsi que nous l'avons défini, un mécanisme de déverrouillage souffre toutefois du grave défaut intrinsèque d'être rejouable, si bien que la connaissance du mot de passe par un adversaire lui permet immédiatement d'usurper l'identité de la personne si aucun autre dispositif n'est en place.

Pour pallier cette vulnérabilité, des mécanismes de mot de passe à usage unique peuvent être imaginés. Ces mécanismes permettent, lorsqu'ils sont correctement conçus et implantés, d'atteindre un niveau de sécurité bien supérieur à celui du mot de passe statique, sans toutefois prétendre atteindre un niveau comparable à un protocole d'authentification cryptographique. Cette limitation est essentiellement due à des contraintes ergonomiques qui font qu'on ne peut demander à l'utilisateur de saisir régulièrement des données aléatoires de taille importante. Rappelons en effet que l'entropie d'un mot de passe peut difficilement être comparée à celle d'une clé cryptographique symétrique qu'il est recommandé de choisir au minimum de 100 bits (voir tableau de la figure 5).

Caractéristiques du mot de passe	Nombres total de symboles	10 symboles (chiffres)			26 symboles (lettres)			62 symboles (chiffres, majuscules, minuscules)			90 symboles (jeu de caractères complet)		
	Nombre de symboles par mot de passe	4	7	10	8	10	16	8	10	16	8	10	16
Taille de clé équivalente (bits)		13	23	33	38	47	75	48	60	95	52	65	104
Cassage exhaustif possible		oui	oui	oui	oui	oui	?	oui	oui	non	oui	oui	non

figure 5 : Entropie d'un mot de passe

Du fait de cette limitation, il est assez facile de réaliser des schémas d'authentification par mot de passe à usage unique dont la sécurité est faible. L'objet de cette partie est donc de préciser pour ces mécanismes particuliers les règles et recommandations à respecter.

C.1.b. Description du mécanisme

C.1.b.1. Adaptation du modèle d'authentification

Le modèle d'authentification de personne que nous avons introduit reste valable (voir figure 6). La particularité d'un mécanisme d'authentification par mot de passe à usage unique est toutefois que l'utilisateur est amené à intervenir pour que son environnement de confiance local puisse réaliser l'authentification de

machine pour son SI local. En effet, ainsi que nous l'avons indiqué, l'utilité d'un mécanisme par mot de passe est qu'il ne nécessite pas de dispositif supplémentaire au niveau du SI local comme un lecteur de carte. L'environnement de confiance local n'est donc pas en mesure d'interagir directement ni avec le SI local, ni avec le SI distant.

Le corollaire de cette intermédiation de l'utilisateur est également que l'environnement de confiance local n'a pas de moyen d'authentifier le SI distant. On en déduit que c'est l'interface de saisie d'une authentification par mot de passe dynamique qui doit authentifier le serveur distant par une authentification de machines.

- L'exemple d'implantation classique consiste à réaliser une connexion SSL au SI distant. Cette connexion permet, par la vérification du certificat du serveur, d'authentifier ce dernier.

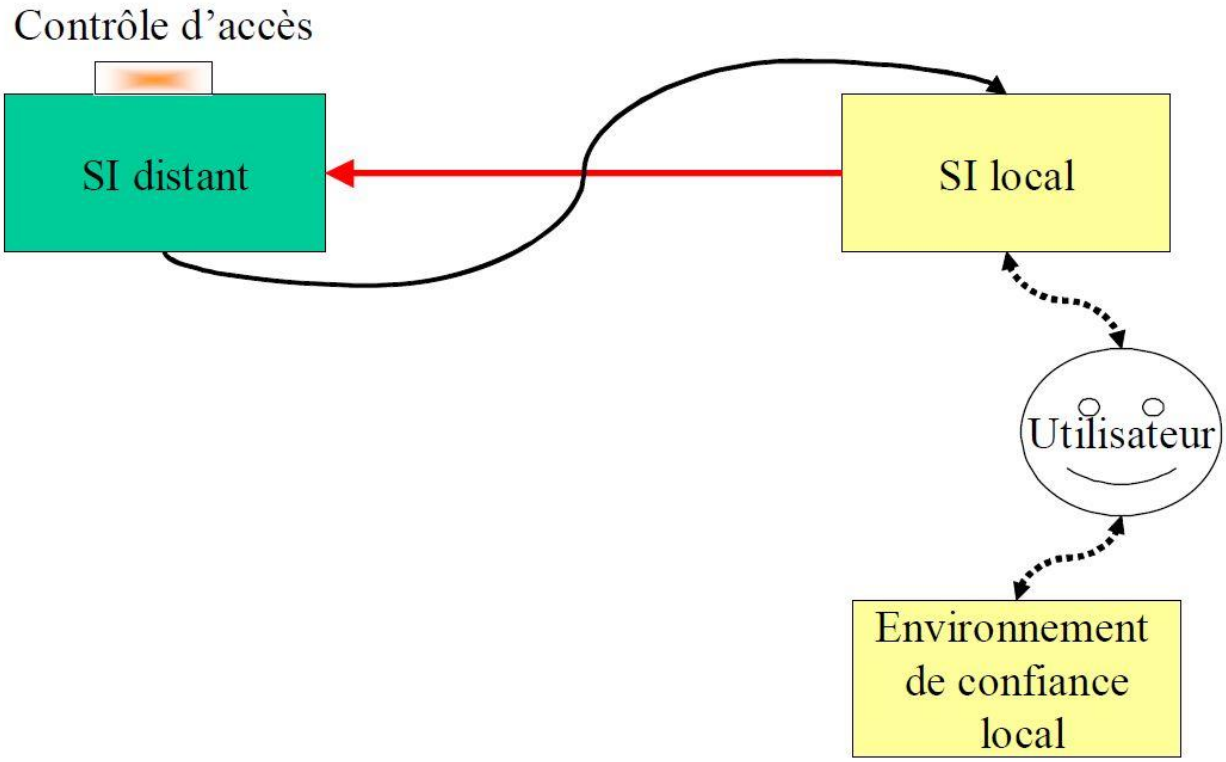


Figure 6 Authentification par mot de passe dynamique

C.1.b.2. Description du protocole

Les protocoles d'authentification par mot de passe dynamique peuvent être décrits de façon générique de la façon suivante.

Les différentes entités du protocole disposent respectivement :

- Pour l'utilisateur :
  - D'un identifiant *id*,
  - d'un éventuel mot de passe statique *smdp*,
  - d'un environnement de confiance local, qui peut également mettre en œuvre un mécanisme de déverrouillage propre (pin-code, empreinte digitale, etc.).
- Pour l'environnement de confiance :
  - D'une clé $K_{\pi}^{(id)}$ dépendant de l'identifiant et permettant de « prouver » cette identité,
  - éventuellement d'un compteur interne t.

- Pour le SI distant :
  - Éventuellement de la valeur H(id)(smdp).
  - d'une clé $K_v^{(id)}$ dépendant de l'identifiant et permettant de « vérifier « cette identité,
  - éventuellement d'un compteur interne t',
  - éventuellement d'un générateur de défi aléatoire chall.

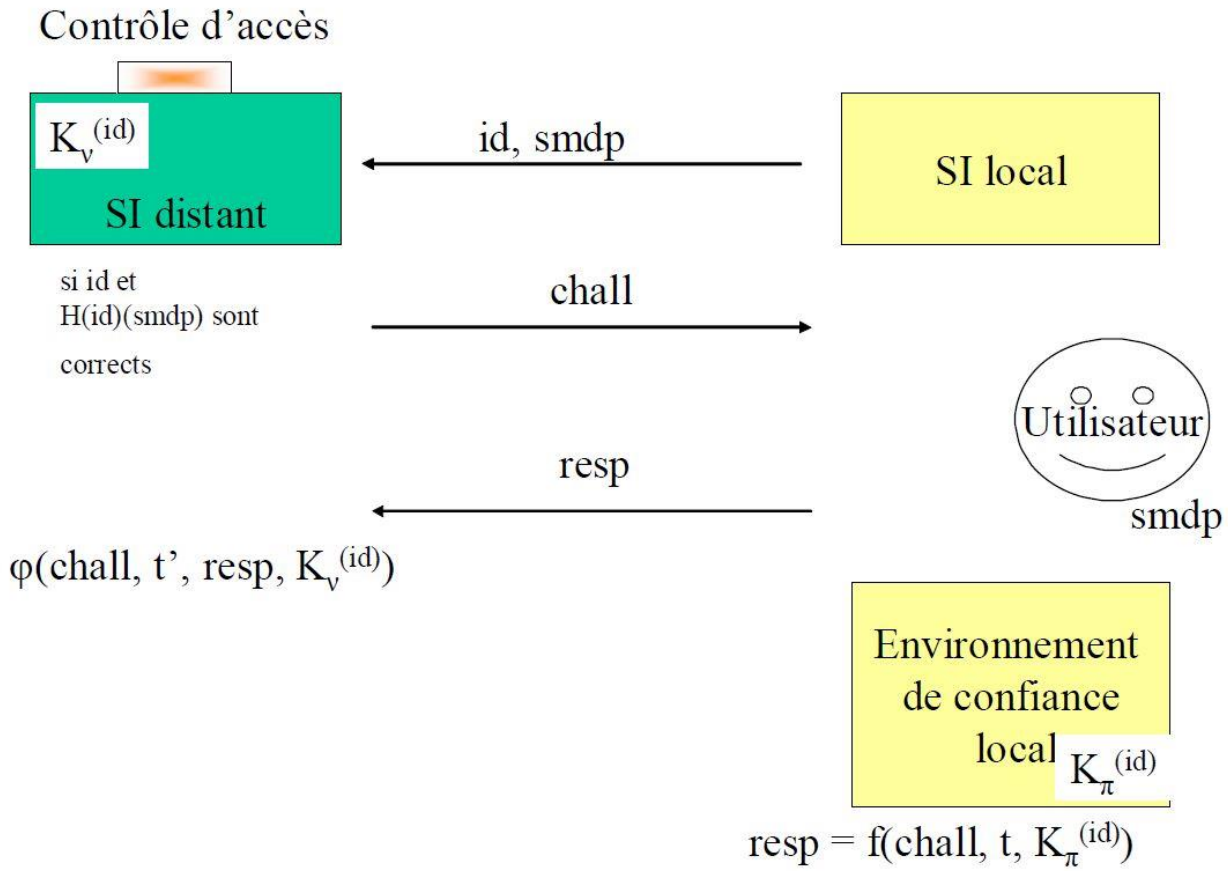


Figure 7 : Protocole générique de mot de passe dynamique

Le protocole peut alors se décomposer en étapes successives (voir figure 7) :

- La première étape du protocole consiste à envoyer au SI distant l'identifiant *id*. Cet identifiant peut être accompagné du mot de passe statique *smdp*.
  - L'intérêt de mettre en place un mot de passe statique est de ne poursuivre le protocole que si cette première vérification est correctement réalisée. S'il n'y a pas de mot de passe statique, alors il est possible de rechercher les identifiants valides en les énumérant pour détecter ceux qui donnent lieu au démarrage du protocole.
- Le SI distant compare alors le résultat de l'application de la fonction $H(^{id})$ au mot de passe transmis avec la valeur de référence qu'il possède.
  - L'utilisation d'une fonction différenciée par identifiant permet, si le fichier des mots de passe du SI distant est compromis, d'éviter qu'une attaque par dictionnaire pré-calculé puisse s'appliquer à l'ensemble des utilisateurs.
  - Le mot de passe statique doit être transmis tel quel par le SI local. En effet, si le SI local transmettait $H(^{id})(smdp)$, alors la compromission du fichier des mots de passe du SI distant donnerait immédiatement le moyen de passer la première étape du protocole.

    - Par conséquent, le mécanisme d'authentification de machines employé par le SI local pour authentifier le SI distant doit également permettre la protection en confidentialité de la session authentifiée.
- Le SI distant peut alors générer un défi aléatoire.
    - Cette étape peut ne pas intervenir si le mécanisme de mot de passe dynamique emploie uniquement un mécanisme de synchronisation. Dans ce cas, l'utilisation d'un mot de passe statique est inutile.
    - S'il y a utilisation d'un défi, celui-ci doit être aléatoire, c'est-à-dire imprédictible. Dans le cas contraire, un attaquant pourrait se retrouver dans une situation telle qu'il puisse demander à l'avance le calcul de réponses à des défis futurs.
- L'utilisateur retranscrit le défi sur son environnement de confiance.
    - L'utilisation de l'environnement de confiance peut nécessiter un déverrouillage particulier. Ce déverrouillage est toutefois indépendant du protocole de mot de passe dynamique.
    - Les contraintes ergonomiques font que l'entropie de ce défi ne peut être comparée à celle obtenue dans un protocole d'authentification cryptographique. C'est là une nouvelle raison pour que le mécanisme d'authentification de machines employé par le SI local pour authentifier le SI distant assure également la protection en confidentialité de la session authentifiée.
- L'environnement de confiance calcule la réponse à partir des différents éléments dont il dispose :
    - La clé de prouveur $K_{\pi}^{(id)}$,
    - un éventuel compteur de synchronisation t,
    - le défi chall éventuellement reçu.
        - La clé de prouveur peut être symétrique ou asymétrique. Il s'agit d'une clé cryptographique à part entière qui doit être gérée et protégée comme telle.
        - La clé de prouveur peut aussi prendre la forme d'un tableau de mots de passe. Dans ce cas le défi s'apparente à « répondre le mot de passe n° N » et chaque nouvelle réponse dévoile petit-à-petit l'intégralité de la clé.
        - Le compteur de synchronisation peut être synchronisé à une horloge interne. Il peut également être incrémenté à chaque utilisation de l'environnement de confiance.
- L'utilisateur retranscrit la réponse sur son SI local qui le transmet au SI distant.
    - Les contraintes ergonomiques font que l'entropie de la réponse ne peut être comparée à celle obtenue dans un protocole d'authentification cryptographique. Au contraire du mot de passe statique ou du défi qui ne sont pas indispensables, la protection de la réponse est obligatoire. Il est donc indispensable que le mécanisme d'authentification de machines employé par le SI local pour authentifier le SI distant assure également la protection en confidentialité de la session authentifiée.
- Le SI distant vérifie la réponse à partir des différents éléments dont il dispose :
    - la clé de vérifieur $K_{v}^{(id)}$,
    - son éventuel propre compteur de synchronisation t',
    - le défi chall éventuellement envoyé,
    - la réponse resp reçue.
        - Le caractère symétrique ou asymétrique de la clé de vérifieur est évidemment lié à celui de la clé de prouveur.
        - Si le temps est utilisé comme compteur de synchronisation, la période temporelle devra être suffisamment large pour garantir que les compteurs t et t'sont bien synchronisés.
        - Si le compteur est incrémenté à chaque authentification réussie, alors il faudra prévoir que l'environnement de confiance puisse être en avance si une erreur de transmission a, par exemple, interrompu l'exécution d'une instance du protocole. La fenêtre de

synchronisation a dans ce cas un impact sur la sécurité, car si on autorise *s* avances de l'environnement de confiance, un attaquant a *s* fois plus de chances de tomber sur une réponse qui satisfera le SI distant.

C.1.c. Conséquences sur les règles et recommandations à appliquer

C.1.c.1. Mécanismes cryptographiques

Les différents mécanismes cryptographiques utilisés doivent évidemment respecter les règles et recommandations du document « Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques ». Il s'agit :

- D'une part, du mécanisme d'authentification de machines qu'utilise le SI local pour authentifier le SI distant. Ce mécanisme doit en outre assurer la confidentialité de la session authentifiée.
- D'autre part, des fonctions de preuve f et de vérification φ qui doivent notamment ne pas divulguer d'information sur les clés cryptographiques employées.

C.1.c.2. Gestion des clés

Les différents mécanismes cryptographiques utilisent des clés dont la gestion doit évidemment respecter les règles et recommandations du document « Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques ».

C.1.c.3. Cas particulier du défi / réponse

Les contraintes ergonomiques font qu'il n'est pas possible d'employer des données de défi / réponse d'entropie comparable à celle obtenue dans un protocole d'authentification cryptographique. C'est la raison pour laquelle la session authentifiée entre le SI local et le SI distant doit être protégée en confidentialité, car statistiquement, la probabilité qu'un défi soit proposé plusieurs fois n'est pas négligeable.

C.1.c.3.1. Cas particulier de l'absence de synchronisation

Il est possible dans le protocole générique proposé de reposer uniquement sur le défi pour réaliser l'authentification par mot de passe dynamique. Il faut toutefois noter que dans ce cas, si un attaquant est en mesure d'observer des couples défi / réponse, il est en mesure de se constituer progressivement un dictionnaire et la probabilité que le SI distant lui propose un défi qu'il connaît déjà est soumise au paradoxe des anniversaires.

- Par exemple, si le défi peut être codé par 7 chiffres décimaux, le tableau de la figure 5 donne une entropie de 23 bits. Ceci donne une probabilité de contournement du mécanisme de $2^{11,5}$.

C.1.c.3.2. Cas général avec synchronisation anti-rejeu

Dans le cas général, le compteur de synchronisation peut être considéré comme un compteur anti-rejeu. Dans ce cas, et sous réserve que ce compteur ne soit jamais réinitialisé et ne boucle pas, l'entropie de la réponse est le facteur discriminant de la sécurité du protocole. Cette entropie doit le cas échéant être corrigée du nombre de tentatives possibles et de l'existence ou non d'une fenêtre de synchronisation.

Annexe C

Référentiel d’exigences applicables aux prestataires d’audit de la SSI

Historique des versions		
Date	**Version**	**Evolution du document**
xxx	1.0	Publication de la première version de l'annexe C du référentiel général de sécurité

Avant propos

Le présent référentiel est pris en application de l'article LP 20 de la loi du Pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices, et de son arrêté d'application.

Le présent document et ses annexes sont une copie adaptée du RGS C – Référentiel d'exigences applicables aux prestataires d'audit de la SSI, en vigueur en métropole, version 2.0 du 14 février 2013.

Le texte fait des renvois à des documents publiés par l'Agence nationale de la sécurité des systèmes d'information[123] (ANSSI) ou encore disponibles sur son site internet www.ssi.gouv.fr, en ce qu'ils reflètent l'état de l'art en matière de sécurité informatique.

Le référentiel et ses annexes sont disponibles en ligne sur le site internet www.lexpol.pf, et leur mise à jour est assurée par la Direction générale de l'économie numérique.

[123] L'ANSSI est un service à compétence nationale rattaché au Secrétaire général de la défense et de la sécurité nationale, l'autorité chargée d'assister le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale. Parmi ses nombreux objectifs, l'un deux consiste à promouvoir un espace de confiance pour les services en ligne. Elle y participe en ce sens notamment au travers de la règlementation (référentiels) et ses labels (certification des produits de sécurité et qualification des produits de sécurité et des prestataires de service de confiance).

I. Introduction

I.1. Présentation générale

I.1.1. Contexte

Les avantages et gains associés à la dématérialisation des processus et documents, aux échanges par voie électronique ainsi que l'interconnexion des systèmes d'information à Internet ne sont plus à démontrer mais ne sont pas sans risques. En effet, les points d'interconnexion avec l'extérieur (et en particulier les téléservices) sont autant d'accès qu'un attaquant externe à l'organisme peut tenter d'utiliser pour s'introduire au sein même du système d'information de l'organisme, pour dérober, dénaturer ou encore détruire son patrimoine informationnel. Les attaquants sont parfois des utilisateurs autorisés à accéder au système d'information (exemples : salariés, stagiaires, prestataires de l'organisme) et il convient de prendre également en considération cette source de menace.

Pour s'en protéger, les organismes doivent, à l'issue d'une démarche de gestion des risques, sécuriser leur système d'information de façon adaptée et proportionnée. Les mesures de sécurité mises en place dans ce but peuvent être de différentes natures : organisationnelles, physiques et techniques. Sur ce dernier volet, la mise en œuvre de produits de sécurité est certes fondamentale, mais elle ne suffit pas : l'absence d'application des mises à jour et des correctifs de sécurité, le maintien de mots de passe faibles ou constructeur, la mauvaise configuration de logiciels ou le non-respect de règles élémentaires de sécurité lors du développement d'un logiciel ou d'une application sont autant de vulnérabilités exploitables par un attaquant.

L'audit est l'un des moyens à disposition de tout organisme pour éprouver et s'assurer du niveau de sécurité de son système d'information. Il permet, en pratique, de mettre en évidence les forces mais surtout les faiblesses et vulnérabilités du système d'information. Ses conclusions permettent d'identifier des axes d'amélioration, de proposer des recommandations et de contribuer ainsi à l'élévation de son niveau de sécurité, en vue, notamment, de son homologation de sécurité.

I.1.2. Objet du document

Le présent document liste les règles et recommandations que les « prestataires d'audit de la sécurité des systèmes d'information » (PASSI) qualifiés délivrant des prestations d'audit d'architecture, d'audit de configuration, d'audit de code source, de tests d'intrusion, et d'audit organisationnel et physique doivent respecter.

Ce référentiel a vocation à permettre la qualification des prestataires d'audit de la sécurité des systèmes d'information, ci-après dénommés « prestataires d'audit », selon les modalités décrites au chapitre III.

Il permet à l'entité auditée de disposer de garanties sur la compétence du prestataire d'audit et de ses auditeurs, sur la qualité des audits qu'ils effectuent, sur la capacité du prestataire d'audit à lui apporter un conseil pertinent et adapté à son contexte et sur la confiance qu'elle peut leur accorder, notamment en matière de confidentialité, avant de lui donner accès à son système et aux informations qu'il contient.

Il peut être utilisé, à titre de bonnes pratiques, en dehors de tout contexte réglementaire lié à l'administration électronique, aux audits de sécurité des systèmes d'information de tous les types d'entités (administration, opérateur d'importance vitale, etc.).

Les prestataires d'audit doivent respecter les règles générales qui leur sont imposées en leur qualité de professionnel, notamment celles concernant leur devoir de conseil vis-à-vis de leurs clients, ainsi que la législation et la règlementation en vigueur et notamment les articles L. 323-1 et suivants du code pénal.

I.1.3. Structure du document

Le chapitre II décrit les activités d'audit visées par le présent référentiel.

Le chapitre III présente les modalités de la qualification, qui atteste de la conformité du prestataire d'audit aux exigences qui leur sont applicables. Ces exigences sont présentées en trois domaines : celles relatives au prestataire d'audit lui-même (chapitre IV), celles relatives à ses auditeurs (chapitre V) et celles relatives au déroulement de l'audit (chapitre VI).

L'annexe 1 présente les documents cités en référence.

L'annexe 2 donne des recommandations à l'intention des autorités administratives dans le but de les aider à exprimer leurs besoins en termes d'audit et à rédiger d'éventuels appels d'offres.

L'annexe 3 détaille les exemples de compétences techniques, théoriques et pratiques dont doit disposer un prestataire d'audit pour être qualifié.

L'annexe 4 propose une échelle de classification des vulnérabilités.

I.2. Identification du document

Le présent référentiel est dénommé « Prestataires d'audit de la sécurité des systèmes d'information – référentiel d'exigences ». Il peut être identifié par son nom, numéro de version et sa date de mise à jour.

I.3. Définitions et acronymes

I.3.1. Acronymes

Les acronymes utilisés dans le présent référentiel sont les :

ANSSI	Agence nationale de la sécurité des systèmes d'information
PASSI	Prestataire d'audit de la sécurité des systèmes d'information
RGS	Référentiel Général de Sécurité

I.3.2. Définitions

Référentiel - le présent document.

Autorité administrative - Ce terme générique, défini à l'article LP 1 de la [LOI DU PAYS], désigne la Polynésie française, ses établissements publics, les autorités administratives indépendantes, les organismes de protection sociale et les autres organismes et personnes de droit public et de droit privé chargés d'une mission de service public administratif.

Système d'information - tout ensemble de moyens destinés à élaborer, traiter, stocker ou transmettre des informations faisant l'objet d'échanges par voie électronique entre autorités administratives et usagers ainsi qu'entre autorités administratives.

Sécurité d'un système d'information - ensemble des moyens techniques et non-techniques de protection, permettant à un système d'information de résister à des événements susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données, traitées ou transmises et des services connexes que ces systèmes offrent ou rendent accessibles.

Audit - processus systématique, indépendant et documenté en vue d'obtenir des preuves d'audit et de les évaluer de manière objective pour déterminer dans quelle mesure les critères d'audit sont satisfaits. Pour les besoins du Référentiel, un audit est constitué d'un sous-ensemble des activités d'audit de la sécurité d'un système d'information décrites au chapitre II et des recommandations assorties.

Critères d'audit - ensemble des référentiels, guides, procédures ou exigences applicables à la sécurité du système d'information audité.

Preuves d'audit - enregistrements, énoncés de faits ou autres informations qui se rapportent aux critères

d'audit et sont vérifiables.

Constats d'audit - résultats de l'évaluation des preuves d'audit recueillies par rapport aux critères d'audit.

Prestataire d'audit - organisme réalisant des prestations d'audit de la sécurité des systèmes d'information.

Auditeur - personne réalisant un audit pour le compte d'un prestataire d'audit.

Responsable d'équipe d'audit - personne responsable de l'audit et de la constitution de l'équipe d'audit, en particulier de la complémentarité de leur compétence.

Commanditaire de l'audit - organisme ou personne pour le compte duquel l'audit est mené.

Audité - organisme(s) responsable(s) de tout ou partie du système d'information audité[124]. Le commanditaire de l'audit peut être l'audité.

Périmètre d'audit - environnement physique, logique et organisationnel dans lequel se trouve le système d'information ou la portion du système d'information, sur lequel l'audit est effectué.

Convention d'audit - accord écrit entre un commanditaire d'audit et un prestataire d'audit pour la réalisation d'un audit. Dans le cas où le prestataire d'audit est un organisme privé, la convention d'audit est le contrat.

Rapport d'audit - document de synthèse élaboré par l'équipe d'audit et remis au commanditaire de l'audit à l'issue de l'audit. Il présente les résultats de l'audit et en particulier les vulnérabilités découvertes ainsi que les mesures correctives proposées.

État de l'art - ensemble des bonnes pratiques, des technologies et des documents de référence relatifs à la sécurité des systèmes d'information publiquement accessibles à un instant donné, et des informations qui en découlent de manière évidente. Ces documents peuvent être mis en ligne sur Internet par la communauté de la sécurité des systèmes d'information, diffusés par des organismes de référence ou encore d'origine réglementaire.

[124] Exemples : prestataires d'hébergement, d'infogérance, d'exploitation et d'administration du système d'information, de tierce maintenance applicative, etc.

II. Activités d'audit visées par le référentiel

Ce chapitre présente les différentes activités d'audit traitées dans le présent document et dont les exigences spécifiques associées sont décrites au chapitre VI.

Chaque activité d'audit est, par principe, associée à la fourniture d'un rapport d'audit regroupant des recommandations et dont la forme et le contenu est décrit au chapitre VI.6.

L'annexe 2 fournit des recommandations de l'ANSSI sur les types d'audit à réaliser en fonction du périmètre de l'audit.

II.1. Audit d'architecture

L'audit d'architecture consiste en la vérification de la conformité des pratiques de sécurité relatives au choix, au positionnement et à la mise en œuvre des dispositifs matériels et logiciels déployés dans un système d'information à l'état de l'art et aux exigences et règles internes de l'audité. L'audit peut être étendu aux interconnexions avec des réseaux tiers, et notamment Internet.

II.2. Audit de configuration

L'audit de configuration a pour vocation de vérifier la mise en œuvre de pratiques de sécurité conformes à l'état de l'art et aux exigences et règles internes de l'audité en matière de configuration des dispositifs matériels et logiciels déployés dans un système d'information. Ces dispositifs peuvent notamment être des équipements réseau, des systèmes d'exploitation (serveur ou poste de travail), des applications ou des produits de sécurité.

II.3. Audit de code source

L'audit de code source consiste en l'analyse de tout ou partie du code source ou des conditions de compilation d'une application dans le but d'y découvrir des vulnérabilités, liées à de mauvaises pratiques de programmation ou des erreurs de logique, qui pourraient avoir un impact en matière de sécurité.

II.4. Tests d'intrusion

Le principe du test d'intrusion est de découvrir des vulnérabilités sur le système d'information audité et de vérifier leur exploitabilité et leur impact, dans les conditions réelles d'une attaque sur le système d'information, à la place d'un attaquant potentiel. Les vulnérabilités testées peuvent également avoir été identifiées au cours d'autres activités d'audit définies dans ce chapitre.

Cette activité d'audit peut être réalisée soit depuis l'extérieur du système d'information audité (notamment depuis Internet ou le réseau interconnecté d'un tiers), soit depuis l'intérieur.

Un test d'intrusion seul n'a pas vocation à être exhaustif. Il s'agit d'une activité qui doit être effectuée en complément d'autres activités d'audit afin d'en améliorer l'efficacité ou de démontrer la faisabilité de l'exploitation des failles et vulnérabilités découvertes à des fins de sensibilisation.

Les tests de vulnérabilité, notamment automatisés, ne représentent pas à eux seuls une activité d'audit au sens du Référentiel.

II.5. Audit organisationnel et physique

L'audit de l'organisation de la sécurité logique et physique vise à s'assurer que :

- Les politiques et procédures de sécurité définies par l'audité pour assurer le maintien en conditions opérationnelles et de sécurité d'une application ou de tout ou partie du système d'information sont conformes au besoin de sécurité de l'organisme audité, à l'état de l'art ou aux normes en vigueur ;

- Elles complètent correctement les mesures techniques mises en place ;
- Elles sont efficacement mises en pratique ;
- Les aspects physiques de la sécurité de l'application ou du système d'information sont correctement couverts.

III. Qualification des prestataires d'audit

III.1. Modalités de la qualification

Le Référentiel contient les exigences et les recommandations à destination des prestataires d'audit. Les exigences doivent être respectées par les prestataires d'audit dans le but d'obtenir la qualification. Les recommandations sont données à titre de bonnes pratiques et ne font pas l'objet d'une quelconque vérification en vue de la qualification.

Le Référentiel donne également des recommandations afin d'orienter les autorités administratives, et plus généralement les commanditaires d'audits, dans leurs expressions de besoins, et les prestataires d'audit dans les solutions qu'ils leur proposent.

La qualification des prestataires d'audit est réalisée conformément aux modalités prévues par l'article LP 22 de la [LOIDUPAYS].

III.2. Portée de la qualification

Le prestataire d'audit peut demander la qualification pour tout ou partie des activités d'audit décrites au chapitre II. Toutefois, la qualification d'un prestataire d'audit ne portant que sur l'activité de tests d'intrusion ou l'activité d'audit organisationnel et physique n'est pas autorisée, une telle activité étant jugée insuffisante si elle est menée seule.

Le prestataire d'audit respectera en conséquence les exigences du chapitre VI.2 en cohérence avec la portée demandée.

La qualification est notamment accordée au regard de la compétence des auditeurs qui réaliseront les prestations qualifiées. Les auditeurs seront reconnus compétents pour tout ou partie des activités pour lequel le prestataire d'audit a demandé la qualification, à l'issue d'un processus d'évaluation par rapport à l'état de l'art. Les auditeurs ainsi que les activités d'audit pour lesquelles ils ont été reconnus compétents sont inscrits dans un registre.

Est considérée comme une prestation qualifiée au sens du Référentiel, une activité d'audit telle que décrite au chapitre II réalisée par un ou plusieurs auditeurs reconnus compétents pour cette activité d'audit et travaillant pour un prestataire d'audit qualifié pour cette même activité d'audit. Une prestation d'audit qualifiée est associée à la fourniture, au commanditaire de l'audit, de recommandations destinées à élever le niveau de sécurité du système d'information de l'audité.

Les prestataires d'audit qualifiés gardent la faculté de réaliser des prestations de services en dehors du périmètre pour lequel ils sont qualifiés, mais ne peuvent, dans ce cas, se prévaloir de la qualification sur ces prestations.

Une prestation qualifiée peut être associée à d'autres prestations complémentaires (développement, intégration de produits de sécurité, etc.) sans perdre le bénéfice de la qualification.

IV. Exigences relatives au prestataire d'audit

IV.1. Exigences générales

Les exigences listées dans ce chapitre portent sur les domaines suivants : juridique, structurel, responsabilité et impartialité du prestataire d'audit.

a) Le prestataire d'audit doit être une entité ou une partie d'une entité dotée de la personnalité morale de façon à pouvoir être tenu juridiquement responsable de toutes ses activités d'audit.

   Une autorité administrative qui réalise des activités d'audit peut être considérée comme un prestataire d'audit quand elle réalise tout ou partie de ces activités pour le compte d'autres entités juridiques.

b) Le prestataire d'audit réalise ses audits dans le cadre d'une convention d'audit préalablement approuvée par le commanditaire de l'audit. La loi applicable à la convention d'audit est la loi française. La convention d'audit doit être conforme aux exigences du chapitre VI.1 du Référentiel.

c) Le prestataire d'audit assume la responsabilité de l'audit qu'il réalise pour le compte du commanditaire de l'audit et, en particulier, des dommages éventuellement causés au cours de l'audit.

   Le prestataire d'audit et le commanditaire de l'audit peuvent préciser les modalités de partage des responsabilités au sein de la convention d'audit. Le prestataire d'audit peut s'exonérer de tout ou partie de sa responsabilité s'il est avéré que le dommage éventuellement subi par le commanditaire de l'audit résulte d'un défaut d'information de ce dernier.

   Il est recommandé que le prestataire d'audit garde, notamment, la responsabilité des actions qu'il effectue lors de l'audit de son propre fait ainsi que de celles pour lesquelles le commanditaire de l'audit ne dispose pas de compétence particulière.

d) Le prestataire d'audit doit pouvoir apporter la preuve qu'il a évalué les risques résultant de ses activités d'audit et qu'il a pris les dispositions appropriées pour couvrir les risques résultant de ses prestations d'audit. Il met à disposition du commanditaire de l'audit ces éléments de preuve.

   Il est, à ce titre, recommandé que le prestataire d'audit souscrive une assurance couvrant les dommages éventuellement causés aux systèmes d'information de ses clients.

e) Le prestataire d'audit peut sous-traiter une partie de l'audit demandé par le commanditaire de l'audit à un prestataire d'audit qualifié conforme aux exigences du Référentiel qui lui sont applicables sous réserve que :

   - Il existe une convention ou un cadre contractuel documentés entre le prestataire d'audit et le sous-traitant ;
   - Le recours à la sous-traitance est connu et accepté par le commanditaire de l'audit et l'audité.

f) Le prestataire d'audit est tenu de respecter la législation et la réglementation en vigueur sur le territoire français, notamment en matière de traitements de données à caractère personnel[125], de prêt

[125] Loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, loi n° 91-646 d 10 juillet 1991 modifiée sur le secret des correspondances, loi n° 2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle.

de main d'œuvre illicite, de propriété intellectuelle[126] et de fraude informatique[127].

g) Le prestataire d'audit doit décrire l'organisation de son activité d'audit au bénéfice de chaque commanditaire d'audit.

h) Le prestataire d'audit doit garantir que les informations qu'il fournit, y compris la publicité, ne sont ni fausses ni trompeuses.

i) Le prestataire d'audit doit s'assurer du consentement du commanditaire de l'audit avant toute communication au public d'éléments d'information relatifs à l'audit, à l'audité ou au commanditaire de l'audit, que ces informations soient obtenues lors de l'audit ou non.

j) Le prestataire d'audit doit s'engager à ce que les audits qu'il effectue soient réalisés en toute impartialité.

i) Le prestataire d'audit doit être en mesure d'apporter une preuve suffisante que les modalités de son fonctionnement, notamment financières, ne sont pas susceptibles de compromettre son impartialité et la qualité de ses prestations à l'égard du commanditaire de l'audit ou de provoquer des conflits d'intérêts.

k) Tous les documents produits par le prestataire d'audit lors des audits doivent être au moins fournis en langue française.

l) Le prestataire d'audit doit réaliser la prestation de manière loyale, en toute bonne foi et dans le respect de l'audité, de son personnel et de ses infrastructures.

Les exigences IV.1.a et IV.1.d ne s'appliquent qu'aux prestataires d'audit privés.

IV.2. Charte d'éthique

a) Le prestataire d'audit doit disposer d'une charte d'éthique prévoyant notamment que :

- Les prestations d'audit sont réalisées avec loyauté, discrétion, impartialité et indépendance ;
- Les auditeurs ne recourent qu'aux méthodes, outils et techniques validés par le prestataire d'audit ;
- Les auditeurs s'engagent à ne pas divulguer, y compris aux autres auditeurs du prestataire d'audit non concernés par l'audit, d'informations obtenues ou générées dans le cadre des audits sauf autorisation du commanditaire de l'audit ;
- Les auditeurs signalent au commanditaire de l'audit tout contenu manifestement illicite découvert durant l'audit ;
- Les auditeurs s'engagent à respecter la loi, la réglementation en vigueur ainsi que les bonnes pratiques liées à l'audit.

b) L'ensemble des auditeurs évalués au titre de la qualification du prestataire d'audit doivent signer la charte d'éthique prévue au paragraphe précédent préalablement à la réalisation d'un quelconque audit.

[126] Exemples : licences des logiciels utilisés, des scripts et programmes développés.

[127] Articles 323-1 et suivants du code pénal.

IV.3. Gestion des ressources et des compétences

a) Le prestataire d'audit doit employer un nombre suffisant d'auditeurs, de responsables d'équipe d'audit et éventuellement de sous-traitants pour assurer totalement et dans tous leurs aspects les audits pour lesquels il a établi des conventions d'audit avec des commanditaires d'audits.

b) Le prestataire d'audit doit s'assurer, pour chaque audit, que les auditeurs désignés pour réaliser l'audit ont les qualités et les compétences requises.

   Des auditeurs débutants du prestataire d'audit peuvent, au titre de leur formation et de leur montée en compétence, être incorporés à l'équipe d'audit. Ils doivent cependant respecter la charte d'éthique du prestataire d'audit ainsi que l'ensemble des obligations contractuelles, réglementaires ou légales imposées aux auditeurs.

c) Le prestataire d'audit doit s'assurer du maintien à jour des compétences des auditeurs. Pour cela, il doit disposer d'un processus de formation et assurer une veille technologique[128].

d) En matière de recrutement, le prestataire d'audit doit procéder à une vérification des formations, qualifications et références professionnelles des auditeurs candidats et de la véracité de leur CV. Le prestataire d'audit peut également demander au candidat une copie du bulletin n° 3 de son casier judiciaire.

e) Un processus disciplinaire doit être élaboré par le prestataire d'audit à l'intention des salariés ayant enfreint les règles de sécurité ou la charte d'éthique.

f) Le prestataire d'audit est responsable des méthodes, outils (logiciels ou matériels) et techniques utilisés par ses auditeurs et de leur bonne utilisation (précautions d'usage, maîtrise de la configuration…). Pour cela, il doit mettre en œuvre un processus de formation des auditeurs à ses outils et assurer une veille technologique sur leur mise à jour et leur pertinence.

g) Le prestataire d'audit justifie, au travers des auditeurs évalués au titre de la qualification du prestataire d'audit, qu'il dispose des compétences techniques, théoriques et pratiques, afférentes aux activités d'audit citées aux chapitres II.1 à II.4, couvrant les domaines suivants :
   a. Réseaux et protocoles ;
   b. Systèmes d'exploitation ;
   c. Couches applicatives ;
   d. Équipements et logiciels de sécurité ;
   e. Développement d'outils utilisés adaptés à la cible auditée dans le cadre des audits ou des tests d'intrusion ;
   f. Techniques d'ingénierie inverse ;
   g. Exigences techniques requises par le RGS.

   Ces domaines sont détaillés en annexe 3.

h) Le prestataire d'audit justifie, au travers des auditeurs évalués au titre de la qualification du prestataire d'audit, qu'il dispose des compétences organisationnelles, théoriques et pratiques, afférentes aux activités d'audit citées au chapitre II.5, couvrant les domaines suivants :

[128] Le prestataire d'audit peut par exemple mettre en place une formation continue, des modules d'auto-formation, des séminaires internes, s'abonner à des revues spécialisées, contracter avec un ou plusieurs CERT, disposer d'un accès à une ou plusieurs bases de vulnérabilités offrant un certain niveau de garantie en matière de couverture et de réactivité ou toute autre méthode lui permettant d'assurer l'évolutivité de ses compétences ainsi que celles de ses auditeurs.

a. Maîtrise des normes relatives à la sécurité des systèmes d'information ;
b. Maîtrise des domaines relatifs à l'organisation de la sécurité des systèmes d'information ;
c. Maîtrise des pratiques liées à l'audit.

Ces domaines sont détaillés en annexe 3.

i) Le prestataire d'audit justifie, au travers des auditeurs évalués au titre de la qualification du prestataire d'audit, qu'il maîtrise les référentiels et guides relatifs à la sécurité des systèmes d'information.

Ces référentiels et guides sont détaillés en annexe 3.

IV.4. Protection de l'information du prestataire d'audit

Les informations sensibles relatives aux audits, et notamment les preuves, les constats et les rapports d'audit, doivent être protégés au minimum au niveau Diffusion Restreinte.

Le système d'information que le prestataire d'audit utilise pour le traitement de ces informations doit respecter les règles établies par l'ANSSI et relatives aux mesures de protection des systèmes d'information traitant d'information sensibles non classifiées de défense de niveau Diffusion Restreinte.

L'ANSSI recommande l'application du Guide d'hygiène informatique cité en annexe 1.

V. Exigences relatives aux auditeurs

V.1. Aptitudes générales

a) L'auditeur doit disposer des qualités personnelles décrites au chapitre 7.2 de la norme ISO 19011.

b) L'auditeur doit maîtriser la réglementation applicable aux activités d'audits qu'il met en œuvre (maîtrise de la réglementation spécifique aux types d'audits, à la nature ou au secteur d'activité du commanditaire de l'audit et de l'audité, etc.).

c) L'auditeur doit disposer de qualités rédactionnelles et de synthèse et savoir s'exprimer à l'oral de façon claire et compréhensible, en langue française.

d) L'auditeur met régulièrement à jour ses compétences par une veille active sur celles-ci, sur la méthodologie, les techniques ou les outils utilisés lors des activités d'audit.

e) Il est recommandé que l'auditeur participe à l'évolution de l'état de l'art par une participation à des évènements professionnels de son domaine de compétence, à des travaux de recherche ou la publication d'articles.

V.2. Expérience

L'auditeur doit avoir reçu une formation en technologie des systèmes d'information et de communication et en audit.

Il est recommandé que l'auditeur :

- Justifie d'aux moins deux années d'expérience dans le domaine des systèmes d'information et de communication ;
- Justifie d'au moins une année d'expérience dans le domaine de la sécurité des systèmes d'information ;
- Justifie d'au moins une année d'expérience dans le domaine de l'audit de systèmes d'information.

Ces recommandations ne sont pas cumulatives.

V.3. Aptitudes et connaissances spécifiques aux activités d'audit

a) L'auditeur doit maîtriser les bonnes pratiques et la méthodologie d'audit décrite dans la norme ISO 19011 et être en mesure de réaliser des audits conformément aux exigences relatives au déroulement d'une prestation d'audit (cf. chapitre VI).

b) L'auditeur doit être compétent dans au moins une des activités d'audit décrites au chapitre II pour lesquelles le prestataire d'audit demande la qualification. Pour cela, l'auditeur doit disposer de connaissances techniques ou organisationnelles approfondies dans au moins un des domaines cités dans les paragraphes IV.3.g et IV.3.h.

c) Il est recommandé que l'auditeur soit sensibilisé à l'ensemble des autres activités d'audit pour lesquelles le prestataire d'audit demande la qualification.

d) Le responsable d'audit doit disposer des compétences de gestion d'équipe nécessaires à la constitution adéquate de l'équipe d'audit par rapport aux objectifs visés dans la convention d'audit.

e) L'auditeur doit avoir un sens pédagogique et des connaissances en matière d'exploitation des systèmes d'information afin de pouvoir proposer, à différents types d'acteurs, des recommandations adaptées aux vulnérabilités identifiées.

f) L'auditeur doit pouvoir exposer et adapter un rapport d'audit et les recommandations associées à des publics distincts (services techniques, organe de direction, etc.).

V.4. Engagements

a) L’auditeur doit avoir un contrat de travail avec le prestataire d’audit.

b) L’auditeur doit avoir signé la charte d’éthique élaborée par le prestataire d’audit.

c) L’auditeur doit s’engager à subir une évaluation personnelle de ses compétences au titre de la procédure de qualification du prestataire d’audit dont il dépend.

VI. Exigences relatives au déroulement d'un audit

La définition du périmètre de l'audit et la description de l'audit attendu, formulées généralement dans un appel d'offres, sont du ressort du commanditaire de l'audit. L'annexe 2 du Référentiel fournit des recommandations de l'ANSSI à cet effet.

Bien que le prestataire d'audit ne puisse qu'adapter et moduler sa proposition de service à la demande, il doit informer, dans la mesure du possible, et à titre de conseil, le commanditaire de l'audit des recommandations issues de l'annexe 2.

Le prestataire d'audit s'assure que le commanditaire lui fournit un environnement de travail adapté à ses missions.

Le prestataire d'audit vérifie que le commanditaire a identifié correctement le système audité ainsi que ses dépendances externes.

Le prestataire d'audit s'assure que l'audit est adapté au contexte et aux objectifs souhaités par le commanditaire de l'audit.

A défaut, le prestataire d'audit en informe le commanditaire de l'audit préalablement à l'audit.

- Dans la suite de ce chapitre, les exigences auxquelles doivent se conformer les prestataires d'audit sont regroupées dans les différentes étapes du déroulement d'un audit, à savoir :
- Établissement de la convention d'audit ;
- Préparation et déclenchement de l'audit ;
- Exécution de l'audit (les exigences spécifiques à chacune des activités d'audit sont listées) ;
- Élaboration du rapport d'audit ;
- Conclusion de l'audit.

D'une manière générale, le déroulement de l'audit doit respecter les dispositions de la norme ISO 19011.

VI.1. Etablissement de la convention d'audit

a) La convention d'audit établie entre le prestataire d'audit et le commanditaire de l'audit doit :

- Décrire le périmètre et les modalités de l'audit (jalons, livrables attendus en entrée, livrables prévus en sortie, objectifs, champs et critères de l'audit, etc.) ;
- Préciser les noms, rôles, responsabilités et le besoin d'en connaître des personnes désignées par le prestataire d'audit, le commanditaire de l'audit et l'audité ;
- Prévoir que l'audit ne peut débuter sans une autorisation formelle du commanditaire de l'audit ;
- Préciser les actions qui ne peuvent être menées sur le système d'information à auditer ou sur les données recueillies sans autorisation expresse du commanditaire de l'audit et éventuellement accord ou présence de l'audité, ainsi que leurs modalités (mise en œuvre, personnes présentes, durée, plage horaire, exécutant, description des données sensible et des actions autorisées, etc.) ;
- Préciser les dispositions d'ordre logistique mises à disposition du prestataire d'audit par l'audité (moyens matériels, humains, techniques, etc.) ;
- Inclure les clauses relatives à l'éthique du prestataire d'audit ;
- Prévoir la non divulgation à un tiers, par le prestataire d'audit et par les auditeurs, de toute information relative à l'audit et à l'audité, sauf autorisation écrite ;

- Stipuler que le prestataire d'audit ne fait pas intervenir d'auditeur n'ayant pas de relation contractuelle avec lui, n'ayant pas signé sa charte d'éthique ou ayant fait l'objet d'une inscription au bulletin n° 3 du casier judiciaire en lien avec les systèmes d'information ;
- Prévoir une clause relative aux risques potentiels liés à la prestation, notamment en matière de disponibilité (déni de service lors du scan de vulnérabilités d'une machine ou d'un serveur par exemple) ;
- Préciser si le prestataire d'audit dispose d'une assurance couvrant les dommages éventuellement causés lors de la réalisation des activités d'audit et, le cas échéant, la surface de couverture de celle-ci ;
- Définir les règles de titularité des éléments protégés par la propriété intellectuelle tels que les outils développés spécifiquement pour l'audit ou le rapport d'audit ;
- Préciser les modalités de conservation, de restitution ou de destruction le cas échéant en fin de mission, des preuves, des constats, des rapports d'audit et des informations ou documents relatifs au système d'information audité obtenue par le prestataire d'audit ;
- Prévoir les livrables ainsi que leurs modalités de restitution ;
- Décrire les publics destinataires des recommandations présentes dans le rapport d'audit ;
- Préciser les modalités (contenu, forme, portée, etc.) de rédaction des recommandations.

b) Le prestataire d'audit peut sous-traiter une partie de l'audit demandé par le commanditaire de l'audit à un prestataire d'audit qualifié conforme aux exigences du présent référentiel sous réserve que :
   - Il existe une convention ou un cadre contractuel documentés entre le prestataire d'audit et le sous-traitant ;
   - Le recours à la sous-traitance est connu et accepté par le commanditaire et l'audité.

c) Il est recommandé que la convention prévoie une procédure de recueil du consentement des audités et des éventuels partenaires pour la réalisation de l'audit.

VI.2. Préparation et déclenchement de l'audit

a) Le prestataire d'audit doit nommer un responsable d'équipe d'audit pour tout audit qu'il effectue.

b) Le responsable d'équipe d'audit doit constituer une équipe d'auditeurs ayant les compétences adaptées à la nature de l'audit. Le responsable d'équipe d'audit peut, s'il dispose des compétences suffisantes, réaliser l'audit lui-même et seul. Il peut incorporer à l'équipe d'audit des auditeurs débutants, au titre de leur formation et de leur montée en compétence sous réserve du respect des obligations décrites au paragraphe IV.3.b alinéa 2.

c) Le responsable d'équipe d'audit doit, dès le début de la préparation de l'audit, établir un contact avec les personnes responsables de l'audit chez l'audité. Ce contact, formel ou informel, a notamment pour objectif d'établir les circuits de communication et de préciser les modalités d'exécution de l'audit.

d) Le responsable d'audit s'assure auprès du commanditaire et de l'audité que les représentants légaux des entités impactées par l'audit ont été préalablement avertis et qu'ils ont donné leur accord.

e) Le responsable d'équipe d'audit élabore un plan d'audit. Ce plan d'audit couvre en particulier les points suivants : les objectifs, champs et critères de l'audit, le périmètre technique et organisationnel de la prestation, les dates et lieux où seront menées les activités d'audit et notamment celles éventuellement menées chez l'audité, les informations générales sur les réunions de démarrage et de clôture de la prestation, les auditeurs qui constituent l'équipe d'audit, la confidentialité des données

récupérées et l'anonymisation des constats et des résultats.

f) Les objectifs, le champ, les critères et le planning de l'audit doivent être définis entre le prestataire d'audit et le commanditaire de l'audit, en considération des contraintes d'exploitation du système d'information de l'audité. Ces éléments doivent figurer dans la convention d'audit ou dans le plan d'audit.

g) En fonction de l'activité d'audit, l'équipe d'auditeurs doit obtenir, au préalable, toute la documentation existante (exemples : politique de sécurité, analyse des risques, procédures d'exploitation de la sécurité, etc.) de l'audité relative à la cible auditée dans l'objectif d'en faire une revue.

h) L'audit ne doit débuter qu'après une réunion formelle au cours de laquelle les représentants habilités du prestataire d'audit et ceux de l'audité confirment leur accord sur l'ensemble des modalités de la prestation. Cette réunion peut être téléphonique mais doit, dans ce cas, faire l'objet d'une confirmation écrite.

i) Le prestataire d'audit doit sensibiliser avant l'audit son client sur l'intérêt de sauvegarder et préserver les données, applications et systèmes présents sur les machines auditées.

j) En préalable, et dans le cas spécifique des tests d'intrusion, une fiche d'autorisation doit être signée par le commanditaire de l'audit, l'audité et d'éventuelles tierces parties. Elle précise en particulier :

- La liste des cibles auditées (adresses IP, noms de domaine, etc.) ;
- La liste des adresses IP de provenance des tests ;
- La date et les heures exclusives des tests ;
- La durée de l'autorisation.

VI.3. Exécution de l'audit

a) Le responsable d'équipe d'audit doit tenir informé le commanditaire de l'audit des vulnérabilités critiques découvertes au cours de l'audit. Il doit rendre compte immédiatement à l'audité de tout élément constaté présentant un risque immédiat et significatif, et dans la mesure du possible, lui proposer des mesures permettant de lever ce risque.

b) L'audit doit être réalisé dans le respect des personnels et des infrastructures physiques et logiques de l'audité.

c) Les constatations et observations effectuées par les auditeurs doivent être factuelles et basées sur la preuve.

d) Les auditeurs doivent rendre compte des constats d'audit au responsable d'équipe d'audit, lequel peut en avertir sans délai sa hiérarchie ainsi que l'audité, dans le respect des clauses de confidentialité fixées dans la convention d'audit.

e) Toute modification effectuée sur le système d'information audité, durant l'audit, doit être tracée, et en fin d'audit, le système d'information concerné doit retrouver un état dont la sécurité n'est pas dégradée par rapport à l'état initial.

f) Les constats d'audit doivent être documentés, tracés, et conservés, par le prestataire d'audit, durant toute la durée de l'audit.

g) Le prestataire d'audit et les auditeurs doivent prendre toutes les précautions utiles pour préserver la confidentialité des documents et informations relatives à l'audité.

h) Les actions et résultats des auditeurs du prestataire d'audit sur le système d'information audité, ainsi

que leurs dates de réalisation, devraient être tracés. Ces traces peuvent par exemple servir à identifier les causes d'un incident technique survenu lors de l'audit.

VI.4. Exigences relatives au prestataire d'audit

Lorsqu'elles sont demandées par le commanditaire de l'audit, les activités d'audit réalisées par le prestataire d'audit doivent être conformes aux exigences précisées dans les chapitres VI.4.1 à VI.4.5.

Le cas échéant, conformément au RGS, il est recommandé d'utiliser des produits qualifiés.

Remarques :

- Les activités techniques décrites dans les paragraphes VI.4.1 à VI.4.4 n'excluent pas l'évaluation de l'organisation de la sécurité logique et physique des éléments audités. Cette évaluation consiste en la vérification que les politiques de sécurité et procédures définies pour assurer le maintien en conditions de sécurité du système d'information audité sont conformes à l'état de l'art ;
- Les énumérations listées dans les chapitres VI.4.1 à VI.4.5 sont données à titre indicatif et ne sont pas exhaustives. Par ailleurs, elles ne doivent être réalisées que lorsqu'elles sont applicables à la cible auditée.

VI.4.1. Audit d'architecture

a) Le prestataire d'audit doit procéder à la revue des documents suivants lorsqu'ils existent :
   - Schémas d'architectures de niveau 2 et 3 du modèle OSI ;
   - Matrices de flux ;
   - Règles de filtrage ;
   - Configuration des équipements réseau (routeurs et commutateurs) ;
   - Interconnexions avec des réseaux tiers ou Internet ;
   - Analyses de risques système ;
   - Documents d'architecture technique liés à la cible.

b) Le prestataire d'audit doit pouvoir organiser des entretiens avec le personnel concerné par la mise en place et l'administration de la cible auditée, notamment en ce qui concerne les procédures d'administration.

VI.4.2. Audit de configuration

a) Les éléments de configuration des cibles auditées doivent être fournis au prestataire d'audit. Ils peuvent être récupérés manuellement ou automatiquement, à partir d'un accès privilégié sur les cibles auditées, sous la forme de fichiers de configuration ou de captures d'écran.

   Cette action peut être entreprise directement par l'auditeur après accord de l'audité.

   Il est recommandé que le prestataire d'audit vérifie, conformément à l'état de l'art ou aux exigences et règles spécifiques de l'audité, la sécurité des configurations :

   - Des équipements réseau filaire ou sans fil de type commutateurs ou routeurs ;
   - Des équipements de sécurité (type pare-feu ou relais inverse (filtrant ou non) et leurs règles de filtrage, chiffreurs, etc.) ;
   - Des systèmes d'exploitation ;

- Des systèmes de gestion de bases de données ;
- Des services d'infrastructure ;
- Des serveurs d'applications ;
- Des postes de travail ;
- Des équipements de téléphonie ;
- Des environnements de virtualisation.

VI.4.3. Audit de code source

a) Le code source, la documentation relative à la mise en œuvre, les méthodes et rapports de tests et l'architecture du système d'information audité doivent être fournis au prestataire d'audit ainsi que la configuration des éléments de compilation et d'exécution, dans les limites des droits dont disposent le commanditaire de l'audit et l'audité.

b) Il est recommandé de procéder à des entretiens avec un développeur ou le responsable de la mise en œuvre du code source audité afin de disposer d'informations relatives au contexte applicatif, aux besoins de sécurité et aux pratiques liées au développement.

c) Il est recommandé que l'audit de code fasse préalablement l'objet d'une analyse de la sécurité de l'application auditée afin de limiter l'audit aux parties critiques de son code.

d) Il est recommandé que le prestataire d'audit vérifie la sécurité des parties du code source relatives :

- Aux mécanismes d'authentification ;
- Aux mécanismes cryptographiques ;
- À la gestion des utilisateurs ;
- Au contrôle d'accès aux ressources ;
- Aux interactions avec d'autres applications ;
- Aux relations avec les systèmes de gestion de bases de données ;
- À la conformité à des exigences de sécurité relative à l'environnement dans laquelle est déployée l'application.

e) Il est recommandé que le prestataire d'audit recherche les vulnérabilités les plus répandues dans les domaines suivants : cross-site scripting, injections SQL, cross-site request forgery, erreurs de logique applicative, débordement de tampon, exécution de commandes arbitraires, inclusion de fichiers (locaux ou distants).

L'audit de code source doit permettre d'éviter les fuites d'information et les altérations du fonctionnement du système d'information.

f) Les audits de code source peuvent être réalisés manuellement ou automatiquement par des outils spécialisés. Les phases automatisées, ainsi que les outils utilisés, doivent être identifiés dans les livrables et en particulier dans le rapport d'audit.

VI.4.4. Tests d'intrusion

a) L'équipe d'audit en charge de la réalisation d'un test d'intrusion sur une cible donnée peut effectuer une ou plusieurs des phases suivantes :

- Phase boîte noire : l'auditeur ne dispose d'aucune autre information que les adresses IP et URL associées à la cible auditée. Cette phase est généralement précédée de la découverte d'informations et l'identification de la cible par interrogation des services DNS, par le balayage des ports ouverts, par la découverte de la présence d'équipements de filtrage, etc. ;
- Phase boîte grise : les auditeurs disposent des connaissances d'un utilisateur standard du système d'information (authentification légitime, poste de travail « standard », etc.). Les identifiants peuvent appartenir à des profils d'utilisateurs différents afin de tester des niveaux de privilèges distincts ;
- Phase boîte blanche : les auditeurs disposent du maximum d'informations techniques (architecture, code source, contacts téléphoniques, identifiants, etc.) avant de démarrer l'analyse. Ils ont également accès à des contacts techniques liés à la cible.

Si plusieurs de ces prestations sont effectuées, il est recommandé de préserver l'ordre d'exécution décrit ci-dessus.

b) Le prestataire d'audit et le commanditaire doivent, préalablement à tout test d'intrusion, définir un profil d'attaquant simulé.

c) Le prestataire d'audit doit avoir un contact permanent avec l'audité et l'auditeur doit prévenir le commanditaire de l'audit et l'audité avant toute action qui pourrait entraîner un dysfonctionnement, voire un déni de service de la cible auditée.

d) Lorsqu'elles sont connues pour rendre la cible auditée instable voire provoquer un déni de service, les vulnérabilités découvertes ne devraient pas être exploitées sauf accord du commanditaire et de l'audité. L'absence de tentative d'exploitation de telles vulnérabilités doit être indiquée et justifiée dans le rapport d'audit.

e) Les vulnérabilités non publiques découvertes lors de l'audit doivent être communiquées à l'ANSSI.

VI.4.5. Audit organisationnel et physique

a) Le prestataire d'audit doit analyser l'organisation de la sécurité des systèmes d'information sur la base des référentiels techniques et réglementaires en accord avec les réglementations et méthodes applicables dans le domaine d'activité de l'audité.

f) L'audit organisationnel et physique doit permettre de mesurer la conformité du système d'information audité par rapport aux référentiels et identifier les écarts présentant les vulnérabilités majeures du système audité.

g) L'audit organisationnel et physique peut intégrer l'analyse des éléments liés à la sécurité des aspects physiques des systèmes d'information et notamment la protection des locaux hébergeant les systèmes d'information et les données de l'audité ou le contrôle d'accès de ces locaux.

VI.5. Réunion de restitution

Dès la fin de l'audit, et sans attendre que le rapport d'audit soit achevé, le responsable d'équipe d'audit doit informer l'audité et le commanditaire de l'audit des constats et des premières conclusions de l'audit.

Le cas échéant, il présente les vulnérabilités majeures et critiques qui nécessiteraient une action rapide et décrit les recommandations associées.

VI.6. Elaboration du rapport d'audit

a) Pour tout audit, le prestataire d'audit doit établir un rapport d'audit.

b) Le rapport d'audit doit être adapté en fonction de l'activité d'audit réalisée par le prestataire d'audit.

c) Le rapport d'audit doit contenir en particulier :

- Une synthèse, compréhensible par des non experts, qui précise :
  - Le contexte et le périmètre de l'audit[129] ;
  - Les vulnérabilités critiques, d'origine technique ou organisationnelle, et les mesures correctives proposées ;
  - L'appréciation du niveau de sécurité du système d'information audité par rapport à l'état de l'art et en considération du périmètre d'audit.
- Un tableau synthétique des résultats de l'audit, qui précise :
  - La synthèse des vulnérabilités relevées, classées selon une échelle de valeur ;
  - La synthèse des mesures correctives proposées, classées par criticité et par complexité ou coût estimé de correction ;
- Lorsque réalisés, une description du déroulement linéaire des tests d'intrusion et de la méthodologie employée pour détecter les vulnérabilités et, le cas échéant, les exploiter ;
- Une analyse de la sécurité du système d'information audité, qui présente les résultats des différentes activités d'audit réalisées.

d) Les vulnérabilités, qu'elles soient d'origine technique ou organisationnelle, doivent être classées en fonction de leur impact sur la sécurité du système d'information et leur difficulté d'exploitation.

Il est recommandé d'utiliser l'échelle proposée par l'ANSSI en annexe 4. A défaut, le prestataire d'audit doit être en mesure de proposer une échelle pertinente.

e) Chaque vulnérabilité doit être associée à une ou plusieurs recommandations adaptées au système d'information de l'audité. Les recommandations décrivent les solutions permettant de résoudre temporairement ou définitivement la vulnérabilité et d'améliorer le niveau de sécurité

f) Le rapport d'audit peut également présenter des recommandations générales non associées à des vulnérabilités et destinées à conseiller l'audité pour les actions liées à la sécurité de son système d'information qu'il entreprend.

g) Le rapport d'audit doit mentionner les réserves relatives à l'exhaustivité des résultats de l'audit (liées aux délais alloués à l'audit, à la disponibilité des informations demandées…) ou à la pertinence de la cible auditée.

h) Le rapport d'audit doit mentionner les noms et coordonnées des auditeurs, responsables d'équipe d'audit et commanditaires de l'audit.

i) Le rapport d'audit doit mentionner qu'il s'agit d'une prestation d'audit qualifiée et préciser les activités d'audit associées.

VI.7. Conclusion de l'audit

a) Il est recommandé qu'une réunion de clôture de l'audit soit organisée avec le commanditaire de l'audit et l'audité suite à la livraison du rapport d'audit. Cette réunion permet de présenter la synthèse du rapport d'audit, des scénarios d'exploitation de certaines failles, des recommandations et

[129] Compte tenu du fait que le commanditaire de l'audit dispose généralement déjà d'une description du périmètre audité, dans la convention d'audit ou dans le plan d'audit, la synthèse du contexte du périmètre de l'audit peut être très succincte.

d'organiser un jeu de questions / réponses. Elle est également l'occasion d'expliquer les recommandations complexes et, éventuellement, de proposer d'autres solutions plus aisées à mettre en œuvre.

b) Le responsable d'équipe d'audit doit demander à l'audité de signer un document attestant que le système d'information qui a été audité est, à l'issue de l'audit, dans un état dont la sécurité n'est pas dégradée par rapport à l'état initial, dégageant ainsi, dans le principe, la responsabilité des auditeurs et du prestataire d'audit de tout problème postérieur à l'audit.

c) Toutes les traces, relevés de configuration, informations ou documents relatifs au système d'information audité obtenus par le prestataire d'audit doivent être restitués à l'audité ou, sur sa demande, détruits conformément à la convention d'audit. Le cas échéant, le responsable d'audit produit un procès verbal de destruction de ces données qu'il remet à l'audité et précisant les données détruites et leur mode de destruction.

d) Afin qu'il puisse s'assurer de la pertinence des mesures correctives mises en œuvre pour corriger les vulnérabilités découvertes lors de l'audit, le commanditaire de l'audit peut demander au prestataire d'audit la fourniture des développements spécifiques autonomes réalisés lors de l'audit pour valider les scénarios d'exploitation des vulnérabilités. Ces développements peuvent être fournis sous la forme de script ou de programmes compilés, accompagnés de leur code source, ainsi que d'une brève documentation de mise en œuvre et d'utilisation. Les modalités relatives à cette mise à disposition sont précisées dans la convention d'audit.

e) L'audit est considéré comme terminé lorsque toutes les activités prévues ont été réalisées et que le commanditaire de l'audit a reçu et attesté que le rapport d'audit est conforme aux objectifs visés dans la convention d'audit.

f) Il est recommandé que le prestataire d'audit propose au commanditaire de l'audit d'effectuer ultérieurement un audit de validation afin de vérifier si les mesures correctives proposées lors de l'audit ont été correctement mises en œuvre.

VII. Annexe 1 : Documents cités en référence

VII.1. Réglementation

Loi du pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices

VII.2. Normes et documents techniques

Norme internationale ISO/IEC 17020:1998 : Critères généraux pour le fonctionnement de différents types d'organismes procédant à l'inspection.

Norme internationale ISO/IEC 19011:2002 : Lignes directrices pour l'audit des systèmes de management de la qualité ou de management environnemental.

Norme internationale ISO/IEC 27001:2005 : Techniques de sécurité – Systèmes de gestion de la sécurité de l'information – Exigences.

Norme internationale ISO/IEC 27002:2005 : Techniques de sécurité – Code de bonne pratique pour la gestion de la sécurité de l'information.

Norme internationale ISO/IEC 27011:2008 : Lignes directrices de la gestion de la sécurité de l'information pour les télécoms.

Guides de l'ANSSI publiés sur son site http://www.ssi.gouv.fr et notamment :

- Méthode de gestion de risques EBIOS 2010 ;
- Guide d'hygiène informatique ;
- Guide pour l'élaboration d'une politique de sécurité des systèmes d'information ;
- Guide d'élaboration de tableaux de bord de sécurité des systèmes d'information ;
- Guide d'intégration de la sécurité des systèmes d'information dans les projets ;
- Guide relatif à la maturité SSI ;
- Guide de l'externalisation ;
- La défense en profondeur appliquée aux systèmes d'information ;
- Sécurité et langage Java (Javasec).

Guides et documentation de l'Open Web Application Security Project (OWASP).

Guides de développement sécurisé Microsoft[130].

Guides de développement sécurité Java[131].

Guides de l'ENISA, notamment Technical Guideline for Minimum Security Measures.

[130] http://msdn.microsoft.com/fr-fr/library/ms954624.aspx

[131] http://www.oracle.com/technetwork/java/seccodeguide-139067.html

VII.3. Autres références documentaires

Défense et sécurité de l'information – Stratégie publique (de la France) – Glossaire. Publié sur http://www.ssi.gouv.fr.

VIII. Annexe 2 : Recommandations à l'intention des commanditaires d'audits

Cette annexe liste les recommandations de l'ANSSI à l'intention des commanditaires d'audits, dans le cadre de la passation de marchés publics ou d'un accord contractuel, ainsi qu'aux prestataires d'audit dans le cadre de leur devoir de conseil.

L'ANSSI peut être consultée pour participer à la définition du cahier des charges des audits faisant l'objet d'un appel d'offres d'une autorité administrative.

VIII.1. Recommandations générales

a) Il est recommandé que le prestataire d'audit puisse fournir des références permettant d'estimer de sa compétence : références clients, participation à des programmes de recherche, etc.

b) Les audits devraient être le plus exhaustif possible, tout en tenant compte des contraintes temporelles et budgétaires allouées à l'audit.

c) La durée de l'audit demandé par les commanditaires d'audits devrait être adaptée en fonction :

- Du périmètre d'audit et de sa complexité ;
- Des exigences de sécurité attendues du système d'information audité.

d) Afin de réduire le volume global d'éléments à auditer et donc le coût de l'audit, et tout en conservant un périmètre d'audit pertinent, il devrait être réalisé un échantillonnage respectant les principes suivants :

- Pour les audits de configuration, seuls les serveurs les plus sensibles sont audités : contrôleurs de domaine Active Directory, serveurs de fichiers, serveurs d'infrastructure (DNS, SMTP, etc.), serveurs applicatifs, etc.
- Pour un audit de code source, seules les parties sensibles du code source sont auditées : gestion des authentifications, gestion des contrôles d'accès des utilisateurs, accès aux bases de données, contrôle des saisies utilisateur, etc.

e) Il est préférable de réaliser les tests d'intrusion sur un environnement de test (ou de « pré production ») afin d'éviter les conséquences liées aux éventuels dysfonctionnements sur un environnement de production. Ceci dit, afin de garantir la pertinence de l'audit, il convient de s'assurer que cet environnement soit similaire à celui de production.

f) L'applicabilité des résultats des audits techniques dans l'environnement de production doit être vérifiée. Les audits d'architecture, de configuration, de code source et organisationnels doivent être réalisés dans l'environnement de production.

g) La définition du périmètre d'un audit doit être basée sur une analyse préalable des risques « métier » de l'audité. Il est recommandé au commanditaire de l'audit d'indiquer les éléments les plus sensibles de la cible auditée au prestataire d'audit.

h) Il est recommandé que le commanditaire de l'audit désigne, en son sein, un référent chargé de la gestion des relations avec le prestataire d'audit et des modalités de réalisation des activités d'audit (horaires des interventions, autorisations, etc.).

i) Il est recommandé que le commanditaire et l'audité prennent les mesures de sauvegarde nécessaires à la protection de leurs systèmes d'information et de leurs données préalablement à tout audit.

j) Il est recommandé que le commanditaire de l'audit ait la capacité à révoquer un auditeur.

k) Il est recommandé que le commanditaire de l'audit demande au prestataire d'audit de lui fournir les attestations de compétence des auditeurs.

VIII.2. Types d'audit recommandés par l'ANSSI

a) L'ANSSI recommande aux commanditaires d'audits et aux prestataires d'audit de recourir et demander des audits composés des activités d'audit suivantes :

- *Audit applicatif :*
  - Audit de code source ;
  - Audit de configuration (serveur d'application, serveur HTTP, base de données, etc.).
- *Audit d'un centre serveur :*
  - Audit d'architecture (liaison entre les différentes zones et entités, filtrage, etc.) ;
  - Audit de configuration (équipements réseau et de sécurité, serveurs d'infrastructure) ;
  - Audit organisationnel et physique.
- *Audit d'un réseau bureautique :*
  - Audit d'architecture ;
  - Audit de configuration (postes bureautique, équipements réseau, serveurs bureautique, serveurs AD, etc.) ;
  - Audit organisationnel et physique.
- *Audit d'une plate-forme de téléphonie :*
  - Audit d'architecture ;
  - Audit de configuration (équipements réseau et de sécurité, IPBX, téléphones, etc.).
- *Audit d'une plate-forme de virtualisation :*
  - Audit d'architecture ;
  - Audit de configuration (équipements réseau et de sécurité, systèmes de virtualisation, etc.).

Cette liste est non exhaustive et peut être complétée par les commanditaires d'audits et les prestataires d'audit.

b) Chacun des types d'audit décrits ci-dessus peut inclure l'activité de tests d'intrusion.

c) En revanche, l'activité de tests d'intrusion ne devrait jamais être réalisée seule et sans aucune autre activité d'audit. En effet, un test d'intrusion peut servir de complément pour un audit de configuration ou de code auquel il est adossé afin d'améliorer la portée, en termes d'impacts, de ce dernier. Ceci permet par exemple de vérifier qu'une faille découverte lors d'un audit de code source est bien exploitable dans les conditions d'exploitation de la plate-forme, ainsi que les conséquences de cette exploitation (exécution de code, fuite d'informations, rebond, etc.).

d) Les tests d'intrusion ne devraient pas être réalisés sur des plates-formes d'hébergement mutualisées sauf accord express de l'hébergeur et après que les risques aient été évalués et maîtrisés, et que les responsabilités aient été clairement établies.

IX. Annexe 3 : Liste détaillée des compétences techniques et organisationnelles d'un prestataire d'audit

IX.1. Compétences techniques

Les éléments suivants sont inclus dans les domaines cités dans l'exigence au paragraphe IV.3.g

- Réseaux et protocoles :
  - Protocoles réseau et infrastructures ;
  - Protocoles applicatifs courants et service d'infrastructure ;
  - Configuration et sécurisation des principaux équipements réseau du marché ;
  - Réseaux de télécommunication ;
  - Technologie sans fil ;
  - Téléphonie ;
- Systèmes d'exploitation (environnement et durcissement) :
  - Architectures Microsoft ;
  - Systèmes UNIX/Linux ;
  - Solution de virtualisation.
- Couche applicative :
  - Méthodes d'intrusion dans le contexte d'applications web ;
  - Guides et principes de développement sécurité ;
  - Applications de type client/serveur ;
  - Langages de programmation dans le cadre d'audits de code ;
  - Mécanismes cryptographiques ;
  - Socle applicatif :
    - Serveurs web ;
    - Serveurs d'application ;
    - Systèmes de gestion de bases de données ;
- Équipements et logiciels de sécurité :
  - Pare-feu ;
  - Système de sauvegarde ;
  - Système de stockage mutualisé ;
  - Serveurs mandataires inverses ;
  - Détection et prévention d'intrusion (réseau et hôte) ;
  - Logiciels de sécurité côté poste client.

IX.2. Compétences organisationnelles et physiques

Les éléments suivants sont inclus dans les domaines cités dans l'exigence au paragraphe IV.3.h

- Maîtrise des référentiels techniques
- Maîtrise du cadre normatif :
  - Les normes ISO/IEC 27001 et ISO 27002 ;
  - Les textes réglementaires relatifs à la sécurité des systèmes d'information, aux audits et aux sujets

connexes[132] ;

- Maîtrise des domaines relatifs à l'organisation de la sécurité des systèmes d'information :
  - Analyse des risques ;
  - Politique de sécurité des systèmes d'information ;
  - Chaines de responsabilités en sécurité des systèmes d'information ;
  - Sécurité liée aux ressources humaines ;
  - Gestion de l'exploitation et de l'administration du système d'information ;
  - Contrôle d'accès logique au système d'information ;
  - Développement et maintenance des applications ;
  - Gestion des incidents liés à la sécurité de l'information ;
  - Gestion du plan de continuité de l'activité ;
  - Sécurité physique.
- Maîtrise des pratiques liées à l'audit :
  - Conduite d'entretien ;
  - Visite sur site ;
  - Analyse documentaire.

IX.3. Connaissances des référentiels

Les éléments suivants sont inclus dans les domaines cités dans l'exigence au paragraphe IV.3.i) : maîtrise du RGS et de ses annexes ; maîtrise des guides et référentiels de l'ANSSI[133].

[132] Notamment les règles relatives à la protection de la vie privée, du secret professionnel, des correspondances privées ou des données à caractère personnel, aux atteintes aux intérêts fondamentaux de la nation, au terrorisme, aux atteintes à la confiance publique, à la propriété intellectuelle, à l'usage des moyens de cryptologie, au patrimoine scientifique et technique national

[133] Voir chapitre VII.2.

X. Annexe 4 : Echelle de classification des vulnérabilités

L'ANSSI propose l'échelle de classification des vulnérabilités suivante.

Les vulnérabilités, qu'elles soient d'origine technique ou organisationnelle, sont classées en fonction du risque qu'elles font peser sur le système d'information, c'est-à-dire en fonction de l'impact de la vulnérabilité sur le système d'information et de sa difficulté d'exploitation.

Le niveau du risque lié à chaque vulnérabilité est apprécié selon l'échelle de valeur suivante :

- *Mineur* : faible risque sur le système d'information et pouvant nécessiter une correction ;
- *Important* : risque modéré sur le système d'information et nécessitant une correction à moyen terme ;
- *Majeur* : risque majeur sur le système d'information nécessitant une correction à court terme ;
- *Critique* : risque critique sur le système d'information et nécessitant une correction immédiate ou imposant un arrêt immédiat du service.

La facilité d'exploitation correspond au niveau d'expertise et aux moyens nécessaires à la réalisation de l'attaque. Elle est appréciée selon l'échelle suivante :

- *Facile* : exploitation triviale, sans outil particulier ;
- *Modérée* : exploitation nécessitant des techniques simples et des outils disponibles publiquement ;
- *Elevée* : exploitation de vulnérabilités publiques nécessitant des compétences en sécurité des systèmes d'information et le développement d'outils simples ;
- *Difficile* : exploitation de vulnérabilités non publiées nécessitant une expertise en sécurité des systèmes d'information et le développement d'outils spécifiques et ciblés.

L'impact correspond aux conséquences que l'exploitation de la vulnérabilité peut entrainer sur le système d'information de l'audité. Il est apprécié selon l'échelle suivante :

- *Mineur* : pas de conséquence directe sur la sécurité du système d'information audité ;
- *Important* : conséquences isolées sur des points précis du système d'information audité ;
- *Majeur* : conséquences restreintes sur une partie du système d'information audité ;
- *Critique* : conséquences généralisées sur l'ensemble du système d'information audité.

Le tableau suivant indique le niveau de risque inhérent à chaque vulnérabilité découverte, en fonction de leur difficulté d'exploitation et de leur impact présumé :

Facilité d'exploitation / **Impact**	**Difficile**	**Elevée**	**Modérée**	**Facile**
Mineur	*Mineur*	*Mineur*	*Important*	*Majeur*
Important	*Mineur*	*Important*	*Important*	*Majeur*
Majeur	*Important*	*Majeur*	*Majeur*	*Critique*
Critique	*Important*	*Majeur*	*Critique*	*Critique*

Annexe D

Guide d'homologation de sécurité d'un téléservice

Historique des versions		
Date	Version	Évolution du document
	1.0	Publication de la première version de l'annexe D du Référentiel Général de Sécurité (RGS PF)

Avant-propos

Ce guide d'homologation s'adresse à l'ensemble des autorités administratives visées au 1° de l'article 1er de la loi du Pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices, à savoir : la Polynésie française, ses établissements publics, les autorités administratives indépendantes, les organismes de protection sociale et les autres organismes et personnes de droit public et de droit privé chargés d'une mission de service public administratif.

Pourquoi l'homologation de sécurité ?

Lorsqu'un responsable (autorité administrative, élu, dirigeant d'entreprise) décide de faire déménager ses équipes dans de nouveaux locaux ou d'ouvrir un établissement recevant du public, il s'assure que les lieux sont conformes à la réglementation et que les bâtiments sont solides, afin que l'ensemble puisse fonctionner en toute sécurité pour les personnes et les biens. Il doit s'en assurer même s'il n'est pas un spécialiste de la construction et il s'appuie pour cela sur des garanties et des arguments portés à sa connaissance par des experts du domaine. Ce responsable atteste par sa décision d'homologation que ses locaux sont conformes à la réglementation en vigueur, que les risques liés au bâtiment et à son exploitation sont identifiés et maitrisés. Le responsable supportera les éventuelles conséquences juridiques d'une homologation.

En matière de services informatiques et plus particulièrement dans ceux ouverts sur l'Internet, l'homologation de sécurité joue le même rôle. Elle permet à un responsable, en s'appuyant sur l'avis d'experts, d'identifier et d'attester aux utilisateurs d'un système d'information que les risques qui pèsent sur eux, sur les informations qu'ils manipulent et sur les services rendus, sont connus et maîtrisés. L'homologation est d'autant plus nécessaire, aujourd'hui, que les systèmes d'information sont de plus en plus complexes et ouverts et que les impacts potentiels d'un incident sont de plus en plus graves. Les cyber attaques vers les systèmes informatiques dont de plus en plus nombreuses. Les atteintes aux systèmes d'information (SI) d'une organisation deviennent bloquantes, perturbantes et souvent couteuses. L'ouverture d'un SI d'une autorité administrative doit donc être prêt aux atteintes des cybercriminels comme aux erreurs ou malveillances internes.

Une démarche d'homologation est donc un préalable à l'instauration de la confiance dans les systèmes d'information et dans leur exploitation. **Sa prononciation par le responsable de l'organisation ou Autorité d'Homologation, est un préalable à l'ouverture du SI ou du Téléservice**.

Pour un certain nombre de systèmes, l'homologation est rendue obligatoire par la loi du pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices. Cette réglementation vise à préciser les dispositions de mise en œuvre de la sécurité des systèmes d'informations d'une autorité administrative, notamment lorsque celle-ci met à disposition des téléservices. Le cadre technique et organisationnel de cette sécurité est le Référentiel Général de Sécurité (RGS) de la Polynésie française.

Ce guide d'homologation RGS est inspiré du Guide d'homologation de sécurité en neuf étapes (version 1.0 - Août 2014), rédigé par l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI). Il peut s'appliquer pour toute autre exigence réglementaire prévue par la Polynésie française.

Qu'est-ce qu'une homologation de sécurité ?

En informatique, comme dans les autres domaines, le risque zéro n'existe pas. La démarche d'homologation de sécurité est destinée à faire connaître et faire comprendre aux responsables les risques liés à l'exploitation d'un système d'information, notamment ceux liés à la cybersécurité

Il s'agit d'un processus d'information et de responsabilisation qui aboutit à une décision, prise par le responsable de l'organisation. Cette décision constitue un acte formel par lequel le responsable :

- atteste de sa connaissance du système d'information et des mesures de sécurité (techniques, organisationnelles ou juridiques) mises en œuvre ;
- accepte les risques qui demeurent, qu'on appelle risques résiduels.

La décision s'appuie sur l'ensemble des documents que le responsable estime nécessaire et suffisant à sa prise de décision.

La démarche d'homologation doit être adaptée aux enjeux de sécurité du système, notamment au contexte d'emploi, à la nature des données contenues, ainsi qu'aux utilisateurs :

- dans les cas de systèmes complexes ou à fort enjeu de sécurité de l'information ou de cybersécurité, il est souhaitable que le responsable s'entoure d'experts techniques et fonctionnels : la Commission d'Homologation complète ;
- dans le cas de systèmes simples moins exposés car moins ouverts sur l'Internet, le responsable peut mettre en place des procédures simplifiées associant un nombre plus limité d'acteurs dans une Commission d'Homologation réduite.

Comment homologuer un système d'information ?

La démarche d'homologation est décomposée en neuf étapes. Chacune de ces étapes est décrite ci-après. La démarche proposée est inspirée de l'approche ouverte de l'ANSSI, mais la Polynésie française a fixé des éléments et pris des options dans son processus d'homologation.

Pour chacune des étapes, le présent guide décrit les actions attendues, les responsables, les acteurs et les livrables attendus pour le déroulement de l'étape et ceux produits par l'étape.

Les étapes d'homologation de sécurité d'un téléservice sont les suivantes:

1. Identification et description du contexte du téléservice
2. Détermination de la démarche d'homologation au regard des enjeux de sécurité
3. Définition de la gouvernance de l'homologation
4. Elaboration du dossier d'homologation et du planning
5. Réalisation de l'analyse des risques du téléservice
6. Evaluation et amélioration du niveau de sécurité du téléservice
7. Mesures de sécurité complémentaires pour couvrir les derniers risques
8. Décision d'homologation du téléservice
9. Surveillance des risques résiduels du téléservice

Table des matières

Objectifs de l'homologation de sécurité

En informatique, comme dans les autres domaines, le *risque zéro* n'existe pas.

L'objectif de la *démarche d'homologation* d'un système d'information (SI) est de trouver un équilibre entre le risque acceptable et les coûts de sécurisation, puis de faire arbitrer cet équilibre, de manière formelle, par un responsable qui a autorité pour le faire.

Cette démarche permet d'améliorer la sécurité pour un coût optimal, en évitant la « sur-sécurité », mais en prenant également en compte le coût d'un éventuel incident de sécurité. L'approche permet de s'assurer que les risques pesant sur un système d'information précis (le périmètre de l'homologation), dans son contexte d'utilisation, sont connus et maîtrisés de manière active, préventive et continue.

La démarche d'homologation est intégrée au cycle de vie du système d'information. Elle comprend neuf étapes clés, détaillées au sein du présent document. Il est nécessaire de les suivre en même temps que les phases de développement du système : opportunité, faisabilité, conception, réalisation, validation, exploitation, maintenance et fin de vie.

A quel moment entrer dans ce processus d'homologation ?

La présente démarche d'homologation doit être activée à des moments clés de la vie d'un projet de téléservice :

- Lors du lancement d'un nouveau projet de téléservice par le Responsable, afin de comprendre le plus tôt possible les enjeux de sécurité pour adapter le processus d'homologation. Ce dernier accompagnera le projet tout au long de son cycle de vie ;
- À tout moment, si la démarche d'homologation formelle n'était pas disponible au moment de la mise en production du téléservice.

Attention, la Loi de Pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices fixe les délais dans lesquels un Téléservice doit être homologué.

La *décision d'homologation* par l'Autorité d'Homologation est le résultat du processus. Son objet est de vérifier que le responsable a analysé les risques de sécurité et a mis en œuvre les dispositifs adaptés à la menace.

Le terme « homologation » recouvre donc deux notions distinctes :

- la démarche d'homologation, avant tout destinée à faire connaître et faire comprendre aux responsables les risques liés à l'exploitation d'un système d'information. Elle se conclut par une décision, soutenue par la constitution et l'analyse d'un dossier de sécurité ;
- la décision formelle d'homologation (également appelée attestation formelle).

Se lancer dans une démarche d'homologation est relativement simple : il s'agit de vérifier que la sécurité n'a pas été oubliée avant la mise en place du téléservice et d'appliquer les mesures de sécurité nécessaires et proportionnées.

Les neuf étapes simples présentées dans ce document permettront à un chef de projet ou à un comité de pilotage SSI de préparer un dossier d'homologation et de le présenter au responsable de l'organisation, désigné *autorité d'homologation*.

L'autorité d'homologation pourra alors prendre une décision éclairée sur la base de ce dossier, qui doit apporter des réponses pertinentes à l'ensemble des questions qu'elle se pose.

Dans la suite du document :

- les documents attendus sont les documents et informations nécessaires pour lancer le processus, l'étape. Ce sont les documents d'entrée de l'étape.
- les livrables sont les documents formalisés à l'issu du processus, de l'étape. Ce sont les documents de sortie de l'étape.

Etape 1 : Identification et description du contexte du téléservice

Document(s) attendu(s) :

- Tous documents permettant de délimiter le périmètre du système (cahier des charges, étude préalable…)

Participants potentiels à l'Étape 1 :

- Responsables métiers ;
- Assistance à maîtrise d'ouvrage ;
- Experts techniques internes ;

1. Délimiter le périmètre du système

Le périmètre du téléservice à homologuer doit comporter tous les éléments indispensables au fonctionnement du système. La délimitation du périmètre ne doit comporter aucune ambiguïté, car elle permet de déterminer et de caractériser précisément les systèmes qui seront homologués. La description de ce périmètre comprend :

- **Des éléments fonctionnels et d'organisation** : fonctionnalités du système, type d'utilisateurs, contexte et règles d'emploi, procédures formalisées, conditions d'emploi des produits de sécurité, gestion des droits, dispositifs de détection et de gestion des incidents ;
- **Des éléments techniques** : architecture du système (en précisant notamment les interconnexions avec d'autres systèmes), possibilité d'utilisation de supports amovibles, d'accès à distance ou de cloisonnement, mécanismes de maintenance, d'exploitation ou de télégestion du système, notamment lorsque ces opérations sont effectuées par des prestataires externes ;
- **Le périmètre géographique et physique** : localisations géographiques et caractéristiques des locaux.

Le périmètre peut évoluer au cours de la démarche d'homologation, mais il est recommandé d'aboutir rapidement à une délimitation stable de celui-ci.

Livrable(s) produit(s) :

- Compte rendu de la réunion lors de laquelle le téléservice a été décrit dans un périmètre donné.

Etape 2 : Détermination de la démarche d'homologation au regard des enjeux de sécurité

Durant cette deuxième étape, vous définissez le niveau de profondeur de la démarche d'homologation, afin que celle-ci soit adaptée aux enjeux de sécurité du téléservice, d'une part, et aux capacités de votre organisme à la mener, d'autre part.

La démarche la plus adaptée à l'homologation du système doit être définie en fonction du contexte, du niveau de complexité et de criticité du système, du niveau de sensibilité des données hébergées (notamment si le téléservice collecte ou traite des données à caractère personnel) et du niveau de maturité en matière de SSI de l'organisme qui met en œuvre l'homologation.

Document(s) attendu(s) :

- Les outils d'autodiagnostic pour l'évaluation des besoins de sécurité du téléservice et de maturité de l'organisme.

Participants potentiels à l'Étape 2 :

- Responsables métiers ;
- Assistance à maîtrise d'ouvrage ;
- Experts techniques internes ;
- RSSI

1. Réaliser l'autodiagnostic des besoins de sécurité du téléservice et le niveau de maturité SSI de l'organisme

Deux outils d'autodiagnostic sont proposés. Ils sont détaillés en annexe du présent document.

L'annexe 1 permet d'évaluer les besoins de sécurité du téléservice à homologuer,

- En estimant la gravité des conséquences potentielles d'une défaillance du SI, la sensibilité des données, le degré d'exposition aux menaces et l'importance des vulnérabilités potentielles du système,
- Un questionnaire simple et rapide permet de déterminer si le besoin de sécurité du système est nul, faible, moyen ou fort.
- L'annexe 2 permet de déterminer votre niveau de maturité SSI,
- C'est-à-dire le niveau de maîtrise et de rigueur atteint par l'organisme, dans la gestion de la sécurité des systèmes d'information,
- Un questionnaire simple et rapide vous permet de déterminer si la maturité SSI de votre organisme est élémentaire, moyenne ou avancée.

2. En déduire la démarche appropriée

En fonction des résultats de l'autodiagnostic des besoins de sécurité et du niveau de maturité, vous pouvez déterminer, à l'aide du tableau ci-dessous, le type de démarche d'homologation à mettre en œuvre dans le cadre de votre projet de téléservice.

Les autodiagnostics doivent être réalisés avec sérieux et objectivité. L'adoption d'une démarche inadaptée aux enjeux ou aux capacités de votre organisme hypothèquerait les chances de réussite de votre projet d'homologation.

		Besoin de sécurité du système		
		Faible	Moyen	Fort
Niveau SSI de l'organisation	Elémentaire	Simple	Avancée	Avancée
	Moyen	Simple	Avancée	Détaillée
	Avancé	Simple	Avancée	Détaillée

Les démarches possibles sont les suivantes :

- **Simple :** démarche autonome à minima, que la Commission d'homologation peut mener sans recours à une assistance conseil externe, par l'application des outils et des indications donnés dans le présent guide,
- **Avancée :** démarche autonome approfondie, que la Commission d'homologation peut mener sans recours à une assistance conseil externe, par l'application des outils et des indications donnés dans le présent guide et ses ressources internes,
- **Détaillée :** démarche assistée approfondie, que la Commission d'homologation mène avec l'aide d'une assistance conseil externe, en plus des outils et des indications données dans le présent guide.

Livrable(s) produit(s) :

- Compte rendu de la réunion lors de laquelle le niveau de profondeur de la démarche d'homologation a été retenu et validé.

Etape 3 : Définition de la gouvernance de l'homologation

Durant cette troisième étape, vous identifiez l'ensemble des acteurs de l'homologation et définir leur rôle (décision, assistance ou expertise technique notamment).

Une homologation s'appuie sur plusieurs acteurs distincts auxquels sont associés différents rôles et niveaux de responsabilité.

Document(s) attendu(s) :

- Aucun document n'est nécessaire pour lancer cette étape.

Participants potentiels à l'Étape 3 :

- Autorité d'homologation
- Responsables métiers ;
- Assistance à maîtrise d'ouvrage ;
- RSSI ;

1. L'autorité d'homologation (AH)

L'autorité d'homologation est la personne physique qui, après instruction du dossier d'homologation, prononce l'homologation de sécurité du téléservice, c'est-à-dire prend la décision d'accepter les risques résiduels identifiés sur le système.

L'autorité d'homologation doit être désignée à un niveau hiérarchique suffisant pour assumer toutes les responsabilités. Il est donc nécessaire que l'autorité d'homologation se situe à un niveau de direction dans votre organisme.

Pour la Polynésie française, l'autorité d'homologation est le Président de la Polynésie française. Ce dernier peut déléguer cette compétence au vice-président et aux ministres du gouvernement de la Polynésie française.

L'autorité d'homologation désigne un responsable du processus d'homologation, qui mènera le projet d'homologation en son nom.

Lorsque cela est nécessaire, l'autorité d'homologation peut rédiger une lettre de mission à l'attention de la personne chargée d'organiser les tâches du processus d'homologation, en lui indiquant de quelle manière la synthèse des résultats de chaque étape de la démarche d'homologation lui sera communiquée.

Lorsque le système est sous la responsabilité de plusieurs autorités, l'autorité d'homologation est désignée conjointement par les autorités concernées

2. La commission d'homologation

La commission d'homologation assiste l'autorité d'homologation pour l'instruction de l'homologation et est chargée de préparer la décision d'homologation.

La taille et la composition de cette commission doivent être adaptées à la nature du téléservice et proportionnées à ses enjeux, en particulier si ce dernier est très sensible, notamment dans le cas d'un téléservice manipulant des données à caractère personnel sensibles.

- La commission est dite **complète** quand elle est composée de :
  - Responsables métiers ;
  - Assistance à maîtrise d'ouvrage ;
  - Experts techniques internes ;
  - Responsable de la production informatique ;
  - RSSI ;
  - Correspondant Informatique et Libertés (CIL) ou Délégué à la Protection des Données (DPO) si le Téléservice manipule des données à caractère personnel.
- La commission est dite **réduite** quand elle est composée de :
  - Responsables métiers ou l'assistance à maîtrise d'ouvrage ;
  - Responsable de la production informatique ;
  - RSSI ;
  - Correspondant Informatique et Libertés (CIL) ou Délégué à la Protection des Données (DPO) si le Téléservice manipule des données à caractère personnel.

La commission d'homologation est chargée du suivi des *plannings*, de l'analyse de l'ensemble des documents versés au dossier d'homologation. Elle se prononce sur la pertinence des livrables et peut les valider dans certains cas.

Si la qualité ou la complétude des documents attendus ne satisfait pas la commission d'homologation, cette dernière peut commander en interne ou en externe des travaux complémentaires sur ces documents.

Le service informatique de la Polynésie française assiste la commission d'homologation dans l'élaboration des documents constituant le dossier d'homologation. Ce dernier assure le secrétariat de la commission d'homologation.

3. Les acteurs de l'homologation

La maîtrise d'ouvrage

La maîtrise d'ouvrage représente les acteurs métier et assure la bonne prise en compte des contraintes liées à l'utilisation du téléservice. Elle joue un rôle-clé dans plusieurs étapes de la maîtrise des risques, y compris dans les arbitrages sur le traitement des risques.

Le RSSI

Lorsque l'entité dispose d'un responsable de la sécurité des systèmes d'information, celui-ci est impliqué nécessairement dans la démarche d'homologation. Selon les cas, il peut être désigné responsable du processus d'homologation ou chargé du secrétariat de la commission d'homologation mais il est toujours membre de droit de cette commission.

Le responsable d'exploitation du système

Le responsable d'exploitation du système, ou autorité d'emploi, remplit le rôle opérationnel. Il s'agit de l'entité exploitant le système d'information destiné à être homologué.

Les prestataires

En fonction de leur statut (interne ou externe), de leur implication dans le projet et de leurs relations avec l'autorité d'homologation, les prestataires peuvent être intégrés dans la commission d'homologation, ou simplement consultés en cas de besoin.

Ils remplissent un rôle d'assistance et produisent des livrables qui seront versés au dossier d'homologation ainsi que des réponses aux interrogations de la commission d'homologation.

Les systèmes interconnectés

Les autorités d'homologation des systèmes interconnectés au système concerné peuvent jouer un rôle dans l'homologation et être associés à la démarche lorsque :

- le système à homologuer à un impact sur leurs propres systèmes ;
- ils émettent des avis ou des certificats qui peuvent concerner le système.

Le Correspondant Informatique et Libertés ou le Délégué à la Protection des Données à Caractère Personnel.

Lorsque l'organisme a désigné un **Correspondant Informatique et Libertés** ou un **Délégué à la Protection des Données à Caractère Personnel**, celui-ci est impliqué nécessairement dans la démarche d'homologation. Il apporte son expertise juridique dans le domaine à la commission d'homologation, et vérifie que les exigences relatives à la protection des données à caractère personnel sont respectées.

Livrable(s) produit(s) :

- Composition et rôle des membres de la commission d'homologation

Etape 4 : Elaboration du dossier d'homologation et du planning

Durant la quatrième étape, vous allez inventorier le contenu du dossier d'homologation et définir le planning de la démarche qui permettra de le constituer et de l'instruire.

Document(s) attendu(s) :

- Les documents attendus par la Commission d'Homologation dépendent de la démarche retenue pour l'homologation. L'objectif de cette étape est donc de fixer la qualité des documents à collecter.

Participants potentiels à l'Étape 4 :

- Commission d'homologation

1. Le contenu du dossier d'homologation

Le dossier d'homologation est alimenté pendant toutes les phases de la démarche, essentiellement avec des documents nécessaires à la conception, à la réalisation, à la validation du projet ou à la maintenance du téléservice après sa mise en service, ainsi que des documents produits spécifiquement pour l'homologation. L'annexe 3 propose une liste complète des documents qui peuvent être intégrés dans un dossier d'homologation.

Le contenu du dossier pourra varier selon la démarche choisie. Le tableau ci-dessous synthétise les éléments constitutifs du dossier d'homologation en fonction de la démarche adoptée. L'annexe 3 établit la liste plus complète des documents pouvant être contenus dans un dossier d'homologation et en propose une description détaillée.

<table>
<tr><td rowspan="2"></td><td colspan="4">Démarche d'homologation (définie à l'étape 2)</td></tr>
<tr><td>Simple</td><td>Avancée</td><td>Détaillée</td><td>Etape</td></tr>
<tr><td>Stratégie d'homologation</td><td colspan="3">Indispensable</td><td>Etape n°4</td></tr>
<tr><td>Référentiels de sécurité :
• Politique de sécurité des systèmes d'information
• la législation ou la réglementation particulière au contexte de l'organisme ;
• le dossier de sécurité des systèmes interconnectés au système à homologuer.</td><td colspan="3">Si existant</td><td>Etape n°4</td></tr>
</table>

Document présentant les risques identifiés et les objectifs de sécurité	Indispensable			Etape n°5
Procédures d'exploitation sécurisée du système	Indispensable			
Journal de bord de l'homologation (CRR)	Fortement recommandé			
Certificats de qualification des produits ou prestataires	Si existant			
Résultats d'audits	Si existant	Recommandé	Fortement recommandé	
Liste des risques résiduels	Indispensable			
Décision d'homologation	Indispensable			
Spécifiquement pour les systèmes déjà en service :				
Tableau de bord des incidents et de leur résolution	Recommandé	Fortement recommandé	Indispensable	
Résultats d'audits Intermédiaires	Si existant	Recommandé		
Journal des évolutions du système	Si existant			

A ces documents attendus par la commission d'homologation, d'autres documents peuvent être réclamés par cette dernière, en fonction du niveau de démarche :

- Démarche simple :

- Tous les documents décrivant les procédures de sécurité en vigueur au sein de votre organisme peuvent être intégrés au dossier, par exemple :
  - votre charte d'utilisation des postes informatiques ;
  - les règles de contrôle d'accès physique et logique au système ;
  - les clauses de sécurité des contrats de sous-traitance informatique.

- Démarche avancée ou détaillée :
  - Les documents constitutifs du référentiel de sécurité de votre organisme peuvent être intégrés au dossier. En particulier :
    - votre politique de sécurité des systèmes d'information (PSSI) ;
    - la législation ou la réglementation particulière au contexte de votre organisme ou d'un de ses secteurs d'activité ;
    - le dossier de sécurité des systèmes interconnectés au système à homologuer.
  - Votre PSSI, quand elle existe, est un document de référence pour l'homologation, car elle contient des éléments stratégiques (périmètre de sécurité, principaux besoins de sécurité et origine des menaces), ainsi que les règles en vigueur au sein de votre organisme.

L'homologation peut aussi être l'occasion de compléter (ou de rédiger) la PSSI, par exemple pour généraliser des règles indispensables au SI homologué.

Livrable(s) produit(s) :

- La validation de la collecte des documents attendus par la démarche est consignée dans le compte rendu de réunion de la commission d'homologation.

2. Planning de l'homologation

L'homologation doit être prononcée préalablement à la mise en service opérationnelle du téléservice. La Loi de Pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices fixe les délais dans lesquels un téléservice doit être homologué.

La démarche visant à l'homologation doit donc être lancée dès la phase de conception du projet puis être totalement intégrée au projet dès les phases d'étude préalable et de conception, afin d'éviter tout risque calendaire.

Le calendrier de l'homologation est directement dépendant du calendrier du projet dont il doit tenir compte en permanence. Les principales étapes de l'homologation sont fixées dans la stratégie d'homologation.

Il est indispensable de déterminer les tâches de chacun des acteurs de l'homologation et les formaliser dans un planning associé, reprenant les principales étapes. Au besoin, en fonction de l'évolution du projet, ces échéances peuvent être révisées, avec l'accord de l'autorité d'homologation.

Ainsi, une homologation est rythmée par deux temps forts :

- la construction du référentiel documentaire et l'analyse des risques ;
- le déploiement, l'audit, la prononciation de l'homologation et la mise en service opérationnel.

Les échéances prévues pour les différentes étapes de la démarche d'homologation devraient figurer dans le planning, par exemple :

1. Lancement de la procédure d'homologation (par exemple date de formalisation de la stratégie d'homologation) ;
2. Début et de fin de l'analyse des risques (dates des entretiens avec l'autorité) ;
3. Remise des différents documents du dossier d'homologation (cf. section suivante) ;
4. Engagements liés à d'éventuels contrats avec des prestataires impliqués dans le système (hébergeurs, fournisseurs de sous-systèmes, d'applications…) ;
5. Réunions de la commission d'homologation ;
6. Audits éventuels sur les composants du système (techniques ou organisationnels), logiciels plates-formes matérielles, interfaces réseaux ;
7. Homologation du système ;
8. Mise en service du système.

Livrable(s) produit(s) :

- La validation du planning du processus d'homologation est consignée dans le compte rendu de réunion de la commission d'homologation.

Etape 5: Réalisation de l'analyse des risques du téléservice

Durant cette cinquième étape, vous identifiez et ordonnez les risques qui pèsent sur le téléservice à homologuer. L'analyse de risques a été réalisée pendant la phase de développement du téléservice ou pas.

Document(s) attendu(s) :

- Les résultats de ou des analyses de risques réalisées dans le cadre du développement du téléservice. La ou les FEROS si le téléservice a fait l'objet d'un développement ;
- Si le processus d'analyse de risques faisait partie de la méthode de développement retenue.

Participants à l'Étape 5 :

- Responsables métiers ;
- Assistance à maîtrise d'ouvrage ;
- Experts techniques internes ;
- RSSI ;

1. L'analyse de risque

Un risque est la combinaison d'un événement redouté (susceptible d'avoir un impact négatif sur la mission de l'entité) et d'un scénario de menaces. On mesure le niveau du risque en fonction de sa gravité (hauteur des impacts) et de sa vraisemblance (possibilité qu'il se réalise).

Il s'agit d'identifier les risques pesant sur la sécurité du téléservice, de les hiérarchiser et de déterminer des objectifs généraux qui permettront de diminuer certains d'entre eux et, à terme, de les amener à un niveau acceptable.

La durée et le coût de la réalisation d'une analyse des risques sont fonction de la complexité du système d'information et de la sensibilité des données (données propres ou données de tiers, telles que celles des usagers ou des partenaires).

L'analyse des risques pesant sur le système peut être simplifiée dans le cadre d'une démarche Simple. Dans le cas d'une démarche Avancée ou Détaillée, on privilégiera l'utilisation d'une méthode éprouvée d'analyse des risques, comme la méthode EBIOS.

Si aucune analyse des risques n'a été menée lors de la conception du téléservice, la commission d'homologation devra commander (en interne ou en externe) une analyse des risques adaptée à la nature de la démarche d'homologation (Simple, Avancée ou Détaillée).

- Démarche Simple
  - Le tableau d'autodiagnostic de l'annexe 1 vous a permis d'identifier, lors de la deuxième étape, que les enjeux de sécurité du système d'information étaient limités et que les besoins de sécurité étaient faibles ;
  - Pour une analyse des risques simplifiée, vous pouvez alors procéder à une analyse des risques de survol.

- Démarche Avancée ou Détaillée
    - Dans le cadre de la mise en œuvre d'une démarche **Avancée** ou **Détaillée**, la mise en œuvre d'une méthode d'analyse des risques éprouvée est très fortement recommandée, telle que la méthode EBIOS;
    - La méthode EBIOS présente les risques et les objectifs de sécurité identifiés dans une **Fiche d'Expression Rationnelle des Objectifs de Sécurité (FEROS) ;**
    - L'analyse est effectuée avec ou sans l'assistance d'un consultant ayant une expérience confirmée de la méthode. Elle nécessite la participation des acteurs clés du téléservice à homologuer, qui sont interrogés sur leurs besoins, leur contexte d'emploi du système et les événements qu'ils redoutent. C'est la direction de l'entreprise ou l'autorité administrative, par exemple, qui fournissent les informations sur les besoins de disponibilité ou de confidentialité du système, ce qui permet d'identifier les objectifs de sécurité du système.

Idéalement, le résultat de l'analyse (la FEROS) peut ensuite constituer un élément du cahier des clauses techniques particulières d'un appel d'offres pour la mise en conformité du téléservice à homologuer. Les soumissionnaires doivent y répondre en indiquant de quelle manière ils proposent d'atteindre les objectifs de sécurité identifiés.

Livrable(s) produit(s) :

- La validation des analyses de risques existantes (rapport et FEROS) est consignée dans le compte rendu de réunion de la commission d'homologation ;
- Sinon les résultats des analyses demandées par la Commission d'homologation.

2. Identifier les mesures de sécurité

À l'issue de l'analyse de risque, il convient de définir les mesures de sécurité permettant de couvrir les risques identifiés. Ceux qui demeurent après l'application des mesures sont considérés comme des *risques résiduels* qui doivent être acceptés dans le cadre de l'homologation.

- Démarche simple
    - Pour déterminer les mécanismes de sécurité à mettre en œuvre, vous pouvez également vous référer à plusieurs documents publiés par l'ANSSI (sur http://www.ssi.gouv.fr) :
        - le guide d'hygiène informatique ;
        - le guide d'externalisation pour les systèmes d'information ;
        - le guide sur la virtualisation ;
        - les notes techniques, notamment celle sur la sécurité web.
- Démarche Avancée ou Détaillée
    - Dans le cadre d'une démarche avancée ou détaillée, les objectifs de sécurité identifiés au cours de l'analyse des risques selon la méthode EBIOS permettront de définir les mesures de sécurité destinées à couvrir les risques considérés comme inacceptables.

Outre les documents présentés dans le paragraphe précédent, de nombreux référentiels de sécurité proposent des catalogues de mesures.

Livrable(s) produit(s) :

- L'analyse de risques produite sera complétée avec les mesures de réduction des risques si l'objectif de sécurité dans le traitement retenu est la réduction des risques ;
- Les mesures de sécurité seront choisies dans différents référentiels, dont les exigences du RGS de Polynésie française ;
- Si le traitement des risques est le transfert du ou des risques, alors il conviendra de justifier du choix et des moyens contractuels mis en œuvre.

Etape 6 : Evaluation et amélioration du niveau de sécurité du téléservice

Durant la sixième étape, vous devez mesurer l'écart entre les résultats de l'étude des risques et la réalité, en réalisant un contrôle de sécurité plus ou moins formalisé du Téléservice. Ce contrôle peut intervenir à tout moment du cycle de vie du téléservice : en amont, avant la mise en service voir au cours de la conception, mais également en aval, si le Téléservice est déjà opérationnel.

Le degré de formalisation du contrôle dépend de la démarche entreprise. Vous avez déterminé lors de la seconde étape quel type d'audit était adapté. Certains systèmes n'appellent qu'une vérification peu formelle. En revanche, un audit complet et indépendant se justifie dans le cas de systèmes à fort enjeu de sécurité.

Document(s) attendu(s) :

- Analyse d'écart ;
- Audits ;

Participants potentiels à l'Étape 6 :

- Responsables métiers ;
- Assistance à maîtrise d'ouvrage ;
- Experts techniques internes ;
- RSSI ;

1. Réalisation du contrôle de sécurité

- Démarche Simple
  - Pour la démarche Simple, un audit technique est optionnel.

- Démarche Avancée ou Détaillée
  - Pour la démarche **Avancée ou Détaillée**, il est fortement recommandé d'effectuer un audit technique du téléservice. Cet audit permettra de mettre en évidence d'éventuelles failles et d'identifier rapidement les risques encourus par l'organisme.

Les audits doivent être menés dans les formes prévues par le référentiel d'exigences relatif aux prestataires d'audit de la sécurité des systèmes d'information, disponible en ligne sur le site internet www.lexpol.pf

2. Définition du périmètre du contrôle de sécurité

Le contrôle de sécurité effectué, qui peut prendre la forme d'un audit formalisé, porte sur un téléservice dont le périmètre doit être soigneusement délimité par l'autorité d'homologation. Les contrôles peuvent être de différente nature

- Audit de tout ou partie du code source ;
- Audit de la configuration des équipements et des logiciels du Téléservice;
- Audit de l'architecture du système ;
- Audit de l'organisation mise en place, etc..

Pour les Téléservices qui par définition sont ouverts sur le réseau Internet, un test d'intrusions devra être effectué.

3. Conséquences du contrôle sur le dossier d'homologation

Le contrôle de sécurité doit faire l'objet d'une trace écrite. A fortiori, s'il s'agit d'un audit de sécurité, celui-ci doit faire l'objet d'un rapport, qui doit faire apparaître :

- une évolution des menaces sur le téléservice ;
- la découverte éventuelle de nouvelles vulnérabilités ;
- la préconisation de mesures correctrices, le cas échéant.

Le ou les rapports d'audit est ou sont intégré(s) au dossier d'homologation, qui doit être complété en tenant compte des nouveaux risques mis en lumière.

Livrable(s) produit(s) :

- Le rapport d'audit doit faire apparaître clairement les écarts, éventuels, avec l'analyse de risques de l'Étape 5 ;
- L'auditeur doit proposer un ensemble de recommandations dans son rapport afin d'assister la Commission d'homologation dans ses décisions.

Etape 7 : Mesures de sécurité complémentaires pour couvrir les derniers risques

Durant la septième étape, vous devez définir un plan d'action pour amener le risque identifié à un niveau acceptable.

Document(s) attendu(s) :

- L'équipe projet doit proposer ici dans un livrable les options retenues suite à l'audit et aux résultats de ce dernier.

Participants potentiels à l'Étape 7 :

- Responsables métiers ;
- Assistance à maîtrise d'ouvrage ;
- Experts techniques internes ;
- RSSI ;

1. Le traitement du risque

Au vu des résultats de l'analyse de risques (Étape 5) et du contrôle de sécurité (Étape 6), l'autorité d'homologation se prononce sur l'ensemble des risques qui ne sont pas, à ce stade, complètement couverts par des mesures de sécurité. Il convient ainsi, pour tout ou partie de chaque risque de choisir parmi les options suivantes :

- l'**éviter** : changer le contexte de telle sorte qu'on n'y soit plus exposé ;
- le **réduire** : prendre des mesures de sécurité pour diminuer l'impact et/ou la vraisemblance ;
- l'**assumer** : en supporter les conséquences éventuelles sans prendre de mesure de sécurité supplémentaire ;
- le **transférer** : partager les pertes occasionnées par un sinistre ou faire assumer la responsabilité à un tiers.

On peut choisir plusieurs options pour chaque risque. Par exemple, un risque peut être partiellement réduit par la mise en œuvre de mesures de sécurité, partiellement transféré par le recours à une assurance et partiellement assumé pour ce qui subsiste.

2. La mise en œuvre de mesures de sécurité

Les mesures de sécurité peuvent être de nature technique, organisationnelle ou juridique. Elles sont décidées par l'autorité d'homologation sur proposition de la commission d'homologation.

En cas de recours à un prestataire externe (hébergement de site ou de services par exemple), les mesures de sécurité peuvent être intégralement mises en œuvre à travers un contrat garantissant, par exemple, que les processus et les données sont protégés et accessibles uniquement aux utilisateurs légitimes. Dans ce cas, le responsable du Téléservices s'assurera de la juste prise en compte des risques identifiés lors de l'Étape

5 en les formalisant dans un Plans d'Assurance Sécurité sur lequel s'engagera le Prestataire d'hébergement ou de service.

3. Définition du plan d'action

Les risques résiduels identifiés lors du contrôle et de l'analyse de risques et qui ne peuvent pas être couverts par des mesures techniques ou organisationnelles sont identifiés dans un plan d'action. Ce dernier indique les vulnérabilités éventuelles, leur degré (critique, majeure, mineure…), l'action correctrice envisagée, le pilote désigné, ainsi que l'échéance associée.

Livrable(s) produit(s) :

- Un rapport formalisant les mesures de sécurité retenues par l'équipe projet en conformité avec les rapports d'audit.

Etape 8 : Décision d'homologation du téléservice

Durant la huitième étape, vous devez concrétiser la décision d'homologation par une attestation formelle autorisant, du point de vue de la sécurité, l'exploitation du téléservice.

La décision d'homologation est l'acte par lequel le responsable de l'autorité administrative atteste de l'existence d'une analyse de sécurité et de sa prise en compte. La décision d'homologation doit nécessairement comprendre un certain nombre d'éléments, référencés ci-dessous.

Document(s) attendu(s) :

- Dossier d'homologation

Participants à l'Étape 8 :

- Commission d'homologation
- Autorité d'homologation

1. Le périmètre de l'homologation

Il doit, au minimum, tenir compte des éléments suivants :

- référentiel réglementaire (dans le cas des téléservices mis en œuvre par les autorités administratives, il s'agit du Référentiel Général de Sécurité de la Polynésie française) ;
- références des pièces du dossier d'homologation ;
- périmètre géographique et physique (localisations géographiques, locaux, etc.) ;
- périmètre fonctionnel et organisationnel (fonctionnalités, types d'informations traitées par le téléservice et sensibilité, types d'utilisateurs, règles d'emploi, procédures, conditions d'emploi des produits de sécurité, etc.) ;
- périmètre technique (cartographie, architecture détaillée du téléservice, produits agréés, prestataires qualifiés, etc.).

2. Les conditions accompagnant l'homologation

L'autorité d'homologation peut, en fonction des risques résiduels identifiés, assortir l'homologation de conditions d'exploitation ainsi que d'un plan d'action visant à maintenir et à améliorer le niveau de sécurité du téléservice dans le temps. À chaque action, ce plan associe une personne pilote ainsi qu'une échéance.

3. La durée de l'homologation

L'homologation doit être décidée pour une durée maximale.

Cette durée doit prendre en compte l'exposition du système d'information aux nouvelles menaces, ainsi que les enjeux de sécurité du téléservice, c'est-à-dire le degré de criticité des informations et des processus du système.

Pour un téléservice bien maîtrisé, avec peu de risques résiduels et ne présentant pas de difficultés particulières, il est recommandé de prononcer une homologation d'une durée maximale de cinq (5) ans,

avec revue annuelle. Cette durée maximale doit être réduite à trois (3) ans pour un système avec de quelques risques résiduels ou à un an (1) pour un système présentant de nombreux risques résiduels.

4. Conditions de suspension ou de retrait de l'homologation

L'homologation de sécurité ne demeure valide que tant que le système d'information est exploité dans le contexte décrit dans le dossier d'homologation. Les changements suivants doivent impliquer un réexamen du dossier, pouvant conduire à une nouvelle décision d'homologation ou à un retrait de la décision :

- raccordement d'un nouveau site sur le téléservice ;
- ajout d'une fonctionnalité majeure ;
- succession de modifications mineures ;
- réduction de l'effectif affecté à une tâche impactant la sécurité ;
- changement d'un ou de plusieurs prestataires ;
- prise de fonction d'une nouvelle autorité d'homologation ;
- non-respect d'au moins une des conditions de l'homologation ;
- changement du niveau de sensibilité des informations traitées et, plus généralement, du niveau du risque ;
- évolution du statut de l'homologation des systèmes interconnectés ;
- publication d'incidents de nature à remettre en cause les garanties recueillies dans le dossier de sécurité ;
- décision de l'autorité d'homologation.

À ce titre, il est recommandé que la commission d'homologation soit réunie annuellement par l'autorité d'homologation, afin de procéder à une revue du respect des conditions de l'homologation.

Livrable(s) produit(s) :

- Décision d'homologation

Etape 9 : Surveillance des risques résiduels du téléservice

Durant cette dernière étape, qui intervient après la décision d'homologation proprement dite, vous devez mettre en œuvre une procédure de révision périodique de l'homologation, ainsi que le plan d'action pour traiter les risques résiduels et les nouveaux risques dans le cycle de vie du téléservice.

Document(s) attendu(s) :

- Dossier d'homologation
- Nouveaux audits
- Evolutions
- Incidents

Participants à l'Étape 9 :

- Commission d'homologation

1. Suivi de l'homologation

À la suite de la décision proprement dite, l'autorité d'homologation doit veiller au maintien du niveau de sécurité du téléservice. La commission d'homologation réalise annuellement un suivi de l'homologation. Cette étape n'est pas une nouvelle instruction. Elle doit donc rester simple et se limiter à une mise à jour du dossier et à une analyse succincte des évolutions et des incidents intervenus au cours de l'année, afin de juger de l'opportunité d'une révision plus approfondie de l'homologation.

En préparation du renouvellement de l'homologation, le dossier d'homologation est régulièrement complété par les éventuelles analyses de vulnérabilités, les comptes rendus de contrôle et les rapports d'audits complémentaires. La version consolidée est transmise aux membres de la commission d'homologation

Il est recommandé de réunir périodiquement la commission d'homologation pour reprendre la liste des critères et vérifier que les conditions d'homologation sont toujours respectées. Cela permet également d'éviter de reprendre l'homologation à zéro au terme de sa durée de validité.

2. Maintien en conditions de sécurité

Il est nécessaire que les conditions de l'homologation soient respectées dans le temps. À ce titre, l'entité en charge du maintien du dossier d'homologation doit également assurer une veille technologique. Celle-ci permet d'identifier les vulnérabilités qui apparaîtraient sur le téléservice et s'assurer qu'elles soient corrigées, notamment les plus sérieuses.

Il est également nécessaire de vérifier :

- les clauses de sécurité et de maintien en conditions de sécurité du téléservice, le cas échéant en se référant au guide d'externalisation publié par l'ANSSI ;
- les capacités d'évolution et d'interopérabilité de son système, notamment au regard de ses capacités de développement ou de ses contrats de prestations de service.

Livrable(s) produit(s) :

- Dossier d'homologation mis à jour

CONSEILS PRATIQUES

La démarche d'homologation est un projet en soi, qui doit s'intégrer complètement au projet global et au cycle de vie du système d'information, le téléservice. C'est une démarche qui peut se révéler complexe et qui se heurte parfois à des difficultés organisationnelles, techniques ou calendaires. Les conseils contenus dans cette fiche vous permettront d'aboutir plus facilement à un résultat satisfaisant.

1. Conseils d'ordre général

Les conseils d'ordre général listés ci-dessous doivent, dans la mesure du possible, être suivis pour maximiser les chances de réussite d'une démarche d'homologation :

- débuter suffisamment tôt la démarche d'homologation ;
- prévoir une validation formelle des décisions au niveau hiérarchique adéquat ;
- désigner un véritable chef de projet, qui sera disponible tout au long du projet ;
- maîtriser le calendrier et ne pas être trop contraint par des nécessités opérationnelles ;
- bien définir le périmètre et disposer d'une architecture précise du système ;
- bien prendre en compte les interconnexions éventuelles ;
- s'appuyer sur des documents écrits, explicites, sans ambiguïté, afin d'éviter les quiproquos entre les parties prenantes au projet.

2. Avant l'étude

Une réflexion menée en amont permet de bien préparer la démarche d'homologation et d'assurer sa réussite de façon optimale.

Au préalable, il faut que la démarche soit portée à haut niveau par l'autorité d'homologation et que l'ensemble des acteurs concernés soit impliqué et motivée.

Il faut également désigner un chef de projet, qui disposera des moyens pour mener à bien sa mission et rapporter toute difficulté à l'autorité d'homologation.

Enfin, dès que les acteurs de l'homologation sont identifiés, il est indispensable de les sensibiliser sur la démarche, les concepts et le vocabulaire qui seront utilisés.

3. Pendant l'étude

Pour chaque activité à réaliser, il est conseillé de s'organiser en mode projet, en identifiant un responsable de l'activité, en constituant un groupe de travail et en lui confiant une mission précise, associée à une date de réalisation.

Certaines missions sont essentielles pour la réussite du projet :

- la sensibilisation des acteurs
    - rappeler l'objectif de l'activité
    - présenter les concepts, le vocabulaire
    - s'assurer que l'ensemble des acteurs ait une vision commune de la problématique
- la collecte des informations
    - réaliser des entretiens
    - rassembler les documents existants sur l'organisme, le projet de téléservice
- le suivi du projet
    - présenter des exemples pour lancer les discussions
    - synthétiser les informations récoltées pour validation par le groupe de travail
    - nommer des responsables et fixer des échéances
    - se rencontrer périodiquement

Il est également nécessaire d'adapter les livrables aux destinataires en ce qui concerne :

- la forme : tableaux, textes, schémas, etc. ;
    - le niveau d'information : recherche d'exhaustivité ou forme synthétique ;
    - l'intégration aux documents existants ;
    - l'adaptation au vocabulaire habituel de l'organisme,
    - leur nomenclature, qui doit être explicite,
    - leur libellé, qui doit être court et descriptif.

Enfin, il est recommandé de faire valider chaque étape par la commission d'homologation. Cela permet d'éviter les retours en arrière improductifs, tout en impliquant les autorités tout au long de la réalisation du dossier de sécurité.

Annexe 1 au guide d'homologation : Estimation rapide du besoin de sécurité d'un système d'information, d'un Téléservice

Le tableau suivant permet d'évaluer les besoins de sécurité d'un Téléservice à homologuer, en estimant la gravité des conséquences potentielles d'une défaillance d'un composant du SI du Téléservice, la sensibilité des données, le potentiel des attaquants, le degré d'exposition aux menaces et l'importance des vulnérabilités intrinsèques du SI.

Dans le tableau suivant la notion de SI (Système d'information) représente l'ensemble des composants logiciels et matériels ainsi que les installations et l'organisation nécessaire à l'exploitation d'un Téléservice. Attention, un Téléservice ne se limite pas à son interface web avec l'Internet. Ce sont l'ensemble des dispositifs informatiques qui permettent de rendre le service aux usagers ou aux autres autorités administratives.

Si vous répondez « Je ne sais pas » à plus de deux questions, faites-vous aider par la maîtrise d'ouvrage, qui connaît les enjeux du SI.

<table>
<tr><td>Thème</td><td colspan="4"></td><td>Note</td><td>Max</td></tr>
<tr><td rowspan="8">Gravité des conséquences potentielles</td><td colspan="4">Question n° 1 : Votre SI est-il important pour remplir vos missions ?</td><td rowspan="2"></td><td rowspan="8">(reportez ici la valeur maximale des réponses aux questions 1 à 3)</td></tr>
<tr><td>1</td><td>2</td><td>3</td><td>4</td></tr>
<tr><td>Non, le SI est accessoire à l’accomplissement des missions</td><td>Oui, les missions seraient fortement perturbées par un dysfonctionnement du SI.</td><td>Oui, les missions dépendent totalement du SI</td><td>Je ne sais pas</td></tr>
<tr><td colspan="4">Question n° 2 : Si un sinistre atteint votre SI, causant un dysfonctionnement ou une perte de données, les conséquences en interne (pour vos services) seraient-elles graves ?
Exemple : une panne électrique ne permet pas d’utiliser le SI, le contenu d’une base de données a été supprimé, le SI subit une cyberattaque, etc.</td><td rowspan="3"></td></tr>
<tr><td>1</td><td>2</td><td>3</td><td>4</td></tr>
<tr><td>Non, les conséquences internes d’un sinistre seraient négligeables</td><td>Oui, les conséquences internes d’un sinistre seraient significatives</td><td>Oui, les conséquences internes d’un sinistre seraient graves, voire fatales</td><td>Je ne sais pas</td></tr>
<tr><td colspan="4">Question n° 3 : Si un sinistre touche la sécurité de votre SI (il ne fonctionne plus ou pas bien, vol d’informations…), les conséquences pour l’extérieur (pour vos usagers, administrés…) seraient-elles graves ?</td><td rowspan="3"></td></tr>
<tr><td>1</td><td>2</td><td>3</td><td>4</td></tr>
<tr><td>Non, les conséquences d’un sinistre pour l’extérieur seraient négligeables</td><td>Oui, les conséquences d’un sinistre pour l’extérieur seraient significatives</td><td>Oui, les conséquences d’un sinistre pour l’extérieur seraient graves, voire fatales</td><td>Je ne sais pas</td></tr>
</table>

<table>
<tr><td>Thème</td><td colspan="4"></td><td>Note</td><td>Max.</td></tr>
<tr><td rowspan="10">Sensibilité des données du SI</td><td colspan="4">Question n° 4 : Le fait que les données de votre SI soient inaccessibles est-il grave ? Exemple : vous ne pouvez pas accéder aux données en raison d’une panne matérielle, ou suite à la blocage par une rançongiciel</td><td rowspan="2"></td><td rowspan="10">(reportez ici la valeur maximale des réponses aux questions 4 à 6)</td></tr>
<tr><td>1</td><td>2</td><td>3</td><td>4</td></tr>
<tr><td>Non, le fait qu’il ne soit pas accessible ne gêne quasiment pas l’activité</td><td>Oui, le fait qu’il ne soit pas accessible perturbera l’activité de manière significative</td><td>Oui, le fait qu’il ne soit pas accessible peut être fatal pour l’activité</td><td>Je ne sais pas</td></tr>
<tr><td colspan="4">Question n° 5 : Le fait que les données de votre SI soient altérées est-il grave ? Exemple : un malware a modifié des valeurs dans une base de données, les remettant toutes à 0.</td><td rowspan="3"></td></tr>
<tr><td>1</td><td>2</td><td>3</td><td>4</td></tr>
<tr><td>Non, le fait que les données soient altérées ne gêne quasiment pas l’activité</td><td>Oui, le fait que les données soient altérées perturbera l’activité de manière significative</td><td>Oui, le fait que les données soient altérées peut être fatal pour l’activité</td><td>Je ne sais pas</td></tr>
<tr><td colspan="4">Question n° 6 : Le fait que les données de votre SI ne soient pas ou plus confidentielles est-il grave ? Exemple : la liste des bénéficiaires du service social est dévoilée.</td><td rowspan="3"></td></tr>
<tr><td>1</td><td>2</td><td>3</td><td>4</td></tr>
<tr><td>Non, le défaut de confidentialité ne gêne quasiment pas l’activité</td><td>Oui, le défaut de confidentialité perturbera l’activité de manière significative</td><td>Oui, le défaut de confidentialité peut être fatal pour l’activité</td><td>Je ne sais pas</td></tr>
</table>

Thème					Note	Max
Base d'estimation des potentiels d'attaques cyber	**Question n° 7** : Quel est le niveau de compétence maximal présumé de l'(cyber)attaquant ou du groupe d'attaquants susceptibles de porter atteinte au SI ?					(reportez ici la valeur maximale des réponses aux questions 7 à 11)
	1	2	3	4		
	Individu isolé de niveau de compétence élémentaire	Individu isolé de niveau de compétence avancé	Groupe d'individus organisés, de niveaux individuels de compétence faibles à moyens, ou individu isolé aux compétences expertes	Groupe d'individus experts, organisés, aux moyens quasi illimités		
	Question n° 8 : Quelle est la précision des (cyber)attaques potentielles envers le SI ?					
	1	2	3	4		
	Attaques « au hasard » sur le cyberespace	Attaques orientées vers le la Polynésie française	Attaques ciblant un groupe de victimes présentant des caractéristiques communes	Attaques visant précisément le SI		
	Question n° 9 : Quel est le niveau de sophistication des (cyber)attaques potentielles contre le SI ?					
	1	2	3	4		
	Outils d'attaque triviaux (logiciel de scan de ports, virus connus, etc.)	Outils élaborés génériques prêts à l'emploi (réseaux de botnet loués, faille connue, etc.)	Outils sophistiqués, adaptés pour le SI (zéro-day, etc.)	Boîte à outils très hautement sophistiquée.		

	Question n° 10 : Quelle est la visibilité des (cyber)attaques potentielles contre le SI ?					
	1	2	3	4		
	Attaque annoncée (revendications « d'hacktivistes », rançon, etc.)	Attaque constatée immédiatement par ses effets sur le SI	Attaque discrète, qui laisse des traces dans les journaux d'événements, mais ne perturbe pas le fonctionnement du SI	Attaque invisible, réalisée en laissant le minimum de traces		
	Question n° 11 : Quelles sont la fréquence et la persistance des (cyber)attaques potentielles contre le SI ?					
	1	2	3	4		
	Unique : l'attaque ne se produit sur la cible qu'une seule fois	Ponctuelle : l'attaque survient plusieurs fois sans régularité dans sa fréquence (elle peut être liée à l'actualité).	Récurrente : attaque par vagues successives importantes	Permanente		

<table>
<tr><td>Thème</td><td colspan="4"></td><td>Note</td><td>Max</td></tr>
<tr><td rowspan="8">Exposition et vulnérabilités</td><td colspan="4">Question n° 12 : Quel est le niveau d’hétérogénéité du SI ? Exemple : plusieurs logiciels, matériels ou réseaux différents pour un même SI.</td><td rowspan="2"></td><td rowspan="8">(reportez ici la valeur maximale des réponses aux questions 12 à 15)</td></tr>
<tr><td>1</td><td>2</td><td>3</td><td>4</td></tr>
<tr><td>Le SI est jugé comme homogène</td><td>Le SI est jugé comme faiblement hétérogène</td><td>Le SI est jugé comme fortement hétérogène</td><td>Je ne sais pas</td></tr>
<tr><td colspan="4">Question n° 13 : Quel est le degré d’ouverture/interconnexion du SI ?
Exemple : Internet, un autre SI interne ou externe (celui d’un prestataire, d’une autre autorité administrative…)…</td><td rowspan="3"></td></tr>
<tr><td>1</td><td>2</td><td>3</td><td>4</td></tr>
<tr><td>Le SI n’est pas ouvert</td><td>Le SI n’est ouvert qu’à des systèmes internes maîtrisés</td><td>Le SI est ouvert à des systèmes internes non maîtrisés ou externes</td><td>Je ne sais pas</td></tr>
<tr><td colspan="4">Question n° 14 : Le contexte dans lequel se trouve le SI et ses composants (matériels, logiciels, réseaux) évolue-t-il régulièrement ?</td><td rowspan="3"></td></tr>
<tr><td>1</td><td>2</td><td>3</td><td>4</td></tr>
<tr><td>Le SI et son contexte sont jugés stables</td><td>Le SI et son contexte changent souvent</td><td>Le SI et son contexte évoluent en permanence</td><td>Je ne sais pas</td></tr>
</table>

Thème					Note	Max
	Question n° 15 : Les composants du SI sont-ils mis régulièrement à jour ?					
	1	2	3	4		
	Les composants du SI sont tous tenus à jour en permanence	Une partie des composants du SI est régulièrement mise à jour	Les mises à jour sont effectuées de manière irrégulière	Je ne sais pas		
	Total des quatre valeurs maximales :					

Avec ces résultats que l'on additionne, on estime ainsi le besoin de sécurité de son SI :

Somme des quatre valeurs de la colonne Max.	Besoin de sécurité du SI
De 4 à 6	1 – Faible
De 7 à 9	2 – Moyen
De 10 à 16	3 – Fort

Annexe 2 au guide d'homologation : Estimation rapide du niveau de maturité de l'organisme

Le tableau suivant permet d'évaluer le niveau de maturité en sécurité de votre organisme.

Le niveau de maturité en sécurité ne correspond pas au niveau réel de sécurité, mais à la capacité de l'organisme à gérer les risques, pour chaque SI d'information.

Niveau	Question	Réponse
Elémentaire	*1. Les activités de sécurité sont- elles réalisées en utilisant des pratiques de base (bonnes pratiques de sécurité, référentiels de mesures…) ?*	Oui/Non
	Si LA case précédente est à Oui, alors votre organisme à un niveau de maturité élémentaire en sécurité	
Moyen	*2. Les activités de sécurité sont-elles planifiées ?*	Oui/Non
	3. Les acteurs affectés à des activités de sécurité sont-ils formés (en interne ou par un organisme de formation) à la SSI (niveau de compétence en sécurité jugé suffisant) ?	Oui/Non
	4. Certaines pratiques de sécurité sont-elles formalisées dans des documents spécifiques (procédures) ?	Oui/Non
	5. Des mesures de sécurité sont-elles en place ?	Oui/Non
	6. Les autorités compétentes sont-elles informées des mesures effectuées ?	Oui/Non
	Si TOUTES les cases précédentes sont à Oui, alors votre organisme a un niveau de maturité moyen en sécurité.	
Avancé	*7. Les processus de sécurité sont-ils définis, standardisés et formalisés (définir la stratégie, gérer les risques, gérer les règles, superviser…) ?*	Oui/Non
	8. Des acteurs spécifiques sont-ils affectés à la gestion des processus de sécurité et sont formés en conséquence ?	Oui/Non
	9. L'organisme dans sa globalité soutient-il les processus de sécurité (les différents niveaux hiérarchiques…) ?	Oui/Non
	10. Les processus de sécurité sont-ils coordonnés dans tout le périmètre choisi ?	Oui/Non
	11. L'efficacité des mesures de sécurité en place est-elle mesurée ?	Oui/Non
	12. Des audits sont-ils effectués pour vérifier la suffisance des mesures en place ? (Les mesures de sécurité effectuées sont-elles contrôlées [auditées] ?)	Oui/Non
	13. Les processus de sécurité sont-ils améliorés en fonction des mesures de sécurité effectuées ?	Oui/Non
	Si TOUTES les cases précédentes sont à Oui, alors votre organisme a un niveau de maturité avancé en sécurité.	

Comment interpréter vos résultats ?

La maturité étant la « Sûreté dans le domaine du jugement, de la réflexion » vous pouvez en déduire la capacité de votre organisation à gérer les risques pesant sur votre Téléservice.

Niveau	Impact sur la démarche
Élémentaire	L'organisme n'a pas encore une culture de la sécurité, la conscience aux bonnes pratiques n'est pas acquise. Les membres de la commission d'homologation ne sont pas autonomes pour réaliser les actions attendues.
Moyen	Des bonnes pratiques sont en place au sein de l'organisation Les membres de la commission d'homologation sont possiblement autonomes pour suivre le processus
Avancé	L'organisme dispose de procédures et met en œuvre une gestion de ses risques Les membres de la commission d'homologation sont autonomes pour réaliser une grande partie des actions de l'homologation

Si vous avez répondu « non » à l'ensemble des cases du tableau de maturité, alors une démarche assistée est indispensable. Cette démarche consiste essentiellement à un accompagnement comme pour le niveau Élémentaire.

Annexe 3 au guide d'homologation : Liste des documents pouvant être contenus dans un dossier d'homologation

Le dossier d'homologation peut contenir, en fonction de leur pertinence au regard du contexte et de la complexité du SI, les éléments suivants.

1. La stratégie d'homologation

L'autorité d'homologation, ou son représentant, formalise l'organisation de l'homologation dans un document de synthèse. Cette stratégie d'homologation décrit les modalités de réalisation du processus d'homologation. Elle rappelle l'ensemble des parties prenantes à l'homologation et précise :

- Le cadre réglementaire applicable (loi du pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices, etc) ;
- L'organisation (acteurs, missions, etc.) ;
- La démarche ;
- Le périmètre ;
- Le calendrier ;
- La criticité des informations utilisées dans le cadre de l'homologation ;
- Les pièces constitutives du dossier d'homologation.

2. L'analyse de risques

Elle doit être menée selon une méthode éprouvée conforme aux normes existantes en matière de gestion des risques SSI. La méthode EBIOS est recommandée. Il est par ailleurs recommandé à l'autorité administrative de mettre en œuvre un processus de gestion des risques sur le périmètre de son Téléservice conforme à la norme international ISO/IEC 27005.

Ce document doit présenter les risques identifiés et les objectifs de sécurité ainsi que les risques résiduels acceptés :

- Il décrit les besoins et objectifs de sécurité du SI en termes de disponibilité, d'intégrité et de confidentialité par rapport aux menaces identifiées. Au besoin, il peut être présenté sous la forme d'une fiche d'expression rationnelle des objectifs de sécurité (FEROS).
- Il indique la nature et la sensibilité des informations traitées par le SI et précise les contraintes qui restreignent la conception, l'exploitation et la maintenance du Téléservice.
- Il doit prendre en compte les architectures d'interconnexion, les moyens partagés avec d'autres entités, leurs conditions d'exploitation et de contrôle.
- Sa rédaction nécessite la participation des acteurs clés du SI à homologuer, qui sont interrogés sur leurs besoins, le contexte d'emploi du système et les événements susceptibles d'impacter positivement ou négativement le système.

3. La politique de sécurité du système d'information (PSSI)

La PSSI définit les principes et les exigences techniques et organisationnelles de sécurité du système d'information. Il s'agit du document de référence SSI applicable à l'ensemble de l'organisme ou dédié à un système comme à un Téléservice

L'homologation peut aussi être l'occasion d'élaborer ou de compléter la politique de sécurité des systèmes d'information (PSSI) de l'organisme, par exemple afin de généraliser des règles indispensables au système d'information homologué. Le guide [PSSI] de l'ANSSI fournit une aide pour élaborer une PSSI.

Ce document revêt différentes formes en fonction des interlocuteurs (directives, procédures, codes de conduite, règles organisationnelles et techniques, etc.).

La PSSI doit reprendre les résultats de l'analyse de risques. Elle mettra l'accent sur les mesures permettant d'adresser les risques pouvant impacter le Téléservice, notamment si ce dernier est exposé à la cybermenace.

La PSSI inclut :

- Les éléments stratégiques ;
- Le périmètre du SI, les enjeux liés, les orientations stratégiques, les aspects légaux et réglementaires ;
- Les exigences de protection des données personnelles si le Téléservice est un des acteurs de leur traitement ;
- Les principes de sécurité par domaine (organisationnel, technique, mise en œuvre, etc.).

Elle peut être complétée par une ou plusieurs politiques d'application, par exemple les procédures de Maintien en Condition de sécurité (MCS).

4. Le journal de bord de l'homologation

Il s'agit du registre des décisions et des principaux événements qui sont intervenus pendant la démarche d'homologation. Il présente les caractéristiques suivantes :

- Il s'enrichit au fur et à mesure du projet (document de travail, feuille de route) pour adapter le processus aux évolutions du projet, notamment pour le planning ;
- Il permet de formaliser les prises de décisions et les mises au point nécessaires et de disposer d'un point de situation sur l'avancement du processus d'homologation (et les blocages éventuels) ;
- Il fait état des mesures des besoins de sécurité du Téléservice et de la maturité évaluée de la Commission d'homologation ;
- Il constitue la base pour réaliser le plan d'action associé à la décision d'homologation ;
- Il peut se présenter sous plusieurs formes :
    - Documents isolés (comptes rendus de réunions, notes, etc.) ;
    - Document unique (registre formel de décisions, ou tableau de synthèse avec renvois à des documents isolés par exemple).

5. Les référentiels de sécurité

La démarche d'homologation doit être réalisée conformément aux exigences décrites dans les référentiels de sécurité de l'autorité et en particulier :

- La politique de sécurité des systèmes d'information (PSSI) de l'autorité ;
- La législation ou la réglementation particulière applicable à l'autorité administrative ;
- Les exigences de sécurité des systèmes interconnectés au système à homologuer.

6. Le tableau de bord de l'application des règles d'hygiène informatique

Les mesures techniques du « Guide d'hygiène informatique » publié par l'ANSSI sont applicables dans toutes les situations. Un tableau de bord mesurant l'application de ces mesures d'hygiène montre la progression au sein du système, l'objectif étant de toutes les appliquer.

7. La cartographie des systèmes d'information de l'organisme

La cartographie complète du réseau local doit être établie. Elle comprend :

- **la cartographie physique du réseau** qui correspond à la répartition géographique des équipements et permet de connaître la position d'un équipement réseau au sein des différents sites.
- **la cartographie logique du réseau** (plan d'adressage IP, noms de sous-réseaux, liens logiques entre ceux-ci, principaux équipements actifs, etc.). Elle fait notamment apparaître les points d'interconnexion avec des entités « extérieures » (partenaires, fournisseurs de services, etc.) ainsi que l'ensemble des interconnexions avec Internet.
- **la cartographie des applications**. Le point de vue applicatif correspond aux applications métier et logiciels d'infrastructure utilisant l'architecture réseau comme support.
- **la cartographie de l'administration du système d'informations.** Elle représente le périmètre et le niveau de privilèges des administrateurs sur les ressources du parc informatique. Ce point de vue permet, en cas de compromission d'un compte d'administration, d'identifier le niveau de privilège de l'attaquant et la portion du parc potentiellement impactée.

8. Les schémas détaillés des architectures du système

Les schémas détaillés des architectures techniques et fonctionnelles dépendent avant tout du périmètre choisi de l'homologation du SI, ainsi que du niveau de maturité de l'organisme.

Les schémas doivent permettre de savoir quelle est la fonction principale du SI et comment ce SI fonctionne.

À cette fin, il faut disposer, au minimum, de l'annuaire (gestion des comptes), du plan d'adressage, de la liste des fonctions de sécurité et de la cartographie du SI.

Cette documentation doit être mise à jour afin de suivre les modifications subies par le SI.

Par exemple, si le périmètre de l'homologation est une application de télé-service, il faut fournir les éléments suivants :

- Les procédures de Maintien en Condition de sécurité (MCS) ;
- Le plan du maintien en condition opérationnelle ;
- La matrice des flux entrant/sortant (interconnexions) ;
- La documentation de la gestion des comptes de l'application ;
- La documentation de l'administration du SI et de l'installation ;
- Le plan de sauvegarde et d'archivage des données ;
- Le plan de continuité ou de reprise d'activité.

9. Les procédures d'exploitation du système

Ces procédures doivent être détaillées et directement applicables. Elles exposent les mesures de sécurité permettant de répondre aux objectifs de sécurité fixés par l'autorité d'homologation. Elles présentent les droits et les devoirs des accédants au système ainsi que les actions à réaliser dans le cadre de l'utilisation quotidienne du système.

Ces procédures sont établies par les équipes d'exploitation internes à l'organisme et/ou par les fournisseurs du système à homologuer, éventuellement à l'aide des guides publiés par l'ANSSI.

L'autorité d'homologation doit s'assurer que les procédures fournies ont été testées avec succès avant de prononcer l'homologation. Un dossier de tests complétera utilement le dossier d'homologation.

10. Les exigences de sécurité à destination des systèmes interconnectés

Les systèmes contenant des informations sensibles ne doivent pas être connectés directement aux réseaux publics tels qu'Internet ou les réseaux Wi Fi des hôtels, des ports ou des aéroports.

11. Les décisions d'homologation des systèmes interconnectés

Si les systèmes connectés au système concerné, ont déjà fait l'objet d'une homologation, il faut joindre les décisions d'homologation associées aux systèmes ainsi que les dossiers associés, si possible et si nécessaire. En effet, il est impératif de savoir, au minimum, par qui le système a été homologué, à quelle date et quelle est la référence de cette dernière homologation.

12. Les attestations de qualification des produits ou prestataires

Dans la mesure où le système met en œuvre des produits de sécurité certifiés ou qualifiés ou encore des services de confiance qualifiés, il est nécessaire d'inclure les attestations correspondantes dans le dossier d'homologation.

Si elles sont disponibles, les analyses de sécurité des produits de sécurité, en particulier les instructions techniques d'emploi, peuvent également être intégrées au dossier d'homologation.

A défaut, la commission d'homologation devra fournir le formulaire : *Arrêté -Annexe2 formulaire Formulaire de motivation du non-recours* motivant ainsi sa décision de ne pas utiliser des produits ou services certifiés ou qualifiés par l'Autorité nationale (ANSSI).

13. Les plans de tests et d'audits

Des documents doivent identifier formellement les tests et les audits nécessaires et préciser par qui ils doivent être effectués et selon quel planning.

Pour mémoire, des audits doivent être prévus après la décision d'homologation, afin d'assurer le maintien en conditions opérationnelles du système.

14. Les rapports de tests et d'audits et les plans d'action associés

Pour les systèmes déjà en production, il est recommandé de procéder d'emblée à un audit technique sur le SI à homologuer, le cas échéant avant l'analyse des risques.

Pour les systèmes en cours de conception, l'audit pourra être réalisé à l'occasion de la procédure de recette applicative.

Pour les systèmes existants requérant un besoin particulier de sécurité, il est recommandé de procéder, en première action, à un audit technique et organisationnel afin d'optimiser la procédure d'homologation.

L'audit doit mener à la l'établissement d'une liste des vulnérabilités détectées et du plan d'action afférent.

Les audits doivent être réalisés par des équipes préalablement validées par l'autorité d'homologation.

Ils doivent porter sur les mesures de sécurité liées à l'exploitation du système et les comparer à l'état de l'art.

Les audits doivent être menés dans les formes prévues par le référentiel d'exigences relatif aux prestataires d'audit de la sécurité des systèmes d'information.

15. Le dossier des risques résiduels

Ce dossier comporte une analyse de la couverture des risques et de l'atteinte des objectifs de sécurité au travers :

- Des procédures d'exploitation sécurisée du système ;
- De la PSSI.

Il présente également les vulnérabilités résiduelles constatées lors des tests et des audits et non corrigées ainsi que les plans d'action associés.

16. Les éventuelles décisions d'homologation antérieures

Le dossier doit comporter tous les documents relatifs aux éventuelles homologations précédentes.

17. Le tableau de bord des incidents et de leur résolution

Ce tableau recueille l'ensemble des incidents survenus sur le SI avec l'identification de leur(s) cause(s), les conséquences et les modalités de résolution de l'incident. Il précise également le plan d'action associé.

18. Le journal des évolutions

Ce journal consigne les évolutions du système, notamment celles ayant une incidence sur les critères et conditions de l'homologation.

Il comprend, en particulier, la liste des mesures de sécurité apportées en prévention de risques ou en correction d'anomalies ou de vulnérabilités constatées dans les audits.

Annexe 4 au guide d'homologation : Liste de menaces, issue de la base de connaissance EBIOS

1. Menaces sur les matériels

Usage d'un équipement ou d'un matériel :

- Utilisation abusive d'un ordinateur à des fins personnelles, voire pour un usage inapproprié ou illicite ;
- Stockage de fichiers personnels sur l'ordinateur de bureau (ex. vidéos non professionnelles) ;
- Usage d'une imprimante à des fins personnelles ou au détriment d'autrui ;
- Stockage d'informations sensibles sur des supports inappropriés (disque dur non protégé, clé USB, CDROM laissé sur un bureau…) ;
- Perte ou vol d'un ordinateur (surtout portable), ou d'un support de données électronique (clé USB, CDROM, disque dur amovible) notamment lors d'un déplacement ou d'un déménagement.

Observation d'un équipement :

- Observation d'un écran à travers une fenêtre ;
- Observation de la saisie d'un code au clavier ;
- Écoute d'une conversation diffusée sur les haut-parleurs de l'ordinateur ;
- Géolocalisation d'un matériel (à partir de son adresse IP ou par le réseau téléphonique) ;
- Interception de signaux compromettants émis par l'affichage à l'écran ou les touches du clavier ;
- Pose d'un dispositif-espion matériel (keylogger) sur la face arrière d'un poste de travail.

Fonctionnement du matériel :

- surcharge d'un disque dur ou d'un serveur aboutissant à une panne ;
- perturbations électriques ou électromagnétiques ;
- panne électrique involontaire (remplacement d'un poste par un ordinateur plus consommateur en énergie, rupture de câbles électriques suite à des travaux de terrassement, court-circuit dû à la foudre, erreur de branchement ou incident électrique…) ;
- vieillissement du matériel susceptible d'entraîner un crash du disque dur ;
- multiples déplacements du matériel (ordinateur portable) ;
- ordinateur travaillant dans un milieu pollué, humide, ou corrosif (atelier industriel…), ou en présence d'ondes électromagnétiques ou de vibrations ;
- chute du matériel pendant une installation ou un déménagement (voir vandalisme) ;
- effacement des données par passage d'un aimant sur un disque dur ;
- présence d'un code malveillant destiné à empêcher le fonctionnement de tout ou partie du matériel.

2. Menaces sur les logiciels

Menaces sur l'usage de logiciels

- un logiciel est piégé (keylogger), ou corrompu par un code malveillant ;
- un logiciel accède ou copie de manière inappropriée voire illicite des données métiers, des données de configuration d'équipements, ou collecte des données métiers partagées dans un réseau ;
- un logiciel supprime de manière inappropriée des données, journaux d'événements, enregistrements de conversations, etc. qu'ils soient en mémoire, sur un disque dur ou sur un support ;

- un logiciel crée ou modifie des données de manière inappropriée : messages injurieux sur un forum, configuration d'un système, insertion d'une page web ou défiguration sur un site Internet, élévation de privilèges d'un compte utilisateur, effacement de traces d'opérations dans un journal d'événements, fraude ;
- un logiciel collecte des données de configuration d'un réseau, balaie les adresses internes réseau ou recense les ports ouverts ;
- un logiciel exploite des données de base pour en extraire des informations confidentielles (recoupement, infocentre) ;
- un logiciel utilise des mécanismes de stéganographie pour transmettre des données discrètement ;
- un agent utilise un logiciel professionnel pour des besoins personnels ;
- un agent connecte son ordinateur portable personnel compromis par un attaquant au réseau ;
- un agent transfère systématiquement tous les messages qu'il reçoit sur un compte de messagerie personnel dont le mot de passe a été cassé par un groupe d'attaquant notoire ;
- une machine du réseau est compromise pour réaliser un envoi massif d'informations par courrier électronique (spam) ;
- un utilisateur utilise, volontairement une copie d'un logiciel dont le fonctionnement n'est pas garanti (par exemple une contrefaçon) ;
- un logiciel est utilisé sans achat de la licence correspondante, ou la licence n'est pas renouvelée ;
- un logiciel est analysé par l'attaquant en vue d'être corrompu : observation de son fonctionnement, observation de l'emploi de son espace mémoire, ingénierie inverse, etc. ;
- tout ou partie du logiciel est détruit par un virus (bombe logique…) ;
- le logiciel est modifié de manière involontaire : mise à jour avec une mauvaise version, modification de la configuration en maintenance, activation ou désactivation de fonctions, changement de paramétrage du réseau, modification des règles de routage ou de résolution des noms de domaine.

3. Menaces sur les réseaux

- un attaquant écoute les informations circulant sur le réseau informatique ou téléphonique, et réémet un message confidentiel vers l'adresse d'un forum public ;
- un attaquant sature le réseau par un envoi massif de messages ;
- un point d'accès sans fil mal configuré permet l'écoute de l'ensemble des données qui transitent par Wifi ;
- un attaquant sectionne les câbles d'une ligne téléphonique (tord la fibre optique) empêchant physiquement la transmission des messages ;
- une équipe de maintenance remplace un câble existant par un autre de moins grande capacité, etc. ;
- des voleurs dérobent les câbles de transmission en cuivre pour les revendre à la ferraille.

4. Menaces sur les personnels

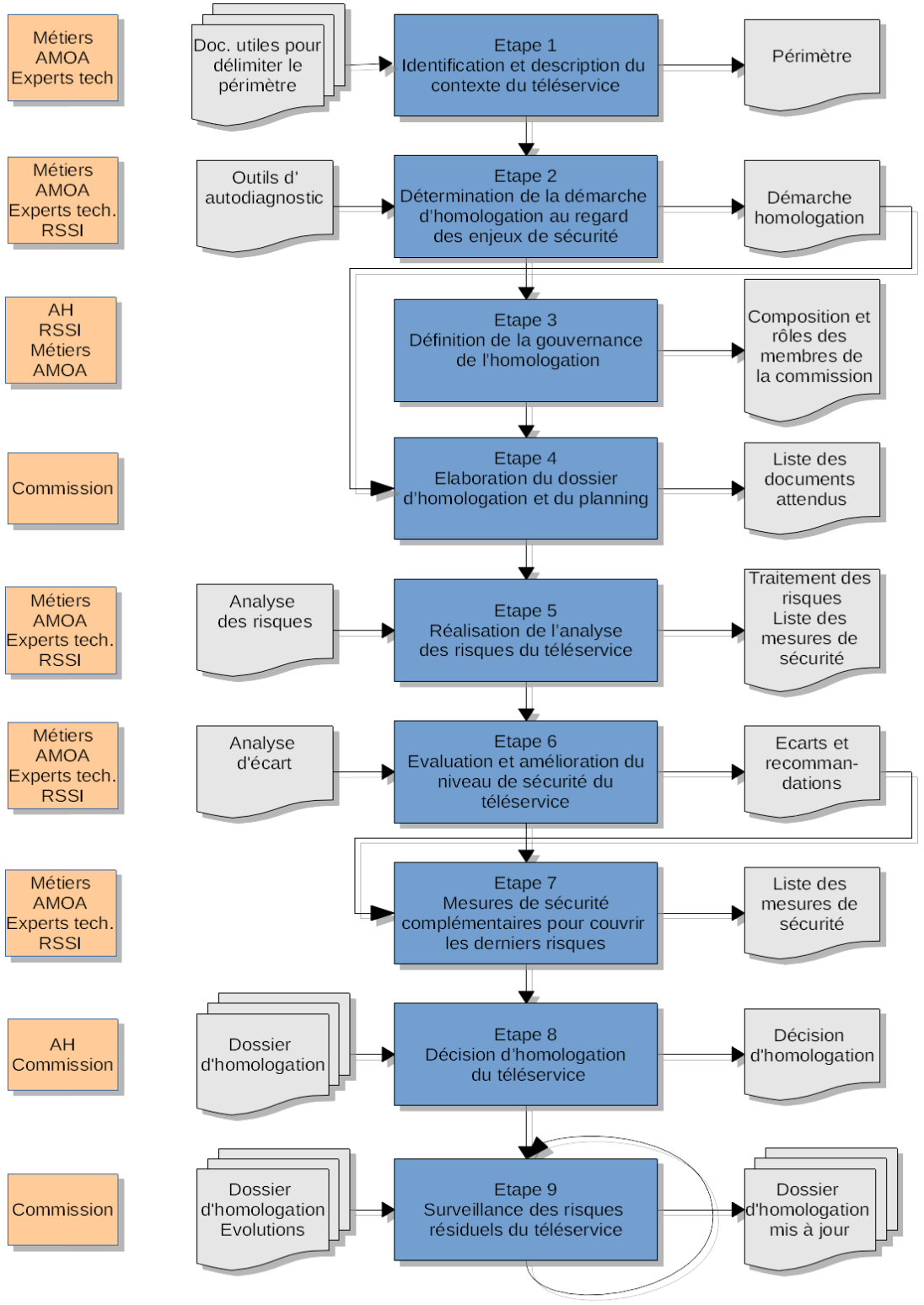
- l'unique administrateur d'une application critique est victime d'une épidémie de grippe
- une grève des transports paralyse l'accès au site hébergeant les postes de travail ;
- une contamination dans le restaurant d'entreprise crée une intoxication alimentaire chez de nombreux agents ;
- l'un des agents se déplaçant régulièrement bavarde avec des inconnus rencontrés dans des aéroports des anomalies de fonctionnement du système ;
- un agent, perturbé par une surcharge de tâches, commet des erreurs de manipulation du système ;
- l'ergonomie du poste de travail (mauvais éclairage, siège inconfortable, etc.) nuit au bon usage du logiciel ;

- un agent passe une part significative de son temps de travail sur les sites de jeux en ligne, ce qui nuit à l'efficacité du système ;
- l'agent expert dans l'usage d'une fonction critique du système demande sa mutation pour se rapprocher de son conjoint ;
- une réorganisation ou un déménagement rompent les échanges entre personnes qui s'étaient établies pour pallier les faiblesses fonctionnelles du système.

5. Menaces sur les locaux

- il existe un risque qu'un incendie se déclenche dans les locaux sans être détecté ;
- le bâtiment hébergeant le système se situe dans une zone industrielle comportant des entreprises soumises à autorisation délivrée localement susceptibles de générer un accident industriel (explosion) ;
- emploi de mauvais matériaux, construction défectueuse, mouvements de terrain sapant les fondations, infiltration d'eau dans le sol, etc.

Annexe 5 au guide d'homologation : Processus d'homologation



ANNEXE 2

Formulaire de motivation de non-recours à des produits de sécurité ou des prestataires de services de confiance qualifiés

Formulaire de motivation de non-recours à des produits de sécurité ou des prestataires de services de confiance qualifiés

Arrêté d'application de la loi du Pays n° 2017-30 du 2 novembre 2017 relatif à la dématérialisation des actes des autorités administratives et aux téléservices.

Service de l'autorité administrative :

Description du système d'information relatif aux échanges électroniques ou au téléservice :

Conclusions de l'analyse des risques menée conformément à l'arrêté en conseil des ministres relatif à la dématérialisation des actes des autorités administratives et aux téléservices et au référentiel général de sécurité :

Motivation de non-recours à un produit de sécurité qualifié ou à un prestataire de services de confiance qualifié :

(à titre d'exemple : pas de revendeur/mainteneur du produit de sécurité qualifié sur le territoire de la Polynésie française, complexité du produit, pas de représentant du prestataire de services de confiance qualifié sur le territoire de la Polynésie française, cout d'acquisition, de support et de maintenance en dehors du budget du projet, etc.)

Présentation du produit de sécurité ou du prestataire de service de confiance non qualifié retenu:

- En quoi répond-il aux motivations énoncées ci-dessus ? :

- Objectifs ou exigences de sécurité couverts :

- Fonctions ou services de sécurité proposés:

Le présent formulaire est versé au dossier d'homologation, conformément à l'article 8 de l'arrêté relatif à la dématérialisation des actes des autorités administratives et aux téléservices

Signature du chef du service de l'autorité administrative :

ANNEXE 3

Liste de référence des prestataires de services de confiance qualifiés et des produits de sécurité

I. Liste de référence des prestataires de services de confiance qualifiés

TSP NAME		Address	AC Name	Regulation	RGS Level*	Standard	Level	OID	Service
ADACOM	EL	Siège : Post: 25, Kreontos Str., 10442 ATHENS - GREECE							
ADACOM	EL	Siège : Post: 25, Kreontos Str., 10442 ATHENS - GREECE	ADACOM CA for EU Qualified e-Signatures	UE 910/2014 eIDAS		EN 319 411-2	QCP-n-qscd	2.16.840.1.113733.1.7.23.2	signature
ADACOM	EL	Siège : Post: 25, Kreontos Str., 10442 ATHENS - GREECE	ADACOM CA for EU Qualified e-Seals	UE 910/2014 eIDAS		EN 319 411-2	QCP-l	2.16.840.1.113733.1.7.23.2	Seal
AGENCE NATIONALE DE LA CERTIFICATION ELECTRONIQUE	TN	Siège: Parc Technologie El Ghazala Route de Raoued Km, 3,5 2083 Ariana Tunisie							
AGENCE NATIONALE DE LA CERTIFICATION ELECTRONIQUE	TN	Siège: Parc Technologie El Ghazala Route de Raoued Km, 3,5 2083 Ariana Tunisie	Tunisian Root Certificate Authority - TunRootCA2			ETSI TS 102 042		21 66 15 05 05 27 05 05 bc 8a b0 1d af 0a be c4	Root CA
AGENCE NATIONALE DE LA CERTIFICATION ELECTRONIQUE	TN	Siège: Parc Technologie El Ghazala Route de Raoued Km, 3,5 2083 Ariana Tunisie	Tunisian Server Certificate Authority - TunServerCA2			ETSI TS 102 042		2.16.788.1.2.6.1.8	Subordinate ca
AGENCE NATIONALE DE LA CERTIFICATION ELECTRONIQUE	TN	Siège: Parc Technologie El Ghazala Route de Raoued Km, 3,5 2083 Ariana Tunisie	Tunisian Server Certificate Authority - TunServerCA2			ETSI TS 102 042	OVCP	2.16.788.1.2.6.1.8	Authentication
AGENCE NATIONALE DES TITRES SÉCURISÉS	FR	Siège : 33 avenue du Maine Tour Maine Montparnasse 75015 PARIS							
AGENCE NATIONALE DES TITRES SÉCURISÉS	FR	Siège : 33 avenue du Maine Tour Maine Montparnasse 75015 PARIS	Autorité de certification services applicatifs	RGS V2.0	*	ETSI TS 102 042	OVCP	1.2.250.1.200.3.3.7.1.1	Authentification serveur-serveur (A_3)
AGENCE NATIONALE DES TITRES SÉCURISÉS	FR	Siège : 33 avenue du Maine Tour Maine Montparnasse 75015 PARIS	Autorité de certification services applicatifs	RGS V2.0	*	ETSI TS 102 042	LCP	1.2.250.1.200.3.3.8.1.1	Authentification serveur-client(A_3)
AGENCE NATIONALE DES TITRES SÉCURISÉS	FR	Siège : 33 avenue du Maine Tour Maine Montparnasse 75015 PARIS	Autorité de certification services applicatifs	RGS V2.0	*	ETSI TS 102 042	LCP	1.2.250.1.200.3.3.9.1.1	Cachet serveur (A_3)

AGENCE NATIONALE DES TITRES SÉCURISÉS	FR	Siège : 33 avenue du Maine Tour Maine Montparnasse 75015 PARIS	Autorité de certification services applicatifs	RGS V2.0	*	ETSI TS 102 042	LCP	1.2.250.1.200.3.3.10.1.1	Cachet serveur (A_3)
AGENCE NATIONALE DES TITRES SÉCURISÉS	FR	Siège : 33 avenue du Maine Tour Maine Montparnasse 75015 PARIS	Autorité de certification services applicatifs	RGS V2.0	*	ETSI TS 102 042	LCP	1.2.250.1.200.3.3.11.1.1	Signature de code (A_3)
AGENCE NATIONALE DES TITRES SÉCURISÉS	FR	Siège : 33 avenue du Maine Tour Maine Montparnasse 75015 PARIS	Autorité de certification services applicatifs	RGS V2.0	*	ETSI TS 102 042	LCP	1.2.250.1.200.3.3.12.1.1	Cachet horodatage (A3)
AGENCE NATIONALE DES TITRES SÉCURISÉS	FR	Siège : 33 avenue du Maine Tour Maine Montparnasse 75015 PARIS	Autorité de certification services applicatifs	RGS V2.0	*	ETSI TS 102 042	LCP	1.2.250.1.200.3.3.13.1.1	Confidentialité (A_3)
AGENCE NATIONALE DES TITRES SÉCURISÉS	FR	Siège : 33 avenue du Maine Tour Maine Montparnasse 75015 PARIS	Autorité de Certification Personnes AAE	RGS V2.0	***	ETSI TS 101 456	NCP+	1.2.250.1.200.3.1.1.3.1	Authentification
AGENCE NATIONALE DES TITRES SÉCURISÉS	FR	Siège : 33 avenue du Maine Tour Maine Montparnasse 75015 PARIS	Autorité de Certification Personnes AAE	UE 910/2014 eIDAS	***	ETSI TS 102 042	QCP Public+SSCD	1.2.250.1.200.3.1.2.3.1	Signature
AGENCE NATIONALE DES TITRES SÉCURISÉS	FR	Siège : 33 avenue du Maine Tour Maine Montparnasse 75015 PARIS	Autorité de Certification Personnes AAE	RGS V2.0	***	ETSI TS 101 456	NCP+	1.2.250.1.200.3.1.4.3.1	Authentification
AGENCE NATIONALE DES TITRES SÉCURISÉS	FR	Siège : 33 avenue du Maine Tour Maine Montparnasse 75015 PARIS	Autorité de Certification Personnes AAE	UE 910/2014 eIDAS	***	ETSI TS 102 042	QCP Public+SSCD	1.2.250.1.200.3.1.5.3.1	Signature
AGENCE NATIONALE DES TITRES SÉCURISÉS	FR	Siège : 33 avenue du Maine Tour Maine Montparnasse 75015 PARIS	Acteurs des Collectivités Territoriales	RGS V2.0	***	ETSI TS 102 042	NCP+	1.2.250.1.200.2.4.1.2	Authentification
AGENCE NATIONALE DES TITRES SÉCURISÉS	FR	Siège : 33 avenue du Maine Tour Maine Montparnasse 75015 PARIS	Acteurs des Collectivités Territoriales	UE 910/2014 eIDAS	***	ETSI TS 101 456	QCP Public+SSCD	1.2.250.1.200.2.5.1.2	Signature
AGENCE NATIONALE DES TITRES SÉCURISÉS	FR	Siège : 33 avenue du Maine Tour Maine Montparnasse 75015 PARIS	Acteurs de l'Administration de l'Etat	RGS V2.0	***	ETSI TS 102 042	NCP+	1.2.250.1.200.2.2.1.2	Authentification
AGENCE NATIONALE DES TITRES SÉCURISÉS	FR	Siège : 33 avenue du Maine Tour Maine Montparnasse 75015 PARIS	Acteurs de l'Administration de l'Etat	UE 910/2014 eIDAS	***	ETSI TS 101 456	QCP Public+SSCD	1.2.250.1.200.2.3.1.2	Signature

ALEAT	AL	Siège : Aleat Sh.p.k Rruga:Xhanfize KEKO TIRANA- ALBANIA							
ALEAT	AL	Siège : Aleat Sh.p.k Rruga:Xhanfize KEKO TIRANA- ALBANIA	CITIZEN Auth CA certification					1.3.6.1.4.1.42090.1 0.2.1	Root
ALEAT	AL	Siège : Aleat Sh.p.k Rruga:Xhanfize KEKO TIRANA- ALBANIA	CITIZEN Auth CA certification	UE 910/2014 eIDAS		EN 319 411-1	LCP	1.3.6.1.4.1.42090.1 0.2.2	Authentication
ALEAT	AL	Siège : Aleat Sh.p.k Rruga:Xhanfize KEKO TIRANA- ALBANIA	CITIZEN Sign CA certification	UE 910/2014 eIDAS		EN 319 411-2	QCP-n- QSCD	1.3.6.1.4.1.42090.1 0.2.3	Signature
ARIADNEXT	FR	HQ: Avenue des champs blancs 35510 Cesson-Sévigné							
ARIADNEXT	FR	HQ: Avenue des champs blancs 35510 Cesson-Sévigné	FR04	RGS V2.0	*	ETSI TS 102 042	LCP	1.3.6.1.4.1.38226.1 0.4.2.1.1.1	Cachet serveur
ARIADNEXT	FR	HQ: Avenue des champs blancs 35510 Cesson-Sévigné	Legal Person CA G2	UE 910/2014 eIDAS	*	EN 319 411-1	LCP	1.3.6.1.4.1.38226.1 0.4.3.3.1.1	Cachet serveur
ARIADNEXT	FR	HQ: Avenue des champs blancs 35510 Cesson-Sévigné	Legal Person CA G2	UE 910/2014 eIDAS	*	EN 319 411-1	LCP	1.3.6.1.4.1.38226.1 0.4.3.4.1.1	Cachet horodatage
ARIADNEXT	FR	HQ: Avenue des champs blancs 35510 Cesson-Sévigné	One Time CA G2	UE 910/2014 eIDAS	*	EN 319 411-1	LCP	1.3.6.1.4.1.38226.1 0.4.5.2.1.1	Signature
Assemblée Permanente des Chambres de Métiers et d'Artisanat	FR								
Assemblée Permanente des Chambres de Métiers et d'Artisanat	FR		CERTMETIERSARTISAN ATV 2	RGS V2.0	**	ETSI 102 042	LCP	1.2.250.1.191.2.1.1. 0	Authentification & signature
BALTSTAMP	LT	Siège : Dariaus ir Girėno Str.40 LT-02189 Vilnius - LITHUANIA							
BALTSTAMP	LT	Siège : Dariaus ir Girėno Str.40 LT-02189 Vilnius - LITHUANIA	Baltstamp TSA	UE 910/2014 eIDAS		EN 319 421		1.3.6.1.4.1.38424.1. 4.2	Time-stamping
BNP PARIBAS	FR	HQ: 6 boulevard des Italiens 75009 PARIS							

BNP PARIBAS	FR	HQ: 6 boulevard des Italiens 75009 PARIS	BNP Paribas Group Customer Ephemeral Certification Authority 1			ETSI TS 102 042	LCP	1.2.250.1.62.10.3.1.1.1	Signature
BNP PARIBAS	FR	HQ: 6 boulevard des Italiens 75009 PARIS	BNP Paribas Group Customer Ephemeral Certification Authority 2			ETSI TS 102 042	LCP	1.2.250.1.62.10.4.1.1.1	Signature
BNP PARIBAS	FR	HQ: 6 boulevard des Italiens 75009 PARIS	BNP Paribas Group Sealing and Timestamping			ETSI TS 102 042	NCP	1.2.250.1.62.10.5.1.1.1	Cachet Serveur
BNP PARIBAS	FR	HQ: 6 boulevard des Italiens 75009 PARIS	BNP Paribas Group Sealing and Timestamping			ETSI TS 102 042	NCP	1.2.250.1.62.10.5.1.2.1	Cachet Serveur
BNP PARIBAS FORTIS	BE	Siège : Montagne du Parc 3, 1000 Brussels							
BNP PARIBAS FORTIS	BE	Siège : Montagne du Parc 3, 1000 Brussels	BNP Paribas FORTIS Customer Ephemeral Certification Authority 1			ETSI TS 102 042	LCP	1.2.250.1.62.10.7.1.1.1	Signature
BNP PARIBAS FORTIS	BE	Siège : Montagne du Parc 3, 1000 Brussels	BNP Paribas FORTIS Customer Ephemeral Certification Authority 2			ETSI TS 102 042	LCP	1.2.250.1.62.10.8.1.1.1	Signature
BORICA AD	BG	Headquarter : #41 Tsar boris III Blvd. Sofia							
BORICA AD	BG	Headquarter : #41 Tsar boris III Blvd. Sofia	B-Trust Root qualified CA						Root
BORICA AD	BG	Headquarter : #41 Tsar boris III Blvd. Sofia	B-Trust Personal Certificate QES with QSignCD	UE 910/2014 eIDAS		EN 319 411-2	QCP-n-qscd	1.3.6.1.4.1.15862.1.6.1.1	Signature
BORICA AD	BG	Headquarter : #41 Tsar boris III Blvd. Sofia	B-Trust Professional Certificate QES with QSignCD	UE 910/2014 eIDAS		EN 319 411-2	QCP-n-qscd	1.3.6.1.4.1.15862.1.6.1.2	Signature
BORICA AD	BG	Headquarter : #41 Tsar boris III Blvd. Sofia	B-Trust TST	UE 910/2014 eIDAS		EN 319 421		0.4.0.2023.1.1	Time-stamp
CAISSE DES DÉPÔTS ET CONSIGNATIONS	FR	Siège : 56, rue de Lille 75356 PARIS@ 07 SP							
CAISSE DES DÉPÔTS ET CONSIGNATIONS	FR	Siège : 56, rue de Lille 75356 PARIS@ 07 SP	CDC-Legalia	RGS V2.0	**	ETSI TS 102 042	NCP+	1.2.250.1.5.1.1.1.2.2	Authentification (RGS_A_7)
CAISSE DES DÉPÔTS ET CONSIGNATIONS	FR	Siège : 56, rue de Lille 75356 PARIS@ 07 SP	CDC-Legalia	RGS V2.0	**	ETSI TS 102 042	NCP+	1.2.250.1.5.1.1.1.3.2	Signature (RGS_A_8)

CAISSE DES DÉPÔTS ET CONSIGNATIONS	FR	Siège : 56, rue de Lille 75356 PARIS@ 07 SP	CDC-Legalia	UE 910/2014 eIDAS		EN 319 411-1	NCP+	1.2.250.1.5.1.1.1.2.3	Authentification
CAISSE DES DÉPÔTS ET CONSIGNATIONS	FR	Siège : 56, rue de Lille 75356 PARIS@ 07 SP	CDC-Legalia	UE 910/2014 eIDAS		EN 319 411-2	QCP-n-qscd	1.2.250.1.5.1.1.1.3.3	Signature
CERTEUROPE	FR	Siège : 26, rue du Faubourg Poissonnière 75010 PARIS							
CERTEUROPE	FR	Siège : 26, rue du Faubourg Poissonnière 75010 PARIS	CERTEUROPE ADVANCED CA V4	UE 910/2014 eIDAS	*	EN 319 411-1	LCP	1.2.250.1.105.12.1.1.0	Cachet
CERTEUROPE	FR	Siège : 26, rue du Faubourg Poissonnière 75010 PARIS	CERTEUROPE ADVANCED CA V4	UE 910/2014 eIDAS	*	EN 319 411-1	OVCP	1.2.250.1.105.18.1.1.0	Authentification serveur
CERTEUROPE	FR	Siège : 26, rue du Faubourg Poissonnière 75010 PARIS	CERTEUROPE ADVANCED CA V4	UE 910/2014 eIDAS	**	EN 319 411-1	NCP	1.2.250.1.105.12.3.1.0	Cachet
CERTEUROPE	FR	Siège : 26, rue du Faubourg Poissonnière 75010 PARIS	CERTEUROPE ADVANCED CA V4	UE 910/2014 eIDAS	*	EN 319 411-1	OVCP	1.2.250.1.105.18.4.1.0	Authentification serveur client
CERTEUROPE	FR	Siège : 26, rue du Faubourg Poissonnière 75010 PARIS	CERTEUROPE ADVANCED CA V4	UE 910/2014 eIDAS	**	EN 319 411-1	OVCP	1.2.250.1.105.18.3.1.0	Authentification serveur
CERTEUROPE	FR	Siège : 26, rue du Faubourg Poissonnière 75010 PARIS	CERTEUROPE ADVANCED CA V4	UE 910/2014 eIDAS	**	EN 319 411-1	NCP+	1.2.250.1.105.10.3.1.3	Authentification
CERTEUROPE	FR	Siège : 26, rue du Faubourg Poissonnière 75010 PARIS	CERTEUROPE ADVANCED CA V4	UE 910/2014 eIDAS	*	EN 319 411-1	LCP	1.2.250.1.105.21.3.1.0	Authentification
CERTEUROPE	FR	Siège : 26, rue du Faubourg Poissonnière 75010 PARIS	CERTEUROPE ADVANCED CA V4	UE 910/2014 eIDAS	*	EN 319 411-1	LCP	1.2.250.1.105.21.4.1.0	Signature
CERTEUROPE	FR	Siège : 26, rue du Faubourg Poissonnière 75010 PARIS	CERTEUROPE ADVANCED CA V4	UE 910/2014 eIDAS	*	EN 319 411-1	LCP	1.2.250.1.105.21.1.1.0	*Authentification* et signature
CERTEUROPE	FR	Siège : 26, rue du Faubourg Poissonnière 75010 PARIS	CERTEUROPE ADVANCED CA V4	UE 910/2014 eIDAS	**	EN 319 411-1	NCP+	1.2.250.1.105.10.1.1.3	*Authentification* et signature
CERTEUROPE	FR	Siège : 26, rue du Faubourg Poissonnière 75010 PARIS	CERTEUROPE ADVANCED CA V4	UE 910/2014 eIDAS	**	Art 51 2 (ETSI EN 319 411-2)	QCP Public+SSCD	1.2.250.1.105.10.4.1.3	Signature (RGS_A_8)
CERTEUROPE	FR	Siège : 26, rue du Faubourg Poissonnière 75010 PARIS	CertEurope eID Root					1.2.250.1.105.22.1.1.0	Root
CERTEUROPE	FR	Siège : 26, rue du Faubourg Poissonnière 75010 PARIS	CertEurope eID User						Intermédiaire

CERTEUROPE	FR	Siège : 26, rue du Faubourg Poissonnière 75010 PARIS	CertEurope eID User	UE 910/2014 eIDAS	*	EN 319 411-2	QCP-n	1.2.250.1.105.23.41 1.2.1.1.1.0	Signature
CERTEUROPE	FR	Siège : 26, rue du Faubourg Poissonnière 75010 PARIS	CertEurope eID User	UE 910/2014 eIDAS	*	EN 319 411-2	QCP-n	1.2.250.1.105.23.41 1.2.1.2.1.0	*Authentification et* Signature
CERTEUROPE	FR	Siège : 26, rue du Faubourg Poissonnière 75010 PARIS	CertEurope eID User	UE 910/2014 eIDAS	**	EN 319 411-2	QCP-n-qscd	1.2.250.1.105.23.41 1.2.2.1.1.0	Signature
CERTEUROPE	FR	Siège : 26, rue du Faubourg Poissonnière 75010 PARIS	CertEurope eID User	UE 910/2014 eIDAS	**	EN 319 411-2	QCP-n-qscd	1.2.250.1.105.23.41 1.2.2.2.1.0	*Authentification et* Signature
CERTEUROPE	FR	Siège : 26, rue du Faubourg Poissonnière 75010 PARIS	CertEurope eID User	UE 910/2014 eIDAS		EN 319 411-1	LCP	1.2.250.1.105.23.41 1.1.1.1.1.0	Signature
CERTEUROPE	FR	Siège : 26, rue du Faubourg Poissonnière 75010 PARIS	CertEurope eID User	UE 910/2014 eIDAS		EN 319 411-1	LCP	1.2.250.1.105.23.41 1.1.1.2.1.0	Authentification
CERTEUROPE	FR	Siège : 26, rue du Faubourg Poissonnière 75010 PARIS	CertEurope eID User	UE 910/2014 eIDAS		EN 319 411-1	LCP	1.2.250.1.105.23.41 1.1.1.3.1.0	Authentification et Signature
CERTEUROPE	FR	Siège : 26, rue du Faubourg Poissonnière 75010 PARIS	CertEurope eID User	UE 910/2014 eIDAS		EN 319 411-1	NCP	1.2.250.1.105.23.41 1.1.2.1.1.0	Signature
CERTEUROPE	FR	Siège : 26, rue du Faubourg Poissonnière 75010 PARIS	CertEurope eID User	UE 910/2014 eIDAS		EN 319 411-1	NCP	1.2.250.1.105.23.41 1.1.2.2.1.0	Authentification
CERTEUROPE	FR	Siège : 26, rue du Faubourg Poissonnière 75010 PARIS	CertEurope eID User	UE 910/2014 eIDAS		EN 319 411-1	NCP	1.2.250.1.105.23.41 1.1.2.3.1.0	Authentification et Signature
CERTEUROPE	FR	Siège : 26, rue du Faubourg Poissonnière 75010 PARIS	CertEurope eID User	UE 910/2014 eIDAS		EN 319 411-1	NCP+	1.2.250.1.105.23.41 1.1.3.1.1.0	Signature
CERTEUROPE	FR	Siège : 26, rue du Faubourg Poissonnière 75010 PARIS	CertEurope eID User	UE 910/2014 eIDAS		EN 319 411-1	NCP+	1.2.250.1.105.23.41 1.1.3.2.1.0	Authentification
CERTEUROPE	FR	Siège : 26, rue du Faubourg Poissonnière 75010 PARIS	CertEurope eID User	UE 910/2014 eIDAS		EN 319 411-1	NCP+	1.2.250.1.105.23.41 1.1.3.3.1.0	Authentification et Signature
CERTEUROPE	FR	Siège : 26, rue du Faubourg Poissonnière 75010 PARIS	CertEurope eID Corp						Intermédiaire
CERTEUROPE	FR	Siège : 26, rue du Faubourg Poissonnière 75010 PARIS	CertEurope eID Corp	UE 910/2014 eIDAS	*	EN 319 411-2	QCP-L	1.2.250.1.105.24.41 1.2.1.1.1.0	Cachet
CERTEUROPE	FR	Siège : 26, rue du Faubourg Poissonnière 75010 PARIS	CertEurope eID Corp	UE 910/2014 eIDAS	**	EN 319 411-2	QCP-L	1.2.250.1.105.24.41 1.2.2.1.1.0	Cachet

CERTEUROPE	FR	Siège : 26, rue du Faubourg Poissonnière 75010 PARIS	CertEurope eID Corp	UE 910/2014 eIDAS		EN 319 411-1	LCP	1.2.250.1.105.24.41 1.1.1.1.1.0	Cachet
CERTEUROPE	FR	Siège : 26, rue du Faubourg Poissonnière 75010 PARIS	CertEurope eID Corp	UE 910/2014 eIDAS		EN 319 411-1	NCP	1.2.250.1.105.24.41 1.1.2.1.1.0	Cachet
CERTEUROPE	FR	Siège : 26, rue du Faubourg Poissonnière 75010 PARIS	CertEurope eID Corp	UE 910/2014 eIDAS		EN 319 411-1	NCP+	1.2.250.1.105.24.41 1.1.3.1.1.0	Cachet
CERTEUROPE	FR	Siège : 26, rue du Faubourg Poissonnière 75010 PARIS	CertEurope eID Website						Intermediate
CERTEUROPE	FR	Siège : 26, rue du Faubourg Poissonnière 75010 PARIS	CertEurope eID Website	UE 910/2014 eIDAS	*	EN 319 411-2	QCP-w	1.2.250.1.105.25.41 1.2.1.1.1.0	Authentification client (Signature)
CERTEUROPE	FR	Siège : 26, rue du Faubourg Poissonnière 75010 PARIS	CertEurope eID Website	UE 910/2014 eIDAS	*	EN 319 411-2	QCP-w	1.2.250.1.105.25.41 1.2.1.2.1.0	Authentification serveur
CERTEUROPE	FR	Siège : 26, rue du Faubourg Poissonnière 75010 PARIS	CertEurope eID Website	UE 910/2014 eIDAS	**	EN 319 411-2	QCP-w	1.2.250.1.105.25.41 1.2.2.1.1.0	Authentification client (Signature)
CERTEUROPE	FR	Siège : 26, rue du Faubourg Poissonnière 75010 PARIS	CertEurope eID Website	UE 910/2014 eIDAS	**	EN 319 411-2	QCP-w	1.2.250.1.105.25.41 1.2.2.2.1.0	Authentification serveur
CERTEUROPE	FR	Siège : 26, rue du Faubourg Poissonnière 75010 PARIS	CertEurope eID Website	UE 910/2014 eIDAS		EN 319 411-1	DVCP	1.2.250.1.105.25.41 1.1.1.1.1.0	Authentification client (Signature)
CERTEUROPE	FR	Siège : 26, rue du Faubourg Poissonnière 75010 PARIS	CertEurope eID Website	UE 910/2014 eIDAS		EN 319 411-1	DVCP	1.2.250.1.105.25.41 1.1.1.2.1.0	Authentification serveur
CERTEUROPE	FR	Siège : 26, rue du Faubourg Poissonnière 75010 PARIS	CertEurope eID Website	UE 910/2014 eIDAS		EN 319 411-1	OVCP	1.2.250.1.105.25.41 1.1.2.1.1.0	Authentification client (Signature)
CERTEUROPE	FR	Siège : 26, rue du Faubourg Poissonnière 75010 PARIS	CertEurope eID Website	UE 910/2014 eIDAS		EN 319 411-1	OVCP	1.2.250.1.105.25.41 1.1.2.2.1.0	Authentification serveur
CERTEUROPE	FR	Siège : 26, rue du Faubourg Poissonnière 75010 PARIS	CertEurope eID Website	UE 910/2014 eIDAS		EN 319 411-1	EVCP	1.2.250.1.105.25.41 1.1.3.1.1.0	Authentification client (Signature)
CERTEUROPE	FR	Siège : 26, rue du Faubourg Poissonnière 75010 PARIS	CertEurope eID Website	UE 910/2014 eIDAS		EN 319 411-1	EVCP	1.2.250.1.105.25.41 1.1.3.2.1.0	Authentification serveur
CERTINOMIS	FR	Siège : 10-12, avenue Charles De Gaulle 94673 CHARENTON LE PONT							

CERTINOMIS	FR	Siège : 10-12, avenue Charles De Gaulle 94673 CHARENTON LE PONT	Certinomis AA et Agents	UE 910/2014 eIDAS	*	EN 319 411-1	LCP	1.2.250.1.86.2.3.7.1.1	Authentification
CERTINOMIS	FR	Siège : 10-12, avenue Charles De Gaulle 94673 CHARENTON LE PONT	Certinomis AA et Agents	UE 910/2014 eIDAS	*	EN 319 411-1	LCP	1.2.250.1.86.2.3.7.2.1	Signature
CERTINOMIS	FR	Siège : 10-12, avenue Charles De Gaulle 94673 CHARENTON LE PONT	Certinomis AA et Agents	UE 910/2014 eIDAS	*	EN 319 411-1	OVCP	1.2.250.1.86.2.3.7.20.1	Authentification serveur
CERTINOMIS	FR	Siège : 10-12, avenue Charles De Gaulle 94673 CHARENTON LE PONT	Certinomis AA et Agents	UE 910/2014 eIDAS	*	EN 319 411-1	LCP	1.2.250.1.86.2.3.7.22.1	Cachet
CERTINOMIS	FR	Siège : 10-12, avenue Charles De Gaulle 94673 CHARENTON LE PONT	Certinomis AA et Agents	UE 910/2014 eIDAS	*	EN 319 411-1	OVCP	1.2.250.1.86.2.3.7.23.1	Authentification serveur client
CERTINOMIS	FR	Siège : 10-12, avenue Charles De Gaulle 94673 CHARENTON LE PONT	Certinomis AA et Agents	UE 910/2014 eIDAS	*	EN 319 411-1	LCP	1.2.250.1.86.2.3.7.3.1	Confidentialité
CERTINOMIS	FR	Siège : 10-12, avenue Charles De Gaulle 94673 CHARENTON LE PONT	Certinomis AA et Agents	UE 910/2014 eIDAS	**	EN 319 411-1	NCP+	1.2.250.1.86.2.3.8.1.1	Authentification
CERTINOMIS	FR	Siège : 10-12, avenue Charles De Gaulle 94673 CHARENTON LE PONT	Certinomis AA et Agents	UE 910/2014 eIDAS	**	EN 319 411-2	QCP-n-qscd	1.2.250.1.86.2.3.8.10.1	*Authentification et* Signature
CERTINOMIS	FR	Siège : 10-12, avenue Charles De Gaulle 94673 CHARENTON LE PONT	Certinomis AA et Agents	UE 910/2014 eIDAS	**	EN 319 411-2	QCP-n-qscd	1.2.250.1.86.2.3.8.2.1	Signature
CERTINOMIS	FR	Siège : 10-12, avenue Charles De Gaulle 94673 CHARENTON LE PONT	Certinomis AA et Agents	UE 910/2014 eIDAS	**	EN 319 411-2	QCP-w	1.2.250.1.86.2.3.8.20.1	Authentification serveur
CERTINOMIS	FR	Siège : 10-12, avenue Charles De Gaulle 94673 CHARENTON LE PONT	Certinomis AA et Agents	UE 910/2014 eIDAS	**	EN 319 411-2	QCP-l	1.2.250.1.86.2.3.8.22.1	Authentification serveur
CERTINOMIS	FR	Siège : 10-12, avenue Charles De Gaulle 94673 CHARENTON LE PONT	Certinomis AA et Agents	UE 910/2014 eIDAS	**	EN 319 411-1	OVCP	1.2.250.1.86.2.3.8.23.1	Authentification serveur client

CERTINOMIS	FR	Siège : 10-12, avenue Charles De Gaulle 94673 CHARENTON LE PONT	Certinomis AA et Agents	UE 910/2014 eIDAS	*	EN 319 411-1	LCP	1.2.250.1.86.2.3.8.3.1	Confidentialité
CERTINOMIS	FR	Siège : 10-12, avenue Charles De Gaulle 94673 CHARENTON LE PONT	Certinomis Easy CA	UE 910/2014 eIDAS	*	EN 319 411-1	LCP	1.2.250.1.86.2.3.1.1.1	Authentification
CERTINOMIS	FR	Siège : 10-12, avenue Charles De Gaulle 94673 CHARENTON LE PONT	Certinomis Easy CA	UE 910/2014 eIDAS	*	EN 319 411-1	LCP	1.2.250.1.86.2.3.1.2.1	Signature
CERTINOMIS	FR	Siège : 10-12, avenue Charles De Gaulle 94673 CHARENTON LE PONT	Certinomis Easy CA	UE 910/2014 eIDAS	*	EN 319 411-1	LCP	1.2.250.1.86.2.3.1.3.1	Confidentialité
CERTINOMIS	FR	Siège : 10-12, avenue Charles De Gaulle 94673 CHARENTON LE PONT	Certinomis Easy CA	UE 910/2014 eIDAS	*	EN 319 411-1	OVCP	1.2.250.1.86.2.3.1.20.1	Authentification serveur
CERTINOMIS	FR	Siège : 10-12, avenue Charles De Gaulle 94673 CHARENTON LE PONT	Certinomis Easy CA	UE 910/2014 eIDAS	*	EN 319 411-1	LCP	1.2.250.1.86.2.3.1.22.1	Cachet
CERTINOMIS	FR	Siège : 10-12, avenue Charles De Gaulle 94673 CHARENTON LE PONT	Certinomis Easy CA	UE 910/2014 eIDAS	*	EN 319 411-1	OVCP	1.2.250.1.86.2.3.1.23.1	Authentification serveur
CERTINOMIS	FR	Siège : 10-12, avenue Charles De Gaulle 94673 CHARENTON LE PONT	Certinomis Easy CA	UE 910/2014 eIDAS	*	EN 319 411-1	LCP	1.2.250.1.86.2.3.4.1.1	Authentification
CERTINOMIS	FR	Siège : 10-12, avenue Charles De Gaulle 94673 CHARENTON LE PONT	Certinomis Easy CA	UE 910/2014 eIDAS	*	EN 319 411-1	LCP	1.2.250.1.86.2.3.4.2.1	Signature
CERTINOMIS	FR	Siège : 10-12, avenue Charles De Gaulle 94673 CHARENTON LE PONT	Certinomis Easy CA	UE 910/2014 eIDAS	*	EN 319 411-1	LCP	1.2.250.1.86.2.3.4.3.1	Confidentialité
CERTINOMIS	FR	Siège : 10-12, avenue Charles De Gaulle 94673 CHARENTON LE PONT	Certinomis Easy CA	UE 910/2014 eIDAS		EN 319 411-1	DVCP	1.2.250.1.86.2.3.1.60.1	Authentification site web
CERTINOMIS	FR	Siège : 10-12, avenue Charles De Gaulle 94673 CHARENTON LE PONT	Certinomis Easy CA	UE 910/2014 eIDAS	*	EN 319 411-1	LCP	1.2.250.1.86.2.3.1.10.1	Authentification et Signature

CERTINOMIS	FR	Siège : 10-12, avenue Charles De Gaulle 94673 CHARENTON LE PONT	Certinomis Easy CA	UE 910/2014 eIDAS	*	EN 319 411-1	LCP	1.2.250.1.86.2.3.4.10.1	Authentification et Signature
CERTINOMIS	FR	Siège : 10-12, avenue Charles De Gaulle 94673 CHARENTON LE PONT	Certinomis one time CA	UE 910/2014 eIDAS		EN 319 411-1	LCP	1.2.250.1.86.2.5.1.2.1	Signature
CERTINOMIS	FR	Siège : 10-12, avenue Charles De Gaulle 94673 CHARENTON LE PONT	Certinomis one time CA	UE 910/2014 eIDAS		EN 319 411-1	LCP	1.2.250.1.86.2.5.11.2.1	Signature
CERTINOMIS	FR	Siège : 10-12, avenue Charles De Gaulle 94673 CHARENTON LE PONT	Certinomis Prime CA	UE 910/2014 eIDAS	**	EN 319 411-1	NCP+	1.2.250.1.86.2.3.3.1.1	Authentification
CERTINOMIS	FR	Siège : 10-12, avenue Charles De Gaulle 94673 CHARENTON LE PONT	Certinomis Prime CA	UE 910/2014 eIDAS	**	EN 319 411-2	QCP-n-qscd	1.2.250.1.86.2.3.3.2.1	Signature
CERTINOMIS	FR	Siège : 10-12, avenue Charles De Gaulle 94673 CHARENTON LE PONT	Certinomis Prime CA	UE 910/2014 eIDAS	**	EN 319 411-2	QCP-l	1.2.250.1.86.2.3.3.22.1	Cachet
CERTINOMIS	FR	Siège : 10-12, avenue Charles De Gaulle 94673 CHARENTON LE PONT	Certinomis Prime CA	UE 910/2014 eIDAS	**	EN 319 411-1	NCP+	1.2.250.1.86.2.3.6.1.1	Authentification
CERTINOMIS	FR	Siège : 10-12, avenue Charles De Gaulle 94673 CHARENTON LE PONT	Certinomis Prime CA	UE 910/2014 eIDAS	**	EN 319 411-2	QCP-n-qscd	1.2.250.1.86.2.3.6.2.1	Signature
CERTINOMIS	FR	Siège : 10-12, avenue Charles De Gaulle 94673 CHARENTON LE PONT	Certinomis Prime CA	UE 910/2014 eIDAS	**	EN 319 411-2	QCP-w	1.2.250.1.86.2.3.3.20.1	Authentification serveur
CERTINOMIS	FR	Siège : 10-12, avenue Charles De Gaulle 94673 CHARENTON LE PONT	Certinomis Prime CA	UE 910/2014 eIDAS	**	EN 319 411-1	OVCP	1.2.250.1.86.2.3.3.23.1	Authentification serveur
CERTINOMIS	FR	Siège : 10-12, avenue Charles De Gaulle 94673 CHARENTON LE PONT	Certinomis Prime CA	UE 910/2014 eIDAS	*	EN 319 411-2	QCP-l	1.2.250.1.86.2.3.3.24.1	Cachet serveur horodatage
CERTINOMIS	FR	Siège : 10-12, avenue Charles De Gaulle 94673 CHARENTON LE PONT	Certinomis Prime CA	UE 910/2014 eIDAS	**	EN 319 411-2	QCP-n-qscd	1.2.250.1.86.2.3.3.10.1	*Authentification et* Signature

CERTINOMIS	FR	Siège : 10-12, avenue Charles De Gaulle 94673 CHARENTON LE PONT	Certinomis Prime CA	UE 910/2014 eIDAS	**	EN 319 411-2	QCP-n-qscd	1.2.250.1.86.2.3.6.1 0.1	*Authentification et* Signature
CERTINOMIS	FR	Siège : 10-12, avenue Charles De Gaulle 94673 CHARENTON LE PONT	Certinomis Standard CA	UE 910/2014 eIDAS		EN 319 411-1	LCP	1.2.250.1.86.2.3.2.3 0.1	Signature
CERTINOMIS	FR	Siège : 10-12, avenue Charles De Gaulle 94673 CHARENTON LE PONT	Certinomis Standard CA	UE 910/2014 eIDAS		EN 319 411-1	LCP	1.2.250.1.86.2.3.5.3 0.1	Signature
CERTINOMIS	FR	Siège : 10-12, avenue Charles De Gaulle 94673 CHARENTON LE PONT	Certinomis Standard CA	UE 910/2014 eIDAS		EN 319 411-1	LCP	1.2.250.1.86.2.3.2.2 2.1	Authentification serveur
CERTIPOST	BE	Siège : Muntcentrum 1000 BRUSSEL - BELGIUM							
CERTIPOST	BE	Siège : Muntcentrum 1000 BRUSSEL - BELGIUM	Belgium Root CA 4	UE 910/2014 eIDAS					Root
CERTIPOST	BE	Siège : Muntcentrum 1000 BRUSSEL - BELGIUM	CITIZEN CA	UE 910/2014 eIDAS					Sub CA
CERTIPOST	BE	Siège : Muntcentrum 1000 BRUSSEL - BELGIUM	CITIZEN CA	UE 910/2014 eIDAS		EN 319 411-2	QCP-n-qscd	Multiple OID	Signature
CERTIPOST	BE	Siège : Muntcentrum 1000 BRUSSEL - BELGIUM	FOREIGNER CA	UE 910/2014 eIDAS					Sub CA
CERTIPOST	BE	Siège : Muntcentrum 1000 BRUSSEL - BELGIUM	FOREIGNER CA	UE 910/2014 eIDAS		EN 319 411-2	QCP-n-qscd	Multiple OID	Signature
CERTSIGN	RO	Siège : Bulevardul Timisoara 5A Bucharest - Romania							
CERTSIGN	RO	Siège : Bulevardul Timisoara 5A Bucharest - Romania	certSIGN ROOT CA G2						Root
CERTSIGN	RO	Siège : Bulevardul Timisoara 5A Bucharest - Romania	certSIGN Qualified CA				NCP+	2.5.29.32.0	Sub CA
CERTSIGN	RO	Siège : Bulevardul Timisoara 5A Bucharest - Romania	certSIGN Qualified CA	UE 910/2014 eIDAS		EN 319 411-2	QCP-n-QSCD	1.3.6.1.4.1.25017.3. 1.3.1	Signature KS
CERTSIGN	RO	Siège : Bulevardul Timisoara 5A Bucharest - Romania	certSIGN Qualified CA	UE 910/2014 eIDAS		EN 319 411-2	QCP-n-QSCD	1.3.6.1.4.1.25017.3. 1.3.2	Signature KC
CERTSIGN	RO	Siège : Bulevardul Timisoara 5A Bucharest - Romania	certSIGN Qualified CA	UE 910/2014 eIDAS		EN 319 411-2	QCP-l	1.3.6.1.4.1.25017.3. 1.3.3	Seal KS

CERTSIGN	RO	Siège : Bulevardul Timisoara 5A Bucharest - Romania	certSIGN Qualified CA	UE 910/2014 eIDAS		EN 319 411-2	QCP-l	1.3.6.1.4.1.25017.3.1.3.4	Seal KC
CERTSIGN	RO	Siège : Bulevardul Timisoara 5A Bucharest - Romania	certSIGN Qualified CA	UE 910/2014 eIDAS		EN 319 411-2	QCP-l	1.3.6.1.4.1.25017.3.1.3.5	Seal KC Timestamping
CERTSIGN	RO	Siège : Bulevardul Timisoara 5A Bucharest - Romania	certSIGN Qualified CA	UE 910/2014 eIDAS		EN 319 411-1	NCP+	1.3.6.1.4.1.25017.3.1.3.6	OCSP
CERTSIGN	RO	Siège : Bulevardul Timisoara 5A Bucharest - Romania	certSIGN Public CA	UE 910/2014 eIDAS		EN 319 411-1	NCP+	2.5.29.32.0	Sub CA
CERTSIGN	RO	Siège : Bulevardul Timisoara 5A Bucharest - Romania	certSIGN Public CA	UE 910/2014 eIDAS		EN 319 411-1	LCP	1.3.6.1.4.1.25017.3.1.2.1	Signature- Authentication KS
CERTSIGN	RO	Siège : Bulevardul Timisoara 5A Bucharest - Romania	certSIGN Public CA	UE 910/2014 eIDAS		EN 319 411-1	LCP	1.3.6.1.4.1.25017.3.1.2.2	Signature- Authentication TKS
CERTSIGN	RO	Siège : Bulevardul Timisoara 5A Bucharest - Romania	certSIGN Public CA	UE 910/2014 eIDAS		EN 319 411-1	LCP	1.3.6.1.4.1.25017.3.1.2.3	Signature- Authentication TKC
CERTSIGN	RO	Siège : Bulevardul Timisoara 5A Bucharest - Romania	certSIGN Public CA	UE 910/2014 eIDAS		EN 319 411-1	LCP	1.3.6.1.4.1.25017.3.1.2.4	Signature- Authentication KC
CERTSIGN	RO	Siège : Bulevardul Timisoara 5A Bucharest - Romania	certSIGN Public CA	UE 910/2014 eIDAS		EN 319 411-1	LCP	1.3.6.1.4.1.25017.3.1.2.5	Encryption KS
CERTSIGN	RO	Siège : Bulevardul Timisoara 5A Bucharest - Romania	certSIGN Public CA	UE 910/2014 eIDAS		EN 319 411-1	LCP	1.3.6.1.4.1.25017.3.1.2.6	Encryption TKS
CERTSIGN	RO	Siège : Bulevardul Timisoara 5A Bucharest - Romania	certSIGN Public CA	UE 910/2014 eIDAS		EN 319 411-1	LCP	1.3.6.1.4.1.25017.3.1.2.7	Encryption TKC
CERTSIGN	RO	Siège : Bulevardul Timisoara 5A Bucharest - Romania	certSIGN Public CA	UE 910/2014 eIDAS		EN 319 411-1	LCP	1.3.6.1.4.1.25017.3.1.2.8	Encryption KC
CERTSIGN	RO	Siège : Bulevardul Timisoara 5A Bucharest - Romania	certSIGN Public CA	UE 910/2014 eIDAS		EN 319 411-1	LCP	1.3.6.1.4.1.25017.3.1.2.9	Seal KS
CERTSIGN	RO	Siège : Bulevardul Timisoara 5A Bucharest - Romania	certSIGN Public CA	UE 910/2014 eIDAS		EN 319 411-1	LCP	1.3.6.1.4.1.25017.3.1.2.10	Seal TKS
CERTSIGN	RO	Siège : Bulevardul Timisoara 5A Bucharest - Romania	certSIGN Public CA	UE 910/2014 eIDAS		EN 319 411-1	LCP	1.3.6.1.4.1.25017.3.1.2.11	Seal TKC

CERTSIGN	RO	Siège : Bulevardul Timisoara 5A Bucharest - Romania	certSIGN Public CA	UE 910/2014 eIDAS		EN 319 411-1	LCP	1.3.6.1.4.1.25017.3.1.2.12	Seal KC
CERTSIGN	RO	Siège : Bulevardul Timisoara 5A Bucharest - Romania	certSIGN Public CA	UE 910/2014 eIDAS		EN 319 411-1	NCP	1.3.6.1.4.1.25017.3.1.2.13	OCSP
CERTSIGN	RO	Siège : Bulevardul Timisoara 5A Bucharest - Romania	certSIGN Web CA				NCP+	2.5.29.32.0	Sub CA
CERTSIGN	RO	Siège : Bulevardul Timisoara 5A Bucharest - Romania	certSIGN Web CA	UE 910/2014 eIDAS		EN 319 411-2	QCP-w EVCP	1.3.6.1.4.1.25017.3.1.4.1	Server- Authentication
CERTSIGN	RO	Siège : Bulevardul Timisoara 5A Bucharest - Romania	certSIGN Web CA	UE 910/2014 eIDAS		EN 319 411-1	OVCP	1.3.6.1.4.1.25017.3.1.4.2	Server- Authentication
CERTSIGN	RO	Siège : Bulevardul Timisoara 5A Bucharest - Romania	certSIGN Web CA	UE 910/2014 eIDAS		EN 319 411-1	NCP+	1.3.6.1.4.1.25017.3.1.4.3	OCSP
CHAMBERSIGN FRANCE	FR	45 Avenue de la Grande Armée 75017 PARIS							
CHAMBERSIGN FRANCE	FR	46 Avenue de la Grande Armée 75017 PARIS	ChamberSign - Probatio identité	RGS V2.0	***	ETSI TS 102 042	NCP+	1.2.250.1.96.1.7.1.2.2	Authentification
CHAMBERSIGN FRANCE	FR	47 Avenue de la Grande Armée 75017 PARIS	ChamberSign - Audacio signature	RGS V2.0	**	ETSI TS 102 042	NCP+	1.2.250.1.96.1.7.2.1.2	Signature
CHAMBERSIGN FRANCE	FR	48 Avenue de la Grande Armée 75017 PARIS	ChamberSign - Audacio identité	RGS V2.0	**	ETSI TS 102 042	NCP+	1.2.250.1.96.1.7.2.2.2	Authentification
CHAMBERSIGN FRANCE	FR	49 Avenue de la Grande Armée 75017 PARIS	ChamberSign - Audacio	RGS V2.0	**	ETSI TS 102 042	NCP+	1.2.250.1.96.1.7.2.3.2	Authentification et signature
CHAMBERSIGN FRANCE	FR	50 Avenue de la Grande Armée 75017 PARIS	ChamberSign - Eurodacio	UE 910/2014 eIDAS	**	ETSI TS 102 042	QCP	1.2.250.1.96.1.7.2.4.1	Authentification et signature
CHAMBERSIGN FRANCE	FR	51 Avenue de la Grande Armée 75017 PARIS	ChamberSign - EuroProbatio	UE 910/2014 eIDAS	***	ETSI TS 101 456	QCPn+QSCD	1.2.250.1.96.1.7.1.1.3	signature
CHAMBERSIGN FRANCE	FR	52 Avenue de la Grande Armée 75017 PARIS	ChamberSign - Initio signature	RGS V2.0	*	ETSI TS 102 042	LCP	1.2.250.1.96.1.7.3.1.2	Signature
CHAMBERSIGN FRANCE	FR	53 Avenue de la Grande Armée 75017 PARIS	ChamberSign - Initio identité	RGS V2.0	*	ETSI TS 102 042	LCP	1.2.250.1.96.1.7.3.2.2	Authentification
CHAMBERSIGN FRANCE	FR	54 Avenue de la Grande Armée 75017 PARIS	ChamberSign - Initio	RGS V2.0	*	ETSI TS 102 042	LCP	1.2.250.1.96.1.7.3.3.2	Authentification et signature

CHAMBERSIGN FRANCE	FR	55 Avenue de la Grande Armée 75017 PARIS	ChamberSign - Certiserv 1*	RGS V2.0	*	ETSI TS 102 042	LCP	1.2.250.1.96.1.7.4.1 .2	Authentification serveur
CHAMBERSIGN FRANCE	FR	56 Avenue de la Grande Armée 75017 PARIS	ChamberSign - Negocio 1*	RGS V2.0	*	ETSI TS 102 042	LCP	1.2.250.1.96.1.7.4.2 .2	Cachet
CLICK & TRUST	FR	siège: 18 quai de la Rapée 75012 PARIS							
CLICK & TRUST	FR	siège: 18 quai de la Rapée 75012 PARIS	Mercanteo authentification/signature **	RGS V2.0	**	ETSI TS 102 042	NCP+	1.2.250.1.98.1.1.18. 1.1.1	Authentification et signature (RGS_A_11)
CLICK & TRUST	FR	siège: 18 quai de la Rapée 75012 PARIS	Mercanteo authentification **	RGS V2.0	**	ETSI TS 102 042	NCP+	1.2.250.1.98.1.1.18. 1.1.2	Authentification (RGS_A_7)
CLICK & TRUST	FR	siège: 18 quai de la Rapée 75012 PARIS	Mercanteo signature **	RGS V2.0	**	ETSI TS 102 042	NCP+	1.2.250.1.98.1.1.19. 1.1.1	Signature (RGS_A_8)
CLICK & TRUST	FR	siège: 18 quai de la Rapée 75012 PARIS	Admineo authentification/signature *	RGS V2.0	*	ETSI TS 102 042	LCP	1.2.250.1.98.1.1.20. 1.1.1	Authentification et signature (RGS_A_11)
CLICK & TRUST	FR	siège: 18 quai de la Rapée 75012 PARIS	Admineo authentification *	RGS V2.0	*	ETSI TS 102 042	LCP	1.2.250.1.98.1.1.20. 1.1.2	Authentification (RGS_A_7)
CLICK & TRUST	FR	siège: 18 quai de la Rapée 75012 PARIS	Admineo signature *	RGS V2.0	*	ETSI TS 102 042	LCP	1.2.250.1.98.1.1.21. 1.1.1	Signature (RGS_A_8)
CLICK & TRUST	FR	siège: 18 quai de la Rapée 75012 PARIS	Mercanteo EU sign	UE 910/2014 eIDAS	***	eIDAS Art. 51 2.	QCP Public+SSCD	1.2.250.1.98.1.1.22. 1.1.1	Signature
CLICK & TRUST	FR	siège: 18 quai de la Rapée 75012 PARIS	Mercanteo EU sign	RGS V2.0	***	ETSI TS 101 456	NCP+	1.2.250.1.98.1.1.22. 1.1.2	Authentification
CLICK & TRUST	FR	siège: 18 quai de la Rapée 75012 PARIS	Mercanteo 2	UE 910/2014 eIDAS		ETSI EN 319 411-1	NCP+	1.2.250.1.98.1.1.18. 3.1.1	Authentification/s ignature
CONSEIL SUPÉRIEUR DE L'ORDRE DES EXPERTS COMPTABLES	FR	18 Rue cognac Jay 75007 PARIS							
CONSEIL SUPÉRIEUR DE L'ORDRE DES EXPERTS COMPTABLES	FR	19 Rue cognac Jay 75007 PARIS	PC Experts comptables	UE 910/2014 eIDAS		EN 319 411-2	QCP-n-QSCD	1.2.250.1.165.1.10. 1.1	Signature
CONSEIL SUPÉRIEUR DE L'ORDRE DES EXPERTS COMPTABLES	FR	20 Rue cognac Jay 75007 PARIS	PC elus	UE 910/2014 eIDAS		EN 319 411-2	QCP-l	1.2.250.1.165.1.10. 11.1	Seal

CONSEIL SUPÉRIEUR DE L'ORDRE DES EXPERTS COMPTABLES	FR	21 Rue cognac Jay 75007 PARIS	PC Cachet cabinet	UE 910/2014 eIDAS		EN 319 411-1	NCP+	1.2.250.1.165.1.11.2.0	Cachet
CONSEIL SUPÉRIEUR DU NOTARIAT	FR	Siège : 60, boulevard de la Tour Maubourg 75007 PARIS							
CONSEIL SUPÉRIEUR DU NOTARIAT	FR	Siège : 60, boulevard de la Tour Maubourg 75007 PARIS	AC REAL SIGN	UE 910/2014 eIDAS		EN 319 411-2	QCP-n-qscd	1.2.250.1.78.2.1.3.1.1.1	Signature
CONSEIL SUPÉRIEUR DU NOTARIAT	FR	Siège : 60, boulevard de la Tour Maubourg 75007 PARIS							
CONSEIL SUPÉRIEUR DU NOTARIAT	FR	Siège : 60, boulevard de la Tour Maubourg 75007 PARIS	Autorité d'Horodatage du Notariat	UE 910/2014 eIDAS		ETSI TS 102 023		1.2.250.1.78.1.1.3.1.4.6.1.6	Horodatage
CORPME- Colegio de Registradores de la Propiedad, Mercantiles y de Bienes Muebles de España	ES	Siège : Diego de Leon, 21 28006 Madrid, Spain							
CORPME- Colegio de Registradores de la Propiedad, Mercantiles y de Bienes Muebles de España	ES	Siège : Diego de Leon, 21 28006 Madrid, Spain	Root CA					1.3.6.14.1.17276	Root
CORPME- Colegio de Registradores de la Propiedad, Mercantiles y de Bienes Muebles de España	ES	Siège : Diego de Leon, 21 28006 Madrid, Spain	Internal CA					1.3.6.14.1.17276.0.1	
CORPME- Colegio de Registradores de la Propiedad, Mercantiles y de Bienes Muebles de España	ES	Siège : Diego de Leon, 21 28006 Madrid, Spain	Registrador	UE 910/2014 eIDAS		EN 319 411-2	QCP-n-qscd	1.3.6.14.1.17276.0.1.1.2	*Authentication* & Signature
CORPME- Colegio de Registradores de la Propiedad, Mercantiles y de Bienes Muebles de España	ES	Siège : Diego de Leon, 21 28006 Madrid, Spain	Personal Interno	UE 910/2014 eIDAS		EN 319 411-2	QCP-n-qscd	1.3.6.14.1.17276.0.1.2.2	*Authentication* &Signature
CORPME- Colegio de Registradores de la Propiedad, Mercantiles y de Bienes Muebles de España	ES	Siège : Diego de Leon, 21 28006 Madrid, Spain	Representante de Persona Jurídica para Facturación Electrónica	UE 910/2014 eIDAS		EN 319 411-2	QCP-n-qscd	1.3.6.14.1.17276.0.1.4.1	*Authentication* & Signature

CORPME- Colegio de Registradores de la Propiedad, Mercantiles y de Bienes Muebles de España	ES	Siège : Diego de Leon, 21 28006 Madrid, Spain	Time-Stamp	UE 910/2014 eIDAS		EN 319 421		1.3.6.14.1.17276.0.3.1.1	Time-Stamp
CORPME- Colegio de Registradores de la Propiedad, Mercantiles y de Bienes Muebles de España	ES	Siège : Diego de Leon, 21 28006 Madrid, Spain	External CA	UE 910/2014 eIDAS				1.3.6.14.1.17276.0.2	
CORPME- Colegio de Registradores de la Propiedad, Mercantiles y de Bienes Muebles de España	ES	Siège : Diego de Leon, 21 28006 Madrid, Spain	Personal	UE 910/2014 eIDAS		EN 319 411-2	QCP-n-qscd	1.3.6.14.1.17276.0.2.1.2	*Authentication &* Signature
CORPME- Colegio de Registradores de la Propiedad, Mercantiles y de Bienes Muebles de España	ES	Siège : Diego de Leon, 21 28006 Madrid, Spain	Representante de Persona Jurídica	UE 910/2014 eIDAS		EN 319 411-2	QCP-n-qscd	1.3.6.14.1.17276.0.2.2.2	*Authentication &* Signature
CORPME- Colegio de Registradores de la Propiedad, Mercantiles y de Bienes Muebles de España	ES	Siège : Diego de Leon, 21 28006 Madrid, Spain	Cargo Administrativo	UE 910/2014 eIDAS		EN 319 411-2	QCP-n-qscd	1.3.6.14.1.17276.0.2.3.2	*Authentication &* Signature
CORPME- Colegio de Registradores de la Propiedad, Mercantiles y de Bienes Muebles de España	ES	Siège : Diego de Leon, 21 28006 Madrid, Spain	Administración Local	UE 910/2014 eIDAS		EN 319 411-2	QCP-n-qscd	1.3.6.14.1.17276.0.2.4.2	*Authentication &* Signature
CORPME- Colegio de Registradores de la Propiedad, Mercantiles y de Bienes Muebles de España	ES	Siège : Diego de Leon, 21 28006 Madrid, Spain	Profesional	UE 910/2014 eIDAS		EN 319 411-2	QCP-n-qscd	1.3.6.14.1.17276.0.2.5.2	*Authentication &* Signature
CORPME- Colegio de Registradores de la Propiedad, Mercantiles y de Bienes Muebles de España	ES	Siège : Diego de Leon, 21 28006 Madrid, Spain	Representante de Entidad sin Personalidad Jurídica	UE 910/2014 eIDAS		EN 319 411-2	QCP-n-qscd	1.3.6.14.1.17276.0.2.6.1	*Authentication &* Signature
CRÉDIT AGRICOLE CARDS & PAYMENTS	FR	Siège: 83 boulevard des Chênes - 78280 Guyancourt							
CRÉDIT AGRICOLE CARDS & PAYMENTS	FR	Siège: 83 boulevard des Chênes - 78280 Guyancourt	CA LCL Certificat RGS Usage Separe	UE 910/2014 eIDAS	**	eIDAS Art. 51 2.	NCP+	1.2.250.1.104.3.1.1.1.1.9.1.1	*Authentication &* Signature

CRÉDIT AGRICOLE CARDS & PAYMENTS	FR	Siège: 83 boulevard des Chênes - 78280 Guyancourt	CA LCL Certificat RGS Usage Mixte	UE 910/2014 eIDAS		eIDAS Art. 51 2.	NCP+	1.2.250.1.104.3.1.1.1.1.5.2.0	*Authentication &* Signature
UNIVERSIGN-CRYPTOLOG INTERNATIONAL	FR	Siège : 7 rue du Faubourg Poissonnière 75009 PARIS							
UNIVERSIGN-CRYPTOLOG INTERNATIONAL	FR	Siège : 7 rue du Faubourg Poissonnière 75009 PARIS	Universign Hardware CA	UE 910/2014 eIDAS		EN 319 411-2	QCP-n	1.3.6.1.4.1.15819.5.1.3.1	Signature
UNIVERSIGN-CRYPTOLOG INTERNATIONAL	FR	Siège : 7 rue du Faubourg Poissonnière 75009 PARIS	Universign hardware CA	UE 910/2014 eIDAS		EN 319 411-1	LCP	1.3.6.1.4.1.15819.5.1.3.3	Signature
UNIVERSIGN-CRYPTOLOG INTERNATIONAL	FR	Siège : 7 rue du Faubourg Poissonnière 75009 PARIS	Universign hardware CA	UE 910/2014 eIDAS		EN 319 411-1	LCP	1.3.6.1.4.1.15819.5.1.3.4	Cachet
UNIVERSIGN-CRYPTOLOG INTERNATIONAL	FR	Siège : 7 rue du Faubourg Poissonnière 75009 PARIS	Universign hardware CA	UE 910/2014 eIDAS		EN 319 411-2	QCP-l	1.3.6.1.4.1.15819.5.1.3.5	Cachet
UNIVERSIGN-CRYPTOLOG INTERNATIONAL	FR	Siège : 7 rue du Faubourg Poissonnière 75009 PARIS	Universign timestamping CA	UE 910/2014 eIDAS	*	EN 319 411-1	LCP	1.3.6.1.4.1.15819.5.1.1	Cachet
UNIVERSIGN-CRYPTOLOG INTERNATIONAL	FR	Siège : 7 rue du Faubourg Poissonnière 75009 PARIS	Universign	UE 910/2014 eIDAS		EN 319 421		1.3.6.1.4.1.15819.5.2.2	Horodatage
UNIVERSIGN-CRYPTOLOG INTERNATIONAL	FR	Siège : 7 rue du Faubourg Poissonnière 75009 PARIS	Universign Hardware Primary CA	UE 910/2014 eIDAS		EN 319 411-1	NCP+	1.3.6.1.4.1.15819.5.1.2.1	Signature
UNIVERSIGN-CRYPTOLOG INTERNATIONAL	FR	Siège : 7 rue du Faubourg Poissonnière 75009 PARIS	Universign Software Primary CA	UE 910/2014 eIDAS		EN 319 411-1	NCP	1.3.6.1.4.1.15819.5.1.2.2	Signature
DHIMYOTIS	FR	Siège : 20, allée de la Râperie 59650 VILLENEUVE D'ASCQ							
DHIMYOTIS	FR	Siège : 20, allée de la Râperie 59650 VILLENEUVE D'ASCQ	Certigna ID PRIS* Pro	RGS V2.0	*	ETSI TS 102 042	LCP	1.2.250.1.177.1.9.1.6	Authentification et signature
DHIMYOTIS	FR	Siège : 20, allée de la Râperie 59650 VILLENEUVE D'ASCQ	Certigna ID PRIS** Pro	RGS V2.0	**	ETSI TS 102 042	NCP+	1.2.250.1.177.1.10.1.6	Authentification et signature

DHIMYOTIS	FR	Siège : 20, allée de la Râperie 59650 VILLENEUVE D'ASCQ	Certigna ID PRIS*** Pro	RGS V2.0	***	ETSI TS 101 456	QCP Public+SSCD	1.2.250.1.177.1.11.1.7	Signature
DHIMYOTIS	FR	Siège : 20, allée de la Râperie 59650 VILLENEUVE D'ASCQ	Certigna Authentification PRIS*** Pro	RGS V2.0	***	ETSI TS 102 042	NCP+	1.2.250.1.177.1.13.1.6	Authentification
DHIMYOTIS	FR	Siège : 20, allée de la Râperie 59650 VILLENEUVE D'ASCQ	Certigna Client Serveur	RGS V2.0	*	ETSI TS 102 042	OVCP	1.2.250.1.177.1.15.1.5	Authentification serveur
DHIMYOTIS	FR	Siège : 20, allée de la Râperie 59650 VILLENEUVE D'ASCQ	Certigna Cachet Serveur	RGS V2.0	*	ETSI TS 102 042	LCP	1.2.250.1.177.1.14.1.5	Cachet
DHIMYOTIS	FR	Siège : 20, allée de la Râperie 59650 VILLENEUVE D'ASCQ	Certigna Cachet serveur (messagerie)	RGS V2.0	*	ETSI TS 102 042	LCP	1.2.250.1.177.1.17.1.5	Cachet
DHIMYOTIS	FR	Siège : 20, allée de la Râperie 59650 VILLENEUVE D'ASCQ	Certigna SSL PRIS	RGS V2.0	*	ETSI TS 102 042	OVCP	1.2.250.1.177.1.5.1.6	Authentification serveur
DHIMYOTIS	FR	Siège : 20, allée de la Râperie 59650 VILLENEUVE D'ASCQ	Certigna Root CA						root
DHIMYOTIS	FR	Siège : 20, allée de la Râperie 59650 VILLENEUVE D'ASCQ	Certigna Entity CA					1.2.250.1.177.2.0.1.1	
DHIMYOTIS	FR	Siège : 20, allée de la Râperie 59650 VILLENEUVE D'ASCQ	Certigna Entity CA	UE 910/2014 eIDAS	*	EN 319 411-1	LCP	1.2.250.1.177.2.6.1.1.1	Cachet
DHIMYOTIS	FR	Siège : 20, allée de la Râperie 59650 VILLENEUVE D'ASCQ	Certigna Entity CA	UE 910/2014 eIDAS	*	EN 319 411-1	LCP	1.2.250.1.177.2.6.1.3.1	Cachet
DHIMYOTIS	FR	Siège : 20, allée de la Râperie 59650 VILLENEUVE D'ASCQ	Certigna Entity CA	UE 910/2014 eIDAS	**	EN 319 411-2	QCP-l + QSealCD	1.2.250.1.177.2.6.1.4.1	Cachet
DHIMYOTIS	FR	Siège : 20, allée de la Râperie 59650 VILLENEUVE D'ASCQ	Certigna Entity CA	UE 910/2014 eIDAS	**	EN 319 411-2	QCP-l + QSealCD	1.2.250.1.177.2.6.1.6.1	Cachet
DHIMYOTIS	FR	Siège : 20, allée de la Râperie 59650 VILLENEUVE D'ASCQ	Certigna Entity Code Signing CA					1.2.250.1.177.2.0.1.1	
DHIMYOTIS	FR	Siège : 20, allée de la Râperie 59650 VILLENEUVE D'ASCQ	Certigna Entity Code Signing CA	UE 910/2014 eIDAS	*	EN 319 411-1	LCP	1.2.250.1.177.2.8.1.1.1	Cachet
DHIMYOTIS	FR	Siège : 20, allée de la Râperie 59650 VILLENEUVE D'ASCQ	Certigna Entity Code Signing CA	UE 910/2014 eIDAS	**	EN 319 411-2	QCP-l + QSealCD	1.2.250.1.177.2.8.1.2.1	Cachet
DHIMYOTIS	FR	Siège : 20, allée de la Râperie 59650 VILLENEUVE D'ASCQ	Certigna Identity CA					1.2.250.1.177.2.0.1.1	

DHIMYOTIS	FR	Siège : 20, allée de la Râperie 59650 VILLENEUVE D'ASCQ	Certigna Identity CA	UE 910/2014 eIDAS	*	EN 319 411-1	LCP	1.2.250.1.177.2.3.1.1.1	Encryption
DHIMYOTIS	FR	Siège : 20, allée de la Râperie 59650 VILLENEUVE D'ASCQ	Certigna Identity CA	UE 910/2014 eIDAS	*	EN 319 411-1	LCP	1.2.250.1.177.2.3.1.2.1	Authentification et signature
DHIMYOTIS	FR	Siège : 20, allée de la Râperie 59650 VILLENEUVE D'ASCQ	Certigna Identity CA	UE 910/2014 eIDAS	*	EN 319 411-1	LCP	1.2.250.1.177.2.3.1.3.1	encryption
DHIMYOTIS	FR	Siège : 20, allée de la Râperie 59650 VILLENEUVE D'ASCQ	Certigna Identity CA	UE 910/2014 eIDAS	*	EN 319 411-1	LCP	1.2.250.1.177.2.3.1.4.1	Authentification et signature
DHIMYOTIS	FR	Siège : 20, allée de la Râperie 59650 VILLENEUVE D'ASCQ	Certigna Identity Plus CA					1.2.250.1.177.2.0.1.1	
DHIMYOTIS	FR	Siège : 20, allée de la Râperie 59650 VILLENEUVE D'ASCQ	Certigna Identity Plus CA	UE 910/2014 eIDAS	**	EN 319 411-2	QCP-n-qscd	1.2.250.1.177.2.4.1.1.1	Authentication & Signature
DHIMYOTIS	FR	Siège : 20, allée de la Râperie 59650 VILLENEUVE D'ASCQ	Certigna Identity Plus CA	UE 910/2014 eIDAS	*	EN 319 411-1	NCP+	1.2.250.1.177.2.4.1.2.1	Authentification
DHIMYOTIS	FR	Siège : 20, allée de la Râperie 59650 VILLENEUVE D'ASCQ	Certigna Identity Plus CA	UE 910/2014 eIDAS	***	EN 319 411-2	QCP-n-qscd	1.2.250.1.177.2.4.1.3.1	Signature
DHIMYOTIS	FR	Siège : 20, allée de la Râperie 59650 VILLENEUVE D'ASCQ	Certigna Identity Plus CA	UE 910/2014 eIDAS	**	EN 319 411-2	QCP-n-qscd	1.2.250.1.177.2.4.1.4.1	Authentication & Signature
DHIMYOTIS	FR	Siège : 20, allée de la Râperie 59650 VILLENEUVE D'ASCQ	Certigna Identity Plus CA	UE 910/2014 eIDAS	*	EN 319 411-1	NCP+	1.2.250.1.177.2.4.1.5.1	Authentification
DHIMYOTIS	FR	Siège : 20, allée de la Râperie 59650 VILLENEUVE D'ASCQ	Certigna Identity Plus CA	UE 910/2014 eIDAS	***	EN 319 411-2	QCP-n-qscd	1.2.250.1.177.2.4.1.6.1	Signature
DHIMYOTIS	FR	Siège : 20, allée de la Râperie 59650 VILLENEUVE D'ASCQ	Certigna Services CA					1.2.250.1.177.2.0.1.1	
DHIMYOTIS	FR	Siège : 20, allée de la Râperie 59650 VILLENEUVE D'ASCQ	Certigna Services CA	UE 910/2014 eIDAS	*	EN 319 411-1	OVCP	1.2.250.1.177.2.5.1.1.1	Authentification serveur
DHIMYOTIS	FR	Siège : 20, allée de la Râperie 59650 VILLENEUVE D'ASCQ	Certigna Services CA	UE 910/2014 eIDAS	*	EN 319 411-1	OVCP	1.2.250.1.177.2.5.1.2.1	Authentification serveur
DHIMYOTIS	FR	Siège : 20, allée de la Râperie 59650 VILLENEUVE D'ASCQ	Certigna Services CA	UE 910/2014 eIDAS	***	EN 319 411-2	QCP-w	1.2.250.1.177.2.5.1.3.1	Authentification serveur
DHIMYOTIS	FR	Siège : 20, allée de la Râperie 59650 VILLENEUVE D'ASCQ	Certigna Services CA	UE 910/2014 eIDAS	*	EN 319 411-1	EVCP	1.2.250.1.177.2.5.1.3.1	Authentification serveur

DHIMYOTIS	FR	Siège : 20, allée de la Râperie 59650 VILLENEUVE D'ASCQ	Certigna Wild CA					1.2.250.1.177.2.0.1.1	
DHIMYOTIS	FR	Siège : 20, allée de la Râperie 59650 VILLENEUVE D'ASCQ	Certigna Wild CA	UE 910/2014 eIDAS	*	EN 319 411-1	OVCP	1.2.250.1.177.2.7.1.1.1	Authentification serveur
DHIMYOTIS	FR	Siège : 20, allée de la Râperie 59650 VILLENEUVE D'ASCQ	Certigna Wild CA	UE 910/2014 eIDAS		EN 319 411-1	OVCP	1.2.250.1.177.2.7.1.2.1	Authentification serveur
DHIMYOTIS	FR	Siège : 20, allée de la Râperie 59650 VILLENEUVE D'ASCQ	FR03 - Certigna Cachet Serveur	UE 910/2014 eIDAS	*	EN 319 411-1	NCP+ - 2D-doc	1.2.250.1.177.2.2.1.1	Cachet
DHIMYOTIS	FR	Siège : 20, allée de la Râperie 59650 VILLENEUVE D'ASCQ	Service d'horodatage	UE 910/2014 eIDAS	*RGS_A5*	EN 319 421		1.2.250.1.1777.2.9.1	horodatage
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE							
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	CERTPLUS CLASS 2 PRIMARY CA					1.3.6.1.4.1.22234.2.5.1.1.3	Root
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	AC Cryptonéo Machines			TS 102042	NCP+		Sub CA
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	AC Cryptonéo Machines			TS 102042	OVCP	1.3.6.1.4.1.46116.1.3.101.11	Server- Authentication
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	AC DKB Solutions Machines			TS 102042	NCP+		Sub CA
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	AC DKB Solutions Machines			TS 102042	OVCP	1.3.6.1.4.1.46111.1.3.101.11	Server- Authentication
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	CLASS 2 KEYNECTIS CA	UE 910/2014 eIDAS		EN 319411-1	PTC-BR	2.5.29.32.0	Sub CA
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	CLASS 2 KEYNECTIS CA	UE 910/2014 eIDAS		EN 319411-1	DVCP	1.3.6.1.4.1.22234.2.5.3.13	Server- Authentication

DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	CLASS 2 KEYNECTIS CA	UE 910/2014 eIDAS		EN 319411-1	OVCP	1.3.6.1.4.1.22234.2.5.3.14	Server- Authentication
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	KEYNECTIS Extended Validation CA	UE 910/2014 eIDAS		EN 319411-1	PTC-BR	2.5.29.32.0	Sub CA
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	KEYNECTIS Extended Validation CA	UE 910/2014 eIDAS		EN 319411-1	EVCP	1.3.6.1.4.1.22234.2.5.2.3.1	Server- Authentication
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	KEYNECTIS SSL RGS	UE 910/2014 eIDAS		EN 319411-1	PTC-BR	2.5.29.32.0	Sub CA
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	*KEYNECTIS SSL RGS*			*TS 102042*	*EVCP*	*1.3.6.1.4.1.22234.2.5.2.3.1*	*Server- Authentication*
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	KEYNECTIS SSL RGS	UE 910/2014 eIDAS	*	EN 319411-1	OVCP	1.3.6.1.4.1.22234.2.5.3.10	Server- Authentication
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	*KEYNECTIS SSL RGS*		*	*TS 102042*	*EVCP*	*1.3.6.1.4.1.22234.2.5.3.12*	*Server- Authentication*
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	KEYNECTIS SSL RGS	UE 910/2014 eIDAS	*	EN 319411-1	LCP	1.3.6.1.4.1.22234.2.5.3.15	Server- Authentication - client
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	KEYNECTIS SSL RGS	UE 910/2014 eIDAS	**	EN 319411-1	NCP+	1.3.6.1.4.1.22234.2.5.3.16	Server- Authentication - client
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	KEYNECTIS SSL RGS	UE 910/2014 eIDAS	**	EN 319411-1	OVCP	1.3.6.1.4.1.22234.2.5.3.17	Server- Authentication
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	KEYNECTIS ICS ADVANCED Class 3 CA	UE 910/2014 eIDAS		EN 319411-1	PTC-BR	1.3.6.1.4.1.22234.2.9.2.1	Sub CA
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	*KEYNECTIS ICS ADVANCED Class 3 CA*		**	*TS 102042*	*NCP+*	*1.3.6.1.4.1.22234.2.9.3.2*	*Signature and Authentication*

DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	*KEYNECTIS ICS ADVANCED Class 3 CA*		*	*TS 102042*	*LCP*	*1.3.6.1.4.1.22234.2.9.3.9*	*Seal*
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	KEYNECTIS ICS ADVANCED Class 3 CA	UE 910/2014 eIDAS	**	EN 319411-1	NCP+	1.3.6.1.4.1.22234.2.9.3.10	Signature and Authentication
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	KEYNECTIS ICS ADVANCED Class 3 CA	UE 910/2014 eIDAS	*	EN 319411-1	LCP	1.3.6.1.4.1.22234.2.9.3.12	Signature and Authentication
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	*KEYNECTIS ICS ADVANCED Class 3 CA*		**	*TS 102042*	*NCP+*	*1.3.6.1.4.1.22234.2.9.3.13*	*Authentication*
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	KEYNECTIS ICS ADVANCED Class 3 CA	UE 910/2014 eIDAS	**	EN 319411-1	NCP+	1.3.6.1.4.1.22234.2.9.3.16	Authentication
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	*KEYNECTIS ICS ADVANCED Class 3 CA*		**	*TS 102042*	*NCP+*	*1.3.6.1.4.1.22234.2.9.3.17*	*Seal*
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	*KEYNECTIS ICS ADVANCED Class 3 CA*		**	*TS 102042*	*NCP+*	*1.3.6.1.4.1.22234.2.9.3.18*	*Seal*
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	KEYNECTIS ICS ADVANCED Class 3 CA	UE 910/2014 eIDAS	*	EN 319411-1	LCP	1.3.6.1.4.1.22234.2.9.3.19	Seal
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	KEYNECTIS ROOT CA					1.3.6.1.4.1.22234.2.9.2	Root
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	Keynectis CDS CA for timestamping	UE 910/2014 eIDAS		EN 319411-1	PTC-BR	2.5.29.32.0	Sub CA
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	Keynectis CDS CA for timestamping	UE 910/2014 eIDAS	*	EN 319411-1	LCP	1.3.6.1.4.1.22234.2.8.3.5	Cachet Horodatage

DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	*CN de la TSU = UH 20170118*	UE 910/2014 eIDAS	*RGS_A5*	*EN 319421*		*1.3.6.1.4.1.22234.2.6.5.3*	*Horodatage*
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	CN de la TSU = UH Qualifiee PA2 20170405	UE 910/2014 eIDAS	*RGS_A6*	EN 319421	Qualified	1.3.6.1.4.1.22234.2.6.5.8	Horodatage
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	KEYNECTIS SSL RGS	UE 910/2014 eIDAS		EN 319411-1	PTC-BR	2.5.29.32.0	Sub CA
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	*KEYNECTIS SSL RGS*			*TS 102042*	*EVCP*	*1.3.6.1.4.1.22234.2.5.2.3.1*	*Server- Authentication*
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	KEYNECTIS SSL RGS	UE 910/2014 eIDAS	*	EN 319411-1	OVCP	1.3.6.1.4.1.22234.2.5.3.10	Server- Authentication
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	*KEYNECTIS SSL RGS*		*	*TS 102042*	*EVCP*	*1.3.6.1.4.1.22234.2.5.3.12*	*Server- Authentication*
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	KEYNECTIS SSL RGS	UE 910/2014 eIDAS	*	EN 319411-1	LCP	1.3.6.1.4.1.22234.2.5.3.15	Server- Authentication - client
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	KEYNECTIS SSL RGS	UE 910/2014 eIDAS	**	EN 319411-1	NCP+	1.3.6.1.4.1.22234.2.5.3.16	Server- Authentication - client
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	KEYNECTIS SSL RGS	UE 910/2014 eIDAS	**	EN 319411-1	OVCP	1.3.6.1.4.1.22234.2.5.3.17	Server- Authentication
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	OpenTrust Qualified CDS CA	UE 910/2014 eIDAS		EN 319411-1	PTC-BR	2.5.29.32.0	Sub CA
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	*OpenTrust Qualified CDS CA*	UE 910/2014 eIDAS	***	*TS 101456*	*QCP+*	*1.3.6.1.4.1.22234.2.8.3.11*	*Signature*
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	KEYNECTIS ICS CA	UE 910/2014 eIDAS		EN 319411-1	PTC-BR	1.3.6.1.4.1.22234.2.9.2	Intermediate CA

DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	AC CRYPTONEO PERSONNES	UE 910/2014 eIDAS		EN 319411-1	PTC-BR		Sub CA
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	AC CRYPTONEO PERSONNES			TS 102042	NCP+	1.3.6.1.4.1.46116.1.2.101.11	Signature
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	AC CRYPTONEO PERSONNES			TS 102042	NCP+	1.3.6.1.4.1.46116.1.2.101.12	Seal
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	AC DKB SOLUTIONS PERSONNES	UE 910/2014 eIDAS		EN 319411-1	PTC-BR		Sub CA
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	AC DKB SOLUTIONS PERSONNES			TS 102042	NCP+	1.3.6.1.4.1.46111.1.2.101.11	Signature
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	AC DKB SOLUTIONS PERSONNES			TS 102042	NCP+	1.3.6.1.4.1.46111.1.2.101.11	Seal
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	KEYNECTIS ICS ADVANCED Class 3 CA	UE 910/2014 eIDAS		EN 319411-1	PTC-BR	1.3.6.1.4.1.22234.2.9.2.1	Sub CA
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	*KEYNECTIS ICS ADVANCED Class 3 CA*		**	*TS 102042*	*NCP+*	*1.3.6.1.4.1.22234.2.9.3.2*	*Signature and Authentication*
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	*KEYNECTIS ICS ADVANCED Class 3 CA*		*	*TS 102042*	*LCP*	*1.3.6.1.4.1.22234.2.9.3.9*	*Seal*
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	KEYNECTIS ICS ADVANCED Class 3 CA	UE 910/2014 eIDAS	**	EN 319411-1	NCP+	1.3.6.1.4.1.22234.2.9.3.10	Signature and Authentication
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	KEYNECTIS ICS ADVANCED Class 3 CA	UE 910/2014 eIDAS	*	EN 319411-1	LCP	1.3.6.1.4.1.22234.2.9.3.12	Signature and Authentication

DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	*KEYNECTIS ICS ADVANCED Class 3 CA*		**	*TS 102042*	*NCP+*	*1.3.6.1.4.1.22234.2.9.3.13*	*Authentication*
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	KEYNECTIS ICS ADVANCED Class 3 CA	UE 910/2014 eIDAS	**	EN 319411-1	NCP+	1.3.6.1.4.1.22234.2.9.3.16	Authentication
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	*KEYNECTIS ICS ADVANCED Class 3 CA*		**	*TS 102042*	*NCP+*	*1.3.6.1.4.1.22234.2.9.3.17*	*Seal*
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	*KEYNECTIS ICS ADVANCED Class 3 CA*		**	*TS 102042*	*NCP+*	*1.3.6.1.4.1.22234.2.9.3.18*	*Seal*
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	KEYNECTIS ICS ADVANCED Class 3 CA	UE 910/2014 eIDAS	*	EN 319411-1	LCP	1.3.6.1.4.1.22234.2.9.3.19	Seal
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	KEYNECTIS ICS QUALIFIED CA	UE 910/2014 eIDAS		EN 319411-1	PTC-BR	1.3.6.1.4.1.22234.2.9.2.1	Sub CA
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	*KEYNECTIS ICS QUALIFIED CA*	UE 910/2014 eIDAS	***	*TS 101456*	*QCP+*	*1.3.6.1.4.1.22234.2.9.3.1*	*Signature*
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	KEYNECTIS ICS QUALIFIED CA	UE 910/2014 eIDAS	***	EN 319411-2	QCP-n-qscd	1.3.6.1.4.1.22234.2.9.3.15	Signature
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	KEYNECTIS ICS QUALIFIED CA	UE 910/2014 eIDAS	**	EN 319411-2	QCP-l	1.3.6.1.4.1.22234.2.9.3.20	Seal
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	KEYNECTIS ICS QUALIFIED CA	UE 910/2014 eIDAS	**	EN 319411-2	QCP-l	1.3.6.1.4.1.22234.2.9.3.21	Seal
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	Keynectis CA for Enterprise signature	UE 910/2014 eIDAS		EN 319411-1	PTC-BR	2.5.29.32.0	Sub CA
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	*Keynectis CA for Enterprise signature*		*	*TS 102042*	*LCP*	*1.3.6.1.4.1.22234.2.12.3.2*	*Signature*

DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	*Keynectis CA for Enterprise signature*		*	*TS 102042*	*LCP*	*1.3.6.1.4.1.22234.2.12.3.3*	*Signature and Authentication*
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	OPENTRUST ROOT CA G1	UE 910/2014 eIDAS		EN 319411-1	PTC-BR	1.3.6.1.4.1.22234.2.14.3.1	Root
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	KEYNECTIS Extended Validation CA	UE 910/2014 eIDAS		EN 319411-1	PTC-BR	2.5.29.32.0	Sub CA
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	KEYNECTIS Extended Validation CA	UE 910/2014 eIDAS		EN 319411-1	EVCP	1.3.6.1.4.1.22234.2.5.2.3.1	Server- Authentication
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	OpenTrust CA for AATL G1	UE 910/2014 eIDAS		EN 319411-1	PTC-BR	1.3.6.1.4.1.22234.2.14.3.1	Intermediate CA
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	KEYNECTIS ICS ADVANCED Class 3 CA	UE 910/2014 eIDAS		EN 319411-1	PTC-BR	1.3.6.1.4.1.22234.2.9.2.1	Sub CA
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	*KEYNECTIS ICS ADVANCED Class 3 CA*		**	*TS 102042*	*NCP+*	*1.3.6.1.4.1.22234.2.9.3.2*	*Signature and Authentication*
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	*KEYNECTIS ICS ADVANCED Class 3 CA*		*	*TS 102042*	*LCP*	*1.3.6.1.4.1.22234.2.9.3.9*	*Seal*
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	KEYNECTIS ICS ADVANCED Class 3 CA	UE 910/2014 eIDAS	**	EN 319411-1	NCP+	1.3.6.1.4.1.22234.2.9.3.10	Signature and Authentication
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	KEYNECTIS ICS ADVANCED Class 3 CA	UE 910/2014 eIDAS	*	EN 319411-1	LCP	1.3.6.1.4.1.22234.2.9.3.12	Signature and Authentication
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	*KEYNECTIS ICS ADVANCED Class 3 CA*		**	*TS 102042*	*NCP+*	*1.3.6.1.4.1.22234.2.9.3.13*	*Authentication*

DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	KEYNECTIS ICS ADVANCED Class 3 CA	UE 910/2014 eIDAS	**	EN 319411-1	NCP+	1.3.6.1.4.1.22234.2.9.3.16	Authentication
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	*KEYNECTIS ICS ADVANCED Class 3 CA*		**	*TS 102042*	*NCP+*	*1.3.6.1.4.1.22234.2.9.3.17*	*Seal*
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	*KEYNECTIS ICS ADVANCED Class 3 CA*		**	*TS 102042*	*NCP+*	*1.3.6.1.4.1.22234.2.9.3.18*	*Seal*
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	KEYNECTIS ICS ADVANCED Class 3 CA	UE 910/2014 eIDAS	*	EN 319411-1	LCP	1.3.6.1.4.1.22234.2.9.3.19	Seal
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	Cloud Signing Personal Signature CA	UE 910/2014 eIDAS		EN 319411-1	PTC-BR	2.5.29.32.0	Sub CA
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	*Cloud Signing Personal Signature CA*			*TS 102042*	*LCP*	*1.3.6.1.4.1.22234.2.8.3.9*	*Signature*
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	Cloud Signing Personal Signature CA	UE 910/2014 eIDAS		EN 319411-2	QCP-n-qscd	1.3.6.1.4.1.22234.2.8.3.20	Signature
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	*Cloud Signing Personal Signature CA*	UE 910/2014 eIDAS		*TS 101456*	*QCP*	*1.3.6.1.4.1.22234.2.8.3.7*	*Signature*
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	DocuSign Cloud Signing CA - SI1	Evrotrust SSL Organization Validated Certificate		EN 319411-1	PTC-BR	2.5.29.32.0	Sub CA
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	DocuSign Cloud Signing CA - SI1	UE 910/2014 eIDAS		EN 319411-1	LCP	1.3.6.1.4.1.22234.2.14.3.32	Signature
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	DocuSign Premium Cloud Signing CA - SI1	UE 910/2014 eIDAS		EN 319411-1	PTC-BR	2.5.29.32.0	Sub CA

DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	DocuSign Premium Cloud Signing CA - SI1	UE 910/2014 eIDAS		EN 319411-2	QCP-n-qscd	1.3.6.1.4.1.22234.2.14.3.31	Signature
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	Keynectis CDS CA for timestamping	UE 910/2014 eIDAS		EN 319411-1	PTC-BR	2.5.29.32.0	Sub CA
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	Keynectis CDS CA for timestamping	UE 910/2014 eIDAS	*	EN 319411-1	LCP	1.3.6.1.4.1.22234.2.8.3.5	Cachet Horodatage
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	*CN de la TSU = UH 20170118*	UE 910/2014 eIDAS	*RGS_A5*	*EN 319421*		*1.3.6.1.4.1.22234.2.6.5.3*	Horodatage
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	CN de la TSU = UH Qualifiee PA2 20170405	UE 910/2014 eIDAS	*RGS_A6*	EN 319421	Qualified	1.3.6.1.4.1.22234.2.6.5.8	Horodatage
DOCUSIGN France	FR	Siège : 145-175 rue Jean-Jacques Rousseau 92130 Issy les Moulineaux - FRANCE	KEYNECTIS ICS QUALIFIED CA	UE 910/2014 eIDAS		EN 319411-1	PTC-BR	1.3.6.1.4.1.22234.2.9.2.1	Sub CA
EVROTRUST TECHNOLOGIES JSC	BG	Headquarter: #101 Tsarigradsko shausse bld. Business active center Sofia 1113, REPUBLIC OF BULGARIA							
EVROTRUST TECHNOLOGIES JSC	BG	Headquarter: #101 Tsarigradsko shausse bld. Business active center Sofia 1113, REPUBLIC OF BULGARIA	Evrotrust RSA Root CA						Root
EVROTRUST TECHNOLOGIES JSC	BG	Headquarter: #101 Tsarigradsko shausse bld. Business active center Sofia 1113, REPUBLIC OF BULGARIA	Evrotrust RSA Operational CA						sub CA
EVROTRUST TECHNOLOGIES JSC	BG	Headquarter: #101 Tsarigradsko shausse bld. Business active center Sofia 1113, REPUBLIC OF BULGARIA	Evrotrust Qualified Natural Person Certificate for QES	UE 910/2014 eIDAS		EN 319 411-2	QCP-n-qscd	1.3.6.1.4.1.47272.2.2	Signature

EVROTRUST TECHNOLOGIES JSC	BG	Headquarter: #101 Tsarigradsko shausse bld. Business active center Sofia 1113, REPUBLIC OF BULGARIA	Evrotrust Qualified Natural Person Attribute Certificate for QES	UE 910/2014 eIDAS		EN 319 411-2	QCP-n-qscd	1.3.6.1.4.1.47272.2.2.1	Signature
EVROTRUST TECHNOLOGIES JSC	BG	Headquarter: #101 Tsarigradsko shausse bld. Business active center Sofia 1113, REPUBLIC OF BULGARIA	Evrotrust Qualified Legal Person Certificate for QESeal	UE 910/2014 eIDAS		EN 319 411-2	QCP-l	1.3.6.1.4.1.47272.2.3	Seal
EVROTRUST TECHNOLOGIES JSC	BG	Headquarter: #101 Tsarigradsko shausse bld. Business active center Sofia 1113, REPUBLIC OF BULGARIA	Evrotrust Qualified Natural Person Certificate for AES	UE 910/2014 eIDAS		EN 319 411-2	QCP-n	1.3.6.1.4.1.47272.2.7	Signature
EVROTRUST TECHNOLOGIES JSC	BG	Headquarter: #101 Tsarigradsko shausse bld. Business active center Sofia 1113, REPUBLIC OF BULGARIA	Evrotrust Qualified Legal Person Certificate for AESeal	UE 910/2014 eIDAS		EN 319 411-2	QCP-l	1.3.6.1.4.1.47272.2.8	Seal
EVROTRUST TECHNOLOGIES JSC	BG	Headquarter: #101 Tsarigradsko shausse bld. Business active center Sofia 1113, REPUBLIC OF BULGARIA	Evrotrust TSA	UE 910/2014 eIDAS		EN 319 421	TSAP	1.3.6.1.4.1.47272.1.2	Time Stamp
EVROTRUST TECHNOLOGIES JSC	BG	Headquarter: #101 Tsarigradsko shausse bld. Business active center Sofia 1113, REPUBLIC OF BULGARIA	Evrotrust SSL Domain Validated Certificate	UE 910/2014 eIDAS		EN 319 411-1	DVCP	1.3.6.1.4.1.47272.2.4.1	Website authentication
EVROTRUST TECHNOLOGIES JSC	BG	Headquarter: #101 Tsarigradsko shausse bld. Business active center Sofia 1113, REPUBLIC OF BULGARIA	Evrotrust SSL Organization Validated Certificate	UE 910/2014 eIDAS		EN 319 411-1	OVCP	1.3.6.1.4.1.47272.2.4.2	Website authentication
EVROTRUST TECHNOLOGIES JSC	BG	Headquarter: #101 Tsarigradsko shausse bld. Business active center Sofia 1113, REPUBLIC OF BULGARIA	Evrotrust Server Certificate	UE 910/2014 eIDAS		EN 319 411-2	QCP-w	1.3.6.1.4.1.47272.2.6	Website authentication
EVROTRUST TECHNOLOGIES JSC	BG	Headquarter: #101 Tsarigradsko shausse bld. Business active center Sofia 1113, REPUBLIC OF BULGARIA	Evrotrust SSL EV Certificate	UE 910/2014 eIDAS		EN 319 411-1	EVCP	1.3.6.1.4.1.47272.2.5	Website authentication

IMPRIMERIE NATIONALE	FR	Siège : 104, avenue du Président Kennedy 75016 Paris - France							
IMPRIMERIE NATIONALE	FR	Siège : 104, avenue du Président Kennedy 75016 Paris - France	AC Imprimerie Nationale Racine				2.5.29.32.0	AC racine	
IMPRIMERIE NATIONALE	FR	Siège : 104, avenue du Président Kennedy 75016 Paris - France	AC Imprimerie Nationale Elevé Personnel				2.5.29.32.0	Ac intermédiaire	
IMPRIMERIE NATIONALE	FR	Siège : 104, avenue du Président Kennedy 75016 Paris - France	AC Imprimerie Nationale Elevé Personnel	UE 910/2014 eIDAS	***	EN 319 411-2	QCP-n-QSCD	1.2.250.1.295.1.1.2 0.7.1.102.1	Signature
IMPRIMERIE NATIONALE	FR	Siège : 104, avenue du Président Kennedy 75016 Paris - France	AC Imprimerie Nationale Substantiel Personnel				2.5.29.32.0	Ac intermédiaire	
IMPRIMERIE NATIONALE	FR	Siège : 104, avenue du Président Kennedy 75016 Paris - France	AC Imprimerie Nationale Substantiel Personnel	UE 910/2014 eIDAS	**	EN 319 411-2	QCP-n-QSCD	1.2.250.1.295.1.1.8. 6.1.102.1	Signature
IMPRIMERIE NATIONALE	FR	Siège : 104, avenue du Président Kennedy 75016 Paris - France	AC Imprimerie Nationale Substantiel Personnel	UE 910/2014 eIDAS	**	EN 319 411-1	NCP+	1.2.250.1.295.1.1.8. 6.1.101.1	Authentification
LE GROUPE LA POSTE	FR	Siège : 44, boulevard de Vaugirard 75757 PARIS							
LE GROUPE LA POSTE	FR	Siège : 44, boulevard de Vaugirard 75757 PARIS	La Poste - Autorité d'horodatage	UE 910/2014 eIDAS		ETSI TS 102 023		1.2.250.1.8.1.1.1.1. 6	Horodatage (RGS_A_12)
LUXTRUST SA	LU	IVY Building 8308 CAPELLEN LUXEMBOURG							
LUXTRUST SA	LU	IVY Building 8308 CAPELLEN LUXEMBOURG	LuxTrust Global Root						Racine
LUXTRUST SA	LU	IVY Building 8308 CAPELLEN LUXEMBOURG	LuxTrust Global Root 2					1.3.171.1.1.1.10	Racine
LUXTRUST SA	LU	IVY Building 8308 CAPELLEN LUXEMBOURG	LuxTrust Global Qualified CA					1.3.171.1.1.1.10.3	Subordonnée
LUXTRUST SA	LU	IVY Building 8308 CAPELLEN LUXEMBOURG	LuxTrust Global Qualified CA 2					1.3.171.1.1.1.10.3	Subordonnée
LUXTRUST SA	LU	IVY Building 8308 CAPELLEN LUXEMBOURG	LuxTrust Global Qualified CA 3					1.3.171.1.1.1.10.3	Subordonnée
LUXTRUST SA	LU	IVY Building 8308 CAPELLEN LUXEMBOURG	LuxTrust Global Qualified CA 3	UE 910/2014 eIDAS		eIDAS Art. 51 2.	QCP+	1.3.171.1.1.10.3.1	Signature
LUXTRUST SA	LU	IVY Building 8308 CAPELLEN LUXEMBOURG	LuxTrust Global Qualified CA 3	UE 910/2014 eIDAS		eIDAS Art. 51 2.	NCP+	1.3.171.1.1.10.3.2	Authentification & Encryption

LUXTRUST SA	LU	IVY Building 8308 CAPELLEN LUXEMBOURG	LuxTrust Global Qualified CA 3	UE 910/2014 eIDAS		eIDAS Art. 51 2.	QCP	1.3.171.1.1.10.3.3	Signature
LUXTRUST SA	LU	IVY Building 8308 CAPELLEN LUXEMBOURG	LuxTrust Global Qualified CA 3	UE 910/2014 eIDAS		eIDAS Art. 51 2.	NCP	1.3.171.1.1.10.3.4	Authentification & Encryption
LUXTRUST SA	LU	IVY Building 8308 CAPELLEN LUXEMBOURG	LuxTrust Global Qualified CA 3	UE 910/2014 eIDAS		eIDAS Art. 51 2.	QCP+	1.3.171.1.1.10.3.13	Signature
LUXTRUST SA	LU	IVY Building 8308 CAPELLEN LUXEMBOURG	LuxTrust Global Qualified CA 3	UE 910/2014 eIDAS		eIDAS Art. 51 2.	NCP+	1.3.171.1.1.10.3.14	Authentification & Encryption
LUXTRUST SA	LU	IVY Building 8308 CAPELLEN LUXEMBOURG	LuxTrust Global Qualified CA 3	UE 910/2014 eIDAS		eIDAS Art. 51 2.	NCP	1.3.171.1.1.10.3.18	Qualified Seal Timestamping
LUXTRUST SA	LU	IVY Building 8308 CAPELLEN LUXEMBOURG	LuxTrust Global Qualified CA 3	UE 910/2014 eIDAS		EN 319 411-2	QCP-l-qscd	1.3.171.1.1.10.3.21	Qualified seal
LUXTRUST SA	LU	IVY Building 8308 CAPELLEN LUXEMBOURG	LuxTrust Global Qualified CA 3	UE 910/2014 eIDAS		EN 319 411-1	NCP+	1.3.171.1.1.10.3.22	Seal
LUXTRUST SA	LU	IVY Building 8308 CAPELLEN LUXEMBOURG	LuxTrust Global Qualified CA 3	UE 910/2014 eIDAS		EN 319 411-1	NCP+	1.3.171.1.1.10.3.23	Seal
LUXTRUST SA	LU	IVY Building 8308 CAPELLEN LUXEMBOURG	LuxTrust Global Qualified CA 3	UE 910/2014 eIDAS		EN 319 411-1	NCP+	1.3.171.1.1.10.3.24	Seal
LUXTRUST SA	LU	IVY Building 8308 CAPELLEN LUXEMBOURG	LuxTrust Global Qualified CA 3	UE 910/2014 eIDAS		EN 319 411-2	QCP-n-qscd	1.3.171.1.1.10.3.26	Signature
LUXTRUST SA	LU	IVY Building 8308 CAPELLEN LUXEMBOURG	LuxTrust Global Qualified CA 3	UE 910/2014 eIDAS		EN 319 411-1	NCP+	1.3.171.1.1.10.3.27	Authentication
LUXTRUST SA	LU	IVY Building 8308 CAPELLEN LUXEMBOURG	LuxTrust Global Qualified CA 3	UE 910/2014 eIDAS		EN 319 411-2	QCP-n-qscd	1.3.171.1.1.10.3.30	Signature
LUXTRUST SA	LU	IVY Building 8308 CAPELLEN LUXEMBOURG	LuxTrust Global Qualified CA 3	UE 910/2014 eIDAS		EN 319 411-1	NCP+	1.3.171.1.1.10.3.31	Authentication
LUXTRUST SA	LU	IVY Building 8308 CAPELLEN LUXEMBOURG	LuxTrust Global Qualified CA 3	UE 910/2014 eIDAS		EN 319 411-2	QCP-n-qscd	1.3.171.1.1.10.3.34	Signature
LUXTRUST SA	LU	IVY Building 8308 CAPELLEN LUXEMBOURG	LuxTrust Global Qualified CA 3	UE 910/2014 eIDAS		EN 319 411-1	NCP+	1.3.171.1.1.10.3.35	Authentication & Encryption
LUXTRUST SA	LU	IVY Building 8308 CAPELLEN LUXEMBOURG	LuxTrust SSL CA	UE 910/2014 eIDAS				1.3.171.1.1.1.10.5	Subordonnée
LUXTRUST SA	LU	IVY Building 8308 CAPELLEN LUXEMBOURG	LuxTrust SSL CA 4	UE 910/2014 eIDAS				1.3.171.1.1.1.10.5	Subordonnée

LUXTRUST SA	LU	IVY Building 8308 CAPELLEN LUXEMBOURG	LuxTrust SSL CA 5	UE 910/2014 eIDAS				1.3.171.1.1.1.10.5	Subordonnée
LUXTRUST SA	LU	IVY Building 8308 CAPELLEN LUXEMBOURG	LuxTrust SSL CA	UE 910/2014 eIDAS		EN 319 411-1	LCP	1.3.171.1.1.10.5.1	Client & Server Authentication OV
LUXTRUST SA	LU	IVY Building 8308 CAPELLEN LUXEMBOURG	LuxTrust SSL CA	UE 910/2014 eIDAS		EN 319 411-1	EVCP	1.3.171.1.1.10.5.2	Client & Server Authentication EV
LUXTRUST SA	LU	IVY Building 8308 CAPELLEN LUXEMBOURG	LuxTrust SSL CA	UE 910/2014 eIDAS		EN 319 411-2	QCP-w	1.3.171.1.1.10.5.6	Client & Server Authentication
LUXTRUST SA	LU	IVY Building 8308 CAPELLEN LUXEMBOURG	LuxTrust Global Timestamping CA			ETSI TS 102 042	LCP	1.3.171.1.1.10.8.1	Cachet Horodatage
LUXTRUST SA	LU	IVY Building 8308 CAPELLEN LUXEMBOURG	Luxtrust Time Stamp			ETSI TS 102 023		1.3.171.1.1.10.8.1.1	Horodatage
MINISTÈRE DE LA JUSTICE	FR	Siège : 13, place Vendôme 75001 PARIS							
MINISTÈRE DE LA JUSTICE	FR	Siège : 13, place Vendôme 75001 PARIS	MJ Signature 3*	UE 910/2014 eIDAS	***	ETSI TS 101 456	QCP Public+SSCD	1.2.250.1.120.2.2.1.3	Signature
MINISTÈRE DE LA JUSTICE	FR	Siège : 13, place Vendôme 75001 PARIS	MJ Authentification 3*	RGS V2.0	***	ETSI TS 102 042	NCP+	1.2.250.1.120.2.3.1.3	Authentification
SAFRAN IDENTITY AND SECURITY	FR	Siège : 11, boulevard Gallieni 92130 Issy-Les-Moulineaux							
SAFRAN IDENTITY AND SECURITY	FR	Siège : 11, boulevard Gallieni 92130 Issy-Les-Moulineaux	Dictao Service Certification Authority	UE 910/2014 eIDAS		EN 319 411-1	LCP	1.2.250.1.195.3.1.2.2	Cachet horodatage
SAFRAN IDENTITY AND SECURITY	FR	Siège : 11, boulevard Gallieni 92130 Issy-Les-Moulineaux	Dictao Service Certification Authority	UE 910/2014 eIDAS		EN 319 411-1	NCP	1.2.250.1.195.3.1.1.2	Cachet
SAFRAN IDENTITY AND SECURITY	FR	Siège : 11, boulevard Gallieni 92130 Issy-Les-Moulineaux	Dictao Instant Certification Authority N°1	UE 910/2014 eIDAS		EN 319 411-1	LCP	1.2.250.1.195.2.1.1.4	Signature
SAFRAN IDENTITY AND SECURITY	FR	Siège : 11, boulevard Gallieni 92130 Issy-Les-Moulineaux	Dictao Instant Certification Authority N°2	UE 910/2014 eIDAS		EN 319 411-1	LCP	1.2.250.1.195.5.1.1.4	Signature
SIA-Sistemas Informáticos Abiertos SA	ES	HQ: Avenida de Europa, 2 Alcor Plaza Edificio B Parque Oeste, Alcorcón 28922 MADRID							
SIA-Sistemas Informáticos Abiertos SA	ES	HQ: Avenida de Europa, 2 Alcor Plaza Edificio B Parque Oeste, Alcorcón 28922 MADRID	SIA Root CA					1.3.6.1.4.1.39131.10.1.1.1.0	Root

SIA-Sistemas Informáticos Abiertos SA	ES	HQ: Avenida de Europa, 2 Alcor Plaza Edificio B Parque Oeste, Alcorcón 28922 MADRID	SIA SUB01	UE 910/2014 eIDAS		EN 319 411-1	NCP+	1.3.6.1.4.1.39131.10.1.5	Authentication
SIA-Sistemas Informáticos Abiertos SA	ES	HQ: Avenida de Europa, 2 Alcor Plaza Edificio B Parque Oeste, Alcorcón 28922 MADRID	SIA SUB01	UE 910/2014 eIDAS		EN 319 411-2	QCP-n-qscd	1.3.6.1.4.1.39131.10.1.5	Signature
SIA-Sistemas Informáticos Abiertos SA	ES	HQ: Avenida de Europa, 2 Alcor Plaza Edificio B Parque Oeste, Alcorcón 28922 MADRID	SIA SUB01	UE 910/2014 eIDAS		EN 319 411-2	QCP-n	1.3.6.1.4.1.39131.10.1.4	*Authentication &* Signature
SIA-Sistemas Informáticos Abiertos SA	ES	HQ: Avenida de Europa, 2 Alcor Plaza Edificio B Parque Oeste, Alcorcón 28922 MADRID	SIA SUB01	UE 910/2014 eIDAS		EN 319 411-1	NCP+	1.3.6.1.4.1.39131.10.1.11	Authentication
SIA-Sistemas Informáticos Abiertos SA	ES	HQ: Avenida de Europa, 2 Alcor Plaza Edificio B Parque Oeste, Alcorcón 28922 MADRID	SIA SUB01	UE 910/2014 eIDAS		EN 319 411-2	QCP-n-qscd	1.3.6.1.4.1.39131.10.1.11	Signature
SIA-Sistemas Informáticos Abiertos SA	ES	HQ: Avenida de Europa, 2 Alcor Plaza Edificio B Parque Oeste, Alcorcón 28922 MADRID	SIA SUB01	UE 910/2014 eIDAS		EN 319 411-1	QCP-n	1.3.6.1.4.1.39131.10.1.8	Authentication & Signature
SIA-Sistemas Informáticos Abiertos SA	ES	HQ: Avenida de Europa, 2 Alcor Plaza Edificio B Parque Oeste, Alcorcón 28922 MADRID	SIA SUB01	UE 910/2014 eIDAS		EN 319 411-1	NCP+	1.3.6.1.4.1.39131.10.1.10	Authentication
SIA-Sistemas Informáticos Abiertos SA	ES	HQ: Avenida de Europa, 2 Alcor Plaza Edificio B Parque Oeste, Alcorcón 28922 MADRID	SIA SUB01	UE 910/2014 eIDAS		EN 319 411-2	QCP-n-qscd	1.3.6.1.4.1.39131.10.1.10	Signature
SIA-Sistemas Informáticos Abiertos SA	ES	HQ: Avenida de Europa, 2 Alcor Plaza Edificio B Parque Oeste, Alcorcón 28922 MADRID	SIA SUB01	UE 910/2014 eIDAS		EN 319 411-1	QCP-n	1.3.6.1.4.1.39131.10.1.2	Authentication & Signature
SIA-Sistemas Informáticos Abiertos SA	ES	HQ: Avenida de Europa, 2 Alcor Plaza Edificio B Parque Oeste, Alcorcón 28922 MADRID	SIA SUB01	UE 910/2014 eIDAS		EN 319 411-1	QCP-l	1.3.6.1.4.1.39131.10.1.12	Seal
SIA-Sistemas Informáticos Abiertos SA	ES	HQ: Avenida de Europa, 2 Alcor Plaza Edificio B Parque Oeste, Alcorcón 28922 MADRID	SIA SUB01	UE 910/2014 eIDAS		EN 319 411-1	QCP-l	1.3.6.1.4.1.39131.10.1.6	Time-Stamping
YOUSIGN	FR	Siège : 34 rue Malfilatre 14000 CAEN							

YOUSIGN	FR	Siège : 34 rue Malfilatre 14000 CAEN	YOUSIGN LSCP certificate profile	UE 910/2014 eIDAS	Néant	EN 319 411-1	LCP	1.2.250.1.302.1.5.1.0	Signature
YOUSIGN	FR	Siège : 34 rue Malfilatre 14000 CAEN	Yousign Qualified TSA	UE 910/2014 eIDAS		EN 319 421		1.2.250.1.302.1.9.1.0	Horodatage
ZETES	BE	Siège : Villalan 13 1601 Ruisbroek, Belgium							
ZETES	BE	Siège : Villalan 13 1601 Ruisbroek, Belgium	ZETES TSP Root CA 001						Root
ZETES	BE	Siège : Villalan 13 1601 Ruisbroek, Belgium	ZETES TSP Qualified CA 001						Intermediate
ZETES	BE	Siège : Villalan 13 1601 Ruisbroek, Belgium	SmartCard / Authentication	UE 910/2014 eIDAS		EN 319 411-1	NCP+	1.3.6.1.4.1.47718.1.2.2.1.10	Authentication
ZETES	BE	Siège : Villalan 13 1601 Ruisbroek, Belgium	SmartCart / Electronic Signature	UE 910/2014 eIDAS		EN 319 411-2	QCP-n-qscd	1.3.6.1.4.1.47718.1.3.2.3.10	Signature
INFORMATION SERVICES JSC	BG	Headquarter: #2 Panayot Volov Str., Sofia 1504, Bulgaria, REPUBLIC OF BULGARIA							
INFORMATION SERVICES JSC	BG	Headquarter: #2 Panayot Volov Str., Sofia 1504, Bulgaria, REPUBLIC OF BULGARIA	StampIT Global Root CA					1.3.6.1.4.1.11290.1.2	root
INFORMATION SERVICES JSC	BG	Headquarter: #2 Panayot Volov Str., Sofia 1504, Bulgaria, REPUBLIC OF BULGARIA	StampIT Global Qualified CA					1.3.6.1.4.1.11290.1.2.1	sub CA
INFORMATION SERVICES JSC	BG	Headquarter: #2 Panayot Volov Str., Sofia 1504, Bulgaria, REPUBLIC OF BULGARIA	StampIT Doc	UE 910/2014 eIDAS		EN 319 411-2	QCP-n-qscd	1.3.6.1.4.1.11290.1.2.1.3	Signature
INFORMATION SERVICES JSC	BG	Headquarter: #2 Panayot Volov Str., Sofia 1504, Bulgaria, REPUBLIC OF BULGARIA	StampIT DocPro	UE 910/2014 eIDAS		EN 319 411-2	QCP-n-qscd	1.3.6.1.4.1.11290.1.2.1.2	Signature
INFORMATION SERVICES JSC	BG	Headquarter: #2 Panayot Volov Str., Sofia 1504, Bulgaria, REPUBLIC OF BULGARIA	StampIT Seal	UE 910/2014 eIDAS		EN 319 411-2	QCP-l-qscd	1.3.6.1.4.1.11290.1.2.1.4	Seal

INFORMATION SERVICES JSC	BG	Headquarter: #2 Panayot Volov Str., Sofia 1504, Bulgaria, REPUBLIC OF BULGARIA	StampIT Enterprise	UE 910/2014 eIDAS		EN 319 411-2	QCP-n	1.3.6.1.4.1.11290.1.2.1.5	Signature
INFORMATION SERVICES JSC	BG	Headquarter: #2 Panayot Volov Str., Sofia 1504, Bulgaria, REPUBLIC OF BULGARIA	StampIT Entreprise Pro	UE 910/2014 eIDAS		EN 319 411-2	QCP-n	1.3.6.1.4.1.11290.1.2.1.6	Signature
INFORMATION SERVICES JSC	BG	Headquarter: #2 Panayot Volov Str., Sofia 1504, Bulgaria, REPUBLIC OF BULGARIA	StampIT Entreprise Seal	UE 910/2014 eIDAS		EN 319 411-2	QCP-l	1.3.6.1.4.1.11290.1.2.1.7	Seal
INFORMATION SERVICES JSC	BG	Headquarter: #2 Panayot Volov Str., Sofia 1504, Bulgaria, REPUBLIC OF BULGARIA	StampIT Global TSA	UE 910/2014 eIDAS		EN 319 421		1.3.6.1.4.1.11290.1.2.1.1	Time Stamp
INFORMATION SERVICES JSC	BG	Headquarter: #2 Panayot Volov Str., Sofia 1504, Bulgaria, REPUBLIC OF BULGARIA	StampIT Server SSL DVC	UE 910/2014 eIDAS		EN 319 411-1	DVCP	1.3.6.1.4.1.11290.1.2.1.8	Website Authentication
INFORMATION SERVICES JSC	BG	Headquarter: #2 Panayot Volov Str., Sofia 1504, Bulgaria, REPUBLIC OF BULGARIA	StampIT Server SSL OVC	UE 910/2014 eIDAS		EN 319 411-1	OVCP	1.3.6.1.4.1.11290.1.2.1.9	Website Authentication
WORLDLINE	FR	Siège : 80 Quai Voltaire 95870 Bezons France							
WORLDLINE	FR	Siège : 80 Quai Voltaire 95870 Bezons France	AC OTU Certificat à usage Signature			ETSI TS 102 043	LCP	1.2.250.1.111.1.2.7.1.1	Signature
WORLDLINE	FR	Siège : 80 Quai Voltaire 95870 Bezons France	Ac OTU Certificat à usage Cachet-serveur			ETSI TS 102 044	LCP	1.2.250.1.111.1.2.7.1.2	Seal
UNIVERSIGN	BE	Siège: 40 RUE DES ANCIENS ETANGS - 1190, FOREST – BELGIQUE							
UNIVERSIGN	BE	Siège: 40 RUE DES ANCIENS ETANGS - 1190, FOREST – BELGIQUE	Universign Primary CA hardware					1.3.6.1.4.1.15819.5.1.2.1 c3:2e:08:bd:f5:97:71:b2:c4:ad:66:63:00:59:57:f4	root

UNIVERSIGN	BE	Siège: 40 RUE DES ANCIENS ETANGS - 1190, FOREST – BELGIQUE	Universign CA hardware					1.3.6.1.4.1.15819.5.1.3.[1/3/4/5] 69:da:6c:43:7f:07:77:91:b9:91:db:e7:99:18:8a:96	sub CA
UNIVERSIGN	BE	Siège: 40 RUE DES ANCIENS ETANGS - 1190, FOREST – BELGIQUE	UNIVERSIGN Certificat Personne Physique QCP-n	UE 910/2014 eIDAS		EN 319 411-2	QCP-n	1.3.6.1.4.1.15819.5.1.3.1	Signature
UNIVERSIGN	BE	Siège: 40 RUE DES ANCIENS ETANGS - 1190, FOREST – BELGIQUE	UNIVERSIGN Certificat Personne Morale QCP-l	UE 910/2014 eIDAS		EN 319 411-2	QCP-l	1.3.6.1.4.1.15819.5.1.3.5	Seal
UNIVERSIGN	BE	Siège: 40 RUE DES ANCIENS ETANGS - 1190, FOREST – BELGIQUE	UNIVERSIGN Certificat Personne Physique LCP	UE 910/2014 eIDAS		EN 319 411-1	LCP	1.3.6.1.4.1.15819.5.1.3.3	Signature
UNIVERSIGN	BE	Siège: 40 RUE DES ANCIENS ETANGS - 1190, FOREST – BELGIQUE	UNIVERSIGN Certificat Personne Moral LCP	UE 910/2014 eIDAS		EN 319 411-1	LCP	1.3.6.1.4.1.15819.5.1.3.4	Seal
PORTIMA	BE	Siège: 150 Chaussée de la Hulpe – 1170 Bruxelles – Belgique							
PORTIMA	BE	Siège: 150 Chaussée de la Hulpe – 1170 Bruxelles – Belgique	PortiSign Root CA					1.3.6.1.4.1.10438.3.2.3.0	Root
PORTIMA	BE	Siège: 150 Chaussée de la Hulpe – 1170 Bruxelles – Belgique	PortiSign Users CA10 for Qualified Certificates	UE 910/2014 eIDAS		EN 319 411-2	QCP-n	1.3.6.1.4.1.10438.3.2.3.10	Signature
PORTIMA	BE	Siège: 150 Chaussée de la Hulpe – 1170 Bruxelles – Belgique	PortiSign Users CA11 for Qualified Certificates	UE 910/2014 eIDAS		EN 319 411-2	QCP-n	1.3.6.1.4.1.10438.3.2.3.11	Signature
E-Tugra	TR	Headquarter: Ceyhun Atuf Kansu Cad. Gözde Plaza 130/58 06520, Ankara - TURKEY							
E-Tugra	TR	Headquarter: Ceyhun Atuf Kansu Cad. Gözde Plaza 130/58 06520, Ankara - TURKEY	E-Tugra Certification Authority					6a 68 3e 9c 51 9b cb 53	Root CA
E-Tugra	TR	Headquarter: Ceyhun Atuf Kansu Cad. Gözde Plaza 130/58 06520, Ankara - TURKEY	E-Tugra qualified certificates						

E-Tugra	TR	Headquarter: Ceyhun Atuf Kansu Cad. Gözde Plaza 130/58 06520, Ankara - TURKEY	E-Tugra Domain Validated CA			EN 319 411-1	NCP+DVCP	2.16.792.3.0.4.1.1.2	Web site authentication
E-Tugra	TR	Headquarter: Ceyhun Atuf Kansu Cad. Gözde Plaza 130/58 06520, Ankara - TURKEY	E-Tugra Organisation Validated CA			EN 319 411-1	NCP+OVCP	2.16.792.3.0.4.1.1.3	Web site authentication
E-Tugra	TR	Headquarter: Ceyhun Atuf Kansu Cad. Gözde Plaza 130/58 06520, Ankara - TURKEY	E-Tugra Extended Validated CA			EN 319 411-1	EVCP + EVCG	2.16.792.3.0.4.1.1.4	Web site authentication
AGENCE NATIONALE DE LA CERTIFICATION ELECTRONIQUE	TN	Siège: Parc Technologie El Ghazala Route de Raoued Km, 3,5 2083 Ariana Tunisie							
AGENCE NATIONALE DE LA CERTIFICATION ELECTRONIQUE	TN	Siège: Parc Technologie El Ghazala Route de Raoued Km, 3,5 2083 Ariana Tunisie	Tunisian National Root CA						Root CA
AGENCE NATIONALE DE LA CERTIFICATION ELECTRONIQUE	TN	Siège: Parc Technologie El Ghazala Route de Raoued Km, 3,5 2083 Ariana Tunisie	Tunisia Gov CA					2.16.788.1.2.6.1.9	Intermediate CA
AGENCE NATIONALE DE LA CERTIFICATION ELECTRONIQUE	TN	Siège: Parc Technologie El Ghazala Route de Raoued Km, 3,5 2083 Ariana Tunisie	Tn Trust Gov CA					2.16.788.1.2.6.1.9	Sub CA
AGENCE NATIONALE DE LA CERTIFICATION ELECTRONIQUE	TN	Siège: Parc Technologie El Ghazala Route de Raoued Km, 3,5 2083 Ariana Tunisie	Tn Trust Gov CA			ETSI EN 319 411-1	OVCP	2.16.788.1.2.6.1.9.1.1	Serveur authentication
AGENCE NATIONALE DE LA CERTIFICATION ELECTRONIQUE	TN	Siège: Parc Technologie El Ghazala Route de Raoued Km, 3,5 2083 Ariana Tunisie	Tn Trust Gov CA			ETSI EN 319 411-1	EVCP	2.16.788.1.2.6.1.9.1.2	Serveur authentication
AGENCE NATIONALE DE LA CERTIFICATION ELECTRONIQUE	TN	Siège: Parc Technologie El Ghazala Route de Raoued Km, 3,5 2083 Ariana Tunisie	Tn Trust Gov CA			ETSI EN 319 411-1	OVCP	2.16.788.1.2.6.1.9.1.3	Seal
AGENCE NATIONALE DE LA CERTIFICATION ELECTRONIQUE	TN	Siège: Parc Technologie El Ghazala Route de Raoued Km, 3,5 2083 Ariana Tunisie	Tn Trust Gov CA			ETSI EN 319 411-1	EVCP	2.16.788.1.2.6.1.9.1.4	Seal
AGENCE NATIONALE DE LA CERTIFICATION ELECTRONIQUE	TN	Siège: Parc Technologie El Ghazala Route de Raoued Km, 3,5 2083 Ariana Tunisie	Tn Trust Gov CA			ETSI EN 319 411-1	NCP+	2.16.788.1.2.6.1.9.1.5	Authentication

AGENCE NATIONALE DE LA CERTIFICATION ELECTRONIQUE	TN	Siège: Parc Technologie El Ghazala Route de Raoued Km, 3,5 2083 Ariana Tunisie	Tn Trust Gov CA			ETSI EN 319 411-1	OVCP	2.16.788.1.2.6.1.9.1.6	Authentication Encryption
AGENCE NATIONALE DE LA CERTIFICATION ELECTRONIQUE	TN	Siège: Parc Technologie El Ghazala Route de Raoued Km, 3,5 2083 Ariana Tunisie	Tn Trust Gov CA			ETSI EN 319 411-1	NCP+	2.16.788.1.2.6.1.9.1.7	Seal
AGENCE NATIONALE DE LA CERTIFICATION ELECTRONIQUE	TN	Siège: Parc Technologie El Ghazala Route de Raoued Km, 3,5 2083 Ariana Tunisie	Tn Trust Qualified Gov CA					2.16.788.1.2.6.1.10	Intermediate CA
AGENCE NATIONALE DE LA CERTIFICATION ELECTRONIQUE	TN	Siège: Parc Technologie El Ghazala Route de Raoued Km, 3,5 2083 Ariana Tunisie	Tn Trust Qualified Gov CA			ETSI EN 319 411-2	QCP-n-QSignCD	2.16.788.1.2.6.1.10.1.1	Signature
AGENCE NATIONALE DE LA CERTIFICATION ELECTRONIQUE	TN	Siège: Parc Technologie El Ghazala Route de Raoued Km, 3,5 2083 Ariana Tunisie	Tn Trust Qualified Gov CA			ETSI EN 319 411-2	QCP-l-QSealCD	2.16.788.1.2.6.1.10.1.2	Seal
AGENCE NATIONALE DE LA CERTIFICATION ELECTRONIQUE	TN	Siège: Parc Technologie El Ghazala Route de Raoued Km, 3,5 2083 Ariana Tunisie	Tunisian Corporate CA					2.16.788.1.2.6.1.9	Intermediate CA
AGENCE NATIONALE DE LA CERTIFICATION ELECTRONIQUE	TN	Siège: Parc Technologie El Ghazala Route de Raoued Km, 3,5 2083 Ariana Tunisie	Tn Trust Corporate CA			ETSI EN 319 411-1		2.16.788.1.2.6.1.9	Sub CA
AGENCE NATIONALE DE LA CERTIFICATION ELECTRONIQUE	TN	Siège: Parc Technologie El Ghazala Route de Raoued Km, 3,5 2083 Ariana Tunisie	Tn Trust Corporate CA			ETSI EN 319 411-1	OVCP	2.16.788.1.2.6.1.9.2.1	Web site authentication
AGENCE NATIONALE DE LA CERTIFICATION ELECTRONIQUE	TN	Siège: Parc Technologie El Ghazala Route de Raoued Km, 3,5 2083 Ariana Tunisie	Tn Trust Corporate CA			ETSI EN 319 411-1	EVCP	2.16.788.1.2.6.1.9.2.2	Web site authentication
AGENCE NATIONALE DE LA CERTIFICATION ELECTRONIQUE	TN	Siège: Parc Technologie El Ghazala Route de Raoued Km, 3,5 2083 Ariana Tunisie	Tn Trust Corporate CA			ETSI EN 319 411-1	OVCP	2.16.788.1.2.6.1.9.2.3	Seal
AGENCE NATIONALE DE LA CERTIFICATION ELECTRONIQUE	TN	Siège: Parc Technologie El Ghazala Route de Raoued Km, 3,5 2083 Ariana Tunisie	Tn Trust Corporate CA			ETSI EN 319 411-1	EVCP	2.16.788.1.2.6.1.9.2.4	Seal
AGENCE NATIONALE DE LA CERTIFICATION ELECTRONIQUE	TN	Siège: Parc Technologie El Ghazala Route de Raoued Km, 3,5 2083 Ariana Tunisie	Tn Trust Corporate CA			ETSI EN 319 411-1	NCP+	2.16.788.1.2.6.1.9.2.5	Authentication

AGENCE NATIONALE DE LA CERTIFICATION ELECTRONIQUE	TN	Siège: Parc Technologie El Ghazala Route de Raoued Km, 3,5 2083 Ariana Tunisie	Tn Trust Corporate CA			ETSI EN 319 411-1	OVCP	2.16.788.1.2.6.1.9.2.6	Authentication and Encryption
AGENCE NATIONALE DE LA CERTIFICATION ELECTRONIQUE	TN	Siège: Parc Technologie El Ghazala Route de Raoued Km, 3,5 2083 Ariana Tunisie	TnTrust Qualified Corporate CA					2.16.788.1.2.6.1.10	Intermediate CA
AGENCE NATIONALE DE LA CERTIFICATION ELECTRONIQUE	TN	Siège: Parc Technologie El Ghazala Route de Raoued Km, 3,5 2083 Ariana Tunisie	TnTrust Qualified Corporate CA			ETSI EN 319 411-2	QCP-n-QSignCD	2.16.788.1.2.6.1.10.2.1	Signature
AGENCE NATIONALE DE LA CERTIFICATION ELECTRONIQUE	TN	Siège: Parc Technologie El Ghazala Route de Raoued Km, 3,5 2083 Ariana Tunisie	TnTrust Qualified Corporate CA			ETSI EN 319 411-2	QCP-l-QSealCD	2.16.788.1.2.6.1.10.2.2	Seal
Worldline	FR	Siège : 80 Quai Voltaire 95870 Bezons France							
Worldline	FR	Siège : 80 Quai Voltaire 95870 Bezons France	AC Racine – Root CA – 2012					1.2.250.1.111.12.0.2	
Worldline	FR	Siège : 80 Quai Voltaire 95870 Bezons France	AC OTU 3					1.2.250.1.111.17.0.3	
Worldline	FR	Siège : 80 Quai Voltaire 95870 Bezons France	Certificats à usage unique	UE 910/2014 eIDAS		ETSI EN 319 411-1	LCP	1.2.250.1.111.17.0.3.1	Signature
Worldline	FR	Siège : 80 Quai Voltaire 95870 Bezons France	Certificats d'organisation	UE 910/2014 eIDAS		ETSI EN 319 411-1	LCP	1.2.250.1.111.17.0.3.2	Signature
Worldline	FR	Siège : 80 Quai Voltaire 95870 Bezons France	Certificats à usage unique, de test	UE 910/2014 eIDAS		ETSI EN 319 411-1	LCP	1.2.250.1.111.17.0.3.3	Signature
Worldline	FR	Siège : 80 Quai Voltaire 95870 Bezons France	Certificats d'organisation, de test	UE 910/2014 eIDAS		ETSI EN 319 411-1	LCP	1.2.250.1.111.17.0.3.4	Signature
BE INVEST International SA	LU	Headquarter: 117, Route d'Arlon - 8009 Strassen - Luxembourg							
BE INVEST International SA	LU	Headquarter: 117, Route d'Arlon - 8009 Strassen - Luxembourg	ALMERYS ROOT CA					1.2.250.1.16.12.5.4 1.1.1.1	Root CA
BE INVEST International SA	LU	Headquarter: 117, Route d'Arlon - 8009 Strassen - Luxembourg	ALMERYS CUSTOMER SERVICES CA NB					1.2.250.1.16.12.5.4 1.1.5.2.1	SubCA

BE INVEST International SA	LU	Headquarter: 117, Route d'Arlon - 8009 Strassen - Luxembourg	ALMERYS CUSTOMER SERVICES CA NB	UE 910/2014 eIDAS		ETSI EN 319 411-1	LCP	1.3.6.1.4.1.48620.4 1.1.5.2.1.1.1	Cachet Serveur
BE INVEST International SA	LU	Headquarter: 117, Route d'Arlon - 8009 Strassen - Luxembourg	ALMERYS CUSTOMER SERVICES CA NB	UE 910/2014 eIDAS		ETSI EN 319 411-1	LCP	1.3.6.1.4.1.48620.4 1.1.5.2.1.2.1	Cachet d'horodatage
BE INVEST International SA	LU	Headquarter: 117, Route d'Arlon - 8009 Strassen - Luxembourg	ALMERYS USER SIGNING CA NB					1.2.250.1.16.12.5.4 1.1.4.2.1	SubCA
BE INVEST International SA	LU	Headquarter: 117, Route d'Arlon - 8009 Strassen - Luxembourg	ALMERYS USER SIGNING CA NB	UE 910/2014 eIDAS		ETSI EN 319 411-1	LCP	1.3.6.1.4.1.48620.4 1.1.4.2.1.1.1	Signature
BE INVEST International SA	LU	Headquarter: 117, Route d'Arlon - 8009 Strassen - Luxembourg	ALMERYS SIGNATURE AND AUTHENTICATION CA NC					1.2.250.1.16.12.5.4 1.1.7.3.1	SubCA
BE INVEST International SA	LU	Headquarter: 117, Route d'Arlon - 8009 Strassen - Luxembourg	ALMERYS SIGNATURE AND AUTHENTICATION CA NC	UE 910/2014 eIDAS		ETSI EN 319 411-2	QCP+	1.3.6.1.4.1.48620.4 1.1.7.3.1.1.1	Signature
BE INVEST International SA	LU	Headquarter: 117, Route d'Arlon - 8009 Strassen - Luxembourg	ALMERYS SIGNATURE AND AUTHENTICATION CA NC	UE 910/2014 eIDAS		ETSI EN 319 411-1	NCP+	1.3.6.1.4.1.48620.4 1.1.7.3.1.2.1	Authentification & Signature
BE INVEST International SA	LU	Headquarter: 117, Route d'Arlon - 8009 Strassen - Luxembourg	ALMERYS AUTORITE D'HORODATAGE	UE 910/2014 eIDAS		ETSI EN 319 411-2	QCP-l	1.3.6.1.4.1.48620.4 1.1.7.3.1.5.1	Cachet d'horodatage
BE INVEST International SA	LU	Headquarter: 117, Route d'Arlon - 8009 Strassen - Luxembourg	ALMERYS SIGNATURE AND AUTHENTICATION CA NC	UE 910/2014 eIDAS		ETSI EN 319 411-2	QCP-l	1.3.6.1.4.1.48620.4 1.1.7.3.1.4.1	Cachet Signature
LEX PERSONA	FR	Technopole de l'Aube en Champagne 10901 TROYES CEDEX 9							
LEX PERSONA	FR	Technopole de l'Aube en Champagne 10901 TROYES CEDEX 10	AC racine Sunnystamp Root CA G2	UE 910/2014 eIDAS				59:85:f1:be:67:98:8a: b6	

LEX PERSONA	FR	Technopole de l'Aube en Champagne 10901 TROYES CEDEX 11	Sunnystamp Natural Persons CA	UE 910/2014 eIDAS		ETSI EN 319 411-1	LCP	1.3.6.1.4.1.22542.100.1.1.1.2	signature
LEX PERSONA	FR	Technopole de l'Aube en Champagne 10901 TROYES CEDEX 12	Sunnystamp Legal Persons CA	UE 910/2014 eIDAS		ETSI EN 319 411-1	NCP+	1.3.6.1.4.1.22542.100.1.1.2.1	seal
LEX PERSONA	FR	Technopole de l'Aube en Champagne 10901 TROYES CEDEX 13	Sunnystamp Legal Persons CA	UE 910/2014 eIDAS		ETSI EN 319 411-1	NCP+	1.3.6.1.4.1.22542.100.1.1.2.2	seal
System for electronic payments (SEP) bulgaria JSC	BG	#1, ZLATOVRAH STR, SOFIA 1164, REPUBLIC OF BULGARIA							
System for electronic payments (SEP) bulgaria JSC	BG	#1, ZLATOVRAH STR, SOFIA 1164, REPUBLIC OF BULGARIA	eSign Sep Root CA	EU 910/2014 eIDAS				Serial number Hex 4B:BB:1A:09:7D:BD:25:52 OID:1.3.6.1.4.1.30299.3	Root
System for electronic payments (SEP) bulgaria JSC	BG	#1, ZLATOVRAH STR, SOFIA 1164, REPUBLIC OF BULGARIA	eSign Sep QES CA	EU 910/2014 eIDAS				Serial number Hex 46:5D:25:53:D1:97:54:90 OID:1.3.6.1.4.1.30299.3.1	Sub CA
System for electronic payments (SEP) bulgaria JSC	BG	#1, ZLATOVRAH STR, SOFIA 1164, REPUBLIC OF BULGARIA	eSign Sep OCSP	EU 910/2014 eIDAS				Serial number Hex 1E:56:70:DD:49:78:87:83 OID:1.3.6.1.4.1.30299.3.1.1	OCSP
System for electronic payments (SEP) bulgaria JSC	BG	#1, ZLATOVRAH STR, SOFIA 1164, REPUBLIC OF BULGARIA	eSign QES Natural	EU 910/2014 eIDAS		ETSI EN 319 411-2	QCP-n-qscd	OID:1.3.6.1.4.1.30299.3.1.3	Signature
System for electronic payments (SEP) bulgaria JSC	BG	#1, ZLATOVRAH STR, SOFIA 1164, REPUBLIC OF BULGARIA	eSign QES Delegated	EU 910/2014 eIDAS		ETSI EN 319 411-2	QCP-n-qscd	OID:1.3.6.1.4.1.30299.3.1.4	Signature
System for electronic payments (SEP) bulgaria JSC	BG	#1, ZLATOVRAH STR, SOFIA 1164, REPUBLIC OF BULGARIA	eSign QESeal	EU 910/2014 eIDAS		ETSI EN 319 411-2	QCP-l	OID:1.3.6.1.4.1.30299.3.1.5	Seal

System for electronic payments (SEP) bulgaria JSC	BG	#1, ZLATOVRAH STR, SOFIA 1164, REPUBLIC OF BULGARIA	eSign Sep TSA	EU 910/2014 eIDAS		ETSI EN 319 421	TSA	OID:1.3.6.1.4.1.30299.3.1.2	Time Stamp
Quicksign	FR	14 Avenue de l'Opéra 75001 PARIS France		EU 910/2014 eIDAS					Autorité d'enregistrement
Keynectis - Idnomic	FR	175, Rue Jean Jacques Rousseau 92130 ISSY-LES-MOULINEAUX France		EU 910/2014 eIDAS					Opérateur de certification
BNP PARIBAS	FR	16 Boulevard des Italiens 75009 PARIS							
BNP PARIBAS	FR	17 Boulevard des Italiens 75009 PARIS	BNP Paribas Group Customer Ephemeral Certification Authority 1	EU 910/2014 eIDAS		ETSI EN 319 411-1	LCP	OID= 1.2.250.1.195.10.3.1.1.2	Signature
BNP PARIBAS	FR	18 Boulevard des Italiens 75009 PARIS	BNP Paribas Group Customer Ephemeral Certification Authority 2	EU 910/2014 eIDAS		ETSI EN 319 411-1	LCP	OID= 1.2.250.1.195.10.4.1.1.2	Signature
BNP PARIBAS	FR	19 Boulevard des Italiens 75009 PARIS	BNP Paribas Group Sealing and Timestamping	EU 910/2014 eIDAS		ETSI EN 319 411-1	NCP	OID=1.2.250.1.195.10.5.1.1.2	Cachet serveur
BNP PARIBAS	FR	20 Boulevard des Italiens 75009 PARIS	BNP Paribas Group Sealing and Timestamping	EU 910/2014 eIDAS		ETSI EN 319 411-1	NCP	OID=1.2.250.1.195.10.5.1.2.2	cachet horodatage
BNP PARIBAS	FR	21 Boulevard des Italiens 75009 PARIS	BNP Paribas Fortis Customer Ephemeral Certification Authority 1	EU 910/2014 eIDAS		ETSI EN 319 411-1	LCP	OID= 1.2.250.1.195.10.7.1.1.2	Signature
BNP PARIBAS	FR	22 Boulevard des Italiens 75009 PARIS	BNP Paribas Fortis Customer Ephemeral Certification Authority 2	EU 910/2014 eIDAS		ETSI EN 319 411-1	LCP	OID= 1.2.250.1.195.10.8.1.1.2	Signature
COMMFIDES NORGE AS	N W	Postboks 405 - 1327 Lysaker - Norway							
COMMFIDES NORGE AS	N W	Postboks 405 - 1327 Lysaker - Norway	CPN RootCA SHA256 Class 3					64653815F10A6EFA	Root
COMMFIDES NORGE AS	N W	Postboks 405 - 1327 Lysaker - Norway	CPN Person High SHA256 CLASS 3					524C7FFB8C17C39B	SubCA

COMMFIDES NORGE AS	N W	Postboks 405 - 1327 Lysaker - Norway	Legal - Central	EU 910/2014 eIDAS		ETSI EN 319 411-1	LCP	2.16.578.1.29.13.30	Electronic Signature
COMMFIDES NORGE AS	N W	Postboks 405 - 1327 Lysaker - Norway		EU 910/2014 eIDAS		ETSI EN 319 411-1	LCP	2.16.578.1.29.13.31	Electronic Signature
COMMFIDES NORGE AS	N W	Postboks 405 - 1327 Lysaker - Norway				ETSI EN 319 411-1	LCP	2.16.578.1.29.13.32	Encryption
INCERT GIE	LX	LOFT 2.0, AM BANN 2, RUE DROSBACH L-3372 LEUDELANGE - Luxembourg		EU 910/2014 eIDAS					opérateur de certification
AR24	FR	17 RUE DE LA HAUTE MONTEE 67000 STRASBOURG - France		EU 910/2014 eIDAS					e-delivery
IMPRIMERIE NATIONALE	FR	104 AVENUE DU PRESIDENT KENNEDY 75016 PARIS France							
IMPRIMERIE NATIONALE	FR	105 AVENUE DU PRESIDENT KENNEDY 75016 PARIS France	AC Imprimerie Nationale Racine					2.5.29.32.0	AC Racine
IMPRIMERIE NATIONALE	FR	106 AVENUE DU PRESIDENT KENNEDY 75016 PARIS France	AC Imprimerie Nationale Elevé Personnel					2.5.29.32.0	AC Intermédiaire
IMPRIMERIE NATIONALE	FR	107 AVENUE DU PRESIDENT KENNEDY 75016 PARIS France	AC Imprimerie Nationale Elevé Personnel	EU 910/2014 eIDAS	***	ETSI EN 319 411-2	QCP-n_QSCD	1.2.250.1.295.1.1.2 0.7.1.102.1	Signature
IMPRIMERIE NATIONALE	FR	108 AVENUE DU PRESIDENT KENNEDY 75016 PARIS France	AC Imprimerie Nationale Subtantiel Personnel					2.5.29.32.0	AC intermédiaire
IMPRIMERIE NATIONALE	FR	109 AVENUE DU PRESIDENT KENNEDY 75016 PARIS France	AC Imprimerie Nationale Subtantiel Personnel	EU 910/2014 eIDAS	**	ETSI EN 319 411-2	QCP-n_QSCD	1.2.250.1.295.1.1.8. 6.1.102.1	Signature
IMPRIMERIE NATIONALE	FR	110 AVENUE DU PRESIDENT KENNEDY 75016 PARIS France	AC Imprimerie Nationale Subtantiel Personnel	EU 910/2014 eIDAS	**	ETSI EN 319 411-1	NCP+	1.2.250.1.295.1.1.8. 6.1.101.1	Authentification
VIALINK	FR	18 QUAI DE LA RAPEE 75012 PARIS - France	VIALINK EU TRUSTED CA	EU 910/2014 eIDAS		ETSI EN 319 411-1	LCP	1.2.250.1.198.2.1.2. 1.0.1	Signature

II. Liste de référence des produits de sécurité qualifiés

LES PRODUITS

DÉVELOPPEUR	PRODUIT QUALIFIÉ	INFORMATIONS	ATTESTATIONS DE SÉCURITÉ
Thales	Boitier MISTRAL CORPORATE TRC 7535 version 4.7.0.2	Solution matérielle	Qualification - Niveau Standard (01/2012) Certification Critères Communs EAL3+ (01/2010)
Thales	Boitier MISTRAL GIGABIT, TRC 7539-11A version 7.0.1	Solution matérielle	Qualification - Niveau Standard (01/2012) Certification Critères Communs EAL3+ (01/2010)
Thales	Boitier MISTRAL TRC 7535 version 4.5.2.2	Solution matérielle	Qualification - Niveau Standard (06/2005) Certification Critères Communs EAL3+ (05/2005)
Thales	Boitier MISTRAL TRC 7535 version 4.6.1	Solution matérielle	Qualification - Niveau Standard (03/2008) Certification Critères Communs EAL3+ (03/2008)
Thales	Boitier MISTRAL TRC 7535 version 4.6.2	Solution matérielle	Qualification - Niveau Standard (09/2008) Certification Critères Communs EAL3+ (03/2008)
Stormshield	FW-VPN Stormshield SNS v2.2.6	Suite logicielle	Qualification - Niveau Standard (02/2017) Qualification - Niveau Standard (10/2016)
NETASQ	NETASQ v9.1.0.5	Solution matérielle et logicielle	Qualification - Niveau Standard (01/2015)
NETASQ	Suite logicielle IPS-Firewall pour boîtiers appliances NETASQ, version 8.0.1.1	Solution logicielle	Qualification - Niveau Standard (07/2009) Certification Critères Communs EAL3+ (07/2009)
TheGreenBow	TheGreenBow VPN Client 5.2	solution logicielle	Qualification - Niveau Standard (01/2015) Certification Critères Communs EAL3+ (12/2014)
Bull	Trustway VPN Appliance v3.01.06	Solution matérielle	Qualification - Niveau Standard (09/2004) Certification Critères Communs EAL2+ (09/2004)
Bull	Trustway VPN Line	Solution matérielle	Qualification - Niveau Standard (04/2009) Certification Critères Communs EAL2+ (04/2009)

CHIFFREMENT DE LIENS

DÉVELOPPEUR	PRODUIT QUALIFIÉ	INFORMATIONS	ATTESTATIONS DE SÉCURITÉ
Nokia	Nokia 9500 Microwave PacketRadio en version 07.01.08		Qualification - Niveau Standard (12/2017) Certification Critères Communs EAL3+ (10/2017)

CONTRÔLE D'ACCÈS PHYSIQUE

DÉVELOPPEUR	PRODUIT QUALIFIÉ	INFORMATIONS	ATTESTATIONS DE SÉCURITÉ
Gunnebo SMI version CSPN-01-01			Qualification - Niveau Elementaire (04/2017) Certification CSPN (03/2017)

EQUIPEMENT INDUSTRIEL

DÉVELOPPEUR	PRODUIT QUALIFIÉ	INFORMATIONS	ATTESTATIONS DE SÉCURITÉ
Siemens	Gamme Simatic S7-1500	PLC (Programmable Logic Controller)	Qualification - Niveau Elementaire (11/2017) Certification CSPN (10/2017)
Siemens	Simatic S7-1518-4	PLC (Programmable Logic Controller)	Qualification - Niveau Elementaire (05/2016) Certification CSPN (04/2016)

IDENTIFICATION, AUTHENTIFICATION ET CONTRÔLE D'ACCÈS

DÉVELOPPEUR	PRODUIT QUALIFIÉ	INFORMATIONS	ATTESTATIONS DE SÉCURITÉ
Systancia	IPdiva Secure – version 8.0 (build 8.1066, patch IPD-15934)		Qualification - Niveau Elementaire (09/2016) Certification CSPN (05/2016)

INFRASTRUCTURES DE GESTION DE CLÉS (IGC)

DÉVELOPPEUR	PRODUIT QUALIFIÉ	INFORMATIONS	ATTESTATIONS DE SÉCURITÉ
Bull	MetaPKI en version 9.2.5	Solution logicielle	Qualification - Niveau Standard (02/2013) Certification Critères Communs EAL3+ (12/2012)
Keynectis	Sequoia v2	Solution logicielle	Qualification - Niveau Standard (10/2010) Certification Critères Communs EAL4+ (09/2010)

PARE-FEU

DÉVELOPPEUR	PRODUIT QUALIFIÉ	INFORMATIONS	ATTESTATIONS DE SÉCURITÉ
ARKOON Network Security	Fast Firewall v3.0/11	Solution matérielle et logicielle	Qualification - Niveau Standard (12/2004) Certification Critères Communs EAL2+ (11/2004)
ARKOON Network Security	FAST360 v5.0/22	Solution matérielle et logicielle	Qualification - Niveau Standard (11/2011) Certification Critères Communs EAL3+ (10/2011)
Stormshield	FW-VPN Stormshield SNS v2.2.6	Suite logicielle	Qualification - Niveau Standard (02/2017) Qualification - Niveau Standard (10/2016) Certification Critères Communs EAL3+ (08/2016)
DenyAll	i-Suite – version 5.5.5 révision 21873	Solution logicielle	Qualification - Niveau Elémentaire (01/2016) Certification CSPN (09/2014)
Stonesoft	Logiciel IPS Stonegate version 5.4.1 sur appliance Stonegate IPS-1205	Solution matérielle et logicielle	Qualification - Niveau Elémentaire (03/2013) Certification CSPN (02/2013)
NETASQ	NETASQ v9.1.0.5	Solution matérielle et logicielle	Qualification - Niveau Standard (01/2015)

DenyAll	rWeb – version 4.1 Feature Pack 1	Solution logicielle	Qualification - Niveau Elémentaire (10/2013) Certification CSPN (06/2013)
Stonesoft	StoneGate Firewall/VPN 5.2.4 build 8069	Solution matérielle et logicielle	Qualification - Niveau Elémentaire (12/2011) Certification CSPN (12/2011)
NETASQ	Suite logicielle IPS Firewall v5	Solution matérielle et logicielle	Qualification - Niveau Standard (03/2005) Certification Critères Communs EAL2+ (03/2005)
NETASQ	Suite logicielle IPS-Firewall pour boîtiers appliances NETASQ, version 8.0.1.1	Solution logicielle	Qualification - Niveau Standard (07/2009) Certification Critères Communs EAL3+ (07/2009)
NETASQ	Suite logicielle IPS-Firewall pour boîtiers appliances NETASQ, version 8.1.3	Solution logicielle et materielle	Qualification - Niveau Standard (07/2012) Certification Critères Communs EAL3+ (06/2012)
Stormshield	Suite logicielle Stormshield Network Security Pare-feu Industriel version 2.3.4 embarquée dans le boîtier pare-feu industriel SNi40	Solution logicielle et materielle	Qualification - Niveau Elémentaire (11/2016) Certification CSPN (07/2016)

PROTECTION DU POSTE DE TRAVAIL

DÉVELOPPEUR	PRODUIT QUALIFIÉ	INFORMATIONS	ATTESTATIONS DE SÉCURITÉ
Blancco	Blancco Data Cleaner+ version 4.8	solution logicielle d'effacement de données	Qualification - Niveau Elémentaire (08/2009) Certification CSPN (11/2008)
Prim'x Technologies	Cryhod	solution logicielle	Qualification - Niveau Standard (08/2011)
Ingenico Healthcare/e-ID	Lecteur sécurisé de carte avec interface homme machine LEO V2, référence PPD001-003-AXY, version PK08.12	Solution logicielle et matérielle	Qualification - Niveau Standard (09/2012) Certification Critères Communs EAL3+ (07/2012)
ARKOON Network Security	Security Box Entreprise – chiffrement transparent de fichier- v.8.0	Solution logicielle	Qualification - Niveau Standard (04/2012) Certification Critères Communs EAL3+ (04/2012)
Stormshield	STORMSHIELD Data Security (SDS)	solution logiciel	Qualification - Niveau Standard (06/2017) Certification Critères Communs EAL3+ (09/2016)
TrueCrypt Foundation	TrueCrypt version 6.0a	solution logicielle de stockage sécurisé	Qualification - Niveau Elémentaire (08/2009) Certification CSPN (12/2008)
Prim'x Technologies	Zed ! v6.1	Solution logicielle	Qualification - Niveau Standard (06/2016) Certification Critères Communs EAL3+ (05/2016)
Prim'x Technologies	Zed!	Solution logicielle	Qualification - Niveau Standard (08/2010) Certification Critères Communs EAL3+ (07/2010)
Prim'x Technologies	Zone Central v3.1	Solution logicielle	Qualification - Niveau Standard (12/2008)
Prim'x Technologies	ZoneCentral v5.0 build 960	Solution logicielle	Qualification - Niveau Standard (03/2012)

Prim'x Technologies	ZonePoint 3.0 build 330	Solution logicielle	Qualification - Niveau Standard (06/2014) Certification Critères Communs EAL3+ (04/2014)

RESSOURCES CRYPTOGRAPHIQUES

DÉVELOPPEUR	PRODUIT QUALIFIÉ	INFORMATIONS	ATTESTATIONS DE SÉCURITÉ
GEMALTO	Application IAS V4 sur la plateforme JavaCard ouverte MultiApp V3 masquée sur le composant M7820 A11 (version du patch 1.5)		Qualification - Niveau Renforcé (07/2014) Certification Critères Communs EAL5+ (02/2014)
Bull	Carte cryptographique TrustWay PCI S302	Solution matérielle	Qualification - Niveau Standard (01/2005) Certification Critères Communs EAL4+ (11/2004)
Bull	Carte cryptographique TrustWay PCI S507 et S709	Solution matérielle	Qualification - Niveau Renforcé (04/2010) Certification Critères Communs EAL4+ (03/2010)
Oberthur Technologies	Carte ID-One citizen IAS-ECC v1.0.1 sur ID-One Cosmo v7.0.1-n	Carte à puce	Qualification - Niveau Renforcé (11/2010) Certification Critères Communs EAL4+ (10/2010)
Oberthur Technologies	Carte ID-One IAS-ECC v1.0.1 R1 sur ID-One Cosmo v7.0-a et v7.0-n	Carte à puce	Qualification - Niveau Renforcé (12/2010) Certification Critères Communs EAL4+ (06/2010)
SAGEM Sécurité	Carte IdealCitiz	Carte à puce	Qualification - Niveau Renforcé (05/2012) Certification Critères Communs EAL5+ (04/2010)
SAGEM Sécurité	Carte Morpho-Citiz32 sur composant Atmel	Carte à puce	Qualification - Niveau Renforcé (08/2009) Qualification - Niveau Standard (02/2008) Certification Critères Communs EAL4+ (09/2007)
SAGEM Sécurité	Carte Morpho-Citiz32 sur composant NXP	Carte à puce	Qualification - Niveau Renforcé (08/2009) Qualification - Niveau Standard (02/2008) Certification Critères Communs EAL4+ (09/2007)
Morpho	Carte VITALE 2 – Application ADELE et VITALE Composant SB23ZL48 masqué par le logiciel SESAM VITALE v1.0.1 avec correctif version 1	Carte à puce	Qualification - Niveau Renforcé (11/2012) Qualification - Niveau Renforcé (11/2012) Certification Critères Communs EAL4+ (06/2012)
Morpho	Carte à puce CC Ideal Citiz versions 1.6.0 et 1.6.1 (applications passeport ICAO EAC et IAS ECC)	Carte à puce	Qualification - Niveau Renforcé (05/2012) Certification Critères Communs EAL5+ (11/2011)
GEMALTO	Cartes MultiApp IAS ECC	cartes à puce	Qualification - Niveau Renforcé (08/2010) Qualification - Niveau Renforcé (03/2010) Certification Critères Communs EAL4+ (02/2010)

Bull	CRYPT2Protect version 8.04-03i	Solution matérielle et logicielle	Qualification - Niveau Elémentaire (05/2012)
Atos	HSM TRUSTWAY PROTECCIO – Système : X130, Module de sécurité V128	Solution matérielle	Qualification - Niveau Renforcé (01/2016) Certification Critères Communs EAL4+ (02/2016)
ARKOON Network Security	Librairie Security BOX Crypto 6.0	Solution logicielle	Qualification - Niveau Standard (07/2004) Certification Critères Communs EAL4+ (05/2004)

SIGNATURE ÉLECTRONIQUE ET GESTION DE LA PREUVE

DÉVELOPPEUR	PRODUIT QUALIFIÉ	INFORMATIONS	ATTESTATIONS DE SÉCURITÉ
DICTAO	AdSigner v5.0.0.1		Qualification - Niveau Standard (06/2012) Certification Critères Communs EAL3+ (06/2012)
DICTAO	AdSignerWeb v3.1.800	Plate-forme de signature électronique	Qualification - Niveau Standard (05/2006) Certification Critères Communs EAL3+ (04/2006)
France Télécom	Applatoo	Plate-forme de signature électronique	Qualification - Niveau Standard (05/2005) Certification Critères Communs EAL2+ (04/2005)
DICTAO	Dictao Validation Server v4.0.6	Serveur de validation de signature	Qualification - Niveau Standard (11/2007) Certification Critères Communs EAL3+ (10/2007)
Caisse des dépots et consignation	FastSignature v1.1	Module de signature électronique	Qualification - Niveau Standard (12/2008) Certification Critères Communs EAL2+ (12/2008)

TITRES D'IDENTITÉ ÉLECTRONIQUES

DÉVELOPPEUR	PRODUIT QUALIFIÉ	INFORMATIONS	ATTESTATIONS DE SÉCURITÉ
Oberthur Technologies	[MINOS] ID-One eIDAS v1.0 en configuration SSCD-2, SSCD-3, SSCD-4, SSCD-S, SSCD-6 sur les composants P60x080PVC/PVG	Carte à puce	Qualification - Niveau Renforcé (09/2016) Certification Critères Communs EAL5+ (05/2016)
Oberthur Technologies	[MINOS] ID-One eIDAS v1.0 en configuration SSCD-2, SSCD-3, SSCD-4, SSCD-S, SSCD-6 sur les composants P60x144PVA/PVE	Carte à puce	Qualification - Niveau Renforcé (09/2016) Certification Critères Communs EAL5+ (06/2016)
Oberthur Technologies	[MINOS] ID-one ePass Full EAC v2 MRTD sur les composants P60x080PVC/PVG en configuration PACE avec AA, CA et PACE CAM, EAC et PACE avec AA, EAC avec AA	Carte à puce	Qualification - Niveau Renforcé (09/2016) Certification Critères Communs EAL5+ (06/2016)

Oberthur Technologies	[MINOS] ID-one ePass Full EAC v2 MRTD sur les composants P60x144PVAPVE en configuration PACE avec AA, CA et PACE CAM, EAC et PACE avec AA, EAC avec AA	Carte à puce	Qualification - Niveau Renforcé (09/2016) Certification Critères Communs EAL5+ (06/2016)
GEMALTO	Application eTravel EAC v2.1, en configuration SAC, sur la carte à puce fermée MultiApp V3.1 masquée sur le composant P60D080PVC (Version du patch : 1.4)	Carte à puce	Qualification - Niveau Renforcé (09/2016) Qualification - Niveau Renforcé (09/2016) Certification Critères Communs EAL5+ (02/2015)
GEMALTO	Application IAS V4 sur la plateforme JavaCard ouverte MultiApp V3 masquée sur le composant M7820 A11 (version du patch 7.0 ou 1.5) – Version application IAS : 4.0.2.K – Version application MOCA Server : 1.0 – Version plateforme JavaCard MultiApp : 3.0	Carte à puce	Qualification - Niveau Renforcé (10/2016) Qualification - Niveau Renforcé (09/2016) Certification Critères Communs EAL5+ (02/2014)
GEMALTO	Application IAS V4.2 sur la plateforme JavaCard ouverte MultiApp V3.1 144K masquée sur le composant P60D144PVA (version du patch 1.3) – Version de l'application IAS : 4.0.2.B, Version de l'application MOCA Server : 1.0, Version de la plateforme JavaCard MultiApp : 3.1	Cartes à puce	Qualification - Niveau Renforcé (09/2016) Certification Critères Communs EAL5+ (02/2016)
GEMALTO	Application IAS V4.2 sur la plateforme JavaCard ouverte MultiApp V3.1 masquée sur le composant P60D080PVC (version du patch 1.4) – Version de l'application IAS : 4.0.2.B, Version de l'application MOCA Server : 1.0, Version de la plateforme JavaCard MultiApp : 3.1	Cartes à puce	Qualification - Niveau Renforcé (09/2016) Certification Critères Communs EAL5+ (03/2015)
GEMALTO	Applications eTravel EAC v2.1 en configuration « EAC on SAC » sur la plateforme JavaCard ouverte ou fermée MultiApp V3.1 masquée sur le composant P60D144PVA (version du patch 1.3)	Cartes à puce	Qualification - Niveau Renforcé (09/2016) Certification Critères Communs EAL5+ (09/2015)
GEMALTO	Applications eTravel Essential 1.0, avec SAC, AA et EAC activés, sur composant M7794 A12/G12	Carte à puce	Qualification - Niveau Renforcé (09/2016) Certification Critères Communs EAL5+ (09/2015)
Morpho	Carte CC Ideal Citiz en versions 1.6.0 et 1.6.1, pour ses fonctions IAS ECC et ICAO EAS sur les microcontrôleurs SB23YR80B et SB23YR48B	Carte à puce	Qualification - Niveau Renforcé (05/2012) Certification Critères Communs EAL5+ (11/2011)

Oberthur Technologies	Carte IAS ECC v1.0.1 : applet version 6179 sur ID-One Cosmo v7.0.1-n R2.0, masquée sur composants NXP P5CC081 et P5CD081, en configuration Standard ou Standard Dual		Qualification - Niveau Renforcé (09/2016) Certification Critères Communs EAL4+ (02/2014)
Morpho	Carte VITALE 2 – Application ADELE – Composant AT90SC24036RCV masqué par le logiciel SESAM VITALE v1.0.1 avec correctif version 1	Carte à puce	Qualification - Niveau Renforcé (09/2016) Certification Critères Communs EAL4+ (05/2013)
Morpho	Carte VITALE 2 – Application VITALE : Composant SB23ZL48 masqué par le logiciel SESAM VITALE v1.04 avec correctif version		Qualification - Niveau Renforcé (09/2016) Certification Critères Communs EAL4+ (10/2015)
GEMALTO	ePassport Sealys eTravel EAC v. 1.1	Logiciel embarqué sur microcontrôleur	Qualification - Niveau Renforcé (08/2009) Qualification - Niveau Standard (01/2009) Certification Critères Communs EAL4+ (12/2008)
GEMALTO	eTravel EAC v1.0	Logiciel embarqué sur microcontrôleur	Qualification - Niveau Renforcé (08/2009) Certification Critères Communs EAL4+ (07/2009)
GEMALTO	eTravel Essential 1.1, PACE, EAC and AA activated sur composant S/Msarvc S3FT9MF		Qualification - Niveau Renforcé (06/2017) Certification Critères Communs EAL5+ (03/2017)
Oberthur Technologies	ID One ePASS v2.1	Logiciel embarqué sur microcontrôleur	Qualification - Niveau Renforcé (08/2009) Certification Critères Communs EAL4+ (07/2009)
Oberthur Technologies	ID-One EPass 64 v2.0	Logiciel embarqué sur microcontrôleur	Qualification - Niveau Renforcé (08/2009) Qualification - Niveau Standard (09/2008) Certification Critères Communs EAL4+ (05/2008)
Oberthur Technologies	ID-One ePass Full EAC v2 MRTD en configuration EAC et PACE avec AA masqué sur le composant P60x080PVC/PVG		Qualification - Niveau Renforcé (04/2017) Certification Critères Communs EAL5+ (06/2016)
Oberthur Technologies	ID-One ePass Full EAC v2 MRTD en configuration EAC et PACE avec AA masqué sur le composant P60x144PVA/PVE		Qualification - Niveau Renforcé (05/2017) Certification Critères Communs EAL5+ (06/2016)
Morpho	IDeal PASS V2 EAC avec PACE		Qualification - Niveau Renforcé (09/2016) Certification Critères Communs EAL5+ (07/2014)
Safran	IDeal PASS, version 2.0.1 – Application EAC with PACE		Qualification - Niveau Renforcé (03/2017) Certification Critères Communs EAL5+ (02/2017)

ARKOON Network Security	Morpho-ePass V3	Logiciel embarqué sur microcontrôleur	Qualification - Niveau Renforcé (08/2009) Qualification - Niveau Standard (09/2008) Certification Critères Communs EAL4+ (07/2008)
SAGEM Sécurité	MorphoePass V1.1.0	Logiciel embarqué sur microcontrôleur	Qualification - Niveau Renforcé (09/2009) Certification Critères Communs EAL4+ (07/2009)

VISIO-CONFÉRENCE SÉCURISÉE

DÉVELOPPEUR	PRODUIT QUALIFIÉ	INFORMATIONS	ATTESTATIONS DE SÉCURITÉ
Tixeo	Tixeo Server version 11.5.2.0		Qualification - Niveau Elémentaire (04/2017) Certification CSPN (03/2017)

ANNEXE 4

Liste nationale des prestataires de services de confiance qualifiés eIDAS

Historique des versions		
Date	**Version**	**Évolution du document**
	1.0	Publication de la première version de la liste nationale des prestataires de services de confiance qualifiés eIDAS

TSL Scheme Information

TSL Id *ID0001*

TSLTag *http://uri.etsi.org/19612/TSLTag*

TSL Version Identifier *5*

TSL Sequence Number *42*

TSL Type *http://uri.etsi.org/TrstSvc/TrustedList/TSLType/EUgeneric*

Scheme Operator Name

Name	*[en]*	*French Network Information Security Agency*
Name	*[fr]*	*Agence nationale de la sécurité des systèmes d'information (ANSSI)*

PostalAddress

Street Address	*[fr]*	*51 boulevard de La Tour-Maubourg*
Locality	*[fr]*	*Paris Cedex 07*
Postal Code	*[fr]*	*75700*
Country Name	*[fr]*	*FR*

PostalAddress

Street Address	*[en]*	*51 boulevard de La Tour-Maubourg*
Locality	*[en]*	*Paris Cedex 07*
Postal Code	*[en]*	*75700*
Country Name	*[en]*	*FR*

ElectronicAddress

URI	*mailto:supervision-eidas@ssi.gouv.fr*
URI	*http://www.ssi.gouv.fr/en*
URI	*mailto:supervision-eidas@ssi.gouv.fr*
URI	*http://www.ssi.gouv.fr*

Scheme Name

Name *[en]* *FR:Trusted list including information related to the qualified trust service providers which are supervised by the issuing Member State, together with information related to the qualified trust services provided by them, in accordance with the relevant provisions laid down in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.*

Name *[fr]* *FR:Liste de confiance comprenant des informations relatives aux prestataires de services de confiance qualifiés qui sont contrôlés par l'État membre émetteur, ainsi que les informations relatives aux services de confiance qualifiés qu'ils fournissent, conformément aux dispositions pertinentes établies par le règlement (UE) no 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE.*

Scheme Information URI

URI *[en]* *http://ssi.gouv.fr/eidas/tl/en*

URI *[fr]* *http://ssi.gouv.fr/eidas/tl/fr*

Status Determination Approach *http://uri.etsi.org/TrstSvc/TrustedList/StatusDetn/EUappropriate*

Scheme Type Community Rules

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUcommon*

URI *[fr]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR*

Scheme Territory *FR*

Policy Or Legal Notice

TSL Legal Notice *[en]* *The applicable legal framework for the present trusted list is Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.*

TSL Legal Notice *[fr]* *Le cadre juridique applicable de la présente liste de confiance est le règlement (UE) no 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE.*

Historical Information Period *65535*

Pointer to other TSL - EUROPEAN UNION

1.EU TSL - MimeType: application/vnd.etsi.tsl+xml

TSL Location *https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml*

EU TSL digital identities

TSL Scheme Operator certificate fields details

Version: *3*

Serial Number: *212676479325590790665103265166958938 79*

X509 Certificate -----BEGIN CERTIFICATE-----

MIID/DCCAuSgAwIBAgIQEAAAAAAAWgS4SGkJJUcHdzANBgkqhkiG9w0BAQUFADAzMQswCQYDVQQG
EwJCRTETMBEGA1UEAxMKQ2l0aXplbiBDQTEPMA0GA1UEBRMGMjAxMzA2MB4XDTEzMDcxNzE3NDQw
OFoXDTE4MDcxMzIzNTk1OVowbjELMAkGA1UEBhMCQkUxITAfBgNVBAMTGFBpZXJyZSBEYW1hcyAo
U2lnbmF0dXJlKTEOMAwGA1UEBBMFRGFtYXMxFjAUBgNVBCoMDVBpZXJyZSBBbmRyw6kxFDASBgNV
BAUTCzYwMDIxMjExOTE5MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCMv+7DvhzLwG3prirU
DGaYRS2+jBZtN2cYXuloKSqAc5Q58FEmk0gsZRF+/4dkt8hgCvbBcpmG6FcvTfNxQbxPX88yYwpB
YsWnJ3aD5P4QrN2+fZxwxfXxRRcX+t30IBpr+WYFv/GhJhoFo0LWUehC4eyvnMfP4J/MR4TGlQRr
cwIDAQABo4IBUzCCAU8wHwYDVR0jBBgwFoAUww/Dck0/3rI43jkuR2RQ//KP88cwbgYIKwYBBQUH
AQEEYjBgMDYGCCsGAQUFBzAChipodHRwOi8vY2VydHMuZWlkLmJlbGdpdW0uYmUvYmVsZ2l1bXJz
Mi5jcnQwJgYIKwYBBQUHMAGGGmh0dHA6Ly9vY3NwLmVpZC5iZWxnaXVtLmJlMEQGA1UdIAQ9MDsw
OQYHYDgJAQECATAuMCwGCCsGAQUFBwIBFiBodHRwOi8vcmVwb3NpdG9yeS5laWQuYmVsZ2l1bS5i
ZTA5BgNVHR8EMjAwMC6gLKAqhihodHRwOi8vY3JsLmVpZC5iZWxnaXVtLmJlL2VpZGMyMDEzMDYu
Y3JsMA4GA1UdDwEB/wQEAwIGQDARBglghkgBhvhCAQEEBAMCBSAwGAYIKwYBBQUHAQMEDDAKMAgG
BgQAjkYBATANBgkqhkiG9w0BAQUFAAOCAQEAEE3KGmLX5XXqArQwIZQmQEE6orKSu3a1z8ey1txs
ZC4rMk1vpvC6MtsfDaU4N6ooprhcM/WAlcIGOPCNhvxV+xcY7gUBwa6myiClnK0CMSiGYHqWcJG8
ns13B9f0+5PJqsoziPoksXb2A9VXkr5aEdEmBYLjh7wG7GwAuDgDT0v87qtphN02/MAlJcNqT3JU
UAotD7yfEybmK245jKo+pTYeCHGh7r1HzVWhbUDcQ/e1PpQXjVqBmr4k1ACtuu4H19t6K1P5kf7t
a5JFEJPFgy3Hxt6YqzoY07WTVEpS4gJqtleIdX1Fhse7jq83ltcCzlfysBRqY/okUzipo1rbQw==

-----END CERTIFICATE-----

Signature algorithm: *SHA1withRSA*

Issuer SERIAL NUMBER: *201306*

Issuer CN: *Citizen CA*

Issuer C: *BE*

Subject SERIAL NUMBER: *60021211919*

Subject GIVEN NAME: *Pierre André*

Subject SURNAME: *Damas*

Subject CN: *Pierre Damas (Signature)*

Subject C: *BE*

Valid from: *Wed Jul 17 19:44:08 CEST 2013*

Valid to: *Sat Jul 14 01:59:59 CEST 2018*

Public Key:

30:81:9F:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:81:8D:00:30:81:89:02:81:81:00:8C:BF:EE:C3:BE:1C:CB:C0:6D:E9:AE:2A:D4:0C:66:98:45:2D:BE:8C
:16:6D:37:67:18:5E:E9:68:29:2A:80:73:94:39:F0:51:26:93:48:2C:65:11:7E:FF:87:64:B7:C8:60:0A:F6:C1:72:99:86:E8:57:2F:4D:F3:71:41:BC:4F:5F:CF:32:63:0A:
41:62:C5:A7:27:76:83:E4:FE:10:AC:DD:BE:7D:9C:70:C5:F5:F1:45:17:17:FA:DD:F4:20:1A:6B:F9:66:05:BF:F1:A1:26:1A:05:A3:42:D6:51:E8:42:E1:EC:AF:9C:C7:CF
:E0:9F:CC:47:84:C6:95:04:6B:73:02:03:01:00:01

Authority Key Identifier *C3:0F:C3:72:4D:3F:DE:B2:38:DE:39:2E:47:64:50:FF:F2:8F:F3:C7*

Authority Info Access *http://certs.eid.belgium.be/belgiumrs2.crt*

http://ocsp.eid.belgium.be

Certificate Policies

Policy OID: 2.16.56.9.1.1.2.1

CPS pointer: http://repository.eid.belgium.be

CRL Distribution Points

http://crl.eid.belgium.be/eidc201306.crl

QCStatements - crit. = false

id_etsi_qcs_QcCompliance

Key Usage:

nonRepudiation

Thumbprint algorithm:

SHA-256

Thumbprint:

FF:EA:7F:0E:D2:9B:EB:07:73:EA:3B:0C:47:29:BB:F8:00:A6:C3:90:B6:21:95:CB:27:0F :12:A4:A A:62:F2:84

EU TSL digital identities

TSL Scheme Operator certificate fields details

Version:

3

Serial Number:

212676479325590780251363897264591942 95

X509 Certificate

-----BEGIN CERTIFICATE-----

MIID/TCCAuWgAwIBAgIQEAAAAAAAWcxEUPr16SDrtzANBgkqhkiG9w0BAQUFADAzMQswCQYDVQQG
EwJCRTETMBEGA1UEAxMKQ2l0aXplbiBDQTEPMA0GA1UEBRMGMjAxMzExMB4XDTEzMDcyNDAxNDUz
MVoXDTE4MDcxODIzNTk1OVowbzELMAkGA1UEBhMCQkUxIjAgBgNVBAMTGU1hYXJ0ZW4gT3R0b3kg
KFNpZ25hdHVyZSkxDjAMBgNVBAQTBU90dG95MRYwFAYDVQQqEw1NYWFydGVuIEpvcmlzMRQwEgYD
VQQFEws4MzEyMTQyNDEwMjCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAjbr1T8USYkuh4X+Y
i+coykq7mbF8PjgyjWQ28uODqRCkynuqJz468tCIYxsM/+/QdqEFq4Z5Z1YDbBYb5KsxfBmkzr9D
+Gt49iWVt9Ig+FhngbOexwCW108t6Q/+NAo6gwl6IKkzv2wpEJIwtc51VFzvM+WkE1mNmclphYRT
L5UCAwEAAaOCAVMwggFPMB8GA1UdIwQYMBaAFLws1Y0dT3YXfAzva5To9R51FmNhMG4GCCsGAQUF
BwEBBGIwYDA2BggrBgEFBQcwAoYqaHR0cDovL2NlcnRzLmVpZC5iZWxnaXVtLmJlL2JlbGdpdW1y
czIuY3J0MCYGCCsGAQUFBzABhhpodHRwOi8vb2NzcC5laWQuYmVsZ2l1bS5iZTBEBgNVHSAEPTA7
MDkGB2A4CQEBAgEwLjAsBggrBgEFBQcCARYgaHR0cDovL3JlcG9zaXRvcnkuZWlkLmJlbGdpdW0u
YmUwOQYDVR0fBDIwMDAuoCygKoYoaHR0cDovL2NybC5laWQuYmVsZ2l1bS5iZS9laWRjMjAxMzEx
LmNybDAOBgNVHQ8BAf8EBAMCBkAwEQYJYIZIAYb4QgEBBAQDAgUgMBgGCCsGAQUFBwEDBAwwCjAI
BgYEAI5GAQEwDQYJKoZIhvcNAQEFBQADggEBAHNRipzOD4aXB7Oo4FgfBbWgPkmUGTqkz2jK9U2t
EWUbyQrhirgqhxK6YMAHBvzL+7BHouMEAuxycZG3ozAfEDRZiznFWyqS8QlnHUe0ThaAvs8v5wYO
UO7lJ6vnaNLLvQj7W3L5kCnEva5h0Jh9wMytlNp89dd02l7MD4BsidXoMN21AE8su39tBmNayLF6
YrFLe3Zob4fQCuIEbx/pj3kYIVC4WM7uuDx+QpEJdNBtB41o2q2JJFqusRP7W0phkxX7sPtYkot6
RXLdgaZNoB4YIRwGozIvcegydRVqpcYrvFSoppNHQqd8ZNzswjGzqBhlWYPsxdjjsxJiUyk7T1c=

-----END CERTIFICATE-----

Signature algorithm:

SHA1withRSA

Issuer SERIAL NUMBER:

201311

Issuer CN:

Citizen CA

Issuer C:

BE

Subject SERIAL NUMBER:

83121424102

Subject GIVEN NAME: *Maarten Joris*

Subject SURNAME: *Ottoy*

Subject CN: *Maarten Ottoy (Signature)*

Subject C: *BE*

Valid from: *Wed Jul 24 03:45:31 CEST 2013*

Valid to: *Thu Jul 19 01:59:59 CEST 2018*

Public Key:

30:81:9F:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:81:8D:00:30:81:89:02:81:81:00:8D:BA:F5:4F:C5:12:62:4B:A1:E1:7F:98:8B:E7:28:CA:4A:BB:99:B1:
7C:3E:38:32:8D:64:36:F2:E3:83:A9:10:A4:CA:7B:AA:27:3E:3A:F2:D0:88:63:1B:0C:FF:EF:D0:76:A1:05:AB:86:79:67:56:03:6C:16:1B:E4:AB:31:7C:19:A4:CE:BF:43
:F8:6B:78:F6:25:95:B7:D2:20:F8:58:67:81:B3:9E:C7:00:96:D7:4F:2D:E9:0F:FE:34:0A:3A:83:09:7A:20:A9:33:BF:6C:29:10:92:30:B5:CE:75:54:5C:EF:33:E5:A4:13:
59:8D:99:C9:69:85:84:53:2F:95:02:03:01:00:01

Authority Key Identifier *BC:2C:D5:8D:1D:4F:76:17:7C:0C:EF:6B:94:E8:F5:1E:75:16:63:61*

Authority Info Access *http://certs.eid.belgium.be/belgiumrs2.crt*

http://ocsp.eid.belgium.be

Certificate Policies *Policy OID: 2.16.56.9.1.1.2.1*

CPS pointer: http://repository.eid.belgium.be

CRL Distribution Points *http://crl.eid.belgium.be/eidc201311.crl*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*

Key Usage: *nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *F7:BC:0D:16:4D:EC:8F:36:70:9A:BE:85:FC:57:02:2F:3B:16:84:70:0A:80:4C:36:8D:34:3 2:90:04:9 0:DF:CB*

EU TSL digital identities

TSL Scheme Operator certificate fields details

Version: *3*

Serial Number: *1743254*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIHATCCBOmgAwIBAgIDGpmWMA0GCSqGSIb3DQEBCwUAME4xCzAJBgNVBAYTAkxVMRYwFAYDVQQK
DA1MdXhUcnVzdCBTLkEuMScwJQYDVQQDDB5MdXhUcnVzdCBHbG9iYWwgUXVhbGlmaWVkIENBIDMw
HhcNMTYwOTE1MDkwMDEyWhcNMTkwOTE1MDkwMDEyWjCB/TELMAkGA1UEBhMCQkUxCzAJBgNVBAcT
AkJFMRwwGgYDVQQKExNFdXJvcGVhbiBDb21taXNzaW9uMRUwEwYDVQQLEwwwOTQ5LjM4My4zNDIx

HDAaBgNVBAMTE01hYXJ0ZW4gSm9yaXMgT3R0b3kxDjAMBgNVBAQTBU90dG95MRYwFAYDVQQqEw1N
YWFydGVuIEpvcmlzMR0wGwYDVQQFExQxMDMwNDQ0NDExMDA4MDgzNzU5MjEpMCcGCSqGSIb3DQEJ
ARYabWFhcnRlbi5vdHRveUBlYy5ldXJvcGEuZXUxHDAaBgNVBAwTE1Byb2Zlc3Npb25hbCBQZXJz
b24wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCyUn5NvdLXpWSAPF7S+tOy/M6uY8Un
5sNt2cHIOs/OHvcfY+ghBXwz91EffNXku2RKqwgw3+dyRBI1eOq2l7r0z9dgNd40zB7a/p9M10Ss
DT41MJB5iQRYE4kQ73FGA61oXD530fYNzxCA9dWXzQ40L+wdpPbrVtfgi+pRTZSXocZF2VHpuiPE
VexHPHt68rX/G8pYHg7zmYOEBPLsjjQAwbrVZIKb9Ypgkwb4ziaFg6UZemMfRtl7S08UWjjhOUUj
Z+216ie9V6cMSXzg+5Co9HVSXPdqooNhMrOShTI7IzDja3rXAcw6TkvPDgZEpCJZ73HCxz+DWnW7
D2JuXMelAgMBAAGjggI2MIICMjAMBgNVHRMBAf8EAjAAMGYGCCsGAQUFBwEBBFowWDAnBggrBgEF
BQcwAYYbaHR0cDovL3FjYS5vY3NwLmx1eHRydXN0Lmx1MC0GCCsGAQUFBzAChiFodHRwOi8vY2Eu
bHV4dHJ1c3QubHUvTFRHUUNBMy5jcnQwggEeBgNVHSAEggEVMIIBETCCAQMGCCuBKwEBCgMBMIH2
MIHHBggrBgEFBQcCAjCBuhqBt0x1eFRydXN0IFF1YWxpZmllZCBDZXJ0aWZpY2F0ZSBvbiBTU0NE
IGNvbXBsaWFudCB3aXRoIEVUU0kgVFMgMTAxIDQ1NiBRQ1ArIGNlcnRpZmljYXRlIHBvbGljeS4g
S2V5IEdlbmVyYXRpb24gYnkgQ1NQLiBTb2xlIEF1dGhvcmlzZWQgVXNhZ2U6IFN1cHBvcnQgb2Yg
UXVhbGlmaWVkIEVsZWN0cm9uaWMgU2lnbmF0dXJlLjAqBggrBgEFBQcCARYeaHR0cHM6Ly9yZXBv
c2l0b3J5Lmx1eHRydXN0Lmx1MAgGBgQAizABATAiBggrBgEFBQcBAwQWMBQwCAYGBACORgEBMAgG
BgQAjkYBBDALBgNVHQ8EBAMCBkAwHwYDVR0jBBgwFoAUY4/CiwOxq47YU0eWHZmoffasqHUwMwYD
VR0fBCwwKjAooCagJIYiaHR0cDovL2NybC5sdXh0cnVzdC5sdS9MVEdRQ0EzLmNybDARBgNVHQ4E
CgQIR8OxCQGxgiswDQYJKoZIhvcNAQELBQADggIBACWb5+Xt6sOaxE8bpakXFo2BoWYphyq5XAXR
M6e7QDS57CaHW8Ly6ep0I23EZ3KcI3mpqg2UDaEZhGhvnE/SVEyh4go6E8Hljv9iyrdGccc+RgTM
87rbkoUi6sZ+BcLlG7WNo2c5BqRyElch5o1/9AEnft3inLK4R47BHtbRkf/FkptiQWjSVzJ6LEHI
i8EF215Qg5X/yaUQdxIfMPcQ580rGujGN/Dl2H9rxBUdPUCO0i7zbPeJtfah1zSXxYjy9V4x2Q+c
VbcMpa5fSys9c/YQA6XAkA5oKrkSsjCGBULDi2APC3FMehp6BcI/5k202iwebq3xgDWFvuD+swgZ
8P0YxS4dZMcjtseYvzGCArFEcoI7buZb30A/Z7K3qx3D895NHupfz20dskujjCV7PVgxx0PCXJPB
quuPFV+aYgDCLr7XQMmU8wo0HGKZ/mXThY2F2POLF0uKgY6F5mZBIhRYU5IgybGrayqEpaEcr8LM
BKzr2DRpLzDojU5k9apmVnoQJ2cSfTrQ87ZXOaG+6h/Md6cVaUI0J8iOpFLinKRGRBEkwE+pxFE2
tOoyaK9iLKurRYdfd8WETatEsEyi4o4CFPD//bthgwvSl0Cfrkj8V5lIR13140D+NQtX0vSx/PHq
5ySOKq9ZPUo42r8ihX/ZP0Z+Vrg5ATqpSCcqn01Z

-----END CERTIFICATE-----

Signature algorithm:	*SHA256withRSA*
Issuer CN:	*LuxTrust Global Qualified CA 3*
Issuer O:	*LuxTrust S.A.*
Issuer C:	*LU*
Subject T:	*Professional Person*
Subject E:	*maarten.ottoy@ec.europa.eu*
Subject SERIAL NUMBER:	*10304444110080837592*
Subject GIVEN NAME:	*Maarten Joris*
Subject SURNAME:	*Ottoy*
Subject CN:	*Maarten Joris Ottoy*
Subject OU:	*0949.383.342*
Subject O:	*European Commission*
Subject L:	*BE*
Subject C:	*BE*

Valid from: *Thu Sep 15 11:00:12 CEST 2016*

Valid to: *Sun Sep 15 11:00:12 CEST 2019*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:B2:52:7E:4D:BD:D2:D7:A5:64:80:3C:5E:D2:FA:D3:B2:FC:CE:AE:63:C5:27:E6:C3:6D:D9:C1:C8:3A:CF:CE:1E:F7:1F:63:E8:21:05:7C:33:F7:51:1F:7C:D5:E4:BB:64:4A:AB:08:30:DF:E7:72:44:12:35:78:EA:B6:97:BA:F4:CF:D7:60:35:DE:34:CC:1E:DA:FE:9F:4C:D7:44:AC:0D:3E:35:30:90:79:89:04:58:13:89:10:EF:71:46:03:AD:68:5C:3E:77:D1:F6:0D:CF:10:80:F5:D5:97:CD:0E:34:2F:EC:1D:A4:F6:EB:56:D7:E0:8B:EA:51:4D:94:97:A1:C6:45:D9:51:E9:BA:23:C4:55:EC:47:3C:7B:7A:F2:B5:FF:1B:CA:58:1E:0E:F3:99:83:84:04:F2:EC:8E:34:00:C1:BA:D5:6
4:82:9B:F5:8A:60:93:06:F8:CE:26:85:83:A5:19:7A:63:1F:46:D9:7B:4B:4F:14:5A:38:E1:39:45:23:67:ED:B5:EA:27:BD:57:A7:0C:49:7C:E0:FB:90:A8:F4:75:52:5C:F7:6A:A2:83:61:32:B3:92:85:32:3B:23:30:E3:6B:7A:D7:01:CC:3A:4E:4B:CF:0E:06:44:A4:22:59:EF:71:C2:C7:3F:83:5A:75:BB:0F:62:6E:5C:C7:A5:02:03:01:00:01

Basic Constraints *IsCA: false*

Authority Info Access *http://qca.ocsp.luxtrust.lu*

http://ca.luxtrust.lu/LTGQCA

3.crt

Certificate Policies *Policy OID: 1.3.171.1.1.10.3.1*

CPS text: [LuxTrust Qualified Certificate on SSCD compliant with ETSI TS 101 456 QCP+ certificate policy. Key Generation by CSP. Sole Authorised Usage: Support of Qualified Electronic Signature.]

CPS pointer: https://repository.luxtrust.lu

Policy OID: 0.4.0.1456.1.1

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*

id_etsi_qcs_Qc
SSCD

Authority Key Identifier *63:8F:C2:8B:03:B1:AB:8E:D8:53:47:96:1D:99:A8:7D:F6:AC:A8:75*

CRL Distribution Points *http://crl.luxtrust.lu/LTGQCA3.crl*

Subject Key Identifier *47:C3:B1:09:01:B1:82:2B*

Key Usage: *nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *9C:1A:3B:64:6E:AF:13:23:98:EF:31:9E:41:C8:E7:ED:72:5B:64:D5:77:25:80:AE:12:5D:59:C0:F6: 84:56:30*

EU TSL digital identities

TSL Scheme Operator certificate fields details

Version: *3*

Serial Number: *1974568*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIHDjCCBPagAwIBAgIDHiEoMA0GCSqGSIb3DQEBCwUAME4xCzAJBgNVBAYTAkxVMRYwFAYDVQQK
DA1MdXhUcnVzdCBTLkEuMScwJQYDVQQDDB5MdXhUcnVzdCBHbG9iYWwgUXVhbGlmaWVkIENBIDMw
HhcNMTcwNTExMTAyNzI1WhcNMjAwNTExMTAyNzI1WjCCAQkxCzAJBgNVBAYTAk5MMQswCQYDVQQH
EwJCRTEcMBoGA1UEChMTRXVyb3BlYW4gQ29tbWlzc2lvbjEVMBMGA1UECxMMMDk0OS4zODMuMzQy
MSEwHwYDVQQDExhNaWNoYWVsIFRoZW9kb29yIGRlIEJvZXIxEDAOBgNVBAQTB2RlIEJvZXIxGTAX
BgNVBCoTEE1pY2hhZWwgVGhlb2Rvb3IxHTAbBgNVBAUTFDEwMzAzOTY5NDUwMDg1MDQ2NDI0MSsw
KQYJKoZIhvcNAQkBFhxtaWNoYWVsLmRlLWJvZXJAZWMuZXVyb3BhLmV1MRwwGgYDVQQMExNQcm9m
ZXNzaW9uYWwgUGVyc29uMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAq2G70g/Tsyt8
nyI1PXYHgIm6a6DawB2ATZMsMxkS1flXjkPNMd/e1Go/G1+IFsqA6iBlfxmFhABJa9FbFallOMBr
E3Ao0SdHpT4UbrhVyWx5iV/DjInxPMCzx3Przus3CVy7YhKHO9Jt/qPruWeLCf3YFMV8N02lig90
4Vbc6pxjx5yqKij7skHSiMyAzdgw/VIQZjJF8PiA10eguvwgS/BU6ip5M03DoGOZPBvIt3q/Av4Y
Htd7LaOFTYl/zRcn2f12FqO4JMiNR5LxfByRbMmUJQe8sjtC0/ho7cG3BWuusLUe/LtQIGCT/uXX
dF9qKuOiPDQ3OpfhJlhElaJPpwIDAQABo4ICNjCCAjIwDAYDVR0TAQH/BAIwADBmBggrBgEFBQcB
AQRaMFgwJwYIKwYBBQUHMAGGG2h0dHA6Ly9xY2Eub2NzcC5sdXh0cnVzdC5sdTAtBggrBgEFBQcw
AoYhaHR0cDovL2NhLmx1eHRydXN0Lmx1L0xUR1FDQTMuY3J0MIIBHgYDVR0gBIIBFTCCAREwggED
BggrgSsBAQoDATCB9jCBxwYIKwYBBQUHAgIwgboagbdMdXhUcnVzdCBRdWFsaWZpZWQgQ2VydGlm
aWNhdGUgb24gU1NDRCBjb21wbGlhbnQgd2l0aCBFVFNJIFRTIDEwMSA0NTYgUUNQKyBjZXJ0aWZp
Y2F0ZSBwb2xpY3kuIEtleSBHZW5lcmF0aW9uIGJ5IENTUC4gU29sZSBBdXRob3Jpc2VkIFVzYWdl
OiBTdXBwb3J0IG9mIFF1YWxpZmllZCBFbGVjdHJvbmljIFNpZ25hdHVyZS4wKgYIKwYBBQUHAgEW
Hmh0dHBzOi8vcmVwb3NpdG9yeS5sdXh0cnVzdC5sdTAIBgYEAIswAQEwIgYIKwYBBQUHAQMEFjAU
MAgGBgQAjkYBATAIBgYEAI5GAQQwCwYDVR0PBAQDAgZAMB8GA1UdIwQYMBaAFGOPwosDsauO2FNH
lh2ZqH32rKh1MDMGA1UdHwQsMCowKKAmoCSGImh0dHA6Ly9jcmwubHV4dHJ1c3QubHUvTFRHUUNB
My5jcmwwEQYDVR0OBAoECED2Gny4nY/ZMA0GCSqGSIb3DQEBCwUAA4ICAQBvdAp4qOITVgjyiZkd
UMoQC5HPDvptyJrF+j4aZmClYbg8UEy5RqurLv5icKUWjp0nYO8Qq4drrMGHbOMlWiVZ6yUiy8oX
v62gv/hiSGGrwDKekfZcJ3K9wUT50TaM3sROmY0BzbYqatsDOoHb2BwhNMooFwo+sUZ+5Qt1Lv+F
MLKHxeO9rM4ezXPO8Vsfh6d5zddGl29WrxbBZj7bp3cfSBHJa1t6NIIr5+sU9Xu+GvTSXuSSht3k
mVU9ofctXetQ8Qq+mxPwPhNTyNu8laQgQQBnWTMb6PQgtIaWOJak9mpRhvvlH9+sdIjNvGO46BCN
ykUPu4Mdgi0Zq5rsoCJUp5EpUWrAmdM5yMufMMKXqW8XHqU0KsTGyBcIkoElmhvtCQBBTfE5vh7y
OS6hYpzTop9fLTJ+uQJI14DTOu+iVSmw5Oh8AYTPKh5wzKkEWTiq5Z0KiwmmOIxo8T9YtlhsAe/7
aO1nC3WxFKaqWAFQx5UPIs4bQ0rRW39n1T6PovJxkKTPEW6TPmYrYjR2DYlsSnIbR9ebHUbRB/v/
o9Pvqx6dArlpVuhDWWDjuAT1bW3ej+/jIJGyQtwKqL9fnDcmuUqzoBa9fXJuB1e8m3+tI1H5e9F/
JH3kdkPsrV9DMS13+MYIeQJgAK3ofJcuKCKYQ5uUEZaU2CKiR6TzvzzGqQ==

-----END CERTIFICATE-----

Signature algorithm:	*SHA256withRSA*
Issuer CN:	*LuxTrust Global Qualified CA 3*
Issuer O:	*LuxTrust S.A.*
Issuer C:	*LU*
Subject T:	*Professional Person*
Subject E:	*michael.de-boer@ec.europa.eu*
Subject SERIAL NUMBER:	*10303969450085046424*
Subject GIVEN NAME:	*Michael Theodoor*
Subject SURNAME:	*de Boer*
Subject CN:	*Michael Theodoor de Boer*
Subject OU:	*0949.383.342*

Subject O: *European Commission*

Subject L: *BE*

Subject C: *NL*

Valid from: *Thu May 11 12:27:25 CEST 2017*

Valid to: *Mon May 11 12:27:25 CEST 2020*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:AB:61:BB:D2:0F:D3:B3:2B:7C:9F:22:35:3D:76:07:80:89:BA:6B:A0:DA:C0:1D:80:4D:93:2C:33:19:12:D5:F9:57:8E:43:CD:31:DF:DE:D4:6A:3F:1B:5F:88:16:CA:80:EA:20:65:7F:19:85:84:00:49:6B:D1:5B:15:A9:65:38:C0:6B:13:70:28:D1:27:47:A5:3E:14:6E:B8:55:C9:6C:79:89:5F:C3:8C:89:F1:3C:C0:B3:C7:73:EB:CE:EB:37:09:5C:BB:62:12:87:3B:D2:6D:FE:A3:EB:B9:67:8B:09:FD:D8:14:C5:7C:37:4D:A5:8A:0F:74:E1:56:DC:EA:9C:63:C7:9C:AA:2A:28:FB:B2:41:D2:88:CC:80:CD:D8:30:FD:52:10:66:32:45:F0:F8:80:D7:47:A0:BA:FC:20:4B:F0:54:EA:2A:79:33:4D:C3:A0:63:99:3C:1B:C8:B7:7A:BF:02:FE:18:1E:D7:7B:2D:A3:85:4D:89:7F:CD:17:27:D9:FD:76:16:A3:B8:24:C8:8D:47:92:F1:7C:1C:91:6C:C9:94:25:07:BC:B2:3B:42:D3:F8:68:ED:C1:B7:05:6B:AE:B0:B5:1E:
FC:BB:50:20:60:93:FE:E5:D7:74:5F:6A:2A:E3:A2:3C:34:37:3A:97:E1:24:88:44:95:A2:4F:A7:02:03:01:00:01

Basic Constraints *IsCA: false*

Authority Info Access *http://qca.ocsp.luxtrust.lu*

http://ca.luxtrust.lu/LTGQCA3.cr

t

Certificate Policies *Policy OID: 1.3.171.1.1.10.3.1*

CPS text: [LuxTrust Qualified Certificate on SSCD compliant with ETSI TS 101 456 QCP+ certificate policy. Key Generation by CSP. Sole Authorised Usage: Support of Qualified Electronic Signature.]

CPS pointer: https://repository.luxtrust.lu

Policy OID: 0.4.0.1456.1.1

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*

id_etsi_qcs_Qc
SSCD

Authority Key Identifier *63:8F:C2:8B:03:B1:AB:8E:D8:53:47:96:1D:99:A8:7D:F6:AC:A8:75*

CRL Distribution Points *http://crl.luxtrust.lu/LTGQCA3.crl*

Subject Key Identifier *40:F6:1A:7C:B8:9D:8F:D9*

Key Usage: *nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *59:A1:BF:29:0B:81:8B:17:7A:D6:1A:C4:B3:E6:DC:DD:D4:6D:A6:D5:BE:95:79:F8:56:4A:DE:A6: F2:CF:07:3E*

EU TSL digital identities

TSL Scheme Operator certificate fields details

Version: *3*

Serial Number: *212676479325588035429928318933206969 44*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIGZzCCBE+gAwIBAgIQEAAAAAAAH6yPXvnVxqcEcDANBgkqhkiG9w0BAQUFADAzMQswCQYDVQQG
EwJCRTETMBEGA1UEAxMKQ2l0aXplbiBDQTEPMA0GA1UEBRMGMjAxNTA4MB4XDTE1MDUwMTE4NTQ1
NFoXDTI1MDQyNTIzNTk1OVowczELMAkGA1UEBhMCQkUxJzAlBgNVBAMTHkplYW4tTWFyYyBWZXJi
ZXJndCAoU2lnbmF0dXJlKTERMA8GA1UEBBMIVmVyYmVyZ3QxEjAQBgNVBCoTCUplYW4tTWFyYzEU
MBIGA1UEBRMLNjcwMjIzMzAzNDAwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCwbnf9
98lxC5nc7YZUhnMIQ+n3VAjrFU2IOIzmHHSJ6aMASYOMYOlLx7XDrjbmh/MyhlpGYmNsF0iLwEYW
XNwF4ChmfHqvoI/P29aqNkcojV2cFpZj+ocgnyf+f2cwn3z/kGh9kI6x4eS5IroFpABvzxWi0WD3
W7wSJKyeRoMaGOtw07iA43S4fjDzjkKTYGor6PIOv6UtCfrZqPjTg+822kFhERz/3KiqSn2Hx324
IIN/mZCSDd5ixKl0tdCsX+bPbXJI4tOyE0RDUl5/+iMAQWjli45opKj8eTMx2kmSycw9Du4zkFzg
np81XGDqEHZp53wSg8uZ5QR8EUjU3xNbAgMBAAGjggI1MIICMTAfBgNVHSMEGDAWgBRqb1HlzCdd
ZQnuqBsSlAPwQKAI8jBwBggrBgEFBQcBAQRkMGIwNgYIKwYBBQUHMAKGKmh0dHA6Ly9jZXJ0cy5l
aWQuYmVsZ2l1bS5iZS9iZWxnaXVtcnMzLmNydDAoBggrBgEFBQcwAYYcaHR0cDovL29jc3AuZWlk
LmJlbGdpdW0uYmUvMjCCARgGA1UdIASCAQ8wggELMIIBBwYHYDgKAQECATCB+zAsBggrBgEFBQcC
ARYgaHR0cDovL3JlcG9zaXRvcnkuZWlkLmJlbGdpdW0uYmUwgcoGCCsGAQUFBwICMIG9GoG6R2Vi
cnVpayBvbmRlcndvcnBlbiBhYW4gYWFuc3ByYWtlbGlqa2hlaWRzYmVwZXJraW5nZW4sIHppZSBD
UFMgLSBVc2FnZSBzb3VtaXMgw6AgZGVzIGxpbWl0YXRpb25zIGRlIHJlc3BvbnNhYmlsaXTDqSwg
dm9pciBDUFMgLSBWZXJ3ZW5kdW5nIHVudGVybGllZ3QgSGFmdHVuZ3NiZXNjaHLDpG5rdW5nZW4s
IGdlbcOkc3MgQ1BTMDkGA1UdHwQyMDAwLqAsoCqGKGh0dHA6Ly9jcmwuZWlkLmJlbGdpdW0uYmUv
ZWlkYzIwMTUwOC5jcmwwDgYDVR0PAQH/BAQDAgZAMBEGCWCGSAGG+EIBAQQEAwIFIDAiBggrBgEF
BQcBAwQWMBQwCAYGBACORgEBMAgGBgQAjkYBBDANBgkqhkiG9w0BAQUFAAOCAgEAJ9OdfZ1C/G+m
WS/MaTIK80oGEjapyYgZnXxJ5sFuUGv4oKev2Tq9FwzeKTpo+ufb6chMSWDguX+HkkwBlCj8Dt3N
D4FFDzAsgoGnorKuWkO54Pa8KpXEb7OjsWvMnJhz2iG/rEnm7b2QjN/jxbS7ZzCJhW6mXuQ1K9FU
nO6VzBV59N3KdoIUEEXZlPMVYhlQEJPG3PsmMXUwcQthDQgRpgbyiPPtzUJdS86dZu0eRds2xjAA
zl7EVnHvSVcBFwaikB9YuECb7NfjD9yU+WshStCjvZb1aW9qGQXb5RrWP2kdKe6VMKsQh9dwpXPZ
0cFABK9lJxAJB0vhV0JKD9FtcCJ4GA8oxX5Ul57oHGeFBVazT+OKaaNwNM/1zpowv6QwYowX4Y9N
ZJ/CYRkMNeNwCuB88mvDvIZY/a/lZTzVwqX2KuGZeFTJInN8esUu1uROd3jRkguSs93R/6Ch8xOS
6uyeNY7IyrlW9lbSJ6Sza9viZRN8FhQARNa0sLPwXeX2zHUQ1xLSU2+E0E7ruBtMT0o5jTbViDmr
mSb0PPmbSRnBlLsjf8PcgKkRzrGUDWfhoGnqu4dJs3uipwsPPVaoInZ26DIPgEDlneLmYi9Kt3T+
yxG57lOq8E9Ip6HzBeiTXKGB+C5o484w32E97mtnP6dvMLL7VsoyegfJhO/3/lU=

-----END CERTIFICATE-----

Signature algorithm: *SHA1withRSA*

Issuer SERIAL NUMBER: *201508*

Issuer CN: *Citizen CA*

Issuer C: *BE*

Subject SERIAL NUMBER: *67022330340*

Subject GIVEN NAME: *Jean-Marc*

Subject SURNAME: *Verbergt*

Subject CN: *Jean-Marc Verbergt (Signature)*

Subject C: *BE*

Valid from: *Fri May 01 20:54:54 CEST 2015*

Valid to: *Sat Apr 26 01:59:59 CEST 2025*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:B0:6E:77:FD:F7:C9:71:0B:99:DC:ED:86:54:86:73:08:43:E9:F7:54:08:EB:15:4D:88:38:8C:E6:1C:74:89:E9:A3:00:49:83:8C:60:E9:4B:C7:B5:C3:AE:36:E6:87:F3:32:86:5A:46:62:63:6C:17:48:8B:C0:46:16:5C:DC:05:E0:28:66:7C:7A:AF:A0:8F:CF:DB:D6:AA:36:47:28:8D:5D:9C:16:96:63:FA:87:20:9F:27:FE:7F:67:30:9F:7C:FF:90:68:7D:90:8E:B1:E1:E4:B9:22:BA:05:A4:00:6F:CF:15:A2:D1:60:F7:5B:BC:12:24:AC:9E:46:83:1A:18:EB:70:D3:B8:80:E3:74:B8:7E:30:F3:8E:42:93:60:6A:2B:E8:F2:0E:BF:A5:2D:09:FA:D9:A8:F8:D3:83:EF:36:DA:41:61:11:1C:FF:DC:A8:AA:4A:7D:87:C7:7D:B8:20:83:7F:99:90:92:0D:DE:62:C4:A9:74:B5:D0:AC:5F:E6:CF:6D:72:48:E2:D3:B2:13:44:43:52:5E:7F:FA:23:00:41:68:E5:8B:8E:68:A4:A8:FC:79:33:31:DA:49:92:C9:CC:3D:0E:EE:33:90:5C:
E0:9E:9F:35:5C:60:EA:10:76:69:E7:7C:12:83:CB:99:E5:04:7C:11:48:D4:DF:13:5B:02:03:01:00:01

Authority Key Identifier *6A:6F:51:E5:CC:27:5D:65:09:EE:A8:1B:12:94:03:F0:40:A0:08:F2*

Authority Info Access *http://certs.eid.belgium.be/belgiumrs3.crt*

http://ocsp.eid.belgium.be/2

Certificate Policies *Policy OID: 2.16.56.10.1.1.2.1*

CPS pointer: http://repository.eid.belgium.be

CPS text: [Gebruik onderworpen aan aansprakelijkheidsbeperkingen, zie CPS - Usage soumis Ã des limitations de responsabilitÃ©, voir CPS - Verwendung unterliegt HaftungsbeschrÃ¤nkungen, gemÃ¤ss CPS]

CRL Distribution Points *http://crl.eid.belgium.be/eidc201508.crl*

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*

id_etsi_qcs_QcSSCD

Key Usage: *nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *54:00:AB:71:2C:41:AA:F0:C4:0B:50:5E:26:4D:54:94:D8:AF:41:80:F8:F6:29:55:D1:62:23:B3:29:0 F:97:C3*

TSL Type *http://uri.etsi.org/TrstSvc/TrustedList/TSLType/EUlistofthelists*

Scheme Territory *EU*

Mime Type *application/vnd.etsi.tsl+xml*

Scheme Operator Name

Name *[en]* *European Commission*

Name *[fr]* *Commission européenne*

Scheme Type Community Rules

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUlistofthelists*

List Issue Date Time *2018-06-30T01:00:00Z*

Next Update

date Time *2018-12-30T00:00:00Z*

Distribution Points

URI *https://ssi.gouv.fr/eidas/TL-FR.xml*

1 - TSP: Agence Nationale des Titres Sécurisés

TSP Name

Name *[en]* *Agence Nationale des Titres Sécurisés*

Name *[fr]* *Agence Nationale des Titres Sécurisés*

TSP Trade Name

Name *[en]* *VATFR-55130003262*

Name *[fr]* *VATFR-55130003262*

PostalAddress

Street Address *[en]* *ANTS - Pôle SSI - Tour Montparnasse 34ème étage - 33 avenue du Maine - B.P.37*

Locality *[en]* *Paris*

Postal Code *[en]* *75755*

Country Name *[en]* *FR*

PostalAddress

Street Address *[fr]* *ANTS - Pôle SSI - Tour Montparnasse 34ème étage - 33 avenue du Maine - B.P.37*

Locality *[fr]* *Paris*

Postal Code *[fr]* *75755*

Country Name *[fr]* *FR*

ElectronicAddress

URI *https://ants.gouv.fr/*

URI *mailto:ants-certification@interieur.gouv.fr*

URI *https://ants.gouv.fr/*

URI *mailto:ants-certification@interieur.gouv.fr*

TSP Information URI

URI *[fr]* *http://sp.ants.gouv.fr/antsv2/*

URI *[en]* *http://sp.ants.gouv.fr/antsv2/en/*

1.1 - Service (withdrawn): Acteur de l'Administration d'Etat - Signature 3 étoiles

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Acteur de l'Administration d'Etat - Signature 3 étoiles*

Name *[fr]* *Acteur de l'Administration d'Etat - Signature 3 étoiles*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *149208020877191455026306880350085286928840 2*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIFPTCCAyWgAwIBAgISESDUY1mis16tVaM/IV/i71HSMA0GCSqGSIb3DQEBCwUAMGIxCzAJBgNV
BAYTAkZSMQ0wCwYDVQQKEwRHb3V2MRcwFQYDVQQLEw4wMDAyIDEzMDAwMzI2MjErMCkGA1UEAwwi
QXV0b3JpdMOpIGRlIGNlcnRpZmljYXRpb24gQU5UUyBWMjAeFw0xMTExMTcwMDAwMDBaFw0xNzEx
MTcwMDAwMDBaMIGUMQswCQYDVQQGEwJGUjEwMC4GA1UECgwnQWdlbmNlIE5hdGlvbmFsZSBkZXMg
VGl0cmVzIFPDqWN1cmlzw6lzMRcwFQYDVQQLEw4wMDAyIDEzMDAwMzI2MjE6MDgGA1UEAwwxQXV0
b3JpdMOpIGRlIGNlcnRpZmljYXRpb24gcG9ydGV1ciBBQUUgMyDDqXRvaWxlczCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBALAWpHdvI/r1XIyfyyYQJv59Qv/EN0Dg1mJ8VqeUsG9Ewx9K
+PN5ZiMH032tIyTRKUGWNJmbuFl0c8X9CmNq0TGFpF3uOgiAGNKHALAAH1lw5JxD3VTXTTbJdnjt
vIRstL9xOo2vtqaJo5fq2KlqM+7kFS+IHCrodjuLWSMBbz8gJdxKHoJA7uvWloqjqPp+yD/vrN6W
4nm56SN3lIDB3LGVNmGPilvbjB33nGbeQohgJFwiLYvHl/mmIUl8OClVc99d9weL+Q6zXtW/Jb+8
Bp4vR7ycpF1g6Q2FasScMvinstYGwR94qoKwPDO+UoswQnRAlC37lUIEeaFsErJle08CAwEAAaOB
uTCBtjAOBgNVHQ8BAf8EBAMCAQYwEgYDVR0TAQH/BAgwBgEB/wIBADA9BgNVHR8ENjA0MDKgMKAu
hixodHRwOi8vY3JsLmFudHMuZ291di5mci9hbnRzdjIvYWNfcmFjaW5lLmNybDARBgNVHSAECjAI
MAYGBFUdIAAwHQYDVR0OBBYEFK0tbwAZg6k4G3+HI+/DwPd9qCVJMB8GA1UdIwQYMBaAFF0cxN5n
Se9GUxwcVP+1yQdbClkJMA0GCSqGSIb3DQEBCwUAA4ICAQA0delGzyhLv8n7jJz7wpG3vGfskEOC
Dvu1y0BwAFwxpoW6a0lOupXrXRC1NUybqwlJBv445buRnmd+xIhKoPhdirHMGUR3CBD15AwZyspP
KLgfsG9Pv6aBfBc3bLRdP/jW7TOoQZ2MsGRhHqv62ZjUTxJeFGMo+egMeGUQNz9HtHXZjuBH0bev
Cr+QqlyPK/rhG+WhU2p2C/fd7AgrBA1CyKn3cHRB3nMKO8hx3Hh+wNdhskuN79cAgOQvGabexiIE
DFnf99IZ4JhnO7hkVuz+Ahs5BqxMhCHeVUGTSzEIwda6nTdgHB+6sn0d6Lcserl3J/PlMhJzg2h1
/qNgbqckz9u+xERaspBo15PwPhe1mGpz8iY6ckveKBVeAEPjtEgovT0819tARjAT+IiNrmUQF0UO
GL152yCDRWPBeprbYgEf7B/6JZS6l0tDMkq6fhiQR18zsz6WnAMk4IjsPddtmEyIaPqoD39kUO57
OKw4uJbOsGopl35bZ1SnLAk/TRFsV2kEsysA4CXh+YSSEGQpKigDqJzQFqwwT6xBxxuxmz6wZA5i

1ki1UECgDzLrkD4unGF6ri8lzu8wYrLVMb/6IoC/PXaV8wuDbXzYXYgCGPDWrNlxfrPSI/a5MW5c
Oq7+dwH9NIo3ome1Rk7G2/dv2ANpJmm0O7y31rnCgKI1gQ==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Autorité de certification ANTS V2*

Issuer OU: *0002 130003262*

Issuer O: *Gouv*

Issuer C: *FR*

Subject CN: *Autorité de certification porteur AAE 3 étoiles*

Subject OU: *0002 130003262*

Subject O: *Agence Nationale des Titres Sécurisés*

Subject C: *FR*

Valid from: *Thu Nov 17 01:00:00 CET 2011*

Valid to: *Fri Nov 17 01:00:00 CET 2017*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:B0:16:A4:77:6F:23:FA:F5:5C:8C:9F:CB:26:10:26:FE:7
D:42:FF:C4:37:40:E0:D6:62:7C:56:A7:94:B0:6F:44:C3:1F:4A:F8:F3:79:66:23:07:D3:7D:AD:23:24:D1:29:41:96:34:99:9B:B8:59:74:73:C5:FD:0A:63:6A:D1:31:85:
A4:5D:EE:3A:08:80:18:D2:87:00:B0:00:1F:59:70:E4:9C:43:DD:54:D7:4D:36:C9:76:78:ED:BC:84:6C:B4:BF:71:3A:8D:AF:B6:A6:89:A3:97:EA:D8:A9:6A:33:EE:E4:1
5:2F:88:1C:2A:E8:76:3B:8B:59:23:01:6F:3F:20:25:DC:4A:1E:82:40:EE:EB:D6:96:8A:A3:A8:FA:7E:C8:3F:EF:AC:DE:96:E2:79:B9:E9:23:77:94:80:C1:DC:B1:95:36:6
1:8F:8A:5B:DB:8C:1D:F7:9C:66:DE:42:88:60:24:5C:22:2D:8B:C7:97:F9:A6:21:49:7C:38:29:55:73:DF:5D:F7:07:8B:F9:0E:B3:5E:D5:BF:25:BF:BC:06:9E:2F:47:BC:
9C:A4:5D:60:E9:0D:85:6A:C4:9C:32:F8:A7:B2:D6:06:C1:1F:78:
AA:82:B0:3C:33:BE:52:8B:30:42:74:40:94:2D:FB:95:42:04:79:A1:6C:12:B2:65:7B:4F:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

CRL Distribution Points *http://crl.ants.gouv.fr/antsv2/ac_racine.crl*

Certificate Policies *Policy OID: 2.5.29.32.0*

Subject Key Identifier *AD:2D:6F:00:19:83:A9:38:1B:7F:87:23:EF:C3:C0:F7:7D:A8:25:49*

Authority Key Identifier *5D:1C:C4:DE:67:49:EF:46:53:1C:1C:54:FF:B5:C9:07:5B:0A:59:09*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *3C:11:14:A0:1F:C4:22:24:43:2E:EC:40:34:85:4B:F3:87:3B:64:9D:04:BA:54:6B:B7:A2:D4:D5:6E:EB:36:BE*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2018-06-01T00:00:00Z*

Scheme Service Definition URI

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Signature-3-Stars*

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS101456/QCPPublic*

TSP Service Definition URI

URI *[fr]* *http://sp.ants.gouv.fr/antsv2/ANTS_AC_AAE_PC_v1.9.pdf*

URI *[en]* *http://sp.ants.gouv.fr/antsv2/en/ANTS_AAE_CA_CP_EN_v1.9.pdf*

1.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.1.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Acteur de l'Administration d'Etat - Signature 3 étoiles*

Name *[fr]* *Acteur de l'Administration d'Etat - Signature 3 étoiles*

Service digital identities

X509SubjectName

Subject CN: *Autorité de certification porteur AAE 3 étoiles*

Subject OU: *0002 130003262*

Subject O: *Agence Nationale des Titres Sécurisés*

Subject C: *FR*

X509SKI

X509 SK I *rS1vABmDqTgbf4cj78PA932oJUk=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

1.1.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.1.3 - History instance n.2 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Acteur de l'Administration d'Etat - Signature 3 étoiles*

Name *[fr]* *Acteur de l'Administration d'Etat - Signature 3 étoiles*

Service digital identities

X509SubjectName

Subject CN: *Autorité de certification porteur AAE 3 étoiles*

Subject OU: *0002 130003262*

Subject O: *Agence Nationale des Titres Sécurisés*

Subject C: *FR*

X509SKI

X509 SK I *rS1vABmDqTgbf4cj78PA932oJUk=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2011-11-16T23:00:00Z*

1.2 - Service (withdrawn): Acteur des Collectivités Territoriales - Signature 3 étoiles

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

	[fr]	*Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name	*[en]*	*Acteur des Collectivités Territoriales - Signature 3 étoiles*
Name	*[fr]*	*Acteur des Collectivités Territoriales - Signature 3 étoiles*

Service digital identities

Certificate fields details

Version:	*3*
Serial Number:	*149197971860414836162156241508299030692791 7*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIFPTCCAyWgAwIBAgISESCIyaXXV9Y9aEIOKeN6NSUtMA0GCSqGSIb3DQEBCwUAMGIxCzAJBgNV
BAYTAkZSMQ0wCwYDVQQKEwRHb3V2MRcwFQYDVQQLEw4wMDAyIDEzMDAwMzI2MjErMCkGA1UEAwwi
QXV0b3JpdMOpIGRlIGNlcnRpZmljYXRpb24gQU5UUyBWMjAeFw0xMTExMTcwMDAwMDBaFw0xNzEx
MTcwMDAwMDBaMIGUMQswCQYDVQQGEwJGUjEwMC4GA1UECgwnQWdlbmNlIE5hdGlvbmFsZSBkZXMg
VGl0cmVzIFPDqWN1cmlzw6lzMRcwFQYDVQQLEw4wMDAyIDEzMDAwMzI2MjE6MDgGA1UEAwwxQXV0
b3JpdMOpIGRlIGNlcnRpZmljYXRpb24gcG9ydGV1ciBBQ1QgMyDDqXRvaWxlczCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAJzluV3j5ZUmsStygMHP+97H/FHD3a4l0Jlv0KcHxYxFlVUt
ogXU9Y7fLVN5/S0sOMfQLdj0LxEa/9nZONoO3nLS2Vy7TaATPvctHdn6Lg//Vjjt2kAjf8uLVFHB
N7wti2DcSbc7rIxtiAtsln+NPcx2xLlWK4VqmPv7buKcsHUTJmPHLCzLVRQpU8m/81wIBwfx7oYM
f9rHLPaHm70hoVkYdE38i6PrsQBaP49alh/cc+0JWHOjJByNE7y3YLdUK4z+mVuAeVcFFfobH8u+
mtIvMBLNi64lQ6LV2jDG+EzI7Ni+IrIJDPX9Zx83jORCKV3Xhx66662c8BFmdEpV+JsCAwEAAaOB
uTCBtjAOBgNVHQ8BAf8EBAMCAQYwEgYDVR0TAQH/BAgwBgEB/wIBADA9BgNVHR8ENjA0MDKgMKAu
hixodHRwOi8vY3JsLmFudHMuZ291di5mci9hbnRzdjIvYWNfcmFjaW5lLmNybDARBgNVHSAECjAI
MAYGBFUdIAAwHQYDVR0OBBYEFK00DoP9TeZcwVYKkAKrPFzHYiI/MB8GA1UdIwQYMBaAFF0cxN5n
Se9GUxwcVP+1yQdbClkJMA0GCSqGSIb3DQEBCwUAA4ICAQBmMoCyuQNysrz9MOIX0432L/T+gucM
63Jy61iUiMEWm13Cw/Zlx7ZJhz2KGTTv0MnXQAGFBICUKykzdg6Pw8r9yThrtSP/fRV6uZZ8Q7g5
bPmwAitAjdro7DnbLJ3v1WmmjBESY89FdbohknCZX15wlfbMJrTCT5+Aa00aW+nXnNrb5xcBaExH
INNYKy4HoFewoRa+GgJoVHt1ZT7HtAxojMRY1spx8ThA1tk8bC2usruXRe8I92ljlxbX2eFk5uoR
9r26gnKZjs+JVeR1qn7teciStqjaCLxo842EGEybWI3Fd9nftk534qZK0t7AeKxBBg1MSS05fEOL
W2amBGqiU7nAlpnJt4SApRgGj5uhPgpGlreyJPuQ84BQjlsrdGHRpSVvztoBTYruyyBVValch1xB
NlP7fLqJW68fNCCNHPfcpEY5wCBl/SrqwMse4tM9EdM/bpjUxTREpMx43HhSkVuJhcAkYvjYPWX8
WAsvX2bnzm6Z2tDnTKanvv4tkwoXT8E6RPbzj+pwcANAe18+fc9JlOQZdHilPd0fBum2My7VH7zG
6Wljy76sct2GhIeJSDBzyqGq3L8N7ibOL20MaJaRxIp6J/x+WlZzogdHFsKgWCpe1S1geyHy523I
7kERXNegagrq3fw6IexLPO44vedYl+IJtGNtRpJgvrJ3zg==

-----END CERTIFICATE-----

Signature algorithm:	*SHA256withRSA*
Issuer CN:	*Autorité de certification ANTS V2*
Issuer OU:	*0002 130003262*
Issuer O:	*Gouv*
Issuer C:	*FR*
Subject CN:	*Autorité de certification porteur ACT 3 étoiles*
Subject OU:	*0002 130003262*

Subject O: *Agence Nationale des Titres Sécurisés*

Subject C: *FR*

Valid from: *Thu Nov 17 01:00:00 CET 2011*

Valid to: *Fri Nov 17 01:00:00 CET 2017*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:9C:E5:B9:5D:E3:E5:95:26:B1:2B:72:80:C1:CF:FB:DE:C7:FC:51:C3:DD:AE:25:D0:99:6F:D0:A7:07:C5:8C:45:95:55:2D:A2:05:D4:F5:8E:DF:2D:53:79:FD:2D:2C:38:C7:D0:2D:D8:F4:2F:11:1A:FF:D9:D9:38:DA:0E:DE:72:D2:D9:5C:BB:4D:A0:13:3E:F7:2D:1D:D9:FA:2E:0F:FF:56:38:ED:DA:40:23:7F:CB:8B:54:51:C1:37:BC:2D:8B:60:DC:49:B7:3B:AC:8C:6D:88:0B:6C:96:7F:8D:3D:CC:76:C4:B9:56:2B:85:6A:98:FB:FB:6E:E2:9C:B0:75:13:26:63:C7:2C:2C:CB:55:14:29:53:C9:BF:F3:5C:08:07:07:F1:EE:86:0C:7F:DA:C7:2C:F6:87:9B:BD:21:A1:59:18:74:4
D:FC:8B:A3:EB:B1:00:5A:3F:8F:5A:96:1F:DC:73:ED:09:58:73:A3:24:1C:8D:13:BC:B7:60:B7:54:2B:8C:FE:99:5B:80:79:57:05:15:FA:1B:1F:CB:BE:9A:D2:2F:30:12:CD:8B:AE:25:43:A2:D5:DA:30:C6:F8:4C:C8:EC:D8:BE:22:B2:09:0C:F5:FD:67:1F:37:8C:E4:42:29:5D:D7:87:1E:BA:EB:AD:9C:F0:11:66:74:4A:55:F8:9B:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

CRL Distribution Points *http://crl.ants.gouv.fr/antsv2/ac_racine.crl*

Certificate Policies *Policy OID: 2.5.29.32.0*

Subject Key Identifier *AD:34:0E:83:FD:4D:E6:5C:C1:56:0A:90:02:AB:3C:5C:C7:62:22:3F*

Authority Key Identifier *5D:1C:C4:DE:67:49:EF:46:53:1C:1C:54:FF:B5:C9:07:5B:0A:59:09*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *DA:B6:1E:66:61:E5:2A:21:1D:63:7B:41:39:FE:05:27:DA:D6:0F:31:62:53:EB:B1:3B:B0:7F:25:6C:74:E5:2E*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2018-06-01T00:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS101456/QCPPublic*

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Signature-3-Stars*

TSP Service Definition URI

URI *[en]* *http://sp.ants.gouv.fr/antsv2/en/ANTS_ACT_CA_CP_EN_v1.9.pdf*

URI *[fr]* *http://sp.ants.gouv.fr/antsv2/ANTS_AC_ACT_PC_v1.9.pdf*

1.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.2.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Acteur des Collectivités Territoriales - Signature 3 étoiles*

Name *[fr]* *Acteur des Collectivités Territoriales - Signature 3 étoiles*

Service digital identities

X509SubjectName

Subject CN: *Autorité de certification porteur ACT 3 étoiles*

Subject OU: *0002 130003262*

Subject O: *Agence Nationale des Titres Sécurisés*

Subject C: *FR*

X509SKI

X509 SK I *rTQOg/1N5lzBVgqQAqs8XMdiIj8=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

1.2.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.2.3 - History instance n.2 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Acteur des Collectivités Territoriales - Signature 3 étoiles*

Name *[fr]* *Acteur des Collectivités Territoriales - Signature 3 étoiles*

Service digital identities

X509SubjectName

Subject CN: *Autorité de certification porteur ACT 3 étoiles*

Subject OU: *0002 130003262*

Subject O: *Agence Nationale des Titres Sécurisés*

Subject C: *FR*

X509SKI

X509 SK I *rTQOg/1N5lzBVgqQAqs8XMdiIj8=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2011-11-16T23:00:00Z*

1.3 - Service (granted): Autorité de Certification Personnes AAE

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[fr]* *Autorité de Certification Personnes AAE*

Name *[en]* *Autorité de Certification Personnes AAE*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *149212416823265182982400884657663394077552 9*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIGCjCCA/KgAwIBAgISESD1daJii2Jal/vo8Ha4T5JpMA0GCSqGSIb3DQEBCwUAMIGaMQswCQYD
VQQGEwJGUjEwMC4GA1UECgwnQWdlbmNlIE5hdGlvbmFsZSBkZXMgVGl0cmVzIFPDqWN1cmlzw6lz
MRcwFQYDVQQLDA4wMDAyIDEzMDAwMzI2MjE0MDIGA1UEAwwrQXV0b3JpdMOpIGRlIENlcnRpZmlj
YXRpb24gUmFjaW5lIEFOVFMvQSBWMzEKMAgGA1UEBRMBMTAeFw0xMzA3MDQwMDAwMDBaFw0xOTA3
MDQwMDAwMDBaMIGXMQswCQYDVQQGEwJGUjEwMC4GA1UECgwnQWdlbmNlIE5hdGlvbmFsZSBkZXMg
VGl0cmVzIFPDqWN1cmlzw6lzMRcwFQYDVQQLDA4wMDAyIDEzMDAwMzI2MjExMC8GA1UEAwwoQXV0
b3JpdMOpIGRlIENlcnRpZmljYXRpb24gUGVyc29ubmVzIEFBRTEKMAgGA1UEBRMBMTCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBAM/1+unw1zpy/8suHFiDCHSl/2FrK87Y/ACjQE+ABlKH
0staGXYeApFNs4nC6W/xfjc775MNHCT5SggGqoaUH2wRz8/hT/jxBDKyAgknHYIuNY2SbsRVK1dR
i2Z3AU0unztbHzjKTSUm0dAbD7bg385tQ+oHslYUMPKk6ZSq/mYvov0+xR99xORnAMT3ALt/bb5d
vkiGJ3SuOrC+0rqiLI0g+D/tgneL2NGMjLB65dG143pooXVe0ctc8AizuxZK8JiPrlxoepy4+Fc8
NtuI1Cv2hLLaA9f7BzlCe+T2mVfW95hpcbmUpJ3eXISGoOckvC7mYMD8/ZZMs3KkxV76fU0CAwEA
AaOCAUkwggFFMBIGA1UdEwEB/wQIMAYBAf8CAQAwDgYDVR0PAQH/BAQDAgEGMBEGA1UdIAQKMAgw
BgYEVR0gADBIBgNVHR8EQTA/MD2gO6A5hjdodHRwOi8vY3JsLmFudHMuZ291di5mci9hbnRzYXYz
L2FjX3JhY2luZV9hbnRzYXYzXzEuY3JsMIGBBggrBgEFBQcBAQR1MHMwQgYIKwYBBQUHMAKGNmh0
dHA6Ly9zcC5hbnRzLmdvdXYuZnIvYW50c2F2My9jYV9yYWNpbmVfYW50c2F2M18xLmNlcjAtBggr
BgEFBQcwAYYhaHR0cDovL29jc3AuYW50cy5nb3V2LmZyL2FudHNhdjMvMB0GA1UdDgQWBBRg2Pwg
W6Kuco7QfrURlJQ8t4osCzAfBgNVHSMEGDAWgBRcA9V3mDVQKk1/j2+aVtuW+BXg4zANBgkqhkiG
9w0BAQsFAAOCAgEAILPrnZ4U6zRHOX9gULsRTHee/ASlaAjxuW0liy+x/c7LazgXEiRQGImAPYSA
lUAcrs4QRqA5wN1tY+srgVTkDSA6d8hoLCRrCIv3c3gybrvPP1iFqDhAY0f3eBC0bFWy+TAB4eNr
A7qC0csfbq6e7mrmhY/c2VAZZFy+DIVha8gtjJ+FoqfsH/Mz+1wo+lr8tuB3yc8vcc1ACoDxiLBd
VQDJm/DEU7QZFPpmCZjbL382mbHpJ9Kx7S+K6M+Hkvt+WEXqqE9THTA3ApBU8GU+QAN0btRD74sJ
xQzyIeyvmLxurt7xs4pynv5dAQg/fyGWOE4ZjOcV7IZcFozrVWq1p+WTNC83ClnlVuuQK/CQHJ8z
mhUHvPuU9V4vHgqGRarl7aUvFw60EbE2DtohndqJAyTk6qY+BBhwz+y7KQv/yDmCiT2hpSmrOsCC
m96e0uQbvRfewL/TR5RiexCV84MkF35fj6RmvHWXzXO/5mAjhIAnyQ3omgnWqzRNx6OxfPiHt8Pm
kZCi/+cw8MGY2uZ4gQnhzLS3KuDypRUeMAHSTUg1m7KWF9lTQ8JVGPHfzoRApQ81W1IlVMwBE/Hr
u/AgNkNedEdxG6uGZ6DcK7Uxz7fmsTkqXdUq4WJTkiT5VX8ZdMALLu2QTWiW94ksxKDzu3R5ovkY heB/ifyzVhezwi0=

-----END CERTIFICATE-----

Signature algorithm:	*SHA256withRSA*
Issuer SERIAL NUMBER:	*1*
Issuer CN:	*Autorité de Certification Racine ANTS/A V3*
Issuer OU:	*0002 130003262*
Issuer O:	*Agence Nationale des Titres Sécurisés*
Issuer C:	*FR*
Subject SERIAL NUMBER:	*1*
Subject CN:	*Autorité de Certification Personnes AAE*
Subject OU:	*0002 130003262*
Subject O:	*Agence Nationale des Titres Sécurisés*
Subject C:	*FR*
Valid from:	*Thu Jul 04 02:00:00 CEST 2013*
Valid to:	*Thu Jul 04 02:00:00 CEST 2019*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:CF:F5:FA:E9:F0:D7:3A:72:FF:CB:2E:1C:58:83:08:74:A5:FF:61:6B:2B:CE:D8:FC:00:A3:40:4F:80:06:52:87:D2:CB:5A:19:76:1E:02:91:4D:B3:89:C2:E9:6F:F1:7E:37:3B:EF:93:0D:1C:24:F9:4A:08:06:AA:86:94:1F:6C:11:CF:CF:E1:4F:F8:F1:04:32:B2:02:09:27:1D:82:2E:35:8D:92:6E:C4:55:2B:57:51:8B:66:77:01:4D:2E:9F:3B:5B:1F:38:CA:4D:25:26:D1:D0:1B:0F:B6:E0:DF:CE:6D:43:EA:07:B2:56:14:30:F2:A4:E9:94:AA:FE:66:2F:A2:FD:3E:C5:1F:7D:C4:E4:67:00:C4:F7:00:BB:7F:6D:BE:5D:BE:48:86:27:74:AE:3A:B0:BE:D2:BA:A2:2C:8D:20:F8:3F:ED:8
2:77:8B:D8:D1:8C:8C:B0:7A:E5:D1:B5:E3:7A:68:A1:75:5E:D1:CB:5C:F0:08:B3:BB:16:4A:F0:98:8F:AE:5C:68:7A:9C:B8:F8:57:3C:36:DB:88:D4:2B:F6:84:B2:DA:03:D7:FB:07:39:42:7B:E4:F6:99:57:D6:F7:98:69:71:B9:94:A4:9D:DE:5C:84:86:A0:E7:24:BC:2E:E6:60:C0:FC:FD:96:4C:B3:72:A4:C5:5E:FA:7D:4D:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

Certificate Policies *Policy OID: 2.5.29.32.0*

CRL Distribution Points *http://crl.ants.gouv.fr/antsav3/ac_racine_antsav3_1.crl*

Authority Info Access *http://sp.ants.gouv.fr/antsav3/ca_racine_antsav3_1.cer*

http://ocsp.ants.gouv.fr/antsav3/

Subject Key Identifier *60:D8:FC:20:5B:A2:AE:72:8E:D0:7E:B5:11:94:94:3C:B7:8A:2C:0B*

Authority Key Identifier *5C:03:D5:77:98:35:50:2A:4D:7F:8F:6F:9A:56:DB:96:F8:15:E0:E3*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *B5:45:6F:7A:69:61:A4:9C:53:7C:CC:1D:50:76:7D:2D:FA:06:5F:54:0E:86:E1:C9:92:FF:32:4E:B8:18:C8:4F*

X509SubjectName

Subject SERIAL NUMBER: *1*

Subject CN: *Autorité de Certification Personnes AAE*

Subject OU: *0002 130003262*

Subject O: *Agence Nationale des Titres Sécurisés*

Subject C: *FR*

X509SKI

X509 SK I *YNj8IFuirnKO0H61EZSUPLeKLAs=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

TSP Service Definition URI

URI *[en]* *https://sp.ants.gouv.fr/antsav3/ANTS_AC_Personnes_AAE_PC.pdf*

URI *[fr]* *https://sp.ants.gouv.fr/antsav3/ANTS_AC_Personnes_AAE_PC.pdf*

1.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.3.2 - Extension (critical): Qualifiers [QCWithSSCD]

Qualifier type description *[en]* *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the presence or absence of Secure Signature Creation Device (SSCD) support ARE supported by an SSCD (i.e. that that the private key associated with the public key in the certificate is stored in a Secure Signature Creation Device conformant with the applicable European legislation);*

[fr] *elle est assurée par le prestataire de service de confiance et contrôlée (modèle de contrôle) ou vérifiés (modèle d'accréditation) par l'État membre de référence (respectivement son Organe de surveillance ou organisme d'accréditation) que tous les certificats qualifiés délivrés dans le cadre du service identifié dans «Service digital identity» et en outre identifié par les informations des filtres utilisés pour identifier plus précisément dans le cadre du "Sdi" de service de confiance identifiés, l'ensemble précis de certificats qualifiés pour lesquels cette information supplémentaire est nécessaire en ce qui concerne la présence ou l'absence de dispositif sécurisé de création de signature (SSCD) de soutien sont pris en charge par un SSCD (à savoir que la clé privée associée à la clé publique du certificat est stocké dans un dispositif sécurisé conforme à la législation européenne applicable de création de signature);*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithSSCD*

Criteria list assert=atLeastOne

Policy Identifier nodes:

Identifier *1.2.250.1.200.3.1.2.3.1*

Policy Identifier nodes:

Identifier *1.2.250.1.200.3.1.5.3.1*

1.3.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[fr]* *Autorité de Certification Personnes AAE*

Name *[en]* *Autorité de Certification Personnes AAE*

Service digital identities

X509SubjectName

Subject SERIAL NUMBER: *1*

Subject CN: *Autorité de Certification Personnes AAE*

Subject OU: *0002 130003262*

Subject O: *Agence Nationale des Titres Sécurisés*

Subject C: *FR*

X509SKI

X509 SK I *YNj8IFuirnKO0H61EZSUPLeKLAs=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

1.3.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.3.3.2 - Extension (critical): Qualifiers [QCWithSSCD]

Qualifier type description *[en]* *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the presence or absence of Secure Signature Creation Device (SSCD) support ARE supported by an SSCD (i.e. that that the private key associated with the public key in the certificate is stored in a Secure Signature Creation Device conformant with the applicable European legislation);*

[fr] *elle est assurée par le prestataire de service de confiance et contrôlée (modèle de contrôle) ou vérifiés (modèle d'accréditation) par l'État membre de référence (respectivement son Organe de surveillance ou organisme d'accréditation) que tous les certificats qualifiés délivrés dans le cadre du service identifié dans «Service digital identity» et en outre identifié par les informations des filtres utilisés pour identifier plus précisément dans le cadre du "Sdi" de service de confiance identifiés, l'ensemble précis de certificats qualifiés pour lesquels cette information supplémentaire est nécessaire en ce qui concerne la présence ou l'absence de dispositif sécurisé de création de signature (SSCD) de soutien sont pris en charge par un SSCD (à savoir que la clé privée associée à la clé publique du certificat est stocké dans un dispositif sécurisé conforme à la législation européenne applicable de création de signature);*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithSSCD*

Criteria list assert=atLeastOne

Policy Identifier nodes:

Identifier *1.2.250.1.200.3.1.2.3.1*

Policy Identifier nodes:

Identifier *1.2.250.1.200.3.1.5.3.1*

1.4 - Service (granted): Autorité de Certification Personnes AAE

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Autorité de Certification Personnes AAE*

Name *[fr]* *Autorité de Certification Personnes AAE*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1491819343655284287526853912557974355166667*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIGCjCCA/KgAwIBAgISESAQIo5h+NzwuM1WQjlWV8XLMA0GCSqGSIb3DQEBCwUAMIGaMQswCQYD
VQQGEwJGUjEwMC4GA1UECgwnQWdlbmNlIE5hdGlvbmFsZSBkZXMgVGl0cmVzIFPDqWN1cmlzw6lz
MRcwFQYDVQQLDA4wMDAyIDEzMDAwMzI2MjE0MDIGA1UEAwwrQXV0b3JpdMOpIGRlIENlcnRpZmlj
YXRpb24gUmFjaW5lIEFOVFMvQSBWMzEKMAgGA1UEBRMBMTAeFw0xNjA1MjQwMDAwMDBaFw0yMjA1
MjQwMDAwMDBaMIGXMQswCQYDVQQGEwJGUjEwMC4GA1UECgwnQWdlbmNlIE5hdGlvbmFsZSBkZXMg
VGl0cmVzIFPDqWN1cmlzw6lzMRcwFQYDVQQLDA4wMDAyIDEzMDAwMzI2MjExMC8GA1UEAwwoQXV0
b3JpdMOpIGRlIENlcnRpZmljYXRpb24gUGVyc29ubmVzIEFBRTEKMAgGA1UEBRMBMjCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBALv0gTcUZ9CAjCaFjXj7343LmGEVGH2El/FW0aYuVhqN
9nXPf4A3s8bkhaaD2N9qCcJXdvy1BUH5JWI+t8cO9dmq1fJi0JbuWIr48TC9KNzVOLN6EAnQYBzA
1EM514buOQMj++YQxss0B5lmnJEaTdoAeI3+WI10ijWruRwgCZNF+GOSJk6s1rNE/bkq4qQTX6RS
PkZl5ByfDeo2+cJj6IZcMVc7bwgzTkQAMw9He0JoVe88RADor1+GC6OWQzBPr5W+XZQ2P3Kd20tN
gESfPBzRHawaO7NKVEBb7JVEFWlyEXW7lky373t+553eBMOEtqeSuwkKZJvW9R3mOfMBJakCAwEA
AaOCAUkwggFFMBIGA1UdEwEB/wQIMAYBAf8CAQAwDgYDVR0PAQH/BAQDAgEGMBEGA1UdIAQKMAgw
BgYEVR0gADBIBgNVHR8EQTA/MD2gO6A5hjdodHRwOi8vY3JsLmFudHMuZ291di5mci9hbnRzYXYz
L2FjX3JhY2luZV9hbnRzYXYzXzEuY3JsMIGBBggrBgEFBQcBAQR1MHMwQgYIKwYBBQUHMAKGNmh0
dHA6Ly9zcC5hbnRzLmdvdXYuZnIvYW50c2F2My9jYV9yYWNpbmVfYW50c2F2M18xLmNlcjAtBggr
BgEFBQcwAYYhaHR0cDovL29jc3AuYW50cy5nb3V2LmZyL2FudHNhdjMvMB0GA1UdDgQWBBTay3b6
httsUMIOPmOB4q0MfAiB9jAfBgNVHSMEGDAWgBRcA9V3mDVQKk1/j2+aVtuW+BXg4zANBgkqhkiG
9w0BAQsFAAOCAgEASF4iuoF6Msq8adhclXASa5Q7v7WaMPJTX2BWg4KPjVH1IkuoiNCO0HFozOKo
kAff4VD1uPdkgq91KjJw6kgAbac2kL1xKADrDMvtvx1a84/gopAmc0Gv8mPma2uR3OVUzwEx24Cv
W2MAZfOmVsdQMGBKPXHZOKxs6dc0Yw7L5ZBuX7NNZSDOXv4TWeINp+Gkw6pscAtNrSP/nLjlMSTM
EtA3mbVhLra/CFJJAapNFqsSDdwSWLyoQbCewIij7nvfriqKJXOT+VlbAJeDNvZJxFMis+zlCcBh
QjkcvhuGfbBvesdIkPPh0tklViJa4hZ+UtunC8hA+AAF6Xj21r/pF/MNs9A7iHX33WRS1kwynQtW
htLtz4256MBffz/09pG8KJm0qX5VIRfE1WTz79aK4LIm9Mk52+kuAfHb+1Si67rffn8wtGh8fKUM
sIKwSWDLxEPpnOkbJilRQpK/gFFVebMWcFiY7ffAN2GGnL0LCzgRLy2eLEp5Rg0lWByzhNjWAcZ1
ZfIsc6UHPdEYfs+8OkBS+q7W8sEcbShQRMLYgu6tdWbdQ+tjcvtxllWXYSSRLq0rhUetA6aTQO5R
qjNTix5eAf1pf2QvT5F+LVIZARcy9AzFEUj1ck65jmxKWe47WcaCpWoucFNOsqAs3EkZqJM0mf4S 7lrWHby3S5D1N5M=

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer SERIAL NUMBER: *1*

Issuer CN: *Autorité de Certification Racine ANTS/A V3*

Issuer OU: *0002 130003262*

Issuer O: *Agence Nationale des Titres Sécurisés*

Issuer C: *FR*

Subject SERIAL NUMBER: *2*

Subject CN: *Autorité de Certification Personnes AAE*

Subject OU: *0002 130003262*

Subject O: *Agence Nationale des Titres Sécurisés*

Subject C: *FR*

Valid from: *Tue May 24 02:00:00 CEST 2016*

Valid to: *Tue May 24 02:00:00 CEST 2022*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:BB:F4:81:37:14:67:D0:80:8C:26:85:8D:78:FB:DF:8D:CB:98:61:15:18:7D:84:97:F1:56:D1:A6:2E:56:1A:8D:F6:75:CF:7F:80:37:B3:C6:E4:85:A6:83:D8:DF:6A:09:C2:57:76:FC:B5:05:41:F9:25:62:3E:B7:C7:0E:F5:D9:AA:D5:F2:62:D0:96:EE:58:8A:F8:F1:30:BD:28:DC:D5:38:B3:7A:10:09:D0:60:1C:C0:D4:43:39:D7:86:EE:39:03:23:FB:E6:10:C6:CB:34:07:99:66:9C:91:1A:4D:DA:00:78:8D:FE:58:8D:74:8A:35:AB:B9:1C:20:09:93:45:F8:63:92:26:4E:AC:D6:B3:44:FD:B9:2A:E2:A4:13:5F:A4:52:3E:46:65:E4:1C:9F:0D:EA:36:F9:C2:63:E8:86:5C:31:57:3B:6F:08:33:4E:44:00:33:0F:47:7B:42:68:55:EF:3C:44:00:E8:AF:5F:86:0B:A3:96:43:30:4F:AF:95:BE:5D:94:36:3F:72:9D:DB:4B:4D:80:44:9F:3C:1C:D1:1D:AC:1A:3B:B3:4A:54:40:5B:EC:95:44:15:69:72:11:75:BB:96:4C:B7:EF:7B:7E:E7:9D:DE:04:C3:84:B6:A7:92:BB:09:0A:64:9B:D6:F5:1D:E6:39:F3:01:25:A9:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

Certificate Policies *Policy OID: 2.5.29.32.0*

CRL Distribution Points *http://crl.ants.gouv.fr/antsav3/ac_racine_antsav3_1.crl*

Authority Info Access *http://sp.ants.gouv.fr/antsav3/ca_racine_antsav3_1.cer*

http://ocsp.ants.gouv.fr/antsav3/

Subject Key Identifier *DA:CB:76:FA:86:DB:6C:50:C2:0E:3E:63:81:E2:AD:0C:7C:08:81:F6*

Authority Key Identifier *5C:03:D5:77:98:35:50:2A:4D:7F:8F:6F:9A:56:DB:96:F8:15:E0:E3*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *75:B7:CC:2E:24:65:11:D8:CD:BB:C5:75:3D:C3:A6:22:50:E3:9E:D3:AD:44:A5:35:9F:0B:56:65:78:17:C9:34*

X509SubjectName

Subject SERIAL NUMBER: *2*

Subject CN: *Autorité de Certification Personnes AAE*

Subject OU: *0002 130003262*

Subject O: *Agence Nationale des Titres Sécurisés*

Subject C: *FR*

X509SKI

X509 SK I *2st2+obbbFDCDj5jgeKtDHwIgfY=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

TSP Service Definition URI

URI *[en]* *https://sp.ants.gouv.fr/antsav3/ANTS_AC_Personnes_AAE_PC.pdf*

URI *[fr]* *https://sp.ants.gouv.fr/antsav3/ANTS_AC_Personnes_AAE_PC.pdf*

1.4.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.4.2 - Extension (critical): Qualifiers [QCWithSSCD]

Qualifier type description *[en]* *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the presence or absence of Secure Signature Creation Device (SSCD) support ARE supported by an SSCD (i.e. that that the private key associated with the public key in the certificate is stored in a Secure Signature Creation Device conformant with the applicable European legislation);*

[fr] *elle est assurée par le prestataire de service de confiance et contrôlée (modèle de contrôle) ou vérifiés (modèle d'accréditation) par l'État membre de référence (respectivement son Organe de surveillance ou organisme d'accréditation) que tous les certificats qualifiés délivrés dans le cadre du service identifié dans «Service digital identity» et en outre identifié par les informations des filtres utilisés pour identifier plus précisément dans le cadre du "Sdi" de service de confiance identifiés, l'ensemble précis de certificats qualifiés pour lesquels cette information supplémentaire est*

nécessaire en ce qui concerne la présence ou l'absence de dispositif sécurisé de création de signature (SSCD) de soutien sont pris en charge par un SSCD (à savoir que la clé privée associée à la clé publique du certificat est stocké dans un dispositif sécurisé conforme à la législation européenne applicable de création de signature);

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithSSCD*

Criteria list assert=atLeastOne

Policy Identifier nodes:

Identifier *1.2.250.1.200.3.1.2.3.1*

Policy Identifier nodes:

Identifier *1.2.250.1.200.3.1.5.3.1*

1.4.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Autorité de Certification Personnes AAE*

Name *[fr]* *Autorité de Certification Personnes AAE*

Service digital identities

X509SubjectName

Subject SERIAL NUMBER: *2*

Subject CN: *Autorité de Certification Personnes AAE*

Subject OU: *0002 130003262*

Subject O: *Agence Nationale des Titres Sécurisés*

Subject C: *FR*

X509 SK I *2st2+obbbFDCDj5jgeKtDHwIgfY=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

1.4.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.4.3.2 - Extension (critical): Qualifiers [QCWithSSCD]

Qualifier type description *[en]* *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the presence or absence of Secure Signature Creation Device (SSCD) support ARE supported by an SSCD (i.e. that that the private key associated with the public key in the certificate is stored in a Secure Signature Creation Device conformant with the applicable European legislation);*

[fr] *elle est assurée par le prestataire de service de confiance et contrôlée (modèle de contrôle) ou vérifiés (modèle d'accréditation) par l'État membre de référence (respectivement son Organe de surveillance ou organisme d'accréditation) que tous les certificats qualifiés délivrés dans le cadre du service identifié dans «Service digital identity» et en outre identifié par les informations des filtres utilisés pour identifier plus précisément dans le cadre du "Sdi" de service de confiance identifiés, l'ensemble précis de certificats qualifiés pour lesquels cette information supplémentaire est nécessaire en ce qui concerne la présence ou l'absence de dispositif sécurisé de création de signature (SSCD) de soutien sont pris en charge par un SSCD (à savoir que la clé privée associée à la clé publique du certificat est stocké dans un dispositif sécurisé conforme à la législation européenne applicable de création de signature);*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithSSCD*

Criteria list assert=atLeastOne

Policy Identifier nodes:

Identifier *1.2.250.1.200.3.1.2.3.1*

Policy Identifier nodes:

Identifier *1.2.250.1.200.3.1.5.3.1*

1.5 - Service (granted): Autorité de certification porteur AAE 3 étoiles V2

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Autorité de certification porteur AAE 3 étoiles V2*

Name *[fr]* *Autorité de certification porteur AAE 3 étoiles V2*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *149184925563579838249276203087367386730589 9*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIFQDCCAyigAwIBAgISESAmo2TiYIA9698SJX2k7aOrMA0GCSqGSIb3DQEBCwUAMGIxCzAJBgNV
BAYTAkZSMQ0wCwYDVQQKEwRHb3V2MRcwFQYDVQQLEw4wMDAyIDEzMDAwMzI2MjErMCkGA1UEAwwi
QXV0b3JpdMOpIGRlIGNlcnRpZmljYXRpb24gQU5UUyBWMjAeFw0xNDA2MTcwMDAwMDBaFw0yMDA2
MTcwMDAwMDBaMIGXMQswCQYDVQQGEwJGUjEwMC4GA1UECgwnQWdlbmNlIE5hdGlvbmFsZSBkZXMg
VGl0cmVzIFPDqWN1cmlzw6lzMRcwFQYDVQQLDA4wMDAyIDEzMDAwMzI2MjE9MDsGA1UEAww0QXV0
b3JpdMOpIGRlIGNlcnRpZmljYXRpb24gcG9ydGV1ciBBQUUgMyDDqXRvaWxlcyBWMjCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBAJ5PMXVTmPtiVL8tacgP8vO4EL+kjjWNdIX5Nmln2fYw
4i5ErrEz2vHbPdVmNX2Efa7MjXuKZff0TrJ4KkS1mmOYVeKT/5ihBLkHZOj9x7tN+zvPtZaefrHs
zmcW9CCi8ozpCa69bBFQWmDo95ZtkHtQ+iWPmkO94oIXGmte9Bj+D3t5233t41i59qGIC+g+2J+R
cPlGZ/1luG8HP271p7f68Y6iQGXehDGgeyPVb6W2cXUwLC8PnkC0kp9TNCrwuOkYaUPUR6QW1OS4
2hyann+lNyd7d6sdySOI0WTkBnk+IpqMRTWQjc7DDzYaECzBDpwwgzx4SCuHnrczeOxgRQ8CAwEA
AaOBuTCBtjAOBgNVHQ8BAf8EBAMCAQYwEgYDVR0TAQH/BAgwBgEB/wIBADA9BgNVHR8ENjA0MDKg
MKAuhixodHRwOi8vY3JsLmFudHMuZ291di5mci9hbnRzdjIvYWNfcmFjaW5lLmNybDARBgNVHSAE
CjAIMAYGBFUdIAAwHQYDVR0OBBYEFO2J4b1VOyGom88vx9iEsHkTuopqMB8GA1UdIwQYMBaAFF0c
xN5nSe9GUxwcVP+1yQdbClkJMA0GCSqGSIb3DQEBCwUAA4ICAQBwzMVN+33Iu6SfdgTxMz4N2trN
UeFuvvzvnm0J1crrp5j5gx368IUJEvtgWACT4zQntMuOXKtVLvJhzL9x/eXW57w+JS1DdyWdKHIW
ky6weOgmdnf0V4c/jMI7UpT+N2VImSOBm71Vz010y0PChckF1ALkQJ27c+pvNOFh9nGg9t9iCuHM
HbdLDUfkCT8tkpJoYRcGjpQj9Kq4ls/eI11WzbX5CkEiV+fu01YMcsfvrj0jUGaijHefLv/fPWBa
6/KNSsh2JXfcrWoCKL0mQqioqkRmKaYG5KMJrls/Ctle4oNkrvcO/PpR/UlFEs4JhMKrSZBYXkNh
6lx6vsKnLpy6mkbzyBYBDadHogclsVuVd/2EHflPNjisDJ0PoLhk8Q6Z4NHRa3x0XyKcYE8U3Pc1
H9OQOXFr+apW5ws4xW8wKQAgCwMQE/cxRSld3O6MV96fHWMsJDHShCn4JTWVdPEgmsb/HjXWJj7z
EGPXqRdpRbvtV7/VgjTT0l2Q3Cg4Y2IWEk7vdFgmPA5nHZbU56nwxV1uvlhTj6Awkka2Y2LKwWbH
7J4pbGjwp/OWy3e/3tGCX0GtWBH6DJILJySkyr2VV73pECFACqGeyBGQQZ1YBl5NEJJwuMUKIyN3
SiYb8DxYyuHK95wAEicAhxWHreMy8iHbgrnbaKwvFiPHPkXnFg==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Autorité de certification ANTS V2*

Issuer OU: *0002 130003262*

Issuer O: *Gouv*

Issuer C: *FR*

Subject CN: *Autorité de certification porteur AAE 3 étoiles V2*

Subject OU: *0002 130003262*

Subject O: *Agence Nationale des Titres Sécurisés*

Subject C: *FR*

Valid from: *Tue Jun 17 02:00:00 CEST 2014*

Valid to: *Wed Jun 17 02:00:00 CEST 2020*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:9E:4F:31:75:53:98:FB:62:54:BF:2D:69:C8:0F:F2:F3:B
8:10:BF:A4:8E:35:8D:74:85:F9:36:69:67:D9:F6:30:E2:2E:44:AE:B1:33:DA:F1:DB:3D:D5:66:35:7D:84:7D:AE:CC:8D:7B:8A:65:F7:F4:4E:B2:78:2A:44:B5:9A:63:98:
55:E2:93:FF:98:A1:04:B9:07:64:E8:FD:C7:BB:4D:FB:3B:CF:B5:96:9E:7E:B1:EC:CE:67:16:F4:20:A2:F2:8C:E9:09:AE:BD:6C:11:50:5A:60:E8:F7:96:6D:90:7B:50:FA:
25:8F:9A:43:BD:E2:82:17:1A:6B:5E:F4:18:FE:0F:7B:79:DB:7D:ED:E3:58:B9:F6:A1:88:0B:E8:3E:D8:9F:91:70:F9:46:67:FD:65:B8:6F:07:3F:6E:F5:A7:B7:FA:F1:8E:
A2:40:65:DE:84:31:A0:7B:23:D5:6F:A5:B6:71:75:30:2C:2F:0F:9E:40:B4:92:9F:53:34:2A:F0:B8:E9:18:69:43:D4:47:A4:16:D4:E4:B8:DA:1C:9A:9E:7F:A5:37:27:7B
:77:AB:1D:C9:23:88:D1:64:E4:06:79:3E:22:9A:8C:45:35:90:8D:CE:C3:0F:36:1A:10:2C:C1:0E:9C:30:83:3C:78:48:2B:87:9E:B7:33:78:EC:60:45:0F:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

CRL Distribution Points *http://crl.ants.gouv.fr/antsv2/ac_racine.crl*

Certificate Policies *Policy OID: 2.5.29.32.0*

Subject Key Identifier *ED:89:E1:BD:55:3B:21:A8:9B:CF:2F:C7:D8:84:B0:79:13:BA:8A:6A*

Authority Key Identifier *5D:1C:C4:DE:67:49:EF:46:53:1C:1C:54:FF:B5:C9:07:5B:0A:59:09*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *D1:64:A7:24:DE:57:57:43:27:74:1E:53:93:97:39:DE:44:07:ED:3C:33:51:5A:27:1F:7F:8B:DE:A3:8D:99:58*

X509SubjectName

Subject CN: *Autorité de certification porteur AAE 3 étoiles V2*

Subject OU: *0002 130003262*

Subject O: *Agence Nationale des Titres Sécurisés*

Subject C: *FR*

X509SKI

X509 SK I *7YnhvVU7Iaibzy/H2ISweRO6imo=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

TSP Service Definition URI

URI *[en]* *http://sp.ants.gouv.fr/antsv2/ANTSv2_AC_AAE_PC.pdf*

URI *[fr]* *http://sp.ants.gouv.fr/antsv2/ANTSv2_AC_AAE_PC.pdf*

1.5.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.5.2 - Extension (critical): Qualifiers [QCWithSSCD]

Qualifier type description	*[en]*	*it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the presence or absence of Secure Signature Creation Device (SSCD) support ARE supported by an SSCD (i.e. that that the private key associated with the public key in the certificate is stored in a Secure Signature Creation Device conformant with the applicable European legislation);*
	[fr]	*elle est assurée par le prestataire de service de confiance et contrôlée (modèle de contrôle) ou vérifiés (modèle d'accréditation) par l'État membre de référence (respectivement son Organe de surveillance ou organisme d'accréditation) que tous les certificats qualifiés délivrés dans le cadre du service identifié dans «Service digital identity» et en outre identifié par les informations des filtres utilisés pour identifier plus précisément dans le cadre du "Sdi" de service de confiance identifiés, l'ensemble précis de certificats qualifiés pour lesquels cette information supplémentaire est nécessaire en ce qui concerne la présence ou l'absence de dispositif sécurisé de création de signature (SSCD) de soutien sont pris en charge par un SSCD (à savoir que la clé privée associée à la clé publique du certificat est stocké dans un dispositif sécurisé conforme à la législation européenne applicable de création de signature);*
Qualifier		*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithSSCD*

Criteria list assert=all

Key Usage	*[nonRepudiation]*	*true*
Policy Identifier nodes:		
Identifier		*1.2.250.1.200.2.3.1.2*

1.5.3 - History instance n.1 - Status: granted

Service Type Identifier		*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*
Service Name		
Name	*[en]*	*Autorité de certification porteur AAE 3 étoiles V2*
Name	*[fr]*	*Autorité de certification porteur AAE 3 étoiles V2*

Service digital identities

X509SubjectName

Subject CN:	*Autorité de certification porteur AAE 3 étoiles V2*
Subject OU:	*0002 130003262*
Subject O:	*Agence Nationale des Titres Sécurisés*
Subject C:	*FR*

X509SKI

X509 SK I	*7YnhvVU7Iaibzy/H2ISweRO6imo=*

Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

1.5.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.5.3.2 - Extension (critical): Qualifiers [QCWithSSCD]

Qualifier type description *[en]* *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the presence or absence of Secure Signature Creation Device (SSCD) support ARE supported by an SSCD (i.e. that that the private key associated with the public key in the certificate is stored in a Secure Signature Creation Device conformant with the applicable European legislation);*

[fr] *elle est assurée par le prestataire de service de confiance et contrôlée (modèle de contrôle) ou vérifiés (modèle d'accréditation) par l'État membre de référence (respectivement son Organe de surveillance ou organisme d'accréditation) que tous les certificats qualifiés délivrés dans le cadre du service identifié dans «Service digital identity» et en outre identifié par les informations des filtres utilisés pour identifier plus précisément dans le cadre du "Sdi" de service de confiance identifiés, l'ensemble précis de certificats qualifiés pour lesquels cette information supplémentaire est nécessaire en ce qui concerne la présence ou l'absence de dispositif sécurisé de création de signature (SSCD) de soutien sont pris en charge par un SSCD (à savoir que la clé privée associée à la clé publique du certificat est stocké dans un dispositif sécurisé conforme à la législation européenne applicable de création de signature);*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithSSCD*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Policy Identifier nodes:

Identifier *1.2.250.1.200.2.3.1.2*

1.6 - Service (granted): Autorité de certification porteur ACT 3 étoiles V2

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Autorité de certification porteur ACT 3 étoiles V2*

Name *[fr]* *Autorité de certification porteur ACT 3 étoiles V2*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *149188071781489898226944020877259318749597 9*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIFQDCCAyigAwIBAgISESA+TsoTvs9uM5M1TMrHxyArMA0GCSqGSIb3DQEBCwUAMGIxCzAJBgNV
BAYTAkZSMQ0wCwYDVQQKEwRHb3V2MRcwFQYDVQQLEw4wMDAyIDEzMDAwMzI2MjErMCkGA1UEAwwi
QXV0b3JpdMOpIGRlIGNlcnRpZmljYXRpb24gQU5UUyBWMjAeFw0xNDA2MTcwMDAwMDBaFw0yMDA2
MTcwMDAwMDBaMIGXMQswCQYDVQQGEwJGUjEwMC4GA1UECgwnQWdlbmNlIE5hdGlvbmFsZSBkZXMg
VGl0cmVzIFPDqWN1cmlzw6lzMRcwFQYDVQQLDA4wMDAyIDEzMDAwMzI2MjE9MDsGA1UEAww0QXV0
b3JpdMOpIGRlIGNlcnRpZmljYXRpb24gcG9ydGV1ciBBQ1QgMyDDqXRvaWxlcyBWMjCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBAKwSk6FgH3nLN5vOPvxQu+tiYcKjAn5kD2R/+luTH38v
ISxE2hI0w8bTFEZ5r+YcyJYzxBHZEo94E35xjL8L2T788X/doRNm1mYJgbiV5p0QFD6uk6Du0z9T
g0LsyJddq92YCfZDkPq24QtazTeE6YMuT4JO/azpj8i+7V9j8gWKQdwocCQVLH0A/35t9Y78JYoX
Px3puTPJZd4wwaHuA9bIAnTFbR3L/yD3KLzCYr7qxQT0M/BYxKvaZElDg2L7Gy9wT/N/PGRIAMPl
gg/ChpUJ/6mw8MxF11b4/E01mgPI2tAk+qy2wIubuCR/DYzCrhsgj9k/+nvykVhAQnlv8wkCAwEA
AaOBuTCBtjAOBgNVHQ8BAf8EBAMCAQYwEgYDVR0TAQH/BAgwBgEB/wIBADA9BgNVHR8ENjA0MDKg
MKAuhixodHRwOi8vY3JsLmFudHMuZ291di5mci9hbnRzdjIvYWNfcmFjaW5lLmNybDARBgNVHSAE
CjAIMAYGBFUdIAAwHQYDVR0OBBYEFHInhbOcP0ik9F3H9LDqqG319yKVMB8GA1UdIwQYMBaAFF0c
xN5nSe9GUxwcVP+1yQdbClkJMA0GCSqGSIb3DQEBCwUAA4ICAQAhgEFKq0n5o7ckzEJ16KizZeEr
Iu5ykVBmr9ldfzthx21DjFXbg4NKvVgo7XgKZHWAJMjspF8Kxk1uxw23CeebdlWGng4e5tedK+0L
o1H27UWVtIynqFsNL1rcQtuEX9J6XtoTOYsVHlN0vxmGbgnAd0Jk1awtira9fTMvyrq1WAMoMhN1
Yp8LKVCcdTtH5be2iBIEu9X+L9Ds1+ZlYsTSg+ZYlCZ1ESC3k0TdpzzaZFfTjbRpOZgI7ayw1PaH
1hsTSpZKM3wgUHSKFoA0whwOe0hMZOeJeq8FrUmmhSQDTT2KUE8hDNyvhWvkTrXWPBA1hukD4eNO
hA6ez1VAmYhuRpw03ObeWSTY4+6oY7gZE+QmBrpqiJV97KYYE1gUXEf/zMiYbT40RmBjnYYZ8PHk
QLeftMYv+uSrWt0nW25tMNQzcgYrSbUT6b7vUAUDETYo2wRRsT1Vsj+gk9z1lTc/INMnl7DwwFZE
vNDFgnYqluUdk1NTRTsifbPVmrqXI2zpSoav8U3h+fFfdDHcyrXY8AQRQBNJg7MAvJWCyMjSp3Ue
TqLk93UFOUdKmgwHs4/WBwV5elgL619llMEGOXhya2s8gETHtMt1MLueKDXnN0oDyF9ak8AuOFRK
QizvRt0hpHUzmK0KL/yPO1tsZEnA+ORvmMJixOTKllzTx1GdqQ==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Autorité de certification ANTS V2*

Issuer OU: *0002 130003262*

Issuer O: *Gouv*

Issuer C: *FR*

Subject CN: *Autorité de certification porteur ACT 3 étoiles V2*

Subject OU: *0002 130003262*

Subject O: *Agence Nationale des Titres Sécurisés*

Subject C: *FR*

Valid from: *Tue Jun 17 02:00:00 CEST 2014*

Valid to: *Wed Jun 17 02:00:00 CEST 2020*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:AC:12:93:A1:60:1F:79:CB:37:9B:CE:3E:FC:50:BB:EB:
62:61:C2:A3:02:7E:64:0F:64:7F:FA:5B:93:1F:7F:2F:21:2C:44:DA:12:34:C3:C6:D3:14:46:79:AF:E6:1C:C8:96:33:C4:11:D9:12:8F:78:13:7E:71:8C:BF:0B:D9:3E:FC:
F1:7F:DD:A1:13:66:D6:66:09:81:B8:95:E6:9D:10:14:3E:AE:93:A0:EE:D3:3F:53:83:42:EC:C8:97:5D:AB:DD:98:09:F6:43:90:FA:B6:E1:0B:5A:CD:37:84:E9:83:2E:4
F:82:4E:FD:AC:E9:8F:C8:BE:ED:5F:63:F2:05:8A:41:DC:28:70:24:15:2C:7D:00:FF:7E:6D:F5:8E:FC:25:8A:17:3F:1D:E9:B9:33:C9:65:DE:30:C1:A1:EE:03:D6:C8:02:7
4:C5:6D:1D:CB:FF:20:F7:28:BC:C2:62:BE:EA:C5:04:F4:33:F0:58:C4:AB:DA:64:49:43:83:62:FB:1B:2F:70:4F:F3:7F:3C:64:48:00:C3:E5:82:0F:C2:86:95:09:FF:A9:B

0:F0:CC:45:D7:56:F8:FC:4D:35:9A:03:C8:DA:D0:24:FA:AC:B6:C0:8B:9B:B8:24:7F:0D:8C:C2:AE:1B:20:8F:D9:3F:FA:7B:F2:91:58:40:42:79:6F:F3:09:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

CRL Distribution Points *http://crl.ants.gouv.fr/antsv2/ac_racine.crl*

Certificate Policies *Policy OID: 2.5.29.32.0*

Subject Key Identifier *72:27:85:B3:9C:3F:48:A4:F4:5D:C7:F4:B0:EA:A8:6D:F5:F7:22:95*

Authority Key Identifier *5D:1C:C4:DE:67:49:EF:46:53:1C:1C:54:FF:B5:C9:07:5B:0A:59:09*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *82:44:91:FD:41:85:12:DF:D3:64:81:A5:CD:4D:BE:49:B1:A4:19:21:72:8F:A1:67:29:04:C5:3E:50:BA:5B:06*

X509SubjectName

Subject CN: *Autorité de certification porteur ACT 3 étoiles V2*

Subject OU: *0002 130003262*

Subject O: *Agence Nationale des Titres Sécurisés*

Subject C: *FR*

X509SKI

X509 SK I *cieFs5w/SKT0Xcf0sOqobfX3IpU=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

TSP Service Definition URI

URI *[en]* *http://sp.ants.gouv.fr/antsv2/ANTSv2_AC_ACT_PC.pdf*

URI *[fr]* *http://sp.ants.gouv.fr/antsv2/ANTSv2_AC_ACT_PC.pdf*

1.6.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.6.2 - Extension (critical): Qualifiers [QCWithSSCD]

Qualifier type description *[en]* *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the presence or absence of Secure Signature Creation Device (SSCD) support ARE supported by an SSCD (i.e. that that the private key associated with the public key in the certificate is stored in a Secure Signature Creation Device conformant with the applicable European legislation);*

[fr] *elle est assurée par le prestataire de service de confiance et contrôlée (modèle de contrôle) ou vérifiés (modèle d'accréditation) par l'État membre de référence (respectivement son Organe de surveillance ou organisme d'accréditation) que tous les certificats qualifiés délivrés dans le cadre du service identifié dans «Service digital identity» et en outre identifié par les informations des filtres utilisés pour identifier plus précisément dans le cadre du "Sdi" de service de confiance identifiés, l'ensemble précis de certificats qualifiés pour lesquels cette information supplémentaire est nécessaire en ce qui concerne la présence ou l'absence de dispositif sécurisé de création de signature (SSCD) de soutien sont pris en charge par un SSCD (à savoir que la clé privée associée à la clé publique du certificat est stocké dans un dispositif sécurisé conforme à la législation européenne applicable de création de signature);*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithSSCD*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Policy Identifier nodes:

Identifier *1.2.250.1.200.2.5.1.2*

1.6.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Autorité de certification porteur ACT 3 étoiles V2*

Name *[fr]* *Autorité de certification porteur ACT 3 étoiles V2*

Service digital identities

X509SubjectName

Subject CN: *Autorité de certification porteur ACT 3 étoiles V2*

Subject OU: *0002 130003262*

Subject O: *Agence Nationale des Titres Sécurisés*

Subject C: *FR*

X509SKI

X509 SK I *cieFs5w/SKT0Xcf0sOqobfX3IpU=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

1.6.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.6.3.2 - Extension (critical): Qualifiers [QCWithSSCD]

Qualifier type description *[en]* *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the presence or absence of Secure Signature Creation Device (SSCD) support ARE supported by an SSCD (i.e. that that the private key associated with the public key in the certificate is stored in a Secure Signature Creation Device conformant with the applicable European legislation);*

[fr] *elle est assurée par le prestataire de service de confiance et contrôlée (modèle de contrôle) ou vérifiés (modèle d'accréditation) par l'État membre de référence (respectivement son Organe de surveillance ou organisme d'accréditation) que tous les certificats qualifiés délivrés dans le cadre du service identifié dans «Service digital identity» et en outre identifié par les informations des filtres utilisés pour identifier plus précisément dans le cadre du "Sdi" de service de confiance identifiés, l'ensemble précis de certificats qualifiés pour lesquels cette information supplémentaire est nécessaire en ce qui concerne la présence ou l'absence de dispositif sécurisé de création de signature (SSCD) de soutien sont pris en charge par un SSCD (à savoir que la clé privée associée à la clé publique du certificat est stocké dans un dispositif sécurisé conforme à la législation européenne applicable de création de signature);*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithSSCD*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Policy Identifier nodes:

Identifier *1.2.250.1.200.2.5.1.2*

1.7 - Service (granted): Autorité de certification porteur AAE 3 étoiles V3 - AC Acteurs de l'Administration de l'Etat - Service de signature

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Autorité de certification porteur AAE 3 étoiles V3 - AC Acteurs de l'Administration de l'Etat - Service de signature*

Name *[fr]* *Autorité de certification porteur AAE 3 étoiles V3 - AC Acteurs de l'Administration de l'Etat -*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *149240330362442702478423408329139126754297l*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIFQDCCAyigAwIBAgISESHHdSe/541787riZyUYwZe7MA0GCSqGSIb3DQEBCwUAMGIxCzAJBgNV
BAYTAkZSMQ0wCwYDVQQKEwRHb3V2MRcwFQYDVQQLEw4wMDAyIDEzMDAwMzI2MjErMCkGA1UEAwwi
QXV0b3JpdMOpIGRlIGNlcnRpZmljYXRpb24gQU5UUyBWMjAeFw0xNzA0MTkwMDAwMDBaFw0yMzA0
MTkwMDAwMDBaMIGXMQswCQYDVQQGEwJGUjEwMC4GA1UECgwnQWdlbmNlIE5hdGlvbmFsZSBkZXMg
VGl0cmVzIFPDqWN1cmlzw6lzMRcwFQYDVQQLDA4wMDAyIDEzMDAwMzI2MjE9MDsGA1UEAww0QXV0
b3JpdMOpIGRlIGNlcnRpZmljYXRpb24gcG9ydGV1ciBBQUUgMyDDqXRvaWxlcyBWMzCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBAMnbXQzeoKO3atB+TJAXV0rL/ccq9JNZ1QB6HysSWzN4
hVK3WRqjo0wNSWjUINQWyhmgcH+l+90m30TQVjS/TOVW+b1wfCvB1WOoslcPsZnuHnZvpFJxZ0FW
7uHS9V09KTwab3OaW5tDQMzz13k3rwMvStNNFydp05CY6z+x3H2INo1/tdFSIE0kA0zrDsQf32+V
J9xNeXwLO30fT1sBpJJlT76r8zZDAPoPoWlYJLHewgaYacVIIESNmUPGvHkHiBeV RjXmOE03Dw9d
eMGLv1dKwoFi3huO20H8BaN4DXkzAzI3nmRk93L+No7/8+gHm1D8+JJR9plL4Jo2c7kjwZ0CAwEA
AaOBuTCBtjASBgNVHRMBAf8ECDAGAQH/AgEAMBEGA1UdIAQKMAgwBgYEVR0gADA9BgNVHR8ENjA0
MDKgMKAuhixodHRwOi8vY3JsLmFudHMuZ291di5mci9hbnRzdjIvYWNfcmFjaW5lLmNybDAOBgNV
HQ8BAf8EBAMCAQYwHQYDVR0OBBYEFMS32cvttMIv/DmqrK2eYVQlLC+iMB8GA1UdIwQYMBaAFF0c
xN5nSe9GUxwcVP+1yQdbClkJMA0GCSqGSIb3DQEBCwUAA4ICAQCbInnoAoIHPpOLRW/5cg/1r80V
9ioDC4PIKeuYY0Cqztcywnx5kWl4OF0rhf8b9tFtV93WSOgtBOs/jtSC5ZeC8lod0R19ckvIcSnX
hl/1mQfgUKfZMDi1D7MuhPLskc/OuggDJc8AkeIRjcmaqZHLLQkkP3Uuw12zWvxRliqQUPwBTbq5
ytmbV5fLY2thLmn/0BBhx7LYCeVDP6frXUQzBd5MmT8hFdZEqU96EXvNWin/vH5VK4/TwdIa5cVH
eOQyn/o564SFCUKljqntClunot3eFGdm4ST3rRFE+7PJ+gPu823lkqkGML+H8OrLWT/oueH3EYLS
QQalEtp6f6re7xRebna2ieJzibi34b/IlitSfq0C6i3MXbkZVi+35B23BBRAQ9eETA7YGHSWmzjC
uzIBMNlw3eMH5PCicJhy2RiP7splT923qE4TP9ZdgD/MvuzWU5aq4KlBv22vOWCgYMo/411kI40P
5mBLkLGCPHOs0x4mbV0wzv1htRLjH/PP2StDHmY6aqrO+wvVZCsGpLjw+utTNBi7FhbAXxu4FNqJ
XmlxagQdF/LjhPxG0DmxpT6iD7zLKR/lskaICgLa443Ul47rYe/i2+klAFi/LykHMAsDZ1oet/pl
3Bc6KoeXLUhJb/AuwHxElv2rCiQ7M87h7UfNBZziDhKdQhbXVQ==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Autorité de certification ANTS V2*

Issuer OU: *0002 130003262*

Issuer O: *Gouv*

Issuer C: *FR*

Subject CN: *Autorité de certification porteur AAE 3 étoiles V3*

Subject OU: *0002 130003262*

Subject O: *Agence Nationale des Titres Sécurisés*

Subject C: *FR*

Valid from: *Wed Apr 19 02:00:00 CEST 2017*

Valid to: *Wed Apr 19 02:00:00 CEST 2023*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C9:DB:5D:0C:DE:A0:A3:B7:6A:D0:7E:4C:90:17:57:4A:CB:FD:C7:2A:F4:93:59:D5:00:7A:1F:2B:12:5B:33:78:85:52:B7:59:1A:A3:A3:4C:0D:49:68:D4:20:D4:16:CA:19:A0:70:7F:A5:FB:DD:26:DF:44:D0:56:34:BF:4C:E5:56:F9:BD:70:7C:2B:C1:D5:63:A8:B2:57:0F:B1:99:EE:1E:76:6F:A4:52:71:67:41:56:EE:E1:D2:F5:5D:3D:29:3C:1A:6F:73:9A:5B:9B:43:40:CC:F3:D7:79:37:AF:03:2F:4A:D3:4D:17:27:69:D3:90:98:EB:3F:B1:DC:7D:88:36:8D:7F:B5:D1:52:20:4D:24:03:4C:EB:0E:C4:1F:DF:6F:95:27:DC:4D:79:7C:0B:3B:7D:1F:4F:5B:01:A4:92:65:4F:BE:AB:F3:36:43:00:FA:0F:A1:69:58:24:B1:DE:C2:06:98:69:C5:48:20:44:8D:99:43:C6:BC:79:07:88:17:95:46:35:E6:38:4D:37:0F:0F:5D:78:C1:8B:BF:57:4A:C2:81:62:DE:1B:8E:DB:41:FC:05:A3:78:0D:79:33:03:32:37:9E:64:64:F
7:72:FE:36:8E:FF:F3:E8:07:9B:50:FC:F8:92:51:F6:99:4B:E0:9A:36:73:B9:23:C1:9D:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

Certificate Policies *Policy OID: 2.5.29.32.0*

CRL Distribution Points *http://crl.ants.gouv.fr/antsv2/ac_racine.crl*

Subject Key Identifier *C4:B7:D9:CB:ED:B4:C2:2F:FC:39:AA:AC:AD:9E:61:54:25:2C:2F:A2*

Authority Key Identifier *5D:1C:C4:DE:67:49:EF:46:53:1C:1C:54:FF:B5:C9:07:5B:0A:59:09*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *CF:B9:1B:16:BF:3D:9C:DC:EE:D8:C6:01:DF:19:B2:3B:1C:79:D0:B3:F8:EB:E8:FB:A7:7E:9B:D3:3B:0B:FA:1A*

X509SubjectName

Subject CN: *Autorité de certification porteur AAE 3 étoiles V3*

Subject OU: *0002 130003262*

Subject O: *Agence Nationale des Titres Sécurisés*

Subject C: *FR*

X509 SK I *xLfZy+20wi/8OaqsrZ5hVCUsL6I=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2017-06-29T22:00:00Z*

TSP Service Definition URI

URI *[en]* *http://sp.ants.gouv.fr/antsv2/ANTSv2_AC_AAE_PC.pdf*

URI *[fr]* *http://sp.ants.gouv.fr/antsv2/ANTSv2_AC_AAE_PC.pdf*

1.7.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.7.2 - Extension (critical): Qualifiers [QCWithQSCD]

Qualifier type description *[en]* *undefined.*

[fr] *undefined.*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithQSCD*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Policy Identifier nodes:

Identifier *1.2.250.1.200.2.3.1.2*

1.8 - Service (granted): Autorité de certification porteur ACT 3 étoiles V3 - AC Acteurs de l'Administration de l'Etat - Service de signature

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Autorité de certification porteur ACT 3 étoiles V3 - AC Acteurs de l'Administration de l'Etat - Service de signature*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *149226287383987147630975442000628755853865 7*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIFQDCCAyigAwIBAgISESFdz1zQeQkxHDOee7l1A3WhMA0GCSqGSIb3DQEBCwUAMGIxCzAJBgNV
BAYTAkZSMQ0wCwYDVQQKEwRHb3V2MRcwFQYDVQQLEw4wMDAyIDEzMDAwMzI2MjErMCkGA1UEAwwi

QXV0b3JpdMOpIGRlIGNlcnRpZmljYXRpb24gQU5UUyBWMjAeFw0xNzA0MTkwMDAwMDBaFw0yMzA0
MTkwMDAwMDBaMIGXMQswCQYDVQQGEwJGUjEwMC4GA1UECgwnQWdlbmNlIE5hdGlvbmFsZSBkZXMg
VGl0cmVzIFPDqWN1cmlzw6lzMRcwFQYDVQQLDA4wMDAyIDEzMDAwMzI2MjE9MDsGA1UEAww0QXV0
b3JpdMOpIGRlIGNlcnRpZmljYXRpb24gcG9ydGV1ciBBQ1QgMyDDqXRvaWxlcyBWMzCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBALKlea3l5MbzT4Py8InTLVlONVkXl1ydRiZ3cQNO0CYk
M+rAX8RrDH5htjqr5x3Xjxwl2KeJTo23Lk/2Sr/mrKtBV6S841TE88BRbxljgts1lHOWXrckFGV6
Cc5UwEvdtOdi19okEIgOoRc1WaP0BXovgMcVPdwLtdb98FwncuZ0W5oHax1/qfjban5y4c10tjyv
e0c1IAr+GLaPm/IL9L80SxL6btekdCXkevIb3oEq3BZtUVg7JN5B9JlA7R0t1kZYXRKQGP0WVggc
uXjhoS6lUEtCwssX20hIVScJ5qp5uxXO19Gweu3q66qbOkiAkyij+oUsI+3SUBLGp59kQpkCAwEA
AaOBuTCBtjASBgNVHRMBAf8ECDAGAQH/AgEAMBEGA1UdIAQKMAgwBgYEVR0gADA9BgNVHR8ENjA0
MDKgMKAuhixodHRwOi8vY3JsLmFudHMuZ291di5mci9hbnRzdjIvYWNfcmFjaW5lLmNybDAOBgNV
HQ8BAf8EBAMCAQYwHQYDVR0OBBYEFGIAiveXQ57WOf5+h3D00sgefPzdMB8GA1UdIwQYMBaAFF0c
xN5nSe9GUxwcVP+1yQdbClkJMA0GCSqGSIb3DQEBCwUAA4ICAQBxhr+7+WDtifCZRxsE1KS+P8mh
/ld1T7nh0avFKQlyvxbCFK3y7yJZFLYRoaMijzcghdoaakecplylxD7MoRULRzbOlFQj9qag7CBG
zgw2OtKQVSSNe+wam4fpeEFx1ZnDsI4Q0IeojM6NfujLsV9y/CgzqFu+Z4oNZ1gKULVByevZu3rJ
vRxIFJETqdgM9SC1dVMhf/CzNby3Lxom87oczmtoS7W3UPooELv82F5KdChfr0CuNuxQwQ+HnrFy
9it6HMtvszl38HoKBAHqNvZ4hRKr14nsyAjXRIXVtWzXg6YGiygWU+hNdRSQopwPOm8uSmBjPYOW
19LMTK3ZaYhA5LwpNFmKr+yNTsha/K1mjAoz1PCLqrtRlmbTd+yk4gstdTesDNBRT3XqJMJ7eAXf
7YPBnaXBZ006YcVDwqVLZviu4BQ7LIbpFlXOvLNfwPrjhXfTBB0DnVxd92f51KnqHg7iDGzovAHX
lAMQZ5J6EojIjhpsL7pQyrhTSIKspdJIz7r3KfrplLBHtklQmbg7GHZhnYQ+JoZTAzu0nUKT7Zur
HLK4JrJ5lzqBzwGXnzgZJD8VnfYXk6ZS22poJZpUUAee0i/3O+/vhLK1Wm4cGVR/VkhhwjMpXVXn
eTUKe9HjvwSnsG1rqt2Ba7kYDcSE0K5hjWNgVJRFAXiI13MOaA==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Autorité de certification ANTS V2*

Issuer OU: *0002 130003262*

Issuer O: *Gouv*

Issuer C: *FR*

Subject CN: *Autorité de certification porteur ACT 3 étoiles V3*

Subject OU: *0002 130003262*

Subject O: *Agence Nationale des Titres Sécurisés*

Subject C: *FR*

Valid from: *Wed Apr 19 02:00:00 CEST 2017*

Valid to: *Wed Apr 19 02:00:00 CEST 2023*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:B2:A5:79:AD:E5:E4:C6:F3:4F:83:F2:F0:89:D3:2D:59:4E:35:59:17:97:5C:9D:46:26:77:71:03:4E:D0:26:24:33:EA:C0:5F:C4:6B:0C:7E:61:B6:3A:AB:E7:1D:D7:8F:1C:25:D8:A7:89:4E:8D:B7:2E:4F:F6:4A:BF:E6:AC:AB:41:57:A4:BC:E3:54:C4:F3:C0:51:6F:19:63:82:DB:35:94:73:96:5E:B7:24:14:65:7A:09:CE:54:C0:4B:DD:B4:E7:62:D7:DA:24:10:88:0E:A1:17:35:59:A3:F4:05:7A:2F:80:C7:15:3D:DC:0B:B5:D6:FD:F0:5C:27:72:E6:74:5B:9A:07:6B:1D:7F:A9:F8:DB:6A:7E:72:E1:CD:74:B6:3C:AF:7B:47:35:20:0A:FE:18:B6:8F:9B:F2:0B:F4:BF:34:4B:12:FA:6E:D7:A4:74:25:E4:7A:F2:1B:DE:81:2A:DC:16:6D:51:58:3B:24:DE:41:F4:99:40:ED:1D:2D:D6:46:58:5D:12:90:18:FD:16:56:08:1C:B9:78:E1:A1:2E:88:50:4B:42:C2:CB:17:DB:48:48:55:27:09:E6:AA:79:BB:15:CE:D7:D1:B0:7A:ED:EA:EB:AA:9B:3A:48:80:93:28:A3:FA:85:2C:23:ED:D2:50:12:C6:A7:9F:64:42:99:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

Certificate Policies *Policy OID: 2.5.29.32.0*

CRL Distribution Points *http://crl.ants.gouv.fr/antsv2/ac_racine.crl*

Subject Key Identifier *62:00:8A:F7:97:43:9E:D6:39:FE:7E:87:70:F4:D2:C8:1E:7C:FC:DD*

Authority Key Identifier *5D:1C:C4:DE:67:49:EF:46:53:1C:1C:54:FF:B5:C9:07:5B:0A:59:09*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *CC:16:3B:91:82:C6:F1:29:AA:03:43:18:6E:9D:57:C3:F9:30:9B:8C:B7:96:0F:3C:22:ED:84:07:93:70:04:D6*

X509SubjectName

Subject CN: *Autorité de certification porteur ACT 3 étoiles V3*

Subject OU: *0002 130003262*

Subject O: *Agence Nationale des Titres Sécurisés*

Subject C: *FR*

X509SKI

X509 SK I *YgCK95dDntY5/n6HcPTSyB58/N0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2017-06-29T22:00:00Z*

TSP Service Definition URI

URI *[en]* *http://sp.ants.gouv.fr/antsv2/ANTSv2_AC_ACT_PC.pdf*

URI *[fr]* *http://sp.ants.gouv.fr/antsv2/ANTSv2_AC_ACT_PC.pdf*

1.8.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

1.8.2 - Extension (critical): Qualifiers [QCWithQSCD]

Qualifier type description	*[en]*	*undefined.*
	[fr]	*undefined.*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithQSCD*

Criteria list assert=all

Key Usage	*[nonRepudiation]*	*true*

Policy Identifier nodes:

Identifier *1.2.250.1.200.2.5.1.2*

2 - TSP: Caisse des dépôts et consignations

TSP Name

Name	*[en]*	*Caisse des dépôts et consignations*
Name	*[fr]*	*Caisse des dépôts et consignations*

TSP Trade Name

Name	*[en]*	*VATFR-77180020026*
Name	*[fr]*	*VATFR-77180020026*

PostalAddress

Street Address	*[en]*	*56, rue de Lille*
Locality	*[en]*	*Paris*
Postal Code	*[en]*	*75007*
Country Name	*[en]*	*FR*

PostalAddress

Street Address	*[fr]*	*56, rue de Lille*
Locality	*[fr]*	*PARIS*
Postal Code	*[fr]*	*75007*
Country Name	*[fr]*	*FR*

ElectronicAddress

URI *http://www.caissedesdepots.fr/confiance.html*

URI *http://www.caissedesdepots.fr/en/trusted-services-program.html*

URI *mailto:igc@caissedesdepots.fr*

URI *mailto:igc@caissedesdepots.fr*

TSP Information URI

URI *[en]* *http://www.caissedesdepots.fr/en/trusted-services-program.html*

URI *[fr]* *http://www.caissedesdepots.fr/confiance.html*

2.1 - Service (granted): CDC - LEGALIA

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *CDC - LEGALIA*

Name *[fr]* *CDC - LEGALIA*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *149232893610134780586482039291177631859917l*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIGkjCCBHqgAwIBAgISESGPgn3Gsw3BbRVmfLZM2bADMA0GCSqGSIb3DQEBCwUAMIGEMQswCQYD
VQQGEwJGUjErMCkGA1UECgwiQ0FJU1NFIERFUyBERVBPVFMgRVQgQ09OU0lHTkFUSU9OUzEYMBYG
A1UEYQwPU0k6RlltMTgwMDIwMDI2MRcwFQYDVQQLDA4wMDAyIDE4MDAyMDAyNjEVMBMGA1UEAwwM
Q0RDIC0gUkFDSU5FMB4XDTE3MDMwODAwMDAwMFoXDTI3MDEwODAwMDAwMFowgYUxCzAJBgNVBAYT
AkZSMSswKQYDVQQKDCJDQUlTU0UgREVTIERFUE9UUyBFVCBDT05TUdOQVRJT05TMRgwFgYDVQRh
DA9TSTpGUi0xODAwMjAwMjYxFzAVBgNVBAsMDjAwMDIgMTgwMDIwMDI2MRYwFAYDVQQDDA1DREMg
LSBMRUdBTElBMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA3XhYeWR0tOf84y7ZwJks
XH88I1h1jopBcZM13bZw5+h1c+eIMZJbpT8ifQPKl0LS9HPWtHJg1OafGvbTinS85FkNrU1dbBu4
uLIEmD1UjEQbkLEcsuatRYsJyWCoimIa/Cx5Qf83/9uVSfEAuzaSxQBqpkzGeCYAKtU0o2y71bL5
wiHHP5PECegCF8A0ChkDoxecX70FM+4iVMNOwm7Kw9vcI3AXvgMOB29md+SeufUpIdPRFcVAX/zP
LogUzZdqrz/tQYzvMR+kCBecspHYJ2YMl/DNu9mkAo1xCOGJl3HFiplanTJMAKkoZQ4CgKkb+shK
Z8z5Ss3FuscVPvduh9S2Ja+R71wqFBZrN+/yPAbR5y2gPTtHbw7w8Y7M3OP76G4SGZXQMfRIAU2U
ku/ncXY5Gmo6BOxfia0p4JVLlh2Q/wYKhm+pL5tjFB6X4RkxX7riyiyAsWUk60pJh3RK0s/nMPyw
4cSPG+ne2dE2d+Jgb2QY2llHv3Lr9GoVoOSxhJ5O3ar1xvMPSQhnSldI6N1K9fBvdwKwl6L8Zofm
Yi3rc34G3+mKZWvdT41IWgo/xJGGuTzVBL/YxZN4/YRnExrrRriFRPnjoWIbLFGHc8LFX8OgzdC8
uFkuis4J33uum8FqlVSCEqlLi8woX9yyDD/VubLAiiFNozpZ7g+b8EkCAwEAAaOB+jCB9zAOBgNV

HQ8BAf8EBAMCAQYwUAYDVR0gBEkwRzBFBgRVHSAAMD0wOwYIKwYBBQUHAgEWL2h0dHA6Ly9pZ2Mt
cGMuY2Fpc3NlZGVzZGVwb3RzLmZyL3BjLWxlZ2FsaWEucGRmMBIGA1UdEwEB/wQIMAYBAf8CAQAw
PwYDVR0fBDgwNjA0oDKgMIYuaHR0cDovL2lnYy5jYWlzc2VkZXNkZXBvdHMuZnIvcmFjaW5lLWVp
ZGFzLmNybDAdBgNVHQ4EFgQUybbKqJmSr0Nai8sqar7UFNc//PAwHwYDVR0jBBgwFoAUKJGGpIv+
+scFw1yq8DsUh2ZbzHswDQYJKoZIhvcNAQELBQADggIBAI6Utgq4T7JXMMepP/cXCecP48x8FBtf
ZqW6ycU55JMbAXATfg9DYbKUfCfkJKT+u//WuGu0h3c0FVQQ5f/ff58wMyFi/FlCTvHeZB7lulqQ
1IjdVq7ZRjnG/9o84CEspYRdzv+YAKSFUGNx0WgAPRYNOdQyyIyiWlMV2d5FxS1fl4LUCOgee7p0
bDHXdQThDS2H8a2HbUrG2nrUx4F7gOUJCvFmMzOgXcRBbsPVpZY3DlDl87t1Gw2LeeFDgRH8RX6O
rY1Cgg4z5gjZMpGUMlHkCsVaGf4hpefFwz2q1iEOlIPf3h4xOA3gZMJuwSUKm/UAdx9+dZkPAzfA
LKm08lULvsnsPNBe7ej2LeSKYQ7t2ErurPzv4kjXHuvMMAJH+RNX7vuLdWR6A2W2hWEnd9y2aiWz
xYKGcxseRigCj1rqk9WFAYuAIEc/PdUhB+FRhlUDhOqpAybIRzJKuM7V67M5WnDlM2acaEvsOV2t
wTD1i0nOZ2GxMWvAXqTkw+wc8rR9FZgNlcxwlSgeD2iKFyINO0y9xR0GXtCddQAftKrQmFQaebnB
NikCEMlaSeU16hvw6urJU6ZhVqnIQWxbhCuj5aXxqb0YbSZuNCbMtzdKxXZskqxA5B4cCESffgXG
/HwIJP3frq//l7h2OdKE8sPzZ+SLuWgt0kMi62I60w+5

-----END CERTIFICATE-----

Signature algorithm:	*SHA256withRSA*
Issuer CN:	*CDC - RACINE*
Issuer OU:	*0002 180020026*
Issuer 2.5.4.97:	*SI:FR-180020026*
Issuer O:	*CAISSE DES DEPOTS ET CONSIGNATIONS*
Issuer C:	*FR*
Subject CN:	*CDC - LEGALIA*
Subject OU:	*0002 180020026*
Subject 2.5.4.97:	*SI:FR-180020026*
Subject O:	*CAISSE DES DEPOTS ET CONSIGNATIONS*
Subject C:	*FR*
Valid from:	*Wed Mar 08 01:00:00 CET 2017*
Valid to:	*Fri Jan 08 01:00:00 CET 2027*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:DD:78:58:79:64:74:B4:E7:FC:E3:2E:D9:C0:99:2C:5C:
7F:3C:23:58:75:8E:8A:41:71:93:35:DD:B6:70:E7:E8:75:73:E7:88:31:92:5B:A5:3F:22:7D:03:CA:97:42:D2:F4:73:D6:B4:72:60:D4:E6:9F:1A:F6:D3:8A:74:BC:E4:59
:0D:AD:4D:5D:6C:1B:B8:B8:B2:04:98:3D:54:8C:44:1B:90:B1:1C:B2:E6:AD:45:8B:09:C9:60:A8:8A:62:1A:FC:2C:79:41:FF:37:FF:DB:95:49:F1:00:BB:36:92:C5:00:6
A:A6:4C:C6:78:26:00:2A:D5:34:A3:6C:BB:D5:B2:F9:C2:21:C7:3F:93:C4:09:E8:02:17:C0:34:0A:19:03:A3:17:9C:5F:BD:05:33:EE:22:54:C3:4E:C2:6E:CA:C3:DB:DC:
23:70:17:BE:03:0E:07:6F:66:77:E4:9E:B9:F5:29:21:D3:D1:15:C5:40:5F:FC:CF:2E:88:14:CD:97:6A:AF:3F:ED:41:8C:EF:31:1F:A4:08:17:9C:B2:91:D8:27:66:0C:97:
F0:CD:BB:D9:A4:02:8D:71:08:E1:89:97:71:C5:8A:99:5A:9D:32:4C:00:A9:28:65:0E:02:80:A9:1B:FA:C8:4A:67:CC:F9:4A:CD:C5:BA:C7:15:3E:F7:6E:87:D4:B6:25:A
F:91:EF:5C:2A:14:16:6B:37:EF:F2:3C:06:D1:E7:2D:A0:3D:3B:47:6F:0E:F0:F1:8E:CC:DC:E3:FB:E8:6E:12:19:95:D0:31:F4:48:01:4D:94:92:EF:E7:71:76:39:1A:6A:3
A:04:EC:5F:89:AD:29:E0:95:4B:96:1D:90:FF:06:0A:86:6F:A9:2F:9B:63:14:1E:97:E1:19:31:5F:BA:E2:CA:2C:80:B1:65:24:EB:4A:49:87:74:4A:D2:CF:E7:30:FC:B0:E
1:C4:8F:1B:E9:DE:D9:D1:36:77:E2:60:6F:64:18:DA:59:47:BF:72:EB:F4:6A:15:A0:E4:B1:84:9E:4E:DD:AA:F5:C6:F3:0F:49:08:67:4A:57:48:E8:DD:4A:F5:F0:6F:77:
02:B0:97:A2:FC:66:87:E6:62:2D:EB:73:7E:06:DF:E9:8A:65:6B:DD:4F:8D:48:5A:0A:3F:C4:91:86:B9:3C:D5:04:BF:D8:C5:93:78:FD:84:67:13:1A:EB:46:B8:85:44:F9
:E3:A1:62:1B:2C:51:87:73:C2:C5:5F:C3:A0:CD:D0:BC:B8:59:2E:8A:CE:09:DF:7B:AE:9B:C1:6A:95:54:82:12:A9:4B:8B:CC:28:5F:DC:B2:0C:3F:D5:B9:B2:C0:8A:21:
4D:A3:3A:59:EE:0F:9B:F0:49:02:03:01:00:01

Certificate Policies	*Policy OID: 2.5.29.32.0*

CPS pointer: http://igc-pc.caissedesdepots.fr/pc-legalia.pdf

Basic Constraints *IsCA: true - Path length: 0*

CRL Distribution Points *http://igc.caissedesdepots.fr/racine-eidas.crl*

Subject Key Identifier *C9:B6:CA:A8:99:92:AF:43:5A:8B:CB:2A:6A:BE:D4:14:D7:3F:FC:F0*

Authority Key Identifier *28:91:86:A4:8B:FE:FA:C7:05:C3:5C:AA:F0:3B:14:87:66:5B:CC:7B*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *B3:63:E6:DF:93:49:73:CD:49:1E:5D:25:4A:E2:73:47:70:29:C2:B0:61:E0:E0:FB:EC:C4:87:D4:BF:44:53:DC*

X509SubjectName

Subject CN: *CDC - LEGALIA*

Subject OU: *0002 180020026*

Subject 2.5.4.97: *SI:FR-180020026*

Subject O: *CAISSE DES DEPOTS ET CONSIGNATIONS*

Subject C: *FR*

X509SKI

X509 SK I *ybbKqJmSr0Nai8sqar7UFNc//PA=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2017-10-31T23:00:00Z*

TSP Service Definition URI

URI *[en]* *https://confiance.caissedesdepots.fr/igc/legalia/pc-legalia.pdf*

URI *[fr]* *https://confiance.caissedesdepots.fr/igc/legalia/pc-legalia.pdf*

2.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

2.1.2 - Extension (critical): Qualifiers [QCWithQSCD, QCForESig]

Qualifier type description *[en]* *undefined.*

[fr] *undefined.*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithQSCD*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForESig*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Policy Identifier nodes:

Identifier *1.2.250.1.5.1.1.1.3.3*

3 - TSP: Click and Trust

TSP Name

Name *[en]* *Click and Trust*

Name *[fr]* *Click and Trust*

TSP Trade Name

Name *[en]* *VATFR-66428786578*

Name *[fr]* *VATFR-66428786578*

PostalAddress

Street Address *[en]* *18 Quai de la Rapée*

Locality *[en]* *Paris*

Postal Code *[en]* *75012*

Country Name *[en]* *FR*

ElectronicAddress

URI *https://www.click-and-trust.com/fr/qui-sommes-nous.html*

URI *mailto:contact-commercial@click-and-trust.com*

URI *https://www.click-and-trust.com/fr/qui-sommes-nous.html*

URI *mailto:contact-commercial@click-and-trust.com*

TSP Information URI

URI *[fr]* *https://www.click-and-trust.com/fr/cgu.html*

URI *[en]* *https://www.click-and-trust.com/fr/cgu.html*

3.1 - Service (granted): MERCANTEO+ EU-SIGN RGS 3E

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *MERCANTEO+ EU-SIGN RGS 3E*

Name *[fr]* *MERCANTEO+ EU-SIGN RGS 3E*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *149197255084578806793064892482330045536597 6*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIHWzCCBUOgAwIBAgISESCDZTARxFprXKbtYRNJBX1YMA0GCSqGSIb3DQEBCwUAMHIxCzAJBgNV
BAYTAkZSMRgwFgYDVQQKDA9DTElDSyBBTkQgVFJVU1QxFzAVBgNVBAsMDjAwMDIgNDI4Nzg2NTc4
MTAwLgYDVQQDDCdDRVJUSUZJQ0FUSU9OIEFVVEhPUklUWS1DTElDSyBBTkQgVFJVU1QwHhcNMTYw
MzAxMDAwMDAwWhcNMjYwMzAxMDAwMDAwWjBiMQswCQYDVQQGEwJGUjEYMBYGA1UECgwPQ0xJQ0sg
QU5EIFRSVVNUMRcwFQYDVQQLDA4wMDAyIDQyODc4NjU3ODEgMB4GA1UEAwwXRVUtU0lHTi1DTElD
SyBBTkQgVFJVU1QwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDJ/cezkkJDp72NxdrO
EwBJGb/mnWLw9pBjSLNEuXMECYmVKdCEODfJ33qgQ0BLH1pFixO2ZlVa1pkucvSP1EzVfZaFLTHp
I3aeRt4Jf4czETYyYTImVDQvEpAgLqeSpvPtm5G5ZAuxPX4LqqTu9Q+VJBEtKLS/NloSgbK7NpxJ
tst5eXPBZBiaHJNWaEUUKpSe5GxC9fv08TfuBxalS/p2bmbljYuUwFLvi2rI+MphSJk8TkxYV0qf
JHF18qKQPMc9001LWOCV8keGrCcp1rEloC3eJO/g1CEpLjlcodVKnyJ+EvcRvW0LZG/Ullwt6US4
JOxwTNAVhIukEHbreBoPTpVgkZAO7qw4TTu2kMIDTZXVnVok30aZEXFJyYD5tJF0tKXXZ/+Yvl/z
SfLeXFu5lWwC0JuyyNBSYUUO4Ih2kCbMyzMz7z9UI3IRSc4pjSsy+wzmN2uZVT+ACszBhggEXrh6
S+JA9AGcajfXvXX4By5ENyCKrUjrYF3SXVm8DEppQf/pV6nOoez3TpRrrcgcoQJcscGALhBTi6sT
wRrSVGl/gEN94D3C7XklDy/SCS04cRGkaubvwrm80jO6bBrwB21YFmJfEx+cH+RbQy+EntRZoZzO
jFQfMcKMWbYEf2sdEFU6hGE2uf+ZI0s5y6AxlOl/NS4oMujpKHfLgQ0XUQIDAQABo4IB+TCCAfUw
DgYDVR0PAQH/BAQDAgEGMF8GA1UdIARYMFYwVAYEVR0gADBMMEoGCCsGAQUFBwIBFj5odHRwczov
L3d3dy5jbGljay1hbmQtdHJ1c3QuY29tL3NpdGUvcGRmL1BDY2xpY2thbmR0cnVzdEFDLnBkZjAS
BgNVHRMBAf8ECDAGAQH/AgEAMIIBLAYDVR0fBIIBIzCCAR8wWqBYoFaGVGh0dHA6Ly93d3cuY2xp
Y2stYW5kLXRydXN0LmNvbS9DTElDS0FORFRSVVNUL0NFUlRJRklDQVRJT05BVVRIT1JJVFljbGlj
a2FuZHRydXN0LmNybDCBwKCBvaCBuoaBt2xkYXA6Ly9sZGFwLmNsaWNrLWFuZC10cnVzdC5jb20v
Q049Q0VSVElGSUNBVElPTiUyMEFVVEhPUklUWS1DTElDSyUyMEFORCUyMFRSVVNULE9VPTAwMDIl
MjA0Mjg3ODY1NzgsTz1DTElDSyUyMEFORCUyMFRSVVNULEM9RlI/Y2VydGlmaWNhdGVyZXZvY2F0
aW9ubGlzdDtiaW5hcnk/YmFzZT9vYmplY3RjbGFzcz1wa2lDQTAdBgNVHQ4EFgQU3N0PdXk2R4yr
QNeKQGmMarkWnDYwHwYDVR0jBBgwFoAUgzbvNXqdm5si4bMeCOPdt+9Sx2wwDQYJKoZIhvcNAQEL
BQADggIBAL33Z8lMITW83nAmoWSAfAbmYrMPDuEquQXuR5Xrc+6/qcIml49zSQo2h8LUG5I880/5
fgpwqUmwvqCgrIixDxeoGCZEESvRctqQacGoxJllZkXUi5HoNZqqSwr2MqcDn1c7vzXex7kekLBz
jYZD20c3hx5hfQ543lbzOGTPm3CYK0e8fVczIQKfkdDcuR9TNQ6Y6mmv43cDkjFBMSeDMw2t+bkz
qZTqp0aSyNvT3NFP+ISHneQi580lIVEnJbmDhzKO0l4ng1tP419xBxb0nn0/omh5zP6gMoGV6cX3
b1uMqWpVlZC11SHYX9FMQdfvDvoktJSl6Kj6uUE5gzNt+3KE/O8YBKlOm9Wh2tkr3fuZ8R1cCPke
zYzlwy4lLu6Doza3ym6wt/xX6ZSqAnc+kOQsj7KXRy9F2kfWtKjkwY0bS6dX8QLriRs+qQOeHLvC
FuBVuTuxnBpGC88CeGGSX4/7tdx0C9/+FJawnF7n/AXnG/071v+8J2hnnitiJ3lo4Q45YiskoEqp
2ZiIyFWfpyI8Rn6cL9My1AJtbLDAyr6LF8iXdUwwYHxhUz3bxSY0BCub3QTPqXbRKadIuQBIXtpE
CxB05G7UkvfRkSJKNxq+3V++NQ5YQfwrCWQAAh5dmcTbALyadvXvscA57L/X+nyf5jIURYwVblEW m7eEnS70

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *CERTIFICATION AUTHORITY-CLICK AND TRUST*

Issuer OU: *0002 428786578*

Issuer O: *CLICK AND TRUST*

Issuer C: *FR*

Subject CN: *EU-SIGN-CLICK AND TRUST*

Subject OU: *0002 428786578*

Subject O: *CLICK AND TRUST*

Subject C: *FR*

Valid from: *Tue Mar 01 01:00:00 CET 2016*

Valid to: *Sun Mar 01 01:00:00 CET 2026*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:C9:FD:C7:B3:92:42:43:A7:BD:8D:C5:DA:CE:13:00:49:19:BF:E6:9D:62:F0:F6:90:63:48:B3:44:B9:73:04:09:89:95:29:D0:84:38:37:C9:DF:7A:A0:43:40:4B:1F:5A:45:8B:13:B6:64:85:5A:D6:99:2E:72:F4:8F:D4:4C:D5:7D:96:85:2D:31:E9:23:76:9E:46:DE:09:7F:87:33:11:36:32:61:32:26:54:34:2F:12:90:20:2E:A7:92:A6:F3:ED:9B:91:B9:64:0B:B1:3D:7E:0B:AA:A4:EE:F5:0F:95:24:11:2D:28:B4:BF:36:5A:12:81:B2:BB:36:9C:49:B6:CB:79:79:73:C1:64:18:9A:1C:93:56:68:45:14:2A:94:9E:E4:6C:42:F5:FB:F4:F1:37:EE:07:16:A5:4B:FA:76:6E:66:E5:8D:8B:94:C0:52:EF:8B:6A:C8:F8:CA:61:48:99:3C:4E:4C:58:57:4A:9F:24:71:75:F2:A2:90:3C:C7:3D:D3:4D:4B:58:E0:95:F2:47:86:AC:27:29:D6:B1:25:A0:2D:DE:24:EF:E0:D4:21:29:2E:39:5C:A1:D5:4A:9F:22:7E:12:F7:11:BD:6D:0B:64:6F:D4:96:5C:2D:E9:44:B8:24:EC:70:4C:D0:15:84:8B:A4:10:76:EB:78:1A:0F:4E:95:60:91:90:0E:EE:AC:38:4D:3B:B6:90:C2:03:4D:95:D5:9D:5A:24:DF:46:99:11:71:49:C9:80:F9:B4:91:74:B4:A5:D7:67:FF:98:BE:5F:F3:49:F2:DE:5C:5B:B9:95:6C:02:D0:9B:B2:C8:D0:52:61:45:0E:E0:88:76:90:26:CC:CB:33:33:EF:3F:54:23:72:11:49:CE:29:8D:2B:32:FB:0C:E6:37:6B:99:55:3F:80:0A:CC:C1:86:08:04:5E:B8:7A:4B:E2:40:F4:01:9C:6A:37:D7:BD:75:F8:07:2E:44:37:20:8A:AD:48:EB:60:5D:D2:5D:59:BC:0C:4A:69:41:FF:E9:57:A9:CE:A1:EC:F7:4E:94:6B:AD:C8:1C:A1:02:5C:B1:C1:80:2E:10:53:8B:AB:13:C1:1A:D2:54:69:7F:80:43:7D:E0:3D:C2:ED:79:25:0F:2F:D2:09:2D:38:71:11:A4:6A:E6:EF:C2:B9:BC:D2:33:BA:6C:1A:F0:07:6D:58:16:62:5F:13:1F:9C:1F:E4:5B:43:2F:84:9E:D4:59:A1:9C:CE:8C:54:1F:31:C2:8C:59:B6:04:7F:6B:1D:10:55:3A:84:61:36:B9:FF:99:23:4B:39:CB:A0:31:94:E9:7F:35:2E:28:32:E8:E9:28:77:CB:81:0D:17:51:02:03:01:00:01

Certificate Policies *Policy OID: 2.5.29.32.0*

CPS pointer: https://www.click-and-trust.com/site/pdf/PCclickandtrustAC.pdf

Basic Constraints *IsCA: true - Path length: 0*

CRL Distribution Points *http://www.click-and-trust.com/CLICKANDTRUST/CERTIFICATIONAUTHORITYclickandtrust.crl*

ldap://ldap.click-and-trust.com/CN=CERTIFICATION%20AUTHORITY-CLICK%20AND%20TRUST,OU=0002%20428786578,O=CLICK%20AND%20TRUST,C=FR?certificaterevocationlist;binary?base?objectclass=pkiCA

Subject Key Identifier *DC:DD:0F:75:79:36:47:8C:AB:40:D7:8A:40:69:8C:6A:B9:16:9C:36*

Authority Key Identifier *83:36:EF:35:7A:9D:9B:9B:22:E1:B3:1E:08:E3:DD:B7:EF:52:C7:6C*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *B3:AC:75:16:92:36:27:19:B8:85:DC:35:24:EF:1B:05:B3:32:BC:14:49:6C:0F:B1:5E:40:BE:30:9C:71:D4:72*

X509SubjectName

Subject CN: *EU-SIGN-CLICK AND TRUST*

Subject OU: *0002 428786578*

Subject O: *CLICK AND TRUST*

Subject C: *FR*

X509SKI

X509 SK I *3N0PdXk2R4yrQNeKQGmMarkWnDY=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2016-09-29T22:00:00Z*

TSP Service Definition URI

URI *[en]* *https://www.click-and-trust.com/PC/EU-SIGN-EN.pdf*

URI *[fr]* *https://www.click-and-trust.com/PC/EU-SIGN.pdf*

3.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

3.1.2 - Extension (critical): Qualifiers [QCWithSSCD, QCForESig]

Qualifier type description *[en]* *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the presence or absence of Secure Signature Creation Device (SSCD) support ARE supported by an SSCD (i.e. that that the private key associated with the public key in the certificate is stored in a Secure Signature Creation Device conformant with the applicable European legislation);*

[fr] *elle est assurée par le prestataire de service de confiance et contrôlée (modèle de contrôle) ou vérifiés (modèle d'accréditation) par l'État membre de référence (respectivement son Organe de surveillance ou organisme d'accréditation) que tous les certificats qualifiés délivrés dans le cadre du service identifié dans «Service digital identity» et en outre identifié par les informations des filtres utilisés pour identifier plus précisément dans le cadre du "Sdi" de service de confiance identifiés, l'ensemble précis de certificats qualifiés pour lesquels cette information supplémentaire est nécessaire en ce qui concerne la présence ou l'absence de dispositif sécurisé de création de signature (SSCD) de soutien sont pris en charge par un SSCD (à savoir que la clé privée associée à la clé publique du certificat est stocké dans un dispositif sécurisé conforme à la législation européenne applicable de création de signature);*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithSSCD*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForESig*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Policy Identifier nodes:

Identifier *1.2.250.1.98.1.1.22.1.1.1*

3.1.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Mercanteo EU sign 1.2.250.1.98.1.1.22.1.1.1*

Name *[fr]* *Mercanteo EU sign 1.2.250.1.98.1.1.22.1.1.1*

Service digital identities

X509SubjectName

Subject CN: *EU-SIGN-CLICK AND TRUST*

Subject OU: *0002 428786578*

Subject O: *CLICK AND TRUST*

Subject C: *FR*

X509SKI

X509 SK I *3N0PdXk2R4yrQNeKQGmMarkWnDY=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-09-29T22:00:00Z*

3.1.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

3.1.3.2 - Extension (critical): Qualifiers [QCWithSSCD]

Qualifier type description *[en]* *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the presence or absence of Secure Signature Creation Device (SSCD) support ARE supported by an SSCD (i.e. that that the private key associated with the public key in the certificate is stored in a Secure Signature Creation Device conformant with the applicable European legislation);*

[fr] *elle est assurée par le prestataire de service de confiance et contrôlée (modèle de contrôle) ou vérifiés (modèle d'accréditation) par l'État membre de référence (respectivement son Organe de surveillance ou organisme d'accréditation) que tous les certificats qualifiés délivrés dans le cadre du service identifié dans «Service digital identity» et en outre identifié par les informations des filtres utilisés pour identifier plus précisément dans le cadre du "Sdi" de service de confiance identifiés, l'ensemble précis de certificats qualifiés pour lesquels cette information supplémentaire est nécessaire en ce qui concerne la présence ou l'absence de dispositif sécurisé de création de signature (SSCD) de soutien*

sont pris en charge par un SSCD (à savoir que la clé privée associée à la clé publique du certificat est stocké dans un dispositif sécurisé conforme à la législation européenne applicable de création de signature);

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithSSCD*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Policy Identifier nodes:

Identifier *1.2.250.1.98.1.1.22.1.1.1*

3.2 - Service (granted): MERCANTEO SIGN RGS 2E

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *MERCANTEO SIGN RGS 2E*

Name *[fr]* *MERCANTEO SIGN RGS 2E*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1491830521538869795637224949050436077848559*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIHXjCCBUagAwIBAgISESAYi1aXyqf47GA9cpxS+YfvMA0GCSqGSIb3DQEBCwUAMHIxCzAJBgNV
BAYTAkZSMRgwFgYDVQQKDA9DTElDSyBBTkQgVFJVU1QxFzAVBgNVBAsMDjAwMDIgNDI4Nzg2NTc4
MTAwLgYDVQQDDCdDRVJUSUZJQ0FUSU9OIEFVVEhPUklUWS1DTElDSyBBTkQgVFJVU1QwHhcNMTIw
OTA2MDAwMDAwWhcNMjIwOTA2MDAwMDAwWjBlMQswCQYDVQQGEwJGUjEYMBYGA1UECgwPQ0xJQ0sg
QU5EIFRSVVNUMRcwFQYDVQQLDA4wMDAyIDQyODc4NjU3ODEjMCEGA1UEAwwaU0lHTi1UT0tFTi1D
TElDSyBBTkQgVFJVU1QwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCWwEn4xpwhUsuB
ZCu4eLqv5gqj0MebQj7XggGpKyijVZhJ601Gq6lf25b59WEDI8zVfrf23Kb6jc6Iko3nYpKzw2XE
OXoIPk31gAh87s3TOqcSeJ9aoVc/DJkO+5+LT71Kkf7yKdsfA9I4piaRuuRZaceBbxCeRIBLHfzk
k0EX3Hb4KywNPkt0gL5jvRqCD/EZPbjnSwwnT2FyUwXB4A/SK8+JCit5rntiFXgqef46fXB0Rt8Z
ZCASh4A8nzF2ERBLhT5Wc4WQh9QpyYBeoS4vGFT8JGLObzRiXBqf+KVBOAeg1GqCYW/t3jNN5nL+
nQzDdvc4MUhyCxtxc/alNP2+VWjSOSmAe4BypsC8bMB9OZLJs7/3bEFX8ntaJgy3lTI3Lez/A8Q+
1oQYvEdr60TgZ2MXmeYTUmTwNZDEb22431ZSXVV5RTKIG3rzho4m7YrTd3uW8bhK67/0ucDokZ9T
jIQ8LB/HML4MOPPZ7Y60GQItkWvVbQvLhhAIZj2WpKMD8oaY2t4cx9gQ/xLu2BgOCs0if2w101EB
HAupjCf0PJXA98iAR6i+QIeh4XUx/ftIHAMnFi73qH/ykOd8b/hJ0k+w4oAh8OxmsCDgTypBMm7a
uONlspalyZIcigWptKvEsMkKww8L6cPsLuD5pbJpxGpFvRNy8I+vWkHPS6sWVwIDAQABo4IB+TCC
AfUwDgYDVR0PAQH/BAQDAgEGMF8GA1UdIARYMFYwVAYEVR0gADBMMEoGCCsGAQUFBwIBFj5odHRw
czovL3d3dy5jbGljay1hbmQtdHJ1c3QuY29tL3NpdGUvcGRmL1BDY2xpY2thbmR0cnVzdEFDLnBk
ZjASBgNVHRMBAf8ECDAGAQH/AgEAMIIBLAYDVR0fBIIBIzCCAR8wWqBYoFaGVGh0dHA6Ly93d3cu
Y2xpY2stYW5kLXRydXN0LmNvbS9DTElDS0FORFRSVVNUL0NFUlRJRklDQVRJT05BVVRIT1JJVFlj

bGlja2FuZHRydXN0LmNybDCBwKCBvaCBuoaBt2xkYXA6Ly9sZGFwLmNsaWNrLWFuZC10cnVzdC5j
b20vQ049Q0VSVElGSUNBVElPTiUyMEFVVEhPUklUWS1DTElDSyUyMEFORCUyMFRSVVNULE9VPTAw
MDIlMjA0Mjg3ODY1NzgsTz1DTElDSyUyMEFORCUyMFRSVVNULEM9RlI/Y2VydGlmaWNhdGVyZXZv
Y2F0aW9ubGlzdDtiaW5hcnk/YmFzZT9vYmplY3RjbGFzcz1wa2lDQTAdBgNVHQ4EFgQU20amp0ns
Qz82FRgQIJ4ERUy5b5kwHwYDVR0jBBgwFoAUgzbvNXqdm5si4bMeCOPdt+9Sx2wwDQYJKoZIhvcN
AQELBQADggIBAJ3hc9azamuqCcw7uOKSXAo9sPW8cV/s9/B30MACRlGor3t7GjyyPhNbcgoLqvNV
/H/ql+S7y3pOXugEXJDjxtHFhT3gJsGMyXCCd3xju7KIKLDpICcaYUYuqjX3p1UldfBIw6lK3pwn
yMGBCAoWikKHsWm22Y7MaDuaOLGyESBrJJnGC8KuA7d5PswmsNWwUAkESGDV4PiXYGmaLG2P0gzB
pie9740634Z3iqDt2sXUUqgMh8aAAhAY8wiZ68TOXRZmJ12Ovb1w8KY/DgTe7fYvLmozmmlvgLn7
8DWTJNiuIZ7dEhLhUsSY6ctQQzgij0YdkNGrHQ4z0ar7sNnRo4VoXY8oPSVkOqjcTO60PmRyZeFC
btW4aGhRCVcDrpvpFh6zBEE+lKrGziBUk2SNE8719vNPa56pGJ+5BMCiEvYH//y7USDtr4FvodfX
9b/dOPcqZm5+jGJ3e7leXhgOxfkS+MObtgwDYXyLVj0hkuP94+OhytKMdJz5q6VzgbKw78dq5xYz
JZaJQd5pR+N+xFEdaxhRCRUhgeqBLthbr8+bwLrxO7i5ctme8J0l/OMciyGTSuXXWaQhnPwUvvb/
4cyPmmPjFiDtnrD35p1NOgfqjnQsWdR5ZIal+BrE+sICNbR+/lQwUJaLj0XXoyHxUTclIBQEP0f1 JL/p3pR9pu2C

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *CERTIFICATION AUTHORITY-CLICK AND TRUST*

Issuer OU: *0002 428786578*

Issuer O: *CLICK AND TRUST*

Issuer C: *FR*

Subject CN: *SIGN-TOKEN-CLICK AND TRUST*

Subject OU: *0002 428786578*

Subject O: *CLICK AND TRUST*

Subject C: *FR*

Valid from: *Thu Sep 06 02:00:00 CEST 2012*

Valid to: *Tue Sep 06 02:00:00 CEST 2022*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:96:C0:49:F8:C6:9C:21:52:CB:81:64:2B:B8:78:BA:AF:
E6:0A:A3:D0:C7:9B:42:3E:D7:82:01:A9:2B:28:A3:55:98:49:EB:4D:46:AB:A9:5F:DB:96:F9:F5:61:03:23:CC:D5:7E:B7:F6:DC:A6:FA:8D:CE:88:92:8D:E7:62:92:B3:C
3:65:C4:39:7A:08:3E:4D:F5:80:08:7C:EE:CD:D3:3A:A7:12:78:9F:5A:A1:57:3F:0C:99:0E:FB:9F:8B:4F:BD:4A:91:FE:F2:29:DB:1F:03:D2:38:A6:26:91:BA:E4:59:69:
C7:81:6F:10:9E:44:80:4B:1D:FC:E4:93:41:17:DC:76:F8:2B:2C:0D:3E:4B:74:80:BE:63:BD:1A:82:0F:F1:19:3D:B8:E7:4B:0C:27:4F:61:72:53:05:C1:E0:0F:D2:2B:CF:
89:0A:2B:79:AE:7B:62:15:78:2A:79:FE:3A:7D:70:74:46:DF:19:64:20:12:87:80:3C:9F:31:76:11:10:4B:85:3E:56:73:85:90:87:D4:29:C9:80:5E:A1:2E:2F:18:54:FC:
24:62:CE:6F:34:62:5C:1A:9F:F8:A5:41:38:07:A0:D4:6A:82:61:6F:ED:DE:33:4D:E6:72:FE:9D:0C:C3:76:F7:38:31:48:72:0B:1B:71:73:F6:A5:34:FD:BE:55:68:D2:39:
29:80:7B:80:72:A6:C0:BC:6C:C0:7D:39:92:C9:B3:BF:F7:6C:41:57:F2:7B:5A:26:0C:B7:95:32:37:2D:EC:FF:03:C4:3E:D6:84:18:BC:47:6B:EB:44:E0:67:63:17:99:E6:
13:52:64:F0:35:90:C4:6F:6D:B8:DF:56:52:5D:55:79:45:32:88:1B:7A:F3:86:8E:26:ED:8A:D3:77:7B:96:F1:B8:4A:EB:BF:F4:B9:C0:E8:91:9F:53:8C:84:3C:2C:1F:C7:
30:BE:0C:38:F3:D9:ED:8E:B4:19:02:2D:91:6B:D5:6D:0B:CB:86:10:08:66:3D:96:A4:A3:03:F2:86:98:DA:DE:1C:C7:D8:10:FF:12:EE:D8:18:0E:0A:CD:22:7F:6C:35:D
3:51:01:1C:0B:A9:8C:27:F4:3C:95:C0:F7:C8:80:47:A8:BE:40:87:A1:E1:75:31:FD:FB:48:1C:03:27:16:2E:F7:A8:7F:F2:90:E7:7C:6F:F8:49:D2:4F:B0:E2:80:21:F0:EC
:66:B0:20:E0:4F:2A:41:32:6E:DA:B8:E3:65:B2:96:A5:C9:92:1C:8A:05:A9:B4:AB:C4:B0:C9:0A:C3:0F:0B:E9:C3:EC:2E:E0:F9:A5:B2:69:C4:6A:45:BD:13:72:F0:8F:A
F:5A:41:CF:4B:AB:16:57:02:03:01:00:01

Certificate Policies *Policy OID: 2.5.29.32.0*

CPS pointer: https://www.click-and-trust.com/site/pdf/PCclickandtrustAC.pdf

Basic Constraints *IsCA: true - Path length: 0*

CRL Distribution Points

http://www.click-and-trust.com/CLICKANDTRUST/CERTIFICATIONAUTHORITYclickandtrust.crl

ldap://ldap.click-and-trust.com/CN=CERTIFICATION%20AUTHORITY-CLICK%20AND%20TRUST,OU=0002%20428786578,O=CLICK%20AND%20TRUST,C=FR?certificaterevocationlist;binary?base?objectclass=pkiCA

Subject Key Identifier

DB:46:A6:A7:49:EC:43:3F:36:15:18:10:20:9E:04:45:4C:B9:6F:99

Authority Key Identifier

83:36:EF:35:7A:9D:9B:9B:22:E1:B3:1E:08:E3:DD:B7:EF:52:C7:6C

Key Usage:

keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

5D:ED:03:00:B9:C2:B0:DF:0A:CE:5D:D6:CB:E2:46:FE:6F:7E:56:37:F6:A4:CA:21:C3:4A:2E:8C:16:97:AE:18

X509SubjectName

Subject CN:

SIGN-TOKEN-CLICK AND TRUST

Subject OU:

0002 428786578

Subject O:

CLICK AND TRUST

Subject C:

FR

X509SKI

X509 SK I

20amp0nsQz82FRgQIJ4ERUy5b5k=

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description

[en] *undefined.*

[fr] *undefined.*

Status Starting Time

2017-10-31T23:00:00Z

TSP Service Definition URI

URI *[en]* *https://www.click-and-trust.com/fr/PDF/PC/PCclickandtrustMERCANTEOrgs_v1.5.pdf*

URI *[fr]* *https://www.click-and-trust.com/fr/PDF/PC/PCclickandtrustMERCANTEOrgs_v1.5.pdf*

3.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

3.2.2 - Extension (critical): Qualifiers [QCWithQSCD, QCForESig]

Qualifier type description *[en]* *undefined.*

[fr] *undefined.*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithQSCD*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForESig*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Policy Identifier nodes:

Identifier *1.2.250.1.98.1.1.19.1.1.1*

3.3 - Service (granted): MERCANTEO AUTH-SIGN RGS 2E

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *MERCANTEO AUTH-SIGN RGS 2E*

Name *[fr]* *MERCANTEO AUTH-SIGN RGS 2E*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *149207917983085412656599363873166416758591 4*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIHXjCCBUagAwIBAgISESDTnS7srdxxBNIzVS3NhMh6MA0GCSqGSIb3DQEBCwUAMHIxCzAJBgNV
BAYTAkZSMRgwFgYDVQQKDA9DTElDSyBBTkQgVFJVU1QxFzAVBgNVBAsMDjAwMDIgNDI4Nzg2NTc4
MTAwLgYDVQQDDCdDRVJUSUZJQ0FUSU9OIEFVVEhPUklUWS1DTElDSyBBTkQgVFJVU1QwHhcNMTIw
OTA2MDAwMDAwWhcNMjIwOTA2MDAwMDAwWjBlMQswCQYDVQQGEwJGUjEYMBYGA1UECgwPQ0xJQ0sg
QU5EIFRSVVNUMRcwFQYDVQQLDA4wMDAyIDQyODc4NjU3ODEjMCEGA1UEAwwaQVVUSC1UT0tFTi1D
TElDSyBBTkQgVFJVU1QwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQC9V3D8CUH/akI9
vs10Iq+bmkQs/SM59dfhYy6yJ3o0uKlN+tQhN/yLO7VakxVRe64iz9hecL6+AKqO7sJEPhVUxhX7
VUjNNjojG4jrpW1raGW3BjEP7JmNNCJrnl8KlxmJ9vcna5oLu9gOUiWM/24ptsNzm0AWCUidL1Cd
AfnANrfLrnv5Wx1wCpipHcDWOMfLJjPBHKszE3+lk7G1MqQX5Ar3IRds2NxmCuLUNphBHN6NW9Ju
9rZa12JIgwOz+Hx7rid/y33A0B0hpO9Twmz/Ror6KHAWxid6UPSCF9RW8EuGHxnC8qc+0Xqh54YF
gXdi5ahlW+28B48PlpbVn4gKDJ4KV/C+AZk+y4F8mj84Y4iFNtdx6hcjnUNgCkasPjai/63Ls5p1
6h25lGq1YEvKV+4xiBwTr/99FNxsgfnoZIG91hyyFXWfYT08Yl+6YdKcMulz8WaxC6c1xFDe1Fhr
B2JK0NVcvBwugj7SonHZ/wNKvZCMdciQzG8rNr/8yz/4z/3wHXHlmGv+hW55upQhlzCRthDeN82f
+Z+VsQaSDzM3R+xtRWoKmU+846fGM7XihO22UfvbtM5lTxQCHYwNexEXS+RoTvpfNOs+YYsjttPP

LfSCcn+eC0IeqE+dZ7f4Q1VZw5D/xXO1KTlWQUIcyFswm8P9khkNnbrT/NJUxwIDAQABo4IB+TCC
AfUwDgYDVR0PAQH/BAQDAgEGMF8GA1UdIARYMFYwVAYEVR0gADBMMEoGCCsGAQUFBwIBFj5odHRw
czovL3d3dy5jbGljay1hbmQtdHJ1c3QuY29tL3NpdGUvcGRmL1BDY2xpY2thbmR0cnVzdEFDLnBk
ZjASBgNVHRMBAf8ECDAGAQH/AgEAMIIBLAYDVR0fBIIBIzCCAR8wWqBYoFaGVGh0dHA6Ly93d3cu
Y2xpY2stYW5kLXRydXN0LmNvbS9DTElDS0FORFRSVVNUL0NFUlRJRklDQVRJT05BVVRIT1JJVFlj
bGlja2FuZHRydXN0LmNybDCBwKCBvaCBuoaBt2xkYXA6Ly9sZGFwLmNsaWNrLWFuZC10cnVzdC5j
b20vQ049Q0VSVElGSUNBVElPTiUyMEFVVEhPUklUWS1DTElDSyUyMEFORCUyMFRSVVNULE9VPTAw
MDIlMjA0Mjg3ODY1NzgsTz1DTElDSyUyMEFORCUyMFRSVVNULEM9Rll/Y2VydGlmaWNhdGVyZXZv
Y2F0aW9ubGlzdDtiaW5hcnk/YmFzZT9vYmplY3RjbGFzcz1wa2lDQTAdBgNVHQ4EFgQUpmrhAVU+
kLSs16mcn5l3XGY02Z4wHwYDVR0jBBgwFoAUgzbvNXqdm5si4bMeCOPdt+9Sx2wwDQYJKoZIhvcN
AQELBQADggIBADLVCssKYRUr43gfo+uHwjMjDmpaSI5hQ7KvqdEYPCwtYYx5gj2f63IxvWd+X01U
/VUJUPdjnhryvRuhY55l5HQ/7wWDblSU/oDAp03H1nMV7lEAUfmORjmep4leOBUhcXYzEOQsAc6S
38eJXvEQrbR01iSZsvCRlG8ifv2qs5JwkgWjoFkqsEtwOa/GbipXqbahFV6+aPBB+S7MjU6qdx9A
GM01X0xq+cMy4KRc97TfwiwPLVzzCEUxysSYDKUtKoDhk0arpp4MmtnA7QDyqrRPMUCHzBHuJTMH
d/hHGqzzMamBMxgOJg2l6tgVs4i++sYJH2ZeCDvqIfVcoBt5dlZ+2QzKJtQQCeciv/U3y/kDVJHa
BccHPjgNvJXcCgfE/W7MdlrpMxHL6FyBwxZbOkCTV2U0Skx304qy1RBGSJgwndBp2lSjsFmalR3C
Xssjvul5JxVs3JGA9d6pl7xseuVqbu+fuUATVrtUuYVko/MGeKxc5CHr9BNj80vjI/uVsJu0bXGc
Hlgrjeq0iFSOz1w1eb48LCon2gNePce/AFarnJ71/F53EXryZjGoXV2G7sOZjxypv25oQ8xzR0dg
MOxBpSZsTMkYZlM1FZiC2xn5kJPIRAo7u+q5jQwczXUJoFP3cUaHECrUDY+P/LiJroIp/2PXywqX rsPVWJcqdjz2

-----END CERTIFICATE-----

Signature algorithm:	*SHA256withRSA*
Issuer CN:	*CERTIFICATION AUTHORITY-CLICK AND TRUST*
Issuer OU:	*0002 428786578*
Issuer O:	*CLICK AND TRUST*
Issuer C:	*FR*
Subject CN:	*AUTH-TOKEN-CLICK AND TRUST*
Subject OU:	*0002 428786578*
Subject O:	*CLICK AND TRUST*
Subject C:	*FR*
Valid from:	*Thu Sep 06 02:00:00 CEST 2012*
Valid to:	*Tue Sep 06 02:00:00 CEST 2022*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:BD:57:70:FC:09:41:FF:6A:42:3D:BE:CD:74:22:AF:9B:
9A:44:2C:FD:23:39:F5:D7:E1:63:2E:B2:27:7A:34:B8:A9:4D:FA:D4:21:37:FC:8B:3B:B5:5A:93:15:51:7B:AE:22:CF:D8:5E:70:BE:BE:00:AA:8E:EE:C2:44:3E:15:54:C6
:15:FB:55:48:CD:36:3A:23:1B:88:EB:A5:6D:6B:68:65:B7:06:31:0F:EC:99:8D:34:22:6B:9E:5F:0A:97:19:89:F6:F7:27:6B:9A:0B:BB:D8:0E:52:25:8C:FF:6E:29:B6:C3
:73:9B:40:16:09:48:9D:2F:50:9D:01:F9:C0:36:B7:CB:AE:7B:F9:5B:1D:70:0A:98:A9:1D:C0:D6:38:C7:CB:26:33:C1:1C:AB:33:13:7F:A5:93:B1:B5:32:A4:17:E4:0A:F
7:21:17:6C:D8:DC:66:0A:E2:D4:36:98:41:1C:DE:8D:5B:D2:6E:F6:B6:5A:D7:62:48:83:03:B3:F8:7C:7B:AE:27:7F:CB:7D:C0:D0:1D:21:A4:EF:53:C2:6C:FF:46:8A:FA
:28:70:16:C6:27:7A:50:F4:82:17:D4:56:F0:4B:86:1F:19:C2:F2:A7:3E:D1:7A:A1:E7:86:05:81:77:62:E5:A8:65:5B:ED:BC:07:8F:0F:96:96:D5:9F:88:0A:0C:9E:0A:57
:F0:BE:01:99:3E:CB:81:7C:9A:3F:38:63:88:85:36:D7:71:EA:17:23:9D:43:60:0A:46:AC:3E:36:A2:FF:AD:CB:B3:9A:75:EA:1D:B9:94:6A:B5:60:4B:CA:57:EE:31:88:1
C:13:AF:FF:7D:14:DC:6C:81:F9:E8:64:81:BD:D6:1C:B2:15:75:9F:61:3D:3C:62:5F:BA:61:D2:9C:32:E9:73:F1:66:B1:0B:A7:35:C4:50:DE:D4:58:6B:07:62:4A:D0:D5:
5C:BC:1
C:2E:82:3E:D2:A2:71:D9:FF:03:4A:BD:90:8C:75:C8:90:CC:6F:2B:36:BF:FC:CB:3F:F8:CF:FD:F0:1D:71:E5:98:6B:FE:85:6E:79:BA:94:21:97:30:91:B6:10:DE:37:CD:9
F:F9:9F:95:B1:06:92:0F:33:37:47:EC:6D:45:6A:0A:99:4F:BC:E3:A7:C6:33:B5:E2:84:ED:B6:51:FB:DB:B4:CE:65:4F:14:02:1D:8C:0D:7B:11:17:4B:E4:68:4E:FA:5F:3
4:EB:3E:61:8B:23:B6:D3:CF:2D:F4:82:72:7F:9E:0B:42:1E:A8:4F:9D:67:B7:F8:43:55:59:C3:90:FF:C5:73:B5:29:39:56:41:42:1C:C8:5B:30:9B:C3:FD:92:19:0D:9D:B
A:D3:FC:D2:54:C7:02:03:01:00:01

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: https://www.click-and-trust.com/site/pdf/PCclickandtrustAC.pdf

Basic Constraints

IsCA: true - Path length: 0

CRL Distribution Points

http://www.click-and-trust.com/CLICKANDTRUST/CERTIFICATIONAUTHORITYclickandtrust.crl

ldap://ldap.click-and-trust.com/CN=CERTIFICATION%20AUTHORITY-CLICK%20AND%20TRUST,OU=0002%20428786578,O=CLICK%20AND%20TRUST,C=FR?certificaterevocationlist;binary?base?objectclass=pkiCA

Subject Key Identifier

A6:6A:E1:01:55:3E:90:B4:AC:D7:A9:9C:9F:99:77:5C:66:34:D9:9E

Authority Key Identifier

83:36:EF:35:7A:9D:9B:9B:22:E1:B3:1E:08:E3:DD:B7:EF:52:C7:6C

Key Usage:

keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

E2:79:82:92:03:67:82:F1:88:7D:6C:89:9E:BE:84:EC:74:97:B2:CB:4E:07:75:B8:E1:65:D4:19:18:B8:C2:29

X509SubjectName

Subject CN:

AUTH-TOKEN-CLICK AND TRUST

Subject OU:

0002 428786578

Subject O:

CLICK AND TRUST

Subject C:

FR

X509 SK I

pmrhAVU+kLSs16mcn5l3XGY02Z4=

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description

[en] *undefined.*

[fr] *undefined.*

Status Starting Time

2017-10-31T23:00:00Z

TSP Service Definition URI

URI *[en]* *https://www.click-and-trust.com/fr/PDF/PC/PCclickandtrustMERCANTEOrgs_v1.5_precharge.pdf*

URI *[fr]* *https://www.click-and-trust.com/fr/PDF/PC/PCclickandtrustMERCANTEOrgs_v1.5_precharge.pdf*

3.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

3.3.2 - Extension (critical): Qualifiers [QCWithQSCD, QCForESig]

Qualifier type description *[en]* *undefined.*

[fr] *undefined.*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithQSCD*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForESig*

Criteria list assert=all

Key Usage *[digitalSignature]* *true*

Key Usage *[nonRepudiation]* *true*

Policy Identifier nodes:

Identifier *1.2.250.1.98.1.1.18.1.1.1*

4 - TSP: CertEurope

TSP Name

Name *[en]* *CertEurope*

Name *[fr]* *CertEurope*

TSP Trade Name

Name *[en]* *VATFR-51434202180*

Name *[fr]* *VATFR-51434202180*

PostalAddress

Street Address *[en]* *26 rue du Faubourg Poissonniere*

Locality *[en]* *Paris*

Postal Code *[en]* *75010*

Country Name *[en]* *FR*

PostalAddress

Street Address	*[fr]*	*26 rue du Faubourg Poissonnière*
Locality	*[fr]*	*PARIS*
Postal Code	*[fr]*	*75010*
Country Name	*[fr]*	*FR*

ElectronicAddress

URI	*http://www.certeurope.fr/*
URI	*http://uk.certeurope.fr/*
URI	*mailto:services@certeurope.fr*
URI	*mailto:services@certeurope.fr*

TSP Information URI

URI	*[fr]*	*https://www.certeurope.fr/chaine-de-confiance*
URI	*[en]*	*https://uk.certeurope.fr/trust-chain*

4.1 - Service (granted): CERTEUROPE ADVANCED CA V4 - Signature

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[fr]	*Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name	*[en]*	*CERTEUROPE ADVANCED CA V4 - Signature*
Name	*[fr]*	*CERTEUROPE ADVANCED CA V4 - Signature*

Service digital identities

Certificate fields details

Version:	*3*
Serial Number:	*141014*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIGHzCCBAegAwIBAgIDAibWMA0GCSqGSIb3DQEBCwUAMFoxCzAJBgNVBAYTAkZSMRMwEQYDVQQK
EwpDZXJ0ZXVyb3BlMRcwFQYDVQQLEw4wMDAyIDQzNDIwMjE4MDEdMBsGA1UEAxMUQ2VydGV1cm9w

ZSBSb290IENBIDMwHhcNMTAwODI1MjIwMDAwWhcNMjAwODI1MjIwMDAwWjBfMQswCQYDVQQGEwJG
UjETMBEGA1UEChMKQ2VydGV1cm9wZTEXMBUGA1UECxMOMDAwMiA0MzQyMDIxODAxIjAgBgNVBAMT
GUNFUlRFVVJPUEUgQURWQU5DRUQgQ0EgVjQwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
AQDCrkzbMV/GeW5I6+4ArDXectwJ5LGd0rZfsF5A0FePfXkDwOEDSMCzTYr93Hc+vthnu5EXxw1F
s1Ko9hpUbjuTqWFcysrEAsjp23IEV96d0DSBEkPpnrKnWSt0yfa0otF20URQioqtecmbzMwEvOpo
FjVGZzjmYdlk4l6YfGl5v6rJ7o1PB6+i7DJrGcqSFOIf8pVVviFFiRhw6FJ4Q3gJZfhFyOnQowpE
iiGA1u2YmknNBEMEa5or/witNbsLG5VvYzZltXX4hRu9QFREVcIRoJ3COWqcAZjkF/l75S1MlMxc
8m414Rj4BTtvn1VtTmDwU26RiFFsI1M9lNkblnQrAgMBAAGjggHnMIIB4zAPBgNVHRMBAf8EBTAD
AQH/MBEGA1UdDgQKBAhAVl9Z8xytBTBVBgNVHSAETjBMMEoGCSqBegFpCAEBADA9MDsGCCsGAQUF
BwIBFi9odHRwOi8vd3d3LmNlcnRldXJvcGUuZnIvcmVmZXJlbmNlL3BjLXJvb3QzLnBkZjATBgNV
HSMEDDAKgAhMZET/aCJpdDAOBgNVHQ8BAf8EBAMCAQYwggE/BgNVHR8EggE2MIIBMjAyoDCgLoYs
aHR0cDovL3d3dy5jZXJ0ZXVyb3BlLmZyL3JlZmVyZW5jZS9yb290My5jcmwwfaB7oHmGd2xkYXA6
Ly9sY3IxLmNlcnRldXJvcGUuZnIvY249Q2VydGV1cm9wZSUyMFJvb3QlMjBDQSUyMDMsb3U9MDAw
MiUyMDQzNDIwMjE4MCxvPUNlcnRldXJvcGUsYz1GUj9jZXJ0aWZpY2F0ZVJldm9jYXRpb25MaXN0
MH2ge6B5hndsZGFwOi8vbGNyMi5jZXJ0ZXVyb3BlLmZyL2NuPUNlcnRldXJvcGUlMjBSb290JTIw
Q0ElMjAzLG91PTAwMDIlMjA0MzQyMDIxODAsbz1DZXJ0ZXVyb3BlLGM9Rll/Y2VydGlmaWNhdGVS
ZXZvY2F0aW9uTGlzdDANBgkqhkiG9w0BAQsFAAOCAgEAJxsiDxjI7OA2/DysnH+cN8F0cZnPHM2/
CeIqz3dK/qazL2OqWH/BuqKwy74adTRDPmyOOj9df2MvQ9R7uwC2+H12QO1gv2JhS1IdQxbIfmGT
AKdUMjTHa+Gc/pOuXxsA88uKnpNr17vHUQlkWj0ib/2eCpEZm6NLrqArBd4B3KrvbSEmfq3lj6F0
RdKMxM89tmBJhGoueUWuU4K2pD+scM2IqY+P7R7G4ah6lZZ6dlNPJdyWAZnAQh5NiXt8W16wFXFq
krDrGh68QISxgRQGkbBsAse3+rZlHWvZ4Gj4zblHq1hIRt7cN9U+w1OtY+6gYJOLntIsFJt14C1q
wUK5o/C6L9VBV1ItOO1bHuw71qWcN2iso6s40OobHlAGjrHHZQpxEvOgLgYCUvH43cU+z9zMENPk
ri2i4IGKnMBuJgvWNpD+D/vR0/O0hEtCxDKX+G/zwobHMNSDWjrLtKULVH3RoSX+K3jGYmEF4Zwb
N+i0RzOS7+kA1QJRXUfEXTzTFcIv7pfnU/B7J8P32+3kNT/b4WoLtUbSa+n+7VOwZyu93dixGJmS
/8eKYEjPDAec1VCDJxUKFrmXplAhF/DDwVpTzRHoEat+oXsDrt2L2df3RyMPWwVQB2F/KUd/fr1a
SPcXLqji41eeuNRaFZNOVAAevYy4IAEq5wGS9kDXzMc=

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Certeurope Root CA 3*

Issuer OU: *0002 434202180*

Issuer O: *Certeurope*

Issuer C: *FR*

Subject CN: *CERTEUROPE ADVANCED CA V4*

Subject OU: *0002 434202180*

Subject O: *Certeurope*

Subject C: *FR*

Valid from: *Thu Aug 26 00:00:00 CEST 2010*

Valid to: *Wed Aug 26 00:00:00 CEST 2020*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C2:AE:4C:DB:31:5F:C6:79:6E:48:EB:EE:00:AC:35:DE:
72:DC:09:E4:B1:9D:D2:B6:5F:B0:5E:40:D0:57:8F:7D:79:03:C0:E1:03:48:C0:B3:4D:8A:FD:DC:77:3E:BE:D8:67:BB:91:17:C7:0D:45:B3:52:A8:F6:1A:54:6E:3B:93:A
9:61:5C:CA:CA:C4:02:C8:E9:DB:72:04:57:DE:9D:D0:34:81:12:43:E9:9E:B2:A7:59:2B:74:C9:F6:B4:A2:D1:76:D1:44:50:8A:8A:AD:79:C9:9B:CC:CC:04:BC:EA:68:1
6:35:46:67:38:E6:61:D9:64:E2:5E:98:7C:69:79:BF:AA:C9:EE:8D:4F:07:AF:A2:EC:32:6B:19:CA:92:14:E2:1F:F2:95:55:BE:21:45:89:18:70:E8:52:78:43:78:09:65:F8
:45:C8:E9:D0:A3:0A:44:8A:21:80:D6:ED:98:9A:49:CD:04:43:04:6B:9A:2B:FF:08:AD:35:BB:0B:1B:95:6F:63:36:65:B5:75:F8:85:1B:BD:40:54:44:55:C2:11:A0:9D:
C2:39:6A:9C:01:98:E4:17:F9:7B:E5:2D:4C:94:CC:5C:F2:6E:35:E
1:18:F8:05:3B:6F:9F:55:6D:4E:60:F0:53:6E:91:88:51:6C:23:53:3D:94:D9:1B:96:74:2B:02:03:01:00:01

Basic Constraints *IsCA: true*

Subject Key Identifier *40:56:5F:59:F3:1C:AD:05*

Certificate Policies *Policy OID: 1.2.250.1.105.8.1.1.0*

CPSpointer: http://www.certeurope.fr/reference/pc-root3.pdf

Authority Key Identifier *4C:64:44:FF:68:22:69:74*

CRL Distribution Points *http://www.certeurope.fr/reference/root3.crl*

ldap://lcr1.certeurope.fr/cn=Certeurope%20Root%20CA%203,ou=0002%20434202180,o=Certeurope,c=FR?certificateRevocationList

ldap://lcr2.certeurope.fr/cn=Certeurope%20Root%20CA%203,ou=0002%20434202180,o=Certeurope,c=FR?certificateRevocationList

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *45:E2:F2:01:24:0C:F8:0E:B9:4E:D1:8C:6B:1D:22:BA:DF:48:9C:9F:A8:C0:2E:2A:0D:05:2C:45:B7:64:9E:98*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

TSP Service Definition URI

URI *[en]* *https://uk.certeurope.fr/trust-chain*

URI *[fr]* *https://www.certeurope.fr/chaine-de-confiance*

4.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

4.1.2 - Extension (critical): Qualifiers [QCWithQSCD, QCForESig]

Qualifier type description *[en]* *undefined.*

[fr] *undefined.*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithQSCD*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForESig*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Policy Identifier nodes:

Identifier *1.2.250.1.105.10.4.1.3*

4.1.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *CERTEUROPE ADVANCED CA V4 - Signature*

Name *[fr]* *CERTEUROPE ADVANCED CA V4 - Signature*

Service digital identities

X509SubjectName

Subject CN: *CERTEUROPE ADVANCED CA V4*

Subject OU: *0002 434202180*

Subject O: *Certeurope*

Subject C: *FR*

X509SKI

X509 SK I *QFZfWfMcrQU=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

4.1.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

4.1.4 - History instance n.2 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *CERTEUROPE ADVANCED CA V4 - Signature*

Name *[fr]* *CERTEUROPE ADVANCED CA V4 - Signature*

Service digital identities

X509SubjectName

Subject CN: *CERTEUROPE ADVANCED CA V4*

Subject OU: *0002 434202180*

Subject O: *Certeurope*

Subject C: *FR*

X509SKI

X509 SK I *QFZfWfMcrQU=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2013-03-10T23:00:00Z*

4.2 - Service (granted): CertEurope eID User - Signature

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *CertEurope eID User - Signature*

Name *[fr]* *CertEurope eID User - Signature*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *10003*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIH/jCCBeagAwIBAgICJxMwDQYJKoZIhvcNAQELBQAwczELMAkGA1UEBhMCRlIxEzARBgNVBAoT
CkNlcnRFdXJvcGUxFzAVBgNVBAsTDjAwMDIgNDM0MjAyMTgwMRwwGgYDVQQDExNDZXJ0RXVyb3Bl
IGVJRCBSb290MRgwFgYDVQRhEw9TSTpGUi00MzQyMDIxODAwHhcNMTYxMTEzMjMwMDAxWhcNMzYx
MTEzMjMwMDAwWjBzMQswCQYDVQQGEwJGUjETMBEGA1UEChMKQ2VydEV1cm9wZTEXMBUGA1UECxMO
MDAwMiA0MzQyMDIxODAxHDAaBgNVBAMTE0NlcnRFdXJvcGUgZUlEIFVzZXIxGDAWBgNVBGETD1NJ
OkZSLTQzNDIwMjE4MDCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAKxtas6jh2JHr24J
DoaXgnL31dmMPtIDesU/iy3MsRDfGD4z5YZ6+P93HPWg88SCGrf3TS98poh7u4Egig0Ce+XSfjwg
zU08e0vczjKqyVp/58dMeNAkFZW1nlZ6r20gZpVTllioyhfm8k9+GNlnUy3XhrFtra7I1Wuwzz1r
P2VJgw/lKG3RmHHGQFFT0E2RjmRec0EbldR0C7nyLfpV1YAGL6EG/teuSfJKfJhjIAf6QfQR1T+8
/moJEcn+aIpV4hbPLfUZ1K1tPAnnfRAuIqd8SA0i/amrI7mhuzbLPDzFPnV2R7UspuItTSBjGdYW
a8q+b/RYBBXC2MHlHd20Ka/jLSyX+nmHP+ljtIwDixN5FTufM0zcHf9jwSWECLIOPO9/3wWZitE5
8Gr0D8oyx2kOfNph2EDsddq8KAt4Fkuw9vCQPBJw4UmDtSXvcnyEpGFjYX30u6gLv7thnStYdLrF
vc867p3Vp2RnsbFDFjlXFI0NBRpKq3xpRE5ZRYutqfJmSrb4iR2IeBx8wDVXUCys5kanvVsAEh08
1/urydGD2C25jjVCB5FkGo7BLNcs1xJPTqomLgr2HyvL8EDLiFy5VocqICKc481NUdS1LWvLX9yr
X8rMYkD1Vj+qrDAdsqhQ2aq/ceFL0rn+8AsQvblflSr2pD+Wa/c47VtLDUAHAgMBAAGjggKaMIIC
ljATBgNVHSMEDDAKgAhCwWKD5sp+PDCBpwYIKwYBBQUHAQEEgZowgZcwKwYIKwYBBQUHMAGGH2h0
dHA6Ly9vY3NwMS5yb290LmNlcnRldXJvcGUuZnIwKwYIKwYBBQUHMAGGH2h0dHA6Ly9vY3NwMi5y
b290LmNlcnRldXJvcGUuZnIwOwYIKwYBBQUHMAKGL2h0dHA6Ly93d3cuY2VydGV1cm9wZS5mci9y
ZWZlcmVuY2UvZWlkX3Jvb3QuY3J0MFMGA1UdIARMMEowSAYJKoF6AWkWAQEAMDswOQYIKwYBBQUH
AgEWLWh0dHBzOi8vd3d3LmNlcnRldXJvcGUuZnIvY2hhaW5lLWRlLWNvbmZpYW5jZTCCAUcGA1Ud
HwSCAT4wggE6MECgPqA8hjpodHRwOi8vd3d3LmNlcnRldXJvcGUuZnIvcmVmZXJlbmNlL2NlcnRl
dXJvcGVfZWlkX3Jvb3QuY3JsMHqgeKB2hnRsZGFwOi8vbGNyMS5jZXJ0ZXVyb3BlLmZyL2NuPUNl
cnRldXJvcGUlMjBlSUQlMjBSb290LG91PTAwMDIlMjA0MzQyMDIxODAsbz1DZXJ0ZXVyb3BlLGM9
RlI/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlzdDB6oHigdoZ0bGRhcDovL2xjcjIuY2VydGV1cm9w
ZS5mci9jbj1DZXJ0ZXVyb3BlJTIwZUlEJTIwUm9vdCxvdT0wMDAyJTIwNDM0MjAyMTgwLG89Q2Vy
dGV1cm9wZSxjPUZSP2NlcnRpZmljYXRlUmV2b2NhdGlvbkxpc3QwEQYDVR0OBAoECELIsiDPGG9l
MA4GA1UdDwEB/wQEAwIBBjASBgNVHRMBAf8ECDAGAQH/AgEAMA0GCSqGSIb3DQEBCwUAA4ICAQAF
QDJ6qoG1xYoPeONB0vHvF55V6TgNtv8j6+SXcJ0GD5yfTbk+7YddQRqK7R9iz+UE5jrZ3MNSddk7
NN6UJdC4WmQ67Gasn22+ezwnHuwy4Pov9gE3ngKyxXsZ6NVWcuHkVfK9wgcLgxWBdNcCSGCsEs81
fUjYc3gzg6K9rakY1S1Bk3mbvintz4vsBMlXj+2NdtCnc0XfSFxyKQ5iWNIOQnpap+vjZ6NrHSpM
TCyxpWvYT49ER+B9d9/13IS4/1d25/9GdlKHiv85wBsdGxYCsy2/OUGwyVEbSL8emKGHhyYQXlis
PdSszfDnG99/m9FYnGO4IN3AT6c8kaqlWNTaGbUtksQti2mmTHg73bvq9JUE4qhFH2r54awQ86U7
lkW+YPpeBbmvU8OuQOYZQ1qrWTMgSiG0JQZsjN00fEfxygheA0siXLWQjW081s0AKvzTTfVZzFoy
LfC73QABZ/uP+PhmZ70N0WdrLGCp4Du8dOToFxYxiaiI5h6Wlr5AAGpeMEGbQGgNCe1UrAlTAmYZ
+d7uF0mQURDG5E3uyEQh3S4F9DhxpqJZjSpyiNyPvzy7Q6hndykBP8P289PxHVzLYPKmDx8rS2ZF
sKoeOq/2Gx5C0BFMpwO/3TuBGOQ98+FNlWsqSTg8+zvouvb/N2AFiU6EIeIftsAUecCFD+0Pkg==

-----END CERTIFICATE-----

Signature algorithm:	*SHA256withRSA*
Issuer 2.5.4.97:	*SI:FR-434202180*
Issuer CN:	*CertEurope eID Root*
Issuer OU:	*0002 434202180*
Issuer O:	*CertEurope*
Issuer C:	*FR*
Subject 2.5.4.97:	*SI:FR-434202180*
Subject CN:	*CertEurope eID User*
Subject OU:	*0002 434202180*

Subject O: *CertEurope*

Subject C: *FR*

Valid from: *Mon Nov 14 00:00:01 CET 2016*

Valid to: *Fri Nov 14 00:00:00 CET 2036*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:AC:6D:6A:CE:A3:87:62:47:AF:6E:09:0E:86:97:82:72:F7:D5:D9:8C:3E:D2:03:7A:C5:3F:8B:2D:CC:B1:10:DF:18:3E:33:E5:86:7A:F8:FF:77:1C:F5:A0:F3:C4:82:1A:B7:F7:4D:2F:7C:A6:88:7B:BB:81:20:8A:0D:02:7B:E5:D2:7E:3C:20:CD:4D:3C:7B:4B:DC:CE:32:AA:C9:5A:7F:E7:C7:4C:78:D0:24:15:95:B5:9E:56:7A:AF:6D:20:66:95:53:96:58:A8:CA:17:E6:F2:4F:7E:18:D9:67:53:2D:D7:86:B1:6D:AD:AE:C8:D5:6B:B0:CF:3D:6B:3F:65:49:83:0F:E5:28:6D:D1:98:71:C6:40:51:53:D0:4D:91:8E:64:5E:73:41:1B:95:D4:74:0B:B9:F2:2D:FA:55:D5:80:06:2F:A1:06:FE:D7:AE:49:F2:4A:7C:98:63:20:07:FA:41:F4:11:D5:3F:BC:FE:6A:09:11:C9:FE:6A:5A:55:E2:16:CF:2D:F5:19:D4:AD:6D:3C:09:E7:7D:10:2E:22:A7:7C:48:0D:22:FD:A9:AB:23:B9:A1:BB:36:CB:3C:3C:C5:3E:75:76:47:B5:2C:A6:E2:2D:4D:20:63:19:D6:16:6B:CA:BE:6F:F4:58:04:15:C2:D8:C1:E5:1D:DD:B4:29:AF:E3:2D:2C:97:FA:79:87:3F:E9:63:B4:8C:03:8B:13:79:15:3B:9F:33:4C:DC:1D:FF:63:C1:25:84:08:B2:0E:3C:EF:7F:DF:05:99:8A:D1:39:F0:6A:F4:0F:CA:32:C7:69:0E:7C:DA:61:D8:40:EC:75:DA:BC:28:0B:78:16:4B:B0:F6:F0:90:3C:12:70:E1:49:83:B5:25:EF:72:7C:84:A4:61:63:61:7D:F4:BB:A8:0B:BF:BB:61:9D:2B:58:74:BA:C5:BD:CF:3A:EE:9D
:D5:A7:64:67:B1:B1:43:16:39:57:14:8D:0D:05:1A:4A:AB:7C:69:44:4E:59:45:8B:AD:A9:F2:66:4A:B6:F8:89:1D:88:78:1C:7C:C0:35:57:50:2C:AC:E6:46:A7:BD:5B:00:12:1D:3C:D7:FB:AB:C9:D1:83:D8:2D:B9:8E:35:42:07:91:64:1A:8E:C1:2C:D7:2C:D7:12:4F:4E:AA:26:2E:0A:F6:1F:2B:CB:F0:40:CB:88:5C:B9:56:87:2A:20:22:9C:E3:CD:4D:51:D4:B5:2D:6B:CB:5F:DC:AB:5F:CA:CC:62:40:F5:56:3F:AA:AC:30:1D:B2:A8:50:D9:AA:BF:71:
E1:4B:D2:B9:FE:F0:0B:10:BD:B9:5F:21:2A:F6:A4:3F:96:6B:F7:38:ED:5B:4B:0D:40:07:02:03:01:00:01

Authority Key Identifier *42:C1:62:83:E6:CA:7E:3C*

Authority Info Access *http://ocsp1.root.certeurope.fr*

http://ocsp2.root.certeurope.fr

http://www.certeurope.fr/reference/eid_root.crt

Certificate Policies *Policy OID: 1.2.250.1.105.22.1.1.0*

CPSpointer: https://www.certeurope.fr/chaine-de-confiance

CRL Distribution Points *http://www.certeurope.fr/reference/certeurope_eid_root.crl*

ldap://lcr1.certeurope.fr/cn=Certeurope%20eID%20Root,ou=0002%20434202180,o=Certeurope,c=FR?certificateRevocationList

ldap://lcr2.certeurope.fr/cn=Certeurope%20eID%20Root,ou=0002%20434202180,o=Certeurope,c=FR?certificateRevocationList

Subject Key Identifier *42:C8:B2:20:CF:18:6F:65*

Basic Constraints *IsCA: true - Path length: 0*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *5D:58:4D:94:3E:29:49:FE:8F:9A:6E:BE:98:6D:96:0F:39:EE:0D:4D:20:E1:A2:F1:C5:73:90:8F:FA:49:5A:E1*

X509SubjectName

Subject 2.5.4.97: *SI:FR-434202180*

Subject CN: *CertEurope eID User*

Subject OU: *0002 434202180*

Subject O: *CertEurope*

Subject C: *FR*

X509SKI

X509 SK I *QsiyIM8Yb2U=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2017-10-31T23:00:00Z*

TSP Service Definition URI

URI *[en]* *https://uk.certeurope.fr/trust-chain*

URI *[fr]* *https://www.certeurope.fr/chaine-de-confiance*

4.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

4.2.2 - Extension (critical): Qualifiers [QCWithQSCD, QCForESig]

Qualifier type description *[en]* *undefined.*

[fr] *undefined.*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithQSCD*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForESig*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Policy Identifier nodes:

Identifier *1.2.250.1.105.23.411.2.1.1.1.0*

Policy Identifier nodes:

Identifier *1.2.250.1.105.23.411.2.1.2.1.0*

Policy Identifier nodes:

Identifier *1.2.250.1.105.23.411.2.2.1.1.0*

Policy Identifier nodes:

Identifier *1.2.250.1.105.23.411.2.2.2.1.0*

4.3 - Service (granted): CertEurope eID Corp - Seal

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *CertEurope eID Corp - Seal*

Name *[fr]* *CertEurope eID Corp - Cachet*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *10004*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIH/jCCBeagAwIBAgICJxQwDQYJKoZIhvcNAQELBQAwczELMAkGA1UEBhMCRlIxEzARBgNVBAoT
CkNlcnRFdXJvcGUxFzAVBgNVBAsTDjAwMDIgNDM0MjAyMTgwMRwwGgYDVQQDExNDZXJ0RXVyb3Bl
IGVJRCBSb290MRgwFgYDVQRhEw9TSTpGUi00MzQyMDIxODAwHhcNMTYxMTEzMjMwMDAyWhcNMzYx
MTEzMjMwMDAwWjBzMQswCQYDVQQGEwJGUjETMBEGA1UEChMKQ2VydEV1cm9wZTEXMBUGA1UECxMO
MDAwMiA0MzQyMDIxODAxHDAaBgNVBAMTE0NlcnRFdXJvcGUgZUlEIENvcnAxGDAWBgNVBGETD1NJ
OkZSLTQzNDIwMjE4MDCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAOPctWs8E4ZGVD79
Hljei+15phnkIsOUzX8FHmXYLHtedj7tyAx7Zx3VHVmlflwFwZfOjDRTC34eh1s/hKABt71wldd4
s1rqKWSOXTLlPXQ86PFEaqLVkY+UbzejnW7uqR1EIdodaZvrfjwx6iZOX3d+3ARd7fDJsz21zhWP
kkyUQdEWwtftK2lFCgiUmbWrNYEvwobYpoSWUGMzOrej3Gtq5wiG9M5RvKhoq2STDdbPk9B/BtQx
xwcNMMrMOpAS3+vLxeMcF5Xx9ONZhn1Uo92Px7hJIkyJonN5Ppq8M1WQBIOFmlH9FX+UeMHRN7UT
FhtN4m9IZPVUHeVGcb+jHEDnn5jywf5Hj/3TZIt5JXQ/J8LeZTKqVTPTgObxxG6rZTCaVf4i18lY
vI+v946IVjC/ueD/vxcqIWzdTWg+CDegxr2m+jaka9H0URwNY9LsqcIDggtVOQC3wLX27L8Ts6MV
kd0PLecwxJ+6u7/1/zkJL0vR7i2lKw1TwFaSub6sfs/cKHu45eFGRhBtlUcrA3B9jVag81284iTi
9HtW2tWfJa1g5HkRis0zrjqSdLUDHwxZYtvp64j9vqJ/uWHAT10hDNDgvsqe9Y/lntr5XWTm01my
xcj8qQ+50jX+zu7ylO31TYxwqIzlLdi9iHmvrbv2ToKDE8HNPbPf343eoxzLAgMBAAGjggKaMIIC
ljATBgNVHSMEDDAKgAhCwWKD5sp+PDCBpwYIKwYBBQUHAQEEgZowgZcwKwYIKwYBBQUHMAGGH2h0
dHA6Ly9vY3NwMS5yb290LmNlcnRldXJvcGUuZnIwKwYIKwYBBQUHMAGGH2h0dHA6Ly9vY3NwMi5y
b290LmNlcnRldXJvcGUuZnIwOwYIKwYBBQUHMAKGL2h0dHA6Ly93d3cuY2VydGV1cm9wZS5mci9y
ZWZlcmVuY2UvZWlkX3Jvb3QuY3J0MFMGA1UdIARMMEowSAYJKoF6AWkWAQEAMDswOQYIKwYBBQUH
AgEWLWh0dHBzOi8vd3d3LmNlcnRldXJvcGUuZnIvY2hhaW5lLWRlLWNvbmZpYW5jZTCCAUcGA1Ud
HwSCAT4wggE6MECgPqA8hjpodHRwOi8vd3d3LmNlcnRldXJvcGUuZnIvcmVmZXJlbmNlL2NlcnRl
dXJvcGVfZWlkX3Jvb3QuY3JsMHqgeKB2hnRsZGFwOi8vbGNyMS5jZXJ0ZXVyb3BlLmZyL2NuPUNl

cnRldXJvcGUlMjBlSUQlMjBSb290LG91PTAwMDIlMjA0MzQyMDIxODAsbz1DZXJ0ZXVyb3BlLGM9
RlI/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlzdDB6oHigdoZ0bGRhcDovL2xjcjIuY2VydGV1cm9w
ZS5mci9jbj1DZXJ0ZXVyb3BlJTIwZUlEJTIwUm9vdCxvdT0wMDAyJTIwNDM0MjAyMTgwLG89Q2Vy
dGV1cm9wZSxjPUZSP2NlcnRpZmljYXRlUmV2b2NhdGlvbkxpc3QwEQYDVR0OBAoECESN/BURaxkx
MA4GA1UdDwEB/wQEAwIBBjASBgNVHRMBAf8ECDAGAQH/AgEAMA0GCSqGSIb3DQEBCwUAA4ICAQBm
DUzYDhG3q9dtS4MyrdK6Dl/DvtwYJh+9493haFwSlosBU6fBIdIcaCU6zJcrMGoCmPWLl8XwgdO5
bkhzr+FP2GOuiObpvIKZDbn0hsul1eJF7gOGIenjeezAmxreK3SEOgFMhB9eOnPMEuGEKaLEplKs
fnw3rxFAasePoYQNrVO8EtMTWcx/H272nT7aSf56/fFTw82f6iRU621GDEHP6KZdPoEiA5unTbVM
yI1H8qZb8LtGgpRQgSr0LUsKzbFdA3P5OrKv+pFYd+QI9dWbvthsDCKIbKFHdl1uAKL4Pujx4mhE
/zR9PPvzVzg0YlIrjvTi62JaRXqt5iYAB9gfjjxAKNcHSEWDyduEd5wPwbh/EJJ2qwHFrthHEvjc
cxJrkCHLgMu6yThV+JQvFbAdMSAMeLEBjoOx125GVvt14AOEV/uJxJN8aRYyT0bkSqG08XPIdfV7
odqX864JJhLf3pX6MpbczCfHrhewOSz+ykwCXHrEFpOF0J+Mqo0KAW2WP9ndJSAFYFlAFNe2MaNF
selLQDO3pe42THV8jR15ovwf/1vxax2WxUbAkXhG4B9UbbpZXYPJNQ36LK77E9MYlaDyNZAb2inf
NBxMzVPRTHjWY/g6HAyus7dIUYem4gVoFwqhK/1l++tOaBGlndt2yIJtbpu+Q6mraM0rQ0N9BA==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer 2.5.4.97: *SI:FR-434202180*

Issuer CN: *CertEurope eID Root*

Issuer OU: *0002 434202180*

Issuer O: *CertEurope*

Issuer C: *FR*

Subject 2.5.4.97: *SI:FR-434202180*

Subject CN: *CertEurope eID Corp*

Subject OU: *0002 434202180*

Subject O: *CertEurope*

Subject C: *FR*

Valid from: *Mon Nov 14 00:00:02 CET 2016*

Valid to: *Fri Nov 14 00:00:00 CET 2036*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:E3:DC:B5:6B:3C:13:86:46:54:3E:FD:1E:58:DE:8B:ED:
79:A6:19:E4:22:C3:94:CD:7F:05:1E:65:D8:2C:7B:5E:76:3E:ED:C8:0C:7B:67:1D:D5:1D:59:A5:7E:5C:05:C1:97:CE:8C:34:53:0B:7E:1E:87:5B:3F:84:A0:01:B7:BD:70
:95:D7:78:B3:5A:EA:29:64:8E:5D:32:E5:3D:74:3C:E8:F1:44:6A:A2:D5:91:8F:94:6F:37:A3:9D:6E:EE:A9:1D:44:21:DA:1D:69:9B:EB:7E:3C:31:EA:26:4E:5F:77:7E:D
C:04:5D:ED:F0:C9:B3:3D:B5:CE:15:8F:92:4C:94:41:D1:16:C2:D7:ED:2B:69:45:0A:08:94:99:B5:AB:35:81:2F:C2:86:D8:A6:84:96:50:63:33:3A:B7:A3:DC:6B:6A:E7
:08:86:F4:CE:51:BC:A8:68:AB:64:93:0D:D6:CF:93:D0:7F:06:D4:31:C7:07:0D:30:CA:CC:3A:90:12:DF:EB:CB:C5:E3:1C:17:95:F1:F4:E3:59:86:7D:54:A3:DD:8F:C7:B
8:49:22:4C:89:A2:73:79:3E:9A:BC:33:55:90:04:83:85:9A:51:FD:15:7F:94:78:C1:D1:37:B5:13:16:1B:4D:E2:6F:48:64:F5:54:1D:E5:46:71:BF:A3:1C:40:E7:9F:98:F
2:C1:FE:47:8F:FD:D3:64:8B:79:25:74:3F:27:C2:DE:65:32:AA:55:33:D3:80:E6:F1:C4:6E:AB:65:30:9A:55:FE:22:D7:C9:58:BC:8F:AF:F7:8E:88:56:30:BF:B9:E0:FF:B
F:17:2A:21:6C:DD:4D:68:3E:08:37:A0:C6:BD:A6:FA:36:A4:6B:D1:F4:51:1C:0D:63:D2:EC:A9:C2:03:82:0B:55:39:00:B7:C0:B5:F6:EC:BF:13:B3:A3:15:91:DD:0F:2
D:E7:30:C
4:9F:BA:BB:BF:F5:FF:39:09:2F:4B:D1:EE:2D:A5:2B:0D:53:C0:56:92:B9:BE:AC:7E:CF:DC:28:7B:B8:E5:E1:46:46:10:6D:95:47:2B:03:70:7D:8D:56:A0:F3:5D:BC:E2:
24:E2:F4:7B:56:DA:D5:9F:25:AD:60:E4:79:11:8A:CD:33:AE:3A:92:74:B5:03:1F:0C:59:62:DB:E9:EB:88:FD:BE:A2:7F:B9:61:C0:4F:5D:21:0C:D0:E0:BE:CA:9E:F5:8
F:E5:9E:DA:F9:5D:64:E6:D3:59:B2:C5:C8:FC:A9:0F:B9:D2:35:FE:CE:EE:F2:94:ED:F5:4D:8C:70:A8:8C:E5:2D:D8:BD:88:79:AF:AD:BB:F6:4E:82:83:13:C1:CD:3D:B3
:DF:DF:8D:DE:A3:1C:CB:02:03:01:00:01

Authority Key Identifier

42:C1:62:83:E6:CA:7E:3C

Authority Info Access

http://ocsp1.root.certeurope.fr

http://ocsp2.root.certeurope.fr

http://www.certeurope.fr/reference/eid_root.crt

Certificate Policies

Policy OID: 1.2.250.1.105.22.1.1.0

CPSpointer: https://www.certeurope.fr/chaine-de-confiance

CRL Distribution Points

http://www.certeurope.fr/reference/certeurope_eid_root.crl

ldap://lcr1.certeurope.fr/cn=Certeurope%20eID%20Root,ou=0002%20434202180,o=Certeurope,c=FR?certificateRevocationList

ldap://lcr2.certeurope.fr/cn=Certeurope%20eID%20Root,ou=0002%20434202180,o=Certeurope,c=FR?certificateRevocationList

Subject Key Identifier

44:8D:FC:15:11:6B:19:31

Basic Constraints

IsCA: true - Path length: 0

Key Usage:

keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

10:1A:9B:BA:C7:B8:12:DA:2B:34:8A:2F:C9:52:A4:6B:8F:7C:7D:7A:5C:99:8C:B1:ED:EF:5F:9F:5E:97:2B:AB

X509SubjectName

Subject 2.5.4.97:

SI:FR-434202180

Subject CN:

CertEurope eID Corp

Subject OU:

0002 434202180

Subject O:

CertEurope

Subject C:

FR

X509SKI

X509 SK I

RI38FRFrGTE=

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description

[en] *undefined.*

[fr] *undefined.*

Status Starting Time

2017-10-31T23:00:00Z

TSP Service Definition URI

URI *[en]* *https://uk.certeurope.fr/trust-chain*

URI *[fr]* *https://www.certeurope.fr/chaine-de-confiance*

4.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

4.3.2 - Extension (critical): Qualifiers [QCWithQSCD, QCForESeal]

Qualifier type description *[en]* *undefined.*

[fr] *undefined.*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithQSCD*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForESeal*

Criteria list assert=all

Key Usage *[digitalSignature]* *true*

Policy Identifier nodes:

Identifier *1.2.250.1.105.24.411.2.1.1.1.0*

Policy Identifier nodes:

Identifier *1.2.250.1.105.24.411.2.2.1.1.0*

4.4 - Service (granted): CertEurope eID Website

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *CertEurope eID Website*

Name *[fr]* *CertEurope eID Website*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *10005*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIIATCCBemgAwIBAgICJxUwDQYJKoZIhvcNAQELBQAwczELMAkGA1UEBhMCRlIxEzARBgNVBAoT
CkNlcnRFdXJvcGUxFzAVBgNVBAsTDjAwMDIgNDM0MjAyMTgwMRwwGgYDVQQDExNDZXJ0RXVyb3Bl
IGVJRCBSb290MRgwFgYDVQRhEw9TSTpGUi00MzQyMDIxODAwHhcNMTYxMTEzMjMwMDAzWhcNMzYx
MTEzMjMwMDAwWjB2MQswCQYDVQQGEwJGUjETMBEGA1UEChMKQ2VydEV1cm9wZTEXMBUGA1UECxMO
MDAwMiA0MzQyMDIxODAxHzAdBgNVBAMTFkNlcnRFdXJvcGUgZUlEIFdlYnNpdGUxGDAWBgNVBGET
D1NJOkZSLTQzNDIwMjE4MDCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAPEPvcPZufMp
pETVBuAITDBHIwICv2rkrmicukE8AzhOOBMrnG3yglJGaRD0QH229Ylrd0AsVEX5aEOT54t+DSCw
GxL5cXE1dqkq9pdMBsieJEY7jAndc0gcSYNAC2po9nKvnhpFb/jiw653GL2RnUmXF322Pw1Hs19H
I4nZnM/CJjRV363kIe1mHbdM1BhYC84Kb9nZ+vIo2z/TSV0Ev0R5AjXSmpE5EJMYpmlUZuJO+Upa
vgpbnq6nbqJJDtZxSBjhTZKyk2qaDdYfCIR7gJEzN1W9b1CUyuw0S3PPSBUq42Hfm1WHSLKaIGcI
SNq3PGGABiRQVxS31LSzXYfaYUe0fyRqmLeqI8BsRIqZJYkS5svlXZKIOXGCZlreoWeH5xj58wLz
WdbDkJ7sUXDxhKQQ83JuajYUhz3Hc18GhXyTrt2SXN285YfU4Xw979GxgZqzgI9yYotzXDKAdHz+
UVqpr3L2Gv7lTmch+VTY6D70eqTjoKvC5iDxUDQgbPfBuhr4BOdGSuaCPSU9oe4hRhihkZG1pP7C
qCZhsJcZFZiyzTHr+4ZUG668w/9IWOlAwLLP26cQMPmbuvFlZ9DiDHMtRauFCR3GmY1xT7C7zdJ8
XOfNoVIx8BzVj2xqoSVCEsLuBuuXFrhAaSy5qvQNwCZM3DsVTl22HhIOb6/Ql1M/AgMBAAGjggKa
MIICljATBgNVHSMEDDAKgAhCwWKD5sp+PDCBpwYIKwYBBQUHAQEEgZowgZcwKwYIKwYBBQUHMAGG
H2h0dHA6Ly9vY3NwMS5yb290LmNlcnRldXJvcGUuZnIwKwYIKwYBBQUHMAGGH2h0dHA6Ly9vY3Nw
Mi5yb290LmNlcnRldXJvcGUuZnIwOwYIKwYBBQUHMAKGL2h0dHA6Ly93d3cuY2VydGV1cm9wZS5m
ci9yZWZlcmVuY2UvZWlkX3Jvb3QuY3J0MFMGA1UdIARMMEowSAYJKoF6AWkWAQEAMDswOQYIKwYB
BQUHAgEWLWh0dHBzOi8vd3d3LmNlcnRldXJvcGUuZnIvY2hhaW5lLWRlLWNvbmZpYW5jZTCCAUcG
A1UdHwSCAT4wggE6MECgPqA8hjpodHRwOi8vd3d3LmNlcnRldXJvcGUuZnIvcmVmZXJlbmNlL2Nl
cnRldXJvcGVfZWlkX3Jvb3QuY3JsMHqgeKB2hnRsZGFwOi8vbGNyMS5jZXJ0ZXVyb3BlLmZyL2Nu
PUNlcnRldXJvcGUlMjBlSUQlMjBSb290LG91PTAwMDIlMjA0MzQyMDIxODAsbz1DZXJ0ZXVyb3Bl
LGM9RII/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlzdDB6oHigdoZ0bGRhcDovL2xjcjIuY2VydGV1
cm9wZS5mci9jbj1DZXJ0ZXVyb3BlJTIwZUlEJTIwUm9vdCxvdT0wMDAyJTIwNDM0MjAyMTgwLG89
Q2VydGV1cm9wZSxjPUZSP2NlcnRpZmljYXRlUmV2b2NhdGlvbkxpc3QwEQYDVR0OBAoECEu2J7zK
/wIzMA4GA1UdDwEB/wQEAwIBBjASBgNVHRMBAf8ECDAGAQH/AgEAMA0GCSqGSIb3DQEBCwUAA4IC
AQB2Id0b0I/PcbDAYdgsVeYlxCn4LCvWZ2PmemYIPlo5yrIVJ4aJX5rb9ql7bA4zflV3hMqP5Q8U
/KS/kK/8FJ/5Dzlhi5rORcSy47wPyxiJOS7AI2LyxWZKTl35n5UfQcwu9WmwkKa8Oe/FShos+dHm
cxnvFB4MOX5NZpE79AQ1Cc8SWFX4oK6h01fF/HzLiH2JxadsytgtQMhiUtXruVwF+aajRxSNB22c
Ar1JOnCWQyveejPztWSG+VXo7Z93/TkmQkRSxn110Uv5yt5aKG0lFnfEMvgo3SCq/pBMgafb38QV
poJnfWONrdEkEsRQXUONqodVS5i6GUbjuXSq9O3O+bVP2SQE+dWLA5JKbxcbEbB3lXzb2yp33XaE
ZZpyVLEVaD632TTQxhirIQlTPf8moMCFfDLIM3NiLVOKOBM8m4YLkm4JJwAaBWBrcQ7xEmHHM0rD
CxhwM7pj/BkaSu9Lq8yMma6Jp4qOTrSuBXF1g5A01MJyxM25/JHB2lzBCcu/WayAqMdJsPgH6jeI
GkikTxRlYn7N1BBj8XQh2zT2h9SHT36c/UeD7ZSlm33ERgcDAWDFruB2Hst9YZjSVXHZyrVioNPd
bNRXR7d0b6Upn7grGpoZuWpM2JndFS9WYkJieGEBGPUX1D5Qv1aaEfwKXhu82ia1VYuTRniMXfft GA==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer 2.5.4.97: *SI:FR-434202180*

Issuer CN: *CertEurope eID Root*

Issuer OU: *0002 434202180*

Issuer O: *CertEurope*

Issuer C: *FR*

Subject 2.5.4.97: *SI:FR-434202180*

Subject CN: *CertEurope eID Website*

Subject OU: *0002 434202180*

Subject O: *CertEurope*

Subject C: *FR*

Valid from: *Mon Nov 14 00:00:03 CET 2016*

Valid to: *Fri Nov 14 00:00:00 CET 2036*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:F1:0F:BD:C3:D9:B9:F3:29:A4:44:D5:06:E0:08:4C:30:47:23:02:02:BF:6A:E4:AE:68:9C:BA:41:3C:03:38:4E:38:13:2B:9C:6D:F2:82:52:46:69:10:F4:40:7D:B6:F5:89:6B:77:40:2C:54:45:F9:68:43:93:E7:8B:7E:0D:20:B0:1B:12:F9:71:71:35:76:A9:2A:F6:97:4C:06:C8:9E:24:46:3B:8C:09:DD:73:48:1C:49:83:40:0B:6A:68:F6:72:AF:9E:1A:45:6F:F8:E2:C3:AE:77:18:BD:91:9D:49:97:17:7D:B6:3F:0D:47:B3:5F:47:23:89:D9:9C:CF:C2:26:34:55:DF:AD:E4:21:ED:66:1D:B7:4C:D4:18:58:0B:CE:0A:6F:D9:D9:FA:F2:28:DB:3F:D3:49:5D:04:BF:44:79:02:35:D2:9A:91:39:10:93:18:A6:69:54:66:E2:4E:F9:4A:5A:BE:0A:5B:9E:AE:A7:6E:A2:49:0E:D6:71:48:18:E1:4D:92:B2:93:6A:9A:0D:D6:1F:08:84:7B:80:91:33:37:55:BD:6F:50:94:CA:EC:34:4B:73:CF:48:15:2A:E3:61:DF:9B:55:87:48:B2:9A:20:67:08:48:DA:B7:3C:61:80:06:24:50:57:14:B7:D4:B4:B3:5D:87:DA:61:47:B4:7F:24:6A:98:B7:AA:97:C0:6C:44:8A:99:25:89:12:E6:CB:E5:5D:92:88:39:71:82:66:5A:DE:A1:67:87:E7:18:F9:F3:02:F3:59:D6:C3:90:9E:EC:51:70:F1:84:A4:10:F3:72:6E:6A:36:14:87:3D:C7:73:5F:06:85:7C:93:AE:DD:92:5C:DD:BC:E5:87:D4:E1:7C:3D:EF:D1:B1:81:9A:B3:80:8F:72:62:8B:73:5C:32:80:74:7C:FE:51:5A:A9:AF:72:F6:1A:FE:E5:4E:67:21:F9:54:D8:E8:3E:F4:7A:A4:E3:A0:AB:C2:E6:20:F1:50:34:20:6C:F7:C1:BA:1A:F8:04:E7:46:4A:E6:82:3D:25:3D:A1:EE:21:46:18:A1:91:91:B5:A4:FE:C2:A8:26:61:B0:97:19:15:98:B2:CD:31:EB:FB:86:54:1B:AE:BC:C3:FF:48:58:E9:40:C0:B2:CF:DB:A7:10:30:F9:9B:BA:F1:65:67:D0:E2:0C:73:2D:45:AB:85:09:1D:C6:99:8D:71:4F:B0:BB:CD:D2:7C:5C:E7:CD:A1:52:31:F0:1C:D5:8F:6C:6A:A1:25:42:12:C2:EE:06:EB:97:16:B8:40:69:2C:B9:AA:F4:0D:C0:26:4C:DC:3B:15:4E:5D:B6:1E:12:0E:6F:AF:D0:97:53:3F:02:03:01:00:01

Authority Key Identifier *42:C1:62:83:E6:CA:7E:3C*

Authority Info Access

http://ocsp1.root.certeurope.fr

http://ocsp2.root.certeurope.fr

http://www.certeurope.fr/reference/eid_root.crt

Certificate Policies

Policy OID: 1.2.250.1.105.22.1.1.0

CPSpointer: https://www.certeurope.fr/chaine-de-confiance

CRL Distribution Points

http://www.certeurope.fr/reference/certeurope_eid_root.crl

ldap://lcr1.certeurope.fr/cn=Certeurope%20eID%20Root,ou=0002%20434202180,o=Certeurope,c=FR?certificateRevocationList

ldap://lcr2.certeurope.fr/cn=Certeurope%20eID%20Root,ou=0002%20434202180,o=Certeurope,c=FR?certificateRevocationList

Subject Key Identifier *4B:B6:27:BC:CA:FF:02:33*

Basic Constraints *IsCA: true - Path length: 0*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *71:AB:42:03:74:15:6C:1E:63:72:CA:BF:FA:CD:86:25:93:C2:CE:AC:1C:85:12:99:D5:0E:D7:DB:97:4C:80:6A*

X509SubjectName

Subject 2.5.4.97: *SI:FR-434202180*

Subject CN: *CertEurope eID Website*

Subject OU: *0002 434202180*

Subject O: *CertEurope*

Subject C: *FR*

X509SKI

X509 SK I *S7YnvMr/AjM=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2017-10-31T23:00:00Z*

TSP Service Definition URI

URI *[en]* *https://uk.certeurope.fr/trust-chain*

URI *[fr]* *https://www.certeurope.fr/chaine-de-confiance*

4.4.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

4.4.2 - Extension (critical): Qualifiers [QCForWSA]

Qualifier type description *[en]* *undefined.*

[fr] *undefined.*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForWSA*

Criteria list assert=all

Policy Identifier nodes:

Identifier *1.2.250.1.105.25.411.2.1.1.1.0*

Policy Identifier nodes:

Identifier *1.2.250.1.105.25.411.2.1.2.1.0*

Policy Identifier nodes:

Identifier *1.2.250.1.105.25.411.2.2.1.1.0*

Policy Identifier nodes:

Identifier *1.2.250.1.105.25.411.2.2.2.1.0*

5 - TSP: Certinomis

TSP Name

Name *[en]* *Certinomis*

Name *[fr]* *Certinomis*

TSP Trade Name

Name *[en]* *VATFR-59433998903*

Name *[fr]* *VATFR-59433998903*

PostalAddress

Street Address *[en]* *10 avenue Charles de Gaulle*

Locality *[en]* *Charenton-le-Pont Cedex*

Postal Code *[en]* *94673*

Country Name *[en]* *FR*

ElectronicAddress

URI *https://www.certinomis.fr/nos-solutions*

URI *mailto:politiquecertification@certinomis.com*

URI *https://www.certinomis.fr/nos-solutions*

URI *mailto:politiquecertification@certinomis.com*

TSP Information URI

URI *[en]* *https://www.certinomis.fr/documents-et-liens/nos-conditions-generales-dutilisation*

URI *[fr]* *https://www.certinomis.fr/documents-et-liens/nos-conditions-generales-dutilisation*

5.1 - Service (withdrawn): Certinomis AC 2 stars

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Certinomis AC 2 stars*

Name *[fr]* *Certinomis AC 2 étoiles*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *22*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIFhjCCA26gAwIBAgIBFjANBgkqhkiG9w0BAQUFADBjMQswCQYDVQQGEwJGUjETMBEGA1UEChMK
Q2VydGlub21pczEXMBUGA1UECxMOMDAwMiA0MzM5OTg5MDMxJjAkBgNVBAMMHUNlcnRpbm9taXMg
LSBBdXRvcml0w6kgUmFjaW5lMB4XDTA4MTIxMjA5MjUxOFoXDTE4MTIxMjA5MjUxOFowXjELMAkG
A1UEBhMCRllxEzARBgNVBAoTCkNlcnRpbm9taXMxFzAVBgNVBAsTDjAwMDIgNDMzOTk4OTAzMSEw
HwYDVQQDDBhDZXJ0aW5vbWlzIEFDIDIgw6l0b2lsZXMwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQDIhRYBPGdC4U0ECP/StHfiru0pUFT4pgjLTeGWiFNbFJiZ2eN44TdWIR7FEe3oLABt
hYIi/Csgk3LLZ63TOocvFUqE4TL6AUtM6yFjwiz8HwC2fPhmTd56dUUei9CyLFMkU96r3YgLWiGp
QBjWqBrSJll09ZqYyBQ40QQ3swdCjEkRnl2rjxbXWwCxoWvzyi6u0cGQS/ltLK6Z+CPCEh5fxYvx
fGO4/WxXyz6QO5xzGDaf71Rz+B7x8jcvz8jM6tKAs8J1NY51hMNIaUz4sJLTdvu88EKqW3KjuZ1K
0xu49+XJjP0M6Qylmm1ugI6596+psDXBflB5dmyC7b5SHGr3AgMBAAGjggFIMIIBRDAPBgNVHRMB
Af8EBTADAQH/MA4GA1UdDwEB/wQEAwIBBjAfBgNVHSMEGDAWgBQNjLZh2kS40RR9w759Xkjwzspq
sDAdBgNVHQ4EFgQU6cOG9YSRb4MJKiZjbKpiEcrF6vswgccGA1UdHwSBvzCBvDA3oDWgM4YxaHR0
cDovL2NybC5jZXJ0aW5vbWlzLmNvbS9BQ19SYWNpbmUvY3JsL2NybC0xLmNybDCBgKB+oHyCE2xk
YXAuY2VydGlub21pcy5jb22kZTBjMQswCQYDVQQGEwJGUjETMBEGA1UEChMKQ2VydGlub21pczEX
MBUGA1UECxMOMDAwMiA0MzM5OTg5MDMxJjAkBgNVBAMMHUNlcnRpbm9taXMgLSBBdXRvcml0w6kg
UmFjaW5lMBcGA1UdIAQQMA4wDAYKKoF6AVYCAgABATANBgkqhkiG9w0BAQUFAAOCAgEAAD75Vk9b
pHI/ng1atgjUzJygSmW+sehEEv0BDFBLFNUgAS1f3bPQIoWoiEiele9QhkYkij+ccD512mg5mFtu
jXBEIGUdq8hFFnilTGc3HmDXti2Yzsm0YGsmow65V+INhcwm8gP3T7v6FlhWzgtof9EAf7p6U/sN
OYPZzn0YYauTtpnDd90f2s+xL4aNyG/+gtHiyqgx0dftTEVNTFFgIvSAE4ktHSD4ZTIdERp+XIhA
ceCbISgKiL9l9zcehdp4Ib61zRTkXlYhmppMmanEQs+r+pgXkmXYTtaTt4uY6pvTf07cBKR1GYtz
WC79/XU0CRoX9malpOn9AaZw8RYr4miv14Q7U3leCdflV8WKHQi5GOaYx+Cj/QkdBmQkNVTMOFHW
DXN0nSbPtux8B+WxqS0BBiXpHcAJgcmh7Cnb1kbSPdQ1M+1wEtAz7y7VJBGH4oT/MbEfApj6yBOZ
C++2KBYnyXa6mrLvlvje7Z9rHmtR2K/9iJm87bmzFRfsJI/V1gASkXcQMiJJg64x43+KS8JkoJfv
9mygf5O3qAbhmrj8G7IBLOKhQXJpMSFKOclTP21Wz7crie1VqshR8uwD4OfBUsawoBI5GcrpRquD
ClYbpCcaCNHn+xwfvpMr4bvlHDt395UJFqCO3Cbu8fakWQy6nubUojXEM/DLrJbsWR0=

-----END CERTIFICATE-----

Signature algorithm: *SHA1withRSA*

Issuer CN: *Certinomis - Autorité Racine*

Issuer OU: *0002 433998903*

Issuer O: *Certinomis*

Issuer C: *FR*

Subject CN: *Certinomis AC 2 étoiles*

Subject OU: *0002 433998903*

Subject O: *Certinomis*

Subject C: *FR*

Valid from: *Fri Dec 12 10:25:18 CET 2008*

Valid to: *Wed Dec 12 10:25:18 CET 2018*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C8:85:16:01:3C:67:42:E1:4D:04:08:FF:D2:B4:77:E2:AE:ED:29:50:54:F8:A6:08:CB:4D:E1:96:88:53:5B:14:98:99:D9:E3:78:E1:37:56:21:1E:C5:11:ED:E8:2C:00:6D:85:82:22:FC:2B:20:93:72:CB:67:AD:D3:3A:87:2F:15:4A:84:E1:32:FA:01:4B:4C:EB:21:63:C2:2C:FC:1F:00:B6:7C:F8:66:4D:DE:7A:75:45:1E:8B:D0:B2:2C:53:24:53:DE:AB:DD:88:0B:5A:21:A9:40:18:D6:A8:1A:D2:26:59:74:F5:9A:98:C8:14:38:D1:04:37:B3:07:42:8C:49:11:9E:5D:AB:8F:16:D7:5B:00:B1:A1:6B:F3:CA:2E:AE:D1:C1:90:4B:F9:6D:2C:AE:99:F8:23:C2:12:1E:5F:C5:8B:F1:7C:63:B8:FD:6C:57:CB:3E:90:3B:9C:73:18:36:9F:EF:54:73:F8:1E:F1:F2:37:2F:CF:C8:CC:EA:D2:80:B3:C2:75:35:8E:75:84:C3:48:69:4C:F8:B0:92:D3:76:FB:BC:F0:42:AA:5B:72:A3:B9:9D:4A:D3:1B:B8:F7:E5:C9:8C:FD:0C:E9:
0C:A5:9A:6D:6E:80:8E:B9:F7:AF:A9:B0:35:C1:7E:50:79:76:6C:82:ED:BE:52:1C:6A:F7:02:03:01:00:01

Basic Constraints *IsCA: true*

Authority Key Identifier *0D:8C:B6:61:DA:44:B8:D1:14:7D:C3:BE:7D:5E:48:F0:CE:CA:6A:B0*

Subject Key Identifier *E9:C3:86:F5:84:91:6F:83:09:2A:26:63:6C:AA:62:11:CA:C5:EA:FB*

CRL Distribution Points *http://crl.certinomis.com/AC_Racine/crl/crl-1.crl*

2: ldap.certinomis.com

C=FR,O=Certinomis,OU=0002 433998903,CN=Certinomis - Autorité Racine

Certificate Policies *Policy OID: 1.2.250.1.86.2.2.0.1.1*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *2B:64:16:EB:64:A7:6A:CE:5E:A4:69:69:BE:2E:44:12:2C:8A:1D:1E:D6:8A:D6:73:EC:A0:8A:55:E0:C0:4D:B0*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description

[en] *undefined.*

[fr] *undefined.*

Status Starting Time *2018-01-30T01:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS101456/QCP+*

TSP Service Definition URI

URI *[en]* *https://www.certinomis.com/publi/rgs/DT-FL-0808-015-PC-ORGA-2E-1.3_EN.pdf*

URI *[fr]* *https://www.certinomis.com/publi/rgs/DT-FL-0808-015-PC-ORGA-2E-1.3.pdf*

5.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

5.1.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Certinomis AC 2 stars*

Name *[fr]* *Certinomis AC 2 étoiles*

Service digital identities

X509SubjectName

Subject CN: *Certinomis AC 2 étoiles*

Subject OU: *0002 433998903*

Subject O: *Certinomis*

Subject C: *FR*

X509SKI

X509 SK I *6cOG9YSRb4MJKiZjbKpiEcrF6vs=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

5.1.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

5.1.3 - History instance n.2 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Certinomis AC 2 stars*

Name *[fr]* *Certinomis AC 2 étoiles*

Service digital identities

X509SubjectName

Subject CN: *Certinomis AC 2 étoiles*

Subject OU: *0002 433998903*

Subject O: *Certinomis*

Subject C: *FR*

X509 SK I *6cOG9YSRb4MJKiZjbKpiEcrF6vs=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2009-03-12T23:00:00Z*

5.2 - Service (granted): Certinomis - Prime CA

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Certinomis - Prime CA*

Name *[fr]* *Certinomis - Prime CA*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *212763915226910061041200221469919728288546259 76*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIGEzCCA/ugAwIBAgIUA7oQ/xodvA0FDUshQkYvPAuAJrgwDQYJKoZIhvcNAQELBQAwWjELMAkG
A1UEBhMCRlIxEzARBgNVBAoTCkNlcnRpbm9taXMxFzAVBgNVBAsTDjAwMDIgNDMzOTk4OTAzMR0w
GwYDVQQDExRDZXJ0aW5vbWlzIC0gUm9vdCBDQTAeFw0xMzEwMjExMDE1NDdaFw0yMzEwMjExMDE1
NDdaMFsxCzAJBgNVBAYTAkZSMRMwEQYDVQQKEwpDZXJ0aW5vbWlzMRcwFQYDVQQLEw4wMDAyIDQz
Mzk5ODkwMzEeMBwGA1UEAxMVQ2VydGlub21pcyAtIFByaW1lIENBMIICIjANBgkqhkiG9w0BAQEF
AAOCAg8AMIICCgKCAgEAzUlhYB1/xkXlj9Ue/V7EWaN9X3xnbe60cV7yP9F9PAH1A4e1oB6al0uk
8hqG55MQw7JsOvgWBLDcGxvs32OtsI1Rn0t/z3Nmj/dbvfZkRFjr1U/+y2+Jh6aVmoK4o2hz5+Y7
3CoYigbqOhlNNnhRJTHe3ep/OyWnsVrgsn7MTUm4aKg6sIpTlnLwP+B5PEoGuILQmDzyluX+b4Yw
OA3yfT01+Z1ow1cDJAbmzoHQReufsWy2MWGMDd0k0ZEscWd8wp2HRfCRSAAEKDd5h0O9XzgypClX
9+dCtbnXuNV4NBmr6pxpoIG/YwMq3OzgWewGOg3zzahgJwbr9urVt6ZzFJO0m70vKTQPTb6TzT5T
53qalXhjvrD5rmNolHktf63Y2OB8OO93JldPdvrtN8XOs/O2mKnb+kN+hf2/auV0a+8cmMbn/y61
+Popor3WAzMluruBGXIDP4NpisgwvqYxFJdFs/hx5n0lTAt+8RisSsJHMDzakUk/Mf4K/L+cyZew
o72UwPTOX5r/55kd2FuggbzATPrcUfl4jtvSUCbFVZPJxsLqOd12ouGFpb93FktBM2ceB1NqYJhf
ddn6+gRJxiEpASLzcnYz/gTfhYjd2xIxsamjJV30wKpHX+giemBJi61scEHKHRV5yhCWg3XakhoD
ledC1m//y1XtTX5wq2MCAwEAAaOBzzCBzDAOBgNVHQ8BAf8EBAMCAQYwDwYDVR0TAQH/BAUwAwEB
/zAdBgNVHQ4EFgQUcImA/BO1dMO/PpmMS1KEMJ4w7Z4wEQYDVR0gBAowCDAGBgRVHSAAMFYGA1Ud
HwRPME0wS6BJoEeGRWh0dHA6Ly9jcmwuaWdjLWczLmNlcnRpbm9taXMuY29tL1JBQ0lORV9HMy9j
cmwvQUNfUmFjaW5lX0czLWNybC0xLmNybDAfBgNVHSMEGDAWgBTvkUz1pcMw6C8I6tNxIqSSaHh0
2TANBgkqhkiG9w0BAQsFAAOCAgEAsoRqY39LsDfKn2TVVoyU5sf1Bu811JveJDPSDHhhaG+IETV4
X8a7nZHgCxlV4xaHc4U07CO2xKgKP4+N9t/YLrHu6TwsR51/2vDBSRQ1cxyVGwGlv57lsEMaSyzl
BFHR7rFbEwL1F7DMiHlJ/eSSOYRhFFZPXIpuT0SmeeDfk7miJ9La3JTC8zbpQUGlFwgeyb3Bgn1Q
re3OHMhYmrfMq9OStY7+g9dWDZsi2nY4GeSs43DIMLazWvHzWhDkmHvAwaNbZrTQj0EAL+Cy67EP
T2Y7+RXrf0pEk5kipKvYGZfS0POH6ZUNvBlIJOmc/lIiGP8c7KmHxT9VmQvohNZ3tLkZZvZ/mtB/
twLH5O3Vhk0WlZmB70qKPo48SINJvatrUd1OQbLp3sS2oRx9vhLezEvPx+RfrIMxY+wcd1h/6rhV
oybFw3yIfkj3F5cFRInECpRSYJLIJDbOJ9eqABbrPqfbokFzDJ+56TzZbGBDrCzHOuEOc3i2vne1
k8NeirxubnLSRhpEjGrNa92Zjno0XmshYMVYcyF5SlHcuzveW9SgXaUw98pz2ZC0h8FmBPyIaoZf
lqK87zjejYT/bxaEBHm7JDTzzYEgfXBKwjIIWJJj+fsEJCZPf1wYm2aDrGEAs+6apMD4DCJg9ITU
+ywYsLx7E3CQDAVavy6TJkXmneA=

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Certinomis - Root CA*

Issuer OU: *0002 433998903*

Issuer O: *Certinomis*

Issuer C: *FR*

Subject CN: *Certinomis - Prime CA*

Subject OU: *0002 433998903*

Subject O: *Certinomis*

Subject C: *FR*

Valid from: *Mon Oct 21 12:15:47 CEST 2013*

Valid to: *Sat Oct 21 12:15:47 CEST 2023*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:CD:49:61:60:1D:7F:C6:45:E5:8F:D5:1E:FD:5E:C4:59:A3:7D:5F:7C:67:6D:EE:B4:71:5E:F2:3F:D1:7D:3C:01:F5:03:87:B5:A0:1E:9A:97:4B:A4:F2:1A:86:E7:93:10:C3:B2:6C:3A:F8:16:04:B0:DC:1B:1B:EC:DF:63:AD:B0:8D:51:9F:4B:7F:CF:73:66:8F:F7:5B:BD:F6:64:44:58:EB:D5:4F:FE:CB:6F:89:87:A6:95:9A:82:B8:A3:68:73:E7:E6:3B:DC:2A:18:8A:06:EA:3A:19:4D:36:78:51:25:31:DE:DD:EA:7F:3B:25:A7:B1:5A:E0:B2:7E:CC:4D:49:B8:68:A8:3A:B0:8A:53:96:72:F0:3F:E0:79:3C:4A:06:B8:82:D0:98:3C:F2:96:E5:FE:6F:86:30:38:0D:F2:7D:3D:35:F9:9D:68:C3:57:03:24:06:E6:CE:81:D0:45:EB:9F:B1:6C:B6:31:61:8C:0D:DD:24:D1:91:2C:71:67:7C:C2:9D:87:45:F0:91:48:00:04:28:37:79:87:43:BD:5F:38:32:A4:29:57:F7:E7:42:B5:B9:D7:B8:D5:78:34:19:AB:EA:9C:69:A0:81:BF:63:03:2A:DC:EC:E0:59:EC:06:3A:0D:F3:CD:A8:60:27:06:EB:F6:EA:D5:B7:A6:73:14:93:B4:9B:BD:2F:29:34:0F:4D:BE:93:CD:3E:53:E7:7A:9A:95:78:63:BE:B0:F9:AE:63:68:94:79:2D:7F:AD:D8:D8:E0:7C:38:EF:77:26:57:4F:76:FA:ED:37:C5:CE:B3:F3:B6:98:A9:DB:FA:43:7E:85:FD:BF:6A:E5:74:6B:EF:1C:98:C6:E7:FF:2E:B5:F8:FA:29:A2:BD:D6:03:33:25:BA:BB:81:19:72:03:3F:83:69:8A:C8:30:BE:A6:31:14:97:45:B3:F8:71:E6:7D:2
5:4C:0B:7E:F1:18:AC:4A:C2:47:30:3C:DA:91:49:3F:31:FE:0A:FC:BF:9C:C9:97:B0:A3:BD:94:C0:F4:CE:5F:9A:FF:E7:99:1D:D8:5B:A0:81:BC:C0:4C:FA:DC:51:F9:78:8E:DB:D2:50:26:C5:55:93:C9:C6:C2:EA:39:DD:76:A2:E1:85:A5:BF:77:16:4B:41:33:67:1E:07:53:6A:60:98:5F:75:D9:FA:FA:04:49:C6:21:29:01:22:F3:72:76:33:FE:04:DF:85:88:DD:DB:12:31:B1:A9:A3:25:5D:F4:C0:AA:47:5F:E8:22:7A:60:49:8B:AD:6C:70:41:CA:1D:15:79:CA:10:96:83:75:DA:92:1A:03:95:E7:42:D6:6F:FF:CB:55:ED:4D:7E:70:AB:63:02:03:01:00:01

Basic Constraints *IsCA: true*

Subject Key Identifier *70:89:80:FC:13:B5:74:C3:BF:3E:99:8C:4B:52:84:30:9E:30:ED:9E*

Certificate Policies *Policy OID: 2.5.29.32.0*

CRL Distribution Points *http://crl.igc-g3.certinomis.com/RACINE_G3/crl/AC_Racine_G3-crl-1.crl*

Authority Key Identifier *EF:91:4C:F5:A5:C3:30:E8:2F:08:EA:D3:71:22:A4:92:68:78:74:D9*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *F9:29:56:18:E7:A7:52:D1:07:42:3C:3D:3E:1F:FE:0D:89:4F:14:36:9A:18:8E:73:3E:EE:36:88:4E:A7:38:53*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS101456/QCP+*

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Signature-2-Stars*

TSP Service Definition URI

URI *[fr]* *https://www.certinomis.fr/documents-et-liens/nos-politiques*

URI *[en]* *https://www.certinomis.fr/documents-et-liens/nos-politiques*

5.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

5.2.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

5.2.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

5.2.4 - Extension (critical): Qualifiers [QCWithQSCD]

Qualifier type description *[en]* *undefined.*

[fr] *undefined.*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithQSCD*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Policy Identifier nodes:

Identifier *1.2.250.1.86.2.3.3.2.1*

Policy Identifier nodes:

Identifier *1.2.250.1.86.2.3.3.10.1*

Policy Identifier nodes:

Identifier *1.2.250.1.86.2.3.3.30.1*

Policy Identifier nodes:

Identifier *1.2.250.1.86.2.3.6.2.1*

Policy Identifier nodes:

Identifier *1.2.250.1.86.2.3.6.10.1*

Policy Identifier nodes:

Identifier *1.2.250.1.86.2.3.6.30.1*

5.2.5 - Extension (critical): Qualifiers [QCWithQSCD]

Qualifier type description *[en]* *undefined.*

[fr] *undefined.*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithQSCD*

Criteria list assert=all

Key Usage *[digitalSignature]* *true*

Policy Identifier nodes:

Identifier *1.2.250.1.86.2.3.3.22.21*

Policy Identifier nodes:

Identifier *1.2.250.1.86.2.3.3.24.1*

5.2.6 - Extension (critical): Qualifiers [QCForWSA]

Qualifier type description *[en]* *undefined.*

[fr] *undefined.*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForWSA*

Criteria list assert=all

Key Usage *[keyAgreement]* *true*

Policy Identifier nodes:

Identifier *1.2.250.1.86.2.3.3.20.1*

5.2.7 - History instance n.1 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Certinomis - Prime CA*

Name *[fr]* *Certinomis - Prime CA*

Service digital identities

X509SubjectName

Subject CN: *Certinomis - Prime CA*

Subject OU: *0002 433998903*

Subject O: *Certinomis*

Subject C: *FR*

X509SKI

X509 SK I *cImA/BO1dMO/PpmMS1KEMJ4w7Z4=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2013-10-21T08:15:47Z*

5.3 - Service (granted): Certinomis - AA et Agents

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Certinomis - AA et Agents*

Name *[fr]* *Certinomis - AA et Agents*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *935279249386816664965831638275890397949458522140*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIGGDCCBACgAwIBAgIVAKPTXz09IMBN15cwA7m9Y194YiAcMA0GCSqGSIb3DQEBCwUAMFoxCzAJ
BgNVBAYTAkZSMRMwEQYDVQQKEwpDZXJ0aW5vbWlzMRcwFQYDVQQLEw4wMDAyIDQzMzk5ODkwMzEd
MBsGA1UEAxMUQ2VydGlub21pcyAtIFJvb3QgQ0EwHhcNMTMxMDIxMTAxNjE3WhcNMjMxMDIxMTAx
NjE3WjBfMQswCQYDVQQGEwJGUjETMBEGA1UEChMKQ2VydGlub21pczEXMBUGA1UECxMOMDAwMiA0

MzM5OTg5MDMxIjAgBgNVBAMTGUNlcnRpbm9taXMgLSBBQSBldCBBZ2VudHMwggIiMA0GCSqGSIb3
DQEBAQUAA4ICDwAwggIKAoICAQCmsQHf9V2qXdzI4cTcf5SPXYINIWmfiIPtEAoeh/OanbVMlMAn
hOzDIGBL7ACk2mAmKIg9N416uxNrjFue93KJN+RNVPV4dxdy692spYMGv4RbR1epYjsRaeL5+k3q
1wg5Pjok6sld8XC5HC2TnIukstaPqus+cjE1dFjk7sqNe8wpArogrTyxn6kaxq2RNEr1oWoP/wnn
rqPFrPKoOS5s+z/4s53bovNm+EoPXpOfRBAt/CaRS3VDQazKjTvzVw8HStirmN9bSyxitvS28SZU
DxPr4+kqPGigiPWEjBbqYsFNGlZYVKZOtB0wTYQwYlqU7hRJsCgFTQsqOyKqNHb9gVOUKkAY6SN/
8rToXwGjZpjvvGbaBSzSwSBMYKdrqNBlIFgpF8XazEKDufSgU88APuKMJxxtBefjwK63kAUq4qP3
TYb3l84CFj/Qg4AW5g2+s0+hqvdGIR/BBdqa+IAHoxZoFnRP5qim2+gjU4FWpIOpKEitrTsecQTs
28jg1BAxD2gCg9hAVWWFUIoqFo+h8aCLBrPBAPWMm+r6MJIUV4Mwdiaphrz9wnWrnnFbsfh3ny3B
ExGMTD48XTZxUoDU6LhsUbvHQUQphdnYqBL6Ptr3s4yqNR1ZzHDLZGDIl9lbw0G1Xn+8M0iOGOc3
VaGAXVoPhChoI6vAY53MoBgc5wIDAQABo4HPMIHMMA4GA1UdDwEB/wQEAwIBBjAPBgNVHRMBAf8E
BTADAQH/MB0GA1UdDgQWBBRILbLLFnj5i1aYZyJHbNZQAaWryDARBgNVHSAECjAIMAYGBFUdIAAw
VgYDVR0fBE8wTTBLoEmgR4ZFaHR0cDovL2NybC5pZ2MtZzMuY2VydGlub21pcy5jb20vUkFDSU5F
X0czL2NybC9BQ19SYWNpbmVfRzMtY3JsLTEuY3JsMB8GA1UdIwQYMBaAFO+RTPWlwzDoLwjq03Ei
pJJoeHTZMA0GCSqGSIb3DQEBCwUAA4ICAQAVqWg0eS82GZrsLxhzAejP+C9btCjNCG1AZrUyhPD1
YVkYvxTzDCOeRvOzWsZ2AjQtu9Xlz5bWnwcdc8mkqRVcACB4orWqwLNqe1mqVpe5Y41NUBt5ocI3
Our43HHRY2W1lT4+hKjOie2Ez48RatwK1MCYf32eAHlkx5uWnx0kzB3y9kzhShPWLjNTjxWe4aMW
RzZREQLm0snpqYSC6l2WRitUDi1VkFSsPKwqKeybkyV6gKsSCemNse7gIIX6DJYiHOGtMC/QJ5uI
5qRoTXiAXwxsjCe+YVQpVhYxaNEupSa9Zubo2BG+y643Vp77zUQWEFsJwe6aOseMqQUuxZ6zap5f
dUIwlXWyKcW7rSZqiLDScQQRO3OoBzn2mOXa2qXr0gLMeEnSxiZEVFKKBzILnU4tds4onex/3WGb
vQoJMONyLE4LDTLHfi8Xb1iVYjDXo/Fy/pyaq3hYkyPeoHoGiANKwbhdVsJRp7BMdEGR/RmZ2Ttt
YDL9V+2JeluqcIdVidETyHE0kVWICZXCHl+qdhMLw/bnCR5id+tYBfzEyojjelnyFByvhPCa4d78
q626N1Nz6XjturJ/wJlVTo+xXQu7dIatb/uXiOZxqIUXL8UopLNYYE567Z3jMCoW9O+Rkjiidzj3 l2bV8izs2WzCv5fZzQeqLI/3pK7JOIGjDg==

-----END CERTIFICATE-----

Signature algorithm:	*SHA256withRSA*
Issuer CN:	*Certinomis - Root CA*
Issuer OU:	*0002 433998903*
Issuer O:	*Certinomis*
Issuer C:	*FR*
Subject CN:	*Certinomis - AA et Agents*
Subject OU:	*0002 433998903*
Subject O:	*Certinomis*
Subject C:	*FR*
Valid from:	*Mon Oct 21 12:16:17 CEST 2013*
Valid to:	*Sat Oct 21 12:16:17 CEST 2023*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:A6:B1:01:DF:F5:5D:AA:5D:DC:C8:E1:C4:DC:7F:94:8F
:5D:82:0D:21:69:9F:88:83:ED:10:0A:1E:87:F3:9A:9D:B5:4C:94:C0:27:84:EC:C3:20:60:4B:EC:00:A4:DA:60:26:28:88:3D:37:8D:7A:BB:13:6B:8C:5B:9E:F7:72:89:3
7:E4:4D:54:F5:78:77:17:72:EB:DD:AC:A5:83:06:BF:84:5B:47:57:A9:62:3B:11:69:E2:F9:FA:4D:EA:D7:08:39:3E:3A:24:EA:C9:5D:F1:70:B9:1C:2D:93:9C:8B:A4:B2:
D6:8F:AA:EB:3E:72:31:35:74:58:E4:EE:CA:8D:7B:CC:29:02:BA:20:AD:3C:B1:9F:A9:1A:C6:AD:91:34:4A:F5:A1:6A:0F:FF:09:E7:AE:A3:C5:AC:F2:A8:39:2E:6C:FB:3
F:F
8:B3:9D:DB:A2:F3:66:F8:4A:0F:5E:93:9F:44:10:2D:FC:26:91:4B:75:43:41:AC:CA:8D:3B:F3:57:0F:07:4A:D8:AB:98:DF:5B:4B:2C:62:B6:F4:B6:F1:26:54:0F:13:EB:
E3:E9:2A:3C:68:A0:88:F5:84:8C:16:EA:62:C1:4D:1A:56:58:54:A6:4E:B4:1D:30:4D:84:30:62:5A:94:EE:14:49:B0:28:05:4D:0B:2A:3B:22:AA:34:76:FD:81:53:94:2
A:40:18:E9:23:7F:F2:B4:E8:5F:01:A3:66:98:EF:BC:66:DA:05:2C:D2:C1:20:4C:60:A7:6B:A8:D0:65:20:58:29:17:C5:DA:CC:42:83:B9:F4:A0:53:CF:00:3E:E2:8C:27:
1C:6D:05:E7:E3:C0:AE:B7:90:05:2A:E2:A3:F7:4D:86:F7:97:CE:02:16:3F:D0:83:80:16:E6:0D:BE:B3:4F:A1:AA:F7:46:21:1F:C1:05:DA:9A:F8:80:07:A3:16:68:16:74
:4F:E6

:A8:A6:DB:E8:23:53:81:56:A4:83:A9:28:48:AD:AD:3B:1E:71:04:EC:DB:C8:E0:D4:10:31:0F:68:02:83:D8:40:55:65:85:50:8A:2A:16:8F:A1:F1:A0:8B:06:B3:C1:00:F5:8C:9B:EA:FA:30:92:14:57:83:30:76:26:A9:86:BC:FD:C2:75:AB:9E:71:5B:B1:F8:77:9F:2D:C1:13:11:8C:4C:3E:3C:5D:36:71:52:80:D4:E8:B8:6C:51:BB:C7:41:44:29:85:D9:D8:A8:12:FA:3E:DA:F7:B3:8C:AA:35:1D:59:CC:70:CB:64:60:C8:97:D9:5B:C3:41:B5:5E:7F:BC:33:48:8E:18:E7:37:55:A1:80:5D:5A:0F:84:28:68:23:AB:C0:63:9D:CC:A0:18:1C:E7:02:03:01:00:01

Basic Constraints *IsCA: true*

Subject Key Identifier *48:2D:B2:CB:16:78:F9:8B:56:98:67:22:47:6C:D6:50:01:A5:AB:C8*

Certificate Policies *Policy OID: 2.5.29.32.0*

CRL Distribution Points *http://crl.igc-g3.certinomis.com/RACINE_G3/crl/AC_Racine_G3-crl-1.crl*

Authority Key Identifier *EF:91:4C:F5:A5:C3:30:E8:2F:08:EA:D3:71:22:A4:92:68:78:74:D9*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *E6:E8:C0:C0:00:8A:F7:B6:91:0E:D5:0D:DD:88:B1:18:16:78:05:95:8D:D6:7A:77:8B:39:0B:72:D9:BB:B5:E6*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS101456/QCP+*

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Authentication-Signature-2-Stars*

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Signature-2-Stars*

TSP Service Definition URI

URI *[en]* *https://www.certinomis.fr/documents-et-liens/nos-politiques*

URI *[fr]* *https://www.certinomis.fr/documents-et-liens/nos-politiques*

5.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

5.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

5.3.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

5.3.4 - Extension (critical): Qualifiers [QCWithQSCD]

Qualifier type description *[en]* *undefined.*

[fr] *undefined.*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithQSCD*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Policy Identifier nodes:

Identifier *1.2.250.1.86.2.3.8.2.1*

Policy Identifier nodes:

Identifier *1.2.250.1.86.2.3.8.10.1*

5.3.5 - Extension (critical): Qualifiers [QCWithQSCD]

Qualifier type description *[en]* *undefined.*

[fr] *undefined.*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithQSCD*

Criteria list assert=all

Key Usage *[digitalSignature]* *true*

Policy Identifier nodes:

Identifier *1.2.250.1.86.2.3.8.22.1*

5.3.6 - Extension (critical): Qualifiers [QCForWSA]

Qualifier type description *[en]* *undefined.*

[fr] *undefined.*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForWSA*

Criteria list assert=all

Key Usage *[keyAgreement]* *true*

Policy Identifier nodes:

Identifier *1.2.250.1.86.2.3.8.20.1*

5.3.7 - History instance n.1 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Certinomis - AA et Agents*

Name *[fr]* *Certinomis - AA et Agents*

Service digital identities

X509SubjectName

Subject CN: *Certinomis - AA et Agents*

Subject OU: *0002 433998903*

Subject O: *Certinomis*

Subject C: *FR*

X509SKI

X509 SK I *SC2yyxZ4+YtWmGciR2zWUAGlq8g=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2013-12-19T00:00:00Z*

6 - TSP: ChamberSign France

TSP Name

Name *[en]* *ChamberSign France*

Name *[fr]* *ChamberSign France*

TSP Trade Name

Name *[en]* *VATFR-83433702479*

Name *[fr]* *VATFR-83433702479*

PostalAddress

Street Address *[fr]* *Place de la Bourse*

Locality *[fr]* *Lyon Cedex 2*

Postal Code *[fr]* *69289*

Country Name *[fr]* *FR*

PostalAddress

Street Address *[en]* *Place de la Bourse*

Locality *[en]* *LYON Cedex 2*

Postal Code *[en]* *69289*

Country Name *[en]* *FR*

ElectronicAddress

URI *http://www.chambersign.fr*

URI *mailto:support@chambersign.fr*

URI *mailto:support@chambersign.fr*

URI *http://www.chambersign.fr*

TSP Information URI

URI *[en]* *http://pc.chambersign.fr/en/docs/*

URI *[fr]* *http://pc.chambersign.fr/docs/*

6.1 - Service (granted): Europrobatio

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified*

by the relevant registration services.

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Europrobatio*

Name *[fr]* *Europrobatio*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *149201978838614161955322945981211322132813*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIGeDCCBGCgAwIBAgISESCm7s6fRDedMRyhbh1/DSitMA0GCSqGSIb3DQEBCwUAMGAxCzAJBgNV
BAYTAkZSMRswGQYDVQQKDBJDaGFtYmVyU2InbiBGcmFuY2UxFzAVBgNVBAsMDjAwMDIgNDMzNzAy
NDc5MRswGQYDVQQDDBJDaGFtYmVyU2lnbiBGcmFuY2UwHhcNMTIxMDE2MDAwMDAwWhcNMjIxMDE2
MDAwMDAwWjBwMQswCQYDVQQGEwJGUjEbMBkGA1UECgwSQ2hhbWJlclNpZ24gRnJhbmNlMRcwFQYD
VQQLDA4wMDAyIDQzMzcwMjQ3OTErMCkGA1UEAwwiQ2hhbWJlclNpZ24gRnJhbmNlIC0gQUMgMyDD
qXRvaWxlczCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBANgLooXnfy12FsM4qA8Nt+29
cAzaIyn1M/MSqAth71SgWVzw9TqNvEcUggJb0+S5BAvpoYoBhycl0XroIzYmQTOEWVwUx7Shyn2e
5iG1yDIobKRr/5fDcMcwwR//XAmWrcdAzBEzjvqsK6Of2ELdykFLfWlOrrEzmdidGAUUaT5piTgZ
MSK1I5SkaottAf2kL2ThtaIxLeV5Qk3/4HLMwwRSkCZleY1wjpDJq7kKpFBHaSWBl1jiKEDkd4iY
/UULSoQ58NjKx/ZtfzeJwQDbvnE65wZ01nZy1kLQGpisxF6UKFiwwlO4rNvDiqJqPV2GNc2I80Tw
GlAZxOZs57WW552r60v9oiHVdeCtri+2xnN+kebhzToLSRvzaTzi8G4yX08W836hC9wIhAiET+M1
il741k3J+ksjaoGk4vsHqsm/nIwTBofgGMj+FRa2TGjYvHptxOrJDOU3jvRqRv6ymf9cUNZgBuWd
OVc9dKtgevHgmUa1igaDgBcQm4ycSzUzaKmYZDtDkT7IUEOLTqApdne2p+4es0mzMKmoU6XUbKZf
0oSnV29ulHEbML57k09qqHCqbf2+hQeBQyHoJ5QzRepCNhz1c+z/m22BDcdHUEiQ0qL8OPK1Zkhk
B4XVdf7jPfEdpcZwChoA0Tdv1LxJp38YiemXZ+FfySktt9keU+A7AgMBAAGjggEaMIIBFjAOBgNV
HQ8BAf8EBAMCAQYwWAYDVR0gBFEwTzBNBggqgXoBYAEHATBBMD8GCCsGAQUFBwIBFjNodHRwOi8v
cGMuY2hhbWJlcnNpZ24uZnIvcmdzL2xjci1kaXJlY3Rlcy8zZXRvaWxlcy8wEgYDVR0TAQH/BAgw
BgEB/wIBADBWBgNVHR8ETzBNMEugSaBHhkVodHRwOi8vY3JsLmNoYW1iZXJzaWduLmZyL2NybC9y
Z3MvbGNyLWRpcmVjdGVzL2NoYW1iZXJzaWduLWZyYW5jZS5jcmwwHQYDVR0OBBYEFJYt1pZu1YAo
UbP7R3gtxt5/O4kcMB8GA1UdIwQYMBaAFPTOYuSVwpaonDgnrSoeRkUGNMmhMA0GCSqGSIb3DQEB
CwUAA4ICAQBY4MoF8ET1h2Gr9zYUROYz5xuRNLdff+jeE7eX39ZGSj7/FCnbUQ1bg7q8wKG6gppR
svRaHTzP+3O2ZmvHfrVD3ebEXWCSRp4EfDYlJjZJz2hTht49SOX7+1k3Gc9h4wHX8ePoA3ERp7zz
EYEpDtmWlYsoCDNzRQOVTw/ijL3Q+DsRyadh0er2Mk0q+2xdDjeaqu7RRFg4MU41j7bDKia/czON
h+QSEfYTDultqdrrM8hm3aPBIRbqTxfdXVkB19yoRcGvMwLsKBBI+cyq6HJZ/iGKePfBGj1tydxo
1cCShp7nSgqDgJUWFDE+p2dT2tflaynBD8WTeUsLw3PieKwbSrTR8XSCc7VdiLzyAOT9Ki68aCZv
5oHecr+AUqbDaSW+duPsF2cqDR9oBx/GK5OinXbtzEx1WKmGFze9v0OtKtxKN9xuo02rpPgcg0FY
20S8azIpy4V9072kdP7TxDjBEXavdHB+KlcyG/NUY4DND6w8KGlo1Cz2yfnRFsNwTp0xSZ+RDpdk
dT8W6p1EYSn1dVI3yMwukoU5l4w09PrvoqITwhQRbmyihgbbMrzgiBuly/Dr7R53YTawqdjJDiUK
vJbFiCbeosNBUULRj3sV4NNp9GrOS2P650wjZlYMd/JF14MwXQvQxEKPxlFpB8uKMT05G9evCWvf LlwtxGUg9Q==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *ChamberSign France*

Issuer OU: *0002 433702479*

Issuer O: *ChamberSign France*

Issuer C:	*FR*
Subject CN:	*ChamberSign France - AC 3 étoiles*
Subject OU:	*0002 433702479*
Subject O:	*ChamberSign France*
Subject C:	*FR*

Valid from: *Tue Oct 16 02:00:00 CEST 2012*

Valid to: *Sun Oct 16 02:00:00 CEST 2022*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:D8:0B:A2:85:E7:7F:2D:76:16:C3:38:A8:0F:0D:B7:ED:BD:70:0C:DA:23:29:F5:33:F3:12:A8:0B:61:EF:54:A0:59:5C:F0:F5:3A:8D:BC:47:14:82:02:5B:D3:E4:B9:04:0B:E9:A1:8A:01:87:27:25:D1:7A:E8:97:36:26:41:33:84:59:5C:14:C7:B4:A1:CA:7D:9E:E6:21:B5:C8:32:28:6C:A4:6B:FF:97:C3:70:C7:30:C1:1F:FF:5C:09:96:AD:C7:40:CC:11:33:8E:FA:AC:2B:A3:9F:D8:42:DD:CA:41:4B:7D:69:4E:AE:B1:33:99:D8:9D:18:05:14:69:3E:69:89:38:19:31:22:B5:23:94:A4:6A:8B:6D:01:FD:A4:2F:64:E1:B5:A2:31:2D:E5:79:42:4D:FF:E0:72:CC:C3:04:52:90:26:65:79:8D:70:8E:90:C9:AB:B9:0A:A4:50:47:69:25:81:97:58:E2:28:40:E4:77:88:98:FD:45:0B:4A:84:39:F0:D8:CA:C7:F6:6D:7F:37:89:C1:00:DB:BE:71:3A:E7:06:74:D6:76:72:D6:42:D0:1A:98:AC:C4:5E:94:28:58:B0:C2:53:B8:AC:DB:C3:8A:A2:6A:3D:5D:86:35:CD:88:F3:44:F0:1A:50:19:C4:E6:6C:E7:B5:96:E7:9D:AB:EB:4B:FD:A2:21:D5:75:E0:AD:AE:2F:B6:C6:73:7E:91:E6:E1:CD:3A:0B:49:1B:F3:69:3C:E2:F0:6E:32:5F:4F:16:F3:7E:A1:0B:DC:08:84:08:84:4F:E3:35:8A:5E:F8:D6:4D:C9:FA:4B:23:6A:81:A4:E2:FB:07:AA:C9:BF:9C:8C:13:06:87:E0:18:C8:FE:15:16:B6:4C:68:D8:BC:7A:6D:C4:EA:C9:0C:E5:37:8E:F4:6A:46:FE:B2:99:FF:5C:50:D6:60:06:E5:9D:39:57:3D:74:AB:60:7A:F1:E0:99:46:B5:8A:06:83:80:17:10:9B:8C:9C:4B:35:33:68:A9:98:64:3B:43:91:3E:C8:50:43:8B:4E:A0:29:76:77:B6:A7:EE:1E:B3:49:B3:30:A9:A8:53:A5:D4:6C:A6:5F:D2:84:A7:57:6F:6E:94:71:1B:30:BE:7B:93:4F:6A:A8:70:AA:6D:FD:BE:85:07:81:43:21:E8:27:94:33:45:EA:42:36:1C:F5:73:EC:FF:9B:6D:81:0D:C7:47:50:48:90:D2:A2:FC:38:F2:B5:66:48:64:07:85:D5:75:FE:E3:3D:F1:1D:A5:C6:70:0A:1A:00:D1:37:6F:D4:BC:49:A7:7F:18:89:E9:97:67:E1:5F:C9:29:2D:B7:D9:1E:53:E0:3B:02:03:01:00:01

Certificate Policies *Policy OID: 1.2.250.1.96.1.7.1*

CPS pointer: http://pc.chambersign.fr/rgs/lcr-directes/3etoiles/

Basic Constraints *IsCA: true - Path length: 0*

CRL Distribution Points *http://crl.chambersign.fr/crl/rgs/lcr-directes/chambersign-france.crl*

Subject Key Identifier *96:2D:D6:96:6E:D5:80:28:51:B3:FB:47:78:2D:C6:DE:7F:3B:89:1C*

Authority Key Identifier *F4:CE:62:E4:95:C2:96:A8:9C:38:27:AD:2A:1E:46:45:06:34:C9:A1*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *F2:95:C9:DE:0B:62:29:94:9B:4C:7D:AE:D1:51:C5:BC:1E:77:29:71:F4:7C:54:6E:2A:E2:B5:B0:37:8D:5C:8F*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

TSP Service Definition URI

URI *[en]* *http://pc.chambersign.fr/rgs/v2/3etoiles/eidas/*

URI *[fr]* *http://pc.chambersign.fr/rgs/v2/3etoiles/eidas/*

6.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

6.1.2 - Extension (critical): Qualifiers [QCWithQSCD, QCForESig]

Qualifier type description *[en]* *undefined.*

[fr] *undefined.*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithQSCD*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForESig*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Policy Identifier nodes:

Identifier *1.2.250.1.96.1.7.1.1.3*

6.1.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Probatio signature ***

Name *[fr]* *Probatio signature ***

Service digital identities

X509SubjectName

Subject CN: *ChamberSign France - AC 3 étoiles*

Subject OU: *0002 433702479*

Subject O: *ChamberSign France*

Subject C: *FR*

X509SKI

X509 SK I *li3Wlm7VgChRs/tHeC3G3n87iRw=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

6.1.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

6.1.4 - History instance n.2 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Probatio signature ****

Name *[fr]* *Probatio signature ****

Service digital identities

X509SubjectName

Subject CN: *ChamberSign France - AC 3 étoiles*

Subject OU: *0002 433702479*

Subject O: *ChamberSign France*

Subject C: *FR*

X509SKI

X509 SK I *li3Wlm7VgChRs/tHeC3G3n87iRw=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2011-10-13T22:00:00Z*

6.2 - Service (withdrawn): Signitio RGS **

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Signitio RGS **

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *149183598803553222213122657489436107695682 6*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIFQzCCAyugAwIBAgISESAcqCWv4TkAQiBGWS1Phf6aMA0GCSqGSIb3DQEBCwUAMFkxCzAJBgNV
BAYTAkZSMRswGQYDVQQKExJDaGFtYmVyU2lnbiBGcmFuY2UxFzAVBgNVBAsTDjAwMDIgNDMzNzAy
NDc5MRQwEgYDVQQDEwtDaGFtYmVyU2lnbjAeFw0xMTA2MjEwMDAwMDBaFw0yMDEyMzEwMTAwMDBa
MGgxCzAJBgNVBAYTAkZSMRswGQYDVQQKExJDaGFtYmVyU2lnbiBGcmFuY2UxFzAVBgNVBAsTDjAw
MDIgNDMzNzAyNDc5MSMwIQYDVQQDDBpDaGFtYmVyU2lnbiAtIFNpZ25hdHVyZSAyKjCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBAOckD5Ekjc7Va1U1M9qdjOsCT7NTpHosyI6gLqHay352
DOo72yTBCkgkYiWfDxCaXbdXnlkzii4k75Z1cxezzidLrlANwZ+Y4HWDSQrIlZZVdO8CxsP1NF1X
dJKkYnhy847nxOr4YI/0tgIRMRMelYnF9Du28XjiH8Ws5daH9nKf3YN8BY1SdCtZEm4Ip9+OhLiy
5NW8qW/KMcCWz6iwHeeT/ihhqAI1GZT7hKU8s86iY35uoBz25Um6iU/YJMIqQ4XjxgKs5fxDlzQU
Cfju4elmJ7RLBSUYSr4QUvlpqENbgkthpEfvTPSHIUVi8BSHdAV/jdD8UYaYoUsXzJziuacCAwEA
AaOB9TCB8jASBgNVHRMBAf8ECDAGAQH/AgEAMA4GA1UdDwEB/wQEAwICBDBJBgNVHSAEQjBAMD4G
ByqBegFgAQYwMzAxBggrBgEFBQcCARYlaHR0cDovL3d3dy5jaGFtYmVyc2lnbi5mci9wYy9yZ3Mv
Mi4yLzBBBgNVHR8EOjA4MDagNKAyhjBodHRwOi8vY3JsLmNoYW1iZXJzaWduLmZyL2NoYW1iZXJz
aWduLWZyYW5jZS5jcmwwHQYDVR0OBBYEFHpBh2P1tiVGWjaUPpibxGkK3HkSMB8GA1UdIwQYMBaA
FCi5W0XkBS5JSYhBbhl8QSiC4jcxMA0GCSqGSIb3DQEBCwUAA4ICAQCOCWcg71PHO46ZVEtezxcq
Dsiuzw+EPcSO9U//jcByUOndrd19WDETOZfC6kNDJB8PDGdBVssfY8JWTcb4Q2nd94YEyuF4siVa
GhEEAYIXaR3LqnSpeMvSASZsAcw66mk16g1OKKIlqCF/84uqczIJzfQAxYzqd3MSvfH2dWyswOOa
VYvd+SkYmDf/szeYlOqWvFMOF+6oeCUQjxrwMNcDoRPYm+95fOL5pJ6LS7gORQwst5e2zB2KjIsX
/pVySmTAhHt/pTm4wB38FpU0HWMZMv2XFbUpuTC349SAbiMM4pvThKWvJSfIjFREmDSLakWNQuCz
4NPdnvFMA5rVgF63IExEi/Fl7Rg1smeAyOcapMevUWmFL3kakRsdh2sOoM1Y9pd7z2Iz+8sdycur
pfLDieK6cYK7XGX6v6bCZUhxGrjXbvD7xLnx7UCya9J46RjQ4JWhMl5VC+nnoFVz4IjkdSFjsgDh
JRNGhwMcvXOKYLFfvYY31iCJFkBdmviSPnIuTVN7O4HMWaWXMffSYZWU+GMFrJTJj392472KbvBH
aiWRhkA8h1RE5qr246O9BQ5d4O+5OME18IRUKUXm3JGtas5tA/t8KENMBOhIoNeKIwih/gpbbtFQ
cARGZ229XWSwLpA6IfPxdxvN59weG7SWQJ8J6VflwbhJy1aWWCMFyg==

-----END CERTIFICATE-----

Signature algorithm:	*SHA256withRSA*
Issuer CN:	*ChamberSign*
Issuer OU:	*0002 433702479*
Issuer O:	*ChamberSign France*
Issuer C:	*FR*
Subject CN:	*ChamberSign - Signature 2**
Subject OU:	*0002 433702479*
Subject O:	*ChamberSign France*
Subject C:	*FR*
Valid from:	*Tue Jun 21 02:00:00 CEST 2011*
Valid to:	*Thu Dec 31 02:00:00 CET 2020*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:E7:24:0F:91:24:8D:CE:D5:6B:55:35:33:DA:9D:8C:EB:
02:4F:B3:53:A4:7A:2C:C8:8E:A0:2E:A1:DA:CB:7E:76:0C:EA:3B:DB:24:C1:0A:48:24:62:25:9F:0F:10:9A:5D:B7:57:9E:59:33:8A:2E:24:EF:96:75:73:17:B3:CE:27:4B
:AE:50:0D:C1:9F:98:E0:75:83:49:0A:C8:95:96:55:74:EF:02:C6:C3:F5:34:5D:57:74:92:A4:62:78:72:F3:8E:E7:C4:EA:F8:60:8F:F4:B6:02:11:31:13:1E:95:89:C5:F4:
3B:B6:F1:78:E2:1F:C5:AC:E5:D6:87:F6:72:9F:DD:83:7C:05:8D:52:74:2B:59:12:6E:08:A7:DF:8E:84:B8:B2:E4:D5:BC:A9:6F:CA:31:C0:96:CF:A8:B0:1D:E7:93:FE:28
:61:A8:02:35:19:94:FB:84:A5:3C:B3:CE:A2:63:7E:6E:A0:1C:F6:E5:49:BA:89:4F:D8:24:C2:2A:43:85:E3:C6:02:AC:E5:FC:43:97:34:14:09:F8:EE:E1:E9:66:27:B4:4B:

Basic Constraints *IsCA: true - Path length: 0*

Certificate Policies *Policy OID: 1.2.250.1.96.1.6*

CPS pointer: http://www.chambersign.fr/pc/rgs/2.2/

CRL Distribution Points *http://crl.chambersign.fr/chambersign-france.crl*

Subject Key Identifier *7A:41:87:63:F5:B6:25:46:5A:36:94:3E:98:9B:C4:69:0A:DC:79:12*

Authority Key Identifier *28:B9:5B:45:E4:05:2E:49:49:88:41:6E:19:7C:41:28:82:E2:37:31*

Key Usage: *keyCertSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *A6:2C:2E:1B:1B:FE:7D:E6:FD:8E:C9:87:F9:D0:4A:31:C0:F2:6A:FB:66:18:BF:11:94:CF:FF:EE:DD:D7:2E:C4*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2017-11-01T01:00:00Z*

Scheme Service Definition URI

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Signature-2-Stars*

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS102042/NCP+*

TSP Service Definition URI

URI *[en]* *http://www.chambersign.fr/medias/documents/PC/ChamberSign-France_PC-Sign2_ENv01.pdf*

URI *[fr]* *http://pc.chambersign.fr/docs/pc/LCR_Indirectes/fr/PC_Signature_2etoiles.pdf*

6.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

6.2.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Signitio RGS ***

Service digital identities

X509SubjectName

Subject CN: *ChamberSign - Signature 2**

Subject OU: *0002 433702479*

Subject O: *ChamberSign France*

Subject C: *FR*

X509SKI

X509 SK I *ekGHY/W2JUZaNpQ+mJvEaQrceRI=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

6.2.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

6.2.3 - History instance n.2 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Signitio RGS ***

Service digital identities

X509SubjectName

Subject CN: *ChamberSign - Signature 2**

Subject OU: *0002 433702479*

Subject O: *ChamberSign France*

Subject C: *FR*

X509SKI

X509 SK I *ekGHY/W2JUZaNpQ+mJvEaQrceRI=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2011-10-13T22:00:00Z*

6.3 - Service (withdrawn): Signitio RGS ***

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Signitio RGS ****

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *149181284268930123119931819619946887327634 9*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIFQzCCAyugAwIBAgISESALPoQDaKoC9qsg2P3q59u9MA0GCSqGSIb3DQEBCwUAMFkxCzAJBgNV
BAYTAkZSMRswGQYDVQQKExJDaGFtYmVyU2lnbiBGcmFuY2UxFzAVBgNVBAsTDjAwMDIgNDMzNzAy
NDc5MRQwEgYDVQQDEwtDaGFtYmVyU2lnbjAeFw0xMTA2MjEwMDAwMDBaFw0yMDEyMzEwMTAwMDBa
MGgxCzAJBgNVBAYTAkZSMRswGQYDVQQKExJDaGFtYmVyU2lnbiBGcmFuY2UxFzAVBgNVBAsTDjAw
MDIgNDMzNzAyNDc5MSMwIQYDVQQDDBpDaGFtYmVyU2lnbiAtIFNpZ25hdHVyZSAzKjCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBAL5I/tJuiab4vd5JMoGvTTUHOhlMRgMJAkoMv/nxPABt
dHXWpsbbKJys1VkbtUit+6vQGvYJG8f7vo3M844WC0mC1DXKVlXx4PtWmQ6Y5my3GKGlQcVTOd8T
h13ax7u/8n1nZJXQLO6YqzDOIskTXIz6DU807Z4Zp39DteDlx00BotHlTbEHBTg25t4wdnvAMji6
7vNaH97c40FEIbQwTnEz2dvtnAzKPjRTJawF0IbSH6jE57TCAXfGvgOVV0NETdEGsVldz+oIdTR2
c//WdGORD/cEt3g0jMBxLDknj9joPkUXOyJ7ELDVt4HALGzNiJ7EA/L2STBTe/eqPDW6O0kCAwEA
AaOB9TCB8jASBgNVHRMBAf8ECDAGAQH/AgEAMA4GA1UdDwEB/wQEAwICBDBJBgNVHSAEQjBAMD4G
ByqBegFgAQYwMzAxBggrBgEFBQcCARYlaHR0cDovL3d3dy5jaGFtYmVyc2lnbi5mci9wYy9yZ3Mv
Mi4yLzBBBgNVHR8EOjA4MDagNKAyhjBodHRwOi8vY3JsLmNoYW1iZXJzaWduLmZyL2NoYW1iZXJz
aWduLWZyYW5jZS5jcmwwHQYDVR0OBBYEFCS0ksrifrr68I0GQFQYY1GDsWP4MB8GA1UdIwQYMBaA
FCi5W0XkBS5JSYhBbhl8QSiC4jcxMA0GCSqGSIb3DQEBCwUAA4ICAQAnWlxAp+pphdACI/kHo0G1
/d7VMyxKXCi99n+RyuRWy1MH5zQP/pqjz5Bn56pMRkTlS6JzqnpVpNXQmT1jLGbyT35OpwE5KxuF
EqhOB2+m36jdDdHHWzAVjreG5mnSar1sOSO/wLjdUs82fYYEunr/Szwb4u8Fw5As/o4m8sJoc8QS
mfPQwQEXEutTrCcS8vsn+xoFTbqObRYyG2tq7ilR8pDl2GYGxS+EzkUrvUVkfFILuVAKbAb3OMSf
V/R55mUV8jsBGrl3751IC68CW+DM47EBwFEslvjgG8K9D1phU4LtzLf25PEKPbBTXE/8HUJyhKk/
Jc7Va95F22az522e5K7P8TJNnbhCDYqODyZmgesDMKVbH32ZK08aelORKN22fDF/Xx4ZbyJmwtF+
TE6yAMhELo+PCA2VAYG78x1ng2J7A86hOTDTxa3AV4Au8SqXuv/rF11r/WAqdfWnuYItAwRIV6NN

kLXUmZoEAHKCsZsatF3al2pVHKmaOFFYToBaIqQDjAepICY6O7w865fZyoy8xBdOzCGbrJlLWJ3v
9kgS0UPVdNlRgwq+QO9ziDPUho/5ATgla39z1enyboWhHcbK2INFYXVA9w92LV/gVdTAZtAQ5drk
GrbT9syKTMhiUE7PhGC00E2RP3PBXH61mxX2HW5KH3apTeclf3TtJQ==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *ChamberSign*

Issuer OU: *0002 433702479*

Issuer O: *ChamberSign France*

Issuer C: *FR*

Subject CN: *ChamberSign - Signature 3**

Subject OU: *0002 433702479*

Subject O: *ChamberSign France*

Subject C: *FR*

Valid from: *Tue Jun 21 02:00:00 CEST 2011*

Valid to: *Thu Dec 31 02:00:00 CET 2020*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:BE:48:FE:D2:6E:89:A6:F8:BD:DE:49:32:81:AF:4D:35:07:3A:19:4C:46:03:09:02:4A:0C:BF:F9:F1:3C:00:6D:74:75:D6:A6:C6:DB:28:9C:AC:D5:59:1B:B5:48:AD:FB:AB:D0:1A:F6:09:1B:C7:FB:BE:8D:CC:F3:8E:16:0B:49:82:D4:35:CA:56:55:F1:E0:FB:56:99:0E:98:E6:6C:B7:18:A1:A5:41:C5:53:39:DF:13:87:5D:DA:C7:BB:BF:F2:7D:67:64:95:D0:2C:EE:98:AB:30:CE:22:C9:13:5C:8C:FA:0D:4F:34:ED:9E:19:A7:7F:43:B5:E0:E5:C7:4D:01:A2:D1:E5:4D:B1:07:05:38:36:E6:DE:30:76:7B:C0:32:38:BA:EE:F3:5A:1F:DE:DC:E3:41:44:21:B4:30:4E:71:33:D9:DB:ED:9C:0C:CA:3E:34:53:25:AC:05:D0:86:D2:1F:A8:C4:E7:B4:C2:01:77:C6:BE:03:95:57:43:44:4D:D1:06:B1:59:5D:CF:EA:08:75:34:76:73:FF:D6:74:63:91:0F:F7:04:B7:78:34:8C:C0:71:2C:39:27:8F:D8:E8:3E:45:17:3B:22:7B:10:B0:D5:B7:81:C0:2C:6C:CD:88:9E:C4:03:F2:F6:49:30:53:7B:F7:AA:3C:35:BA:3B:49:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

Certificate Policies *Policy OID: 1.2.250.1.96.1.6*

CPSpointer: http://www.chambersign.fr/pc/rgs/2.2/

CRL Distribution Points *http://crl.chambersign.fr/chambersign-france.crl*

Subject Key Identifier *24:B4:92:CA:E2:7E:BA:FA:F0:8D:06:40:54:18:63:51:83:B1:63:F8*

Authority Key Identifier *28:B9:5B:45:E4:05:2E:49:49:88:41:6E:19:7C:41:28:82:E2:37:31*

Key Usage: *keyCertSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *AB:CB:B7:EE:9A:74:50:B8:10:7D:F7:92:C6:01:11:07:71:21:5F:8E:5B:14:66:20:D5:9C:AF:BE:12:*

82:3B:B9

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS101456/QCPPublic*

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Signature-3-Stars*

TSP Service Definition URI

URI *[fr]* *http://www.chambersign.fr/pc/rgs/2.2/3etoiles-signature/*

URI *[en]* *http://www.chambersign.fr/medias/documents/PC/ChamberSign-France_PC-Sign3_ENv01.pdf*

6.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

6.3.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Signitio RGS ****

Service digital identities

X509SubjectName

Subject CN: *ChamberSign - Signature 3**

Subject OU: *0002 433702479*

Subject O: *ChamberSign France*

Subject C: *FR*

X509SKI

X509 SK I *JLSSyuJ+uvrwjQZAVBhjUYOxY/g=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

6.3.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

6.3.3 - History instance n.2 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Signitio RGS ****

Service digital identities

X509SubjectName

Subject CN: *ChamberSign - Signature 3**

Subject OU: *0002 433702479*

Subject O: *ChamberSign France*

Subject C: *FR*

X509SKI

X509 SK I *JLSSyuJ+uvrwjQZAVBhjUYOxY/g=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2011-10-13T22:00:00Z*

6.4 - Service (granted): Eurodacio

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Eurodacio*

Name *[fr]* *Eurodacio*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *149180873813101009196644836666275184801374l*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIGeDCCBGCgAwIBAgISESAIKAGqTbXaOJMm+2uOBJ+tMA0GCSqGSIb3DQEBCwUAMGAxCzAJBgNV
BAYTAkZSMRswGQYDVQQKDBJDaGFtYmVyU2lnbiBGcmFuY2UxFzAVBgNVBAsMDjAwMDIgNDMzNzAy
NDc5MRswGQYDVQQDDBJDaGFtYmVyU2lnbiBGcmFuY2UwHhcNMTIxMDE2MDAwMDAwWhcNMjIxMDE2
MDAwMDAwWjBwMQswCQYDVQQGEwJGUjEbMBkGA1UECgwSQ2hhbWJlclNpZ24gRnJhbmNlMRcwFQYD
VQQLDA4wMDAyIDQzMzcwMjQ3OTErMCkGA1UEAwwiQ2hhbWJlclNpZ24gRnJhbmNlIC0gQUMgMiDD
qXRvaWxlczCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAKNWE1IMFRKok32hVr7mhPZn
oPXRSe9/jk0pPkzf6gBUNN9CJpig0LZGp5Y57rWdQNHT0BnaTNxl1BEoP3MSokzByv+BWQuDuI9H
5IUsM1HEPm/JxLB/Ccq84H2OeJs9s9LEvDcLqGSxSxIsvTiq7oJ28oO3Yey914sxjd6PAb9TBFbh
G4SpAnzFV+BOnfje8qbZlfidifDlOiMjzGx3RpUNuOCxMteOemw2UhllD7cUuMAGhXfz9FdTa9VP
1JtxCvmZXL8PPnbEJ5lcqkkxL5ZbkZKdWCN/En4tq2PlLq8z3J7ldZLovZ+UFbE3eamZnCNu4l6R
dD8bvEjrMfwrxpPJMA51OgViIHfZOgA8PLOHaUnNSeIaPZV3fI8D8+JWpOFVW5DmdUx8qxejUG6u
MYz4c00qfFRMPRkS3x3gOQvQXi0uIbQ8lhrV4++1TR8rrRaVydOZlviVbGZiO04UribDnZSWgExq
N62MvRo+zvP/hVJnn8vbAzdiWYk3rau4otznKmjKaHg8jz5JDVXOtJov28hF32t6vayOLt/TawNH
TKhkoZ3qvs9YymjN0PQ2VtRLlZ2qksUwfi4vpqEoSWaIgbr2tbH+S1sXe5vx5AH8fVlwKJsxFC36
ICEeRqqF+DtYMtBogeMqp49oxm3IqoZSIrC8zi4Jg9ex4VkrALO9AgMBAAGjggEaMIIBFjAOBgNV
HQ8BAf8EBAMCAQYwWAYDVR0gBFEwTzBNBggqgXoBYAEHAjBBMD8GCCsGAQUFBwIBFjNodHRwOi8v
cGMuY2hhbWJlcnNpZ24uZnIvcmdzL2xjci1kaXJlY3Rlcy8yZXRvaWxlcy8wEgYDVR0TAQH/BAgw
BgEB/wIBADBWBgNVHR8ETzBNMEugSaBHhkVodHRwOi8vY3JsLmNoYW1iZXJzaWduLmZyL2NybC9y
Z3MvbGNyLWRpcmVjdGVzL2NoYW1iZXJzaWduLWZyYW5jZS5jcmwwHQYDVR0OBBYEFJNjdtubIchZ
+DA8zPJVudWhNJTUMB8GA1UdIwQYMBaAFPTOYuSVwpaonDgnrSoeRkUGNMmhMA0GCSqGSIb3DQEB
CwUAA4ICAQC/9ryHjh3MMaTGz4dMDYPUUr102P9GJbomoW8POBB1A+SqaEeyVRKCOewEQlmpvti7
PtW4awI1r1G9DXqRQHPcscelwZwCtcuER3UI4F4ZI3iPXggb0JeLr2JQllfsViSm4pAzgjZ0rJfY
Mbs2wiNTNQpb313vAWQlvlT8NNNYc3KS+0TqcTH8l+X1T5enNdQrPHJGMW8qmGVRrqSDCg/1b0En
0Iw8ijSkSoIkBnQ43qWedQKcX/8qp6OdZOGv2RoGQfh6dscy+PyfTPdHR8t5EgKRcraaRPtuE6fb
jNFE/7dMOIZUfBw1UcrR8WzC53EkonjX06RUtvs1W2Ep/13Ls2Y6CUfyBh1aODlCSZszkiSi3OPL
gRg5ttKL8aLitt+DW/rHOS2QKnAHNZ9aF4ZZDcQX3U7mUfp3RS9396PREInibgPK3ci+uHAnmaYE
pJPS17VvL1qQgImOUATYzP3oBmqC8sdBoMEz9aOB8iY8WspAqoorvpAjHS9E5F17c2b9gKMhAoQc
aE2GiYBT08iIIBSZTwCzhCaLuHKU0q0NPLuFTyUhuDkPQVAePRIJMWaT3muxu8UGLS+SgQJJ7Zfh
JlRaqAFpx3zQpdKnXtYHgn6joLY0Ay4HvtBBS1lX919bJbYB8PB7nSgJMaAWTCZA3T5vMZ+3XM6A QluomB1d5Q==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *ChamberSign France*

Issuer OU: *0002 433702479*

Issuer O: *ChamberSign France*

Issuer C: *FR*

Subject CN: *ChamberSign France - AC 2 étoiles*

Subject OU: *0002 433702479*

Subject O: *ChamberSign France*

Subject C: *FR*

Valid from: *Tue Oct 16 02:00:00 CEST 2012*

Valid to: *Sun Oct 16 02:00:00 CEST 2022*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:A3:56:13:52:0C:15:12:A8:93:7D:A1:56:BE:E6:84:F6:67:A0:F5:D1:49:EF:7F:8E:4D:29:3E:4C:DF:EA:00:54:34:DF:42:26:98:A0:D0:B6:46:A7:96:39:EE:B5:9D:40:D1:D3:D0:19:DA:4C:DC:65:D4:11:28:3F:73:12:A2:4C:C1:CA:FF:81:59:0B:83:B8:8F:47:E4:85:2C:33:51:C4:3E:6F:C9:C4:B0:7F:09:CA:BC:E0:7D:8E:78:9B:3D:B3:D2:C4:BC:37:0B:A8:64:B1:4B:12:2C:BD:38:AA:EE:82:76:F2:83:B7:61:EC:BD:D7:8B:31:8D:DE:8F:01:BF:53:04:56:E1:1B:84:A9:02:7C:C5:57:E0:4E:9D:F8:DE:F2:A6:D9:95:F8:9D:89:F0:E5:3A:23:23:CC:6C:77:46:95:0D:B8:E0:B1:32:D7:8E:7A:6C:36:52:19:65:0F:B7:14:B8:C0:06:85:77:F3:F4:57:53:6B:D5:4F:D4:9B:71:0A:F9:99:5C:BF:0F:3E:76:C4:27:99:5C:AA:49:31:2F:96:5B:91:92:9D:58:23:7F:12:7E:2D:AB:63:E5:2E:AF:33:DC:9E:E5:75:92:E8:BD:9F:94:15:B1:37:79:A9:99:9C:23:6E:E2:5E:91:74:3F:1B:BC:48:EB:31:FC:2B:C6:93:C9:30:0E:75:3A:05:62:20:77:D9:3A:00:3C:3C:B3:87:69:49:CD:49:E2:1A:3D:95:77:7C:8F:03:F3:E2:56:A4:E1:55:5B:90:E6:75:4C:7C:AB:17:A3:50:6E:AE:31:8C:F8:73:4D:2A:7C:54:4C:3D:19:12:DF:1D:E0:39:0B:D0:5E:2D:2E:21:B4:3C:96:1A:D5:E3:EF:B5:4D:1F:2B:AD:16:95:C9:D3:99:96:F8:95:6C:66:62:3B:4E:14:AE:26:C3:9D:94:96:80:4C:6A:37:AD:8C:BD:1A:3E:CE:F3:FF:85:52:67:9F:CB:DB:03:37:62:59:89:37:AD:AB:B8:A2:DC:E7:2A:68:CA:68:78:3C:8F:3E:49:0D:55:CE:B4:9A:2F:DB:C8:45:DF:6B:7A:BD:AC:8E:2E:DF:D3:6B:03:47:4C:A8:64:A1:9D:EA:BE:CF:58:CA:68:CD:D0:F4:36:56:D4:4B:95:9D:AA:92:C5:30:7E:2E:2F:A6:A1:28:49:66:88:81:BA:F6:B5:B1:FE:4B:5B:17:7B:9B:F1:E4:01:FC:7D:59:70:28:9B:31:14:2D:FA:20:21:1E:46:AA:85:F8:3B:58:32:D0:68:81:E3:2A:A7:8F:68:C6:6D:C8:AA:86:52:22:B0:BC:CE:2E:09:83:D7:B1:E1:59:2B:00:B3:BD:02:03:01:00:01

Certificate Policies *Policy OID: 1.2.250.1.96.1.7.2*

CPS pointer: http://pc.chambersign.fr/rgs/lcr-directes/2etoiles/

Basic Constraints *IsCA: true - Path length: 0*

CRL Distribution Points *http://crl.chambersign.fr/crl/rgs/lcr-directes/chambersign-france.crl*

Subject Key Identifier *93:63:76:DB:9B:21:C8:59:F8:30:3C:CC:F2:55:B9:D5:A1:34:94:D4*

Authority Key Identifier *F4:CE:62:E4:95:C2:96:A8:9C:38:27:AD:2A:1E:46:45:06:34:C9:A1*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *B8:2D:97:EE:0F:61:44:AA:70:56:5F:5B:A2:36:78:76:DF:CC:26:8C:0D:48:11:23:AE:E4:50:C6:87: A0:EF:FA*

X509SubjectName

Subject CN: *ChamberSign France - AC 2 étoiles*

Subject OU: *0002 433702479*

Subject O: *ChamberSign France*

Subject C: *FR*

X509SKI

X509 SK I *k2N225shyFn4MDzM8lW51aE0lNQ=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2017-10-31T23:00:00Z*

TSP Service Definition URI

URI *[en]* *http://pc.chambersign.fr/rgs/v2/2etoiles/eidas/*

URI *[fr]* *http://pc.chambersign.fr/rgs/v2/2etoiles/eidas/*

6.4.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

6.4.2 - Extension (critical): Qualifiers [QCWithQSCD, QCForESig]

Qualifier type description *[en]* *undefined.*

[fr] *undefined.*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithQSCD*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForESig*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Policy Identifier nodes:

Identifier *1.2.250.1.96.1.7.2.4.1*

7 - TSP: Cryptolog International

TSP Name

Name *[en]* *Cryptolog International*

Name *[fr]* *Cryptolog International*

TSP Trade Name

Name *[en]* *VATFR-46439129164*

Name *[fr]* *VATFR-46439129164*

PostalAddress

Street Address *[fr]* *5-7 Rue du Faubourg Poissonnière*

Locality *[fr]* *Paris*

Postal Code *[fr]* *75009*

Country Name *[fr]* *FR*

PostalAddress

Street Address *[en]* *5-7 Rue du Faubourg Poissonnière*

Locality *[en]* *PARIS*

Postal Code *[en]* *75009*

Country Name *[en]* *FR*

ElectronicAddress

URI *http://www.cryptolog.com/fr/*

URI *http://www.cryptolog.com/en/*

URI *mailto:contact@universign.eu*

URI *mailto:contact@universign.eu*

TSP Information URI

URI *[en]* *https://www.universign.eu/en/repository/*

URI *[fr]* *https://www.universign.eu/fr/repository/*

7.1 - Service (recognisedatnationallevel): Certification Authority for Universign Time Stamping

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/PKC*

Service type description *[en]* *A certificate generation service creating and signing non-qualified public key certificates based on the identity and other attributes verified by the relevant registration services.*

	[fr]	*Un service de génération de certificat et la signature de la création de certificats de clés publiques non-qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name	*[en]*	*Certification Authority for Universign Time Stamping*
Name	*[fr]*	*Autorité de certification pour l'horodatage Universign*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *311583423277221956465219911797114909 84*

X509 Certificate -----BEGIN CERTIFICATE-----

MIID9TCCAt2gAwIBAgIQF3Dg4iQuLQxzMPFRPs8rqDANBgkqhkiG9w0BAQsFADByMSMwIQYDVQQD
ExpVbml2ZXJzaWduIFRpbWVzdGFtcGluZyBDQTEcMBoGA1UECxMTMDAwMiA0MzkxMjkxNjQwMDAy
NjEgMB4GA1UEChMXQ3J5cHRvbG9nIEludGVybmF0aW9uYWwxCzAJBgNVBAYTAkZSMB4XDTEwMDUw
NjA5MzA1OVoXDTIwMDUwNjA5MzA1OVowcjEjMCEGA1UEAxMaVW5pdmVyc2lnbiBUaW1lc3RhbXBp
bmcgQ0ExHDAaBgNVBAsTEzAwMDIgNDM5MTI5MTY0MDAwMjYxIDAeBgNVBAoTF0NyeXB0b2xvZyBJ
bnRlcm5hdGlvbmFsMQswCQYDVQQGEwJGUjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AMF2r8Q+dqh3iA6fPMn0bOw50sKTsCPCocGVNPf75b6dERmkuiXj48/M6poFaPxV96Y01B8LjTUF
YGQr6Vbf/15HvVskV6ZSTb8PXNZef6vv7681qnMp7NZVyrWO9zjg4NcZ9qVKFlzZe2NCGHAZi+5z
7Y4Phnvg7XdLu0B92oERAIoconTcsHO6BSg9nhv0c+xDsUNdRKF1groYZtAwNO1L1j5kLY3PukPP
Ka0+uyrJ8j56mGGUGWKaZxLuKafn5M3tYMousgKxQ/5cDHnjntTFBXfm7+Jg0PeiJP6boM2nZDTc
nPBt+wvXzo27L4GV0GvZfoi0CVa27hkURRSnsJcCAwEAAaOBhjCBgzAPBgNVHRMBAf8EBTADAQH/
MA4GA1UdDwEB/wQEAwIBBjBBBgNVHSAEOjA4MDYGCisGAQQB+0sFAQEwKDAmBggrBgEFBQcCARYa
aHR0cDovL2RvY3MudW5pdmVyc2lnbi5ldS8wHQYDVR0OBBYEFOzknxQd8GYKOfVELMDFf8PMwaW1
MA0GCSqGSIb3DQEBCwUAA4IBAQAySgYJxVNszlupDmOTfKcSXRohKwxfgv/wVJhH7ypgqX9z+KM8
sh0FDrO2TbEyU/rnpJwauTUwPoa40plvLcBV3zcsA72mzG9fgjmftj0D5Lxhkqsn7B13YOP/tlqo
e4f1jyfysxc/JpoBKXklJIBMW5DAbPxZPehVRpBJqrd0ZJNhKZFbBZvVIZ7KO5PX10k1016yiB8L
IuASeJfGMHlzvX0qorvl+98g868vQQB6xyMC8WcikEVsVrTBXnNsdD2F6EkC+HJ88qT5XfUGMxq8
8hvufpwfD3kTkqDm5RDhn0a0o8eIRlze2XopYWz17GWyUVyawoZcEfFYlDxjbo1p

-----END CERTIFICATE-----

Signature algorithm:	*SHA256withRSA*
Issuer C:	*FR*
Issuer O:	*Cryptolog International*
Issuer OU:	*0002 43912916400026*
Issuer CN:	*Universign Timestamping CA*
Subject C:	*FR*
Subject O:	*Cryptolog International*
Subject OU:	*0002 43912916400026*

Subject CN: *Universign Timestamping CA*

Valid from: *Thu May 06 11:30:59 CEST 2010*

Valid to: *Wed May 06 11:30:59 CEST 2020*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C1:76:AF:C4:3E:76:A8:77:88:0E:9F:3C:C9:F4:6C:EC:39:D2:C2:93:B0:23:C2:A1:C1:95:34:F7:FB:E5:BE:9D:11:19:A4:BA:25:E3:E3:CF:CC:EA:9A:05:68:FC:55:F7:A6:34:D4:1F:0B:8D:35:05:60:64:2B:E9:56:DF:FF:5E:47:BD:5B:24:57:A6:52:4D:BF:0F:5C:D6:5E:7F:AB:EF:EF:AF:35:AA:73:29:EC:D6:55:CA:B5:8E:F7:38:E0:E0:D7:19:F6:A5:4A:16:5C:D9:7B:63:42:18:70:19:8B:EE:73:ED:8E:0F:86:7B:E0:ED:77:4B:BB:40:7D:DA:81:11:00:8A:1C:A2:74:DC:B0:73:BA:05:28:3D:9E:1B:F4:73:EC:43:B1:43:5D:44:A1:75:82:BA:18:66:D0:30:34:ED:4B:D6:3E:64:2D:8D:CF:BA:43:CF:29:AD:3E:BB:2A:C9:F2:3E:7A:98:61:94:19:62:9A:67:12:EE:29:A7:E7:E4:CD:ED:60:CA:2E:B2:02:B1:43:FE:5C:0C:79:E3:9E:D4:C5:05:77:E6:EF:E2:60:D0:F7:A2:24:FE:9B:A0:CD:A7:64:34:DC:9C:F0:6D:FB:0B:D7:CE:8D:BB:2F:81:95:D0:6B:D9:7E:88:B4:09:56:B6:EE:19:14:45:14:A7:B0:97:02:03:01:00:01

Basic Constraints *IsCA: true*

Certificate Policies *Policy OID: 1.3.6.1.4.1.15819.5.1.1*
CPS pointer:
http://docs.universign.eu/

Subject Key Identifier *EC:E4:9F:14:1D:F0:66:0A:39:F5:44:2C:C0:C5:7F:C3:CC:C1:A5:B5*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *4F:60:07:66:6E:1C:29:A2:01:B1:45:DE:7F:9B:BE:16:0E:10:B3:C6:07:43:77:3A:2E:83:8E:AC:0F:C4:D7:9A*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/recognisedatnationallevel*

Service status description
[en] *undefined.*
[fr] *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

Scheme Service Definition URI

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Server-Stamp-1-Star*

URI *[en]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Server-Stamp-1-Star*

TSP Service Definition URI

URI *[en]* *https://www.universign.eu/en/documents/universign-pc_en.pdf*

URI *[fr]* *https://www.universign.eu/fr/documents/universign-pc_fr.pdf*

7.1.1 - History instance n.1 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/PKC*

Service Name

Name *[en]* *Certification Authority for Universign Time Stamping*

Name *[fr]* *Autorité de certification pour l'horodatage Universign*

Service digital identities

X509SubjectName

Subject C: *FR*

Subject O: *Cryptolog International*

Subject OU: *0002 43912916400026*

Subject CN: *Universign Timestamping CA*

X509SKI

X509 SK I *7OSfFB3wZgo59UQswMV/w8zBpbU=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2010-05-05T22:00:00Z*

7.2 - Service (granted): Universign CA hardware

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Universign CA hardware*

Name *[fr]* *AC Matérielle Universign*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *443087468865672937800377456207625919 59*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIEYTCCA0mgAwIBAgIQIVWN4tmvyrr2CljMBjGC1zANBgkqhkiG9w0BAQsFADB2MQswCQYDVQQG
EwJGUjEgMB4GA1UEChMXQ3J5cHRvbG9nIEludGVybmF0aW9uYWwxHDAaBgNVBAsTEzAwMDIgNDM5
MTI5MTY0MDAwMjYxJzAlBgNVBAMTHlVuaXZlcnNpZ24gUHJpbWFyeSBDQSBoYXJkd2FyZTAeFw0x
MjA2MTUxMjU2MjVaFw0yMjA2MTUxMjU2MjVaMG4xCzAJBgNVBAYTAkZSMSAwHgYDVQQKExdDcnlw
dG9sb2cgSW50ZXJuYXRpb25hbDEcMBoGA1UECxMTMDAwMiA0MzkxMjkxNjQwMDAyNjEfMB0GA1UE
AxMWVW5pdmVyc2lnbiBDQSBoYXJkd2FyZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AKHfv76grtwK9PRFTBq4BDtmmLaaHDAqkj1wd0lHIN2QH1jM6hKWeS4U/wy8QuYtvw0aFxYxiMWz
S/vrj0Sczv5hAt8reE1Eg1uQcx6+aSUBqJ6a+1TbM7PtkHg1ozgbmVXGuiOLyviLhhUo8XmeeGEh
ux+cyRNiYCs37VPN5OVrKks29dspMkvllkexfrxiPfc+gB58EU+iNEcip/YrZLu4ZqErlCePIVBL
yX9skb7QwKXDW8XBIgAzpoBj0U9/4Vxaiyj209xT1Uuz2vKsuT8Hq7I1vt7miYviHg/ovsWXH6yG
cNomxX55l0qWQ4z+mGlVhCLDPMKmspY5D+1kSqsCAwEAAaOB8jCB7zA7BgNVHSAENDAyMDAGBFUd
IAAwKDAmBggrBgEFBQcCARYaaHR0cDovL2RvY3MudW5pdmVyc2lnbi5ldS8wEgYDVR0TAQH/BAgw
BgEB/wIBADBMBgNVHR8ERTBDMEGgP6A9hjtodHRwOi8vY3JsLnVuaXZlcnNpZ24uZXUvdW5pdmVy
c2lnbl9wcmltYXJ5X2NhX2hhcmR3YXJlLmNybDAOBgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFGDk
MN3uetTQfl0l2f07eyFkT927MB8GA1UdIwQYMBaAFE3Z/Kgtx8hapK1fSa5opNyeihIiMA0GCSqG
SIb3DQEBCwUAA4IBAQAQrQJxwn+DBwN+KTt75IuOkaPOnZ+FfmF/1V7zDt3YNz7n1hRXlflbx9wB
Jn30TwyuTuZ/Cq1gEiA+TJMrsdZPKvagY8a/q7oCm6jYw6cBhopErwV/sZ9R3Ic+fphKSxoEnygp
Zs4uKMU2bB7nbul+sdJkP/OrIHKfHydMk3ayeAxnnieOj8EU+Z5w3fpekOGOtb4VUTESWU/xQfDZ
cNaauNRU2DYFi1eDypfVnyD8tORDoFVaAqzdIJuMJ06jJB5fnmNBXU7GOQFLcdK7hy3ZDmPNh5FN
GnaQRrlY2st7lXfV3mu9AgHmjPjxrbAwgo1GzLRY0byI9bfitN0sLT+d

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Universign Primary CA hardware*

Issuer OU: *0002 43912916400026*

Issuer O: *Cryptolog International*

Issuer C: *FR*

Subject CN: *Universign CA hardware*

Subject OU: *0002 43912916400026*

Subject O: *Cryptolog International*

Subject C: *FR*

Valid from: *Fri Jun 15 14:56:25 CEST 2012*

Valid to: *Wed Jun 15 14:56:25 CEST 2022*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:A1:DF:BF:BE:A0:AE:DC:0A:F4:F4:45:4C:1A:B8:04:3B:66:98:B6:9A:1C:30:2A:92:3D:70:77:49:47:20:DD:90:1F:58:CC:EA:12:96:79:2E:14:FF:0C:BC:42:E6:2D:BF:0D:1A:17:16:31:88:C5:B3:4B:FB:EB:8F:44:9C:CE:FE:61:02:DF:2B:78:4D:44:83:5B:90:73:1E:BE:69:25:01:A8:9E:9A:FB:54:DB:33:B3:ED:90:78:35:A3:38:1B:99:55:C6:BA:23:8B:CA:F8:8B:86:15:28:F1:79:9E:78:61:21:BB:1F:9C:C9:13:62:60:2B:37:ED:53:CD:E4:E5:6B:2A:4B:36:F5:DB:29:32:4B:E5:96:47:B1:7E:BC:62:3D:F7:3E:80:1E:7C:11:4F:A2:34:47:22:A7:F6:2B:64:BB:B8:66:A1:2B:94:27:8F:21:50:4B:C9:7F:6C:91:BE:D0:C0:A5:C3:5B:C5:C1:22:00:33:A6:80:63:D1:4F:7F:E1:5C:5A:8B:28:F6:D3:DC:53:D5:4B:B3:DA:F2:AC:B9:3F:07:AB:B2:35:BE:DE:E6:89:8B:E2:1E:0F:E8:BE:C5:97:1F:AC:86:70:DA:26:C5:7E:79:97:4A:96:43:8C:FE:98:69:55:84:22:C3:3C:C2:A6:B2:96:39:0F:ED:64:4A:AB:02:03:01:00:01

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: http://docs.universign.eu/

Basic Constraints

IsCA: true - Path length: 0

CRL Distribution Points

http://crl.universign.eu/universign_primary_ca_hardware.crl

Subject Key Identifier

60:E4:30:DD:EE:7A:D4:D0:7E:5D:25:D9:FD:3B:7B:21:64:4F:DD:BB

Authority Key Identifier

4D:D9:FC:A8:2D:C7:C8:5A:A4:AD:5F:49:AE:68:A4:DC:9E:8A:12:22

Key Usage:

keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

2C:72:B1:2D:77:DF:A1:0E:DD:D4:78:D9:67:EB:80:FB:31:4D:EA:1F:7D:96:2D:DC:81:65:24:1E:96:31:77:AC

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description

[en] *undefined.*

[fr] *undefined.*

Status Starting Time

2016-06-30T22:00:00Z

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS102042/NCP+*

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS101456/QCPPublic*

TSP Service Definition URI

URI *[en]* *https://www.universign.eu/en/documents/universign-sub_ca_pc_dpc_en.pdf*

URI *[fr]* *https://www.universign.eu/en/documents/universign-sub_ca_cp_cps_fr.pdf*

7.2.1 - Extension (not critical): Qualifiers [QCNoQSCD, NotQualified]

Qualifier type description

[en] *undefined.*

[fr] *undefined.*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCNoQSCD*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/NotQualified*

Criteria list assert=atLeastOne

Policy Identifier nodes:

Identifier *1.3.6.1.4.1.15819.5.1.3.2*

7.2.2 - Extension (not critical): Qualifiers [QCNoQSCD]

Qualifier type description *[en]* *undefined.*

[fr] *undefined.*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCNoQSCD*

Criteria list assert=atLeastOne

Policy Identifier nodes:

Identifier *1.3.6.1.4.1.15819.5.1.3.1*

7.2.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

7.2.4 - History instance n.1 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Universign CA hardware*

Name *[fr]* *AC Matérielle Universign*

Service digital identities

X509SubjectName

Subject CN: *Universign CA hardware*

Subject OU: *0002 43912916400026*

Subject O: *Cryptolog International*

Subject C: *FR*

X509SKI

X509 SK I *YOQw3e561NB+XSXZ/Tt7IWRP3bs=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2012-06-14T22:00:00Z*

7.2.4.1 - Extension (not critical): Qualifiers [QCNoSSCD, QCForLegalPerson]

Qualifier type description

[en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the presence or absence of Secure Signature Creation Device (SSCD) support ARE NOT supported by an SSCD (i.e. that that the private key associated with the public key in the certificate is not stored in a Secure Signature Creation Device conformant with the applicable European legislation).*

[fr] *elle est assurée par le prestataire de service de confiance et contrôlée (modèle de contrôle) ou vérifiés (modèle d'accréditation) par l'État membre de référence (respectivement son Organe de surveillance ou organisme d'accréditation) que tous les certificats qualifiés délivrés dans le cadre du service identifié dans «Service digital identity» et en outre identifié par les informations des filtres utilisés pour identifier plus précisément dans le cadre du "Sdi" de service de confiance identifiés, l'ensemble précis de certificats qualifiés pour lesquels cette information supplémentaire est nécessaire en ce qui concerne la présence ou l'absence de dispositif sécurisé de création de signature (SSCD) de soutien ne sont pas pris en charge par un SSCD (c'est à dire que la clé privée associée à la clé publique dans le certificat ne sont pas stockées dans un dispositif sécurisé conforme à la législation européenne applicable de création de signature).*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCNoSSCD*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForLegalPerson*

Criteria list assert=atLeastOne

Policy Identifier nodes:

Identifier *1.3.6.1.4.1.15819.5.1.3.2*

7.2.4.2 - Extension (not critical): Qualifiers [QCNoSSCD]

Qualifier type description

[en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the presence or absence of Secure Signature Creation Device (SSCD) support ARE NOT supported by an SSCD (i.e. that that the private key associated with the public key in the certificate is not stored in a Secure Signature Creation Device conformant with the applicable European legislation).*

[fr] *elle est assurée par le prestataire de service de confiance et contrôlée (modèle de contrôle) ou vérifiés (modèle d'accréditation) par l'État membre de référence (respectivement son Organe de surveillance ou organisme d'accréditation) que tous les certificats qualifiés délivrés dans le cadre du service identifié dans «Service digital identity» et en outre identifié par les informations des filtres utilisés pour identifier plus précisément dans le cadre du "Sdi" de service de confiance identifiés, l'ensemble précis de certificats qualifiés pour lesquels cette information supplémentaire est nécessaire en ce qui concerne la présence ou l'absence de dispositif sécurisé de création de signature (SSCD) de soutien ne sont pas pris en charge par un SSCD (c'est à dire que la clé privée associée à la clé publique dans le certificat ne sont pas stockées dans un dispositif sécurisé conforme à la législation européenne applicable de création de signature).*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCNoSSCD*

Criteria list assert=atLeastOne

Policy Identifier nodes:

Identifier *1.3.6.1.4.1.15819.5.1.3.1*

7.3 - Service (recognisedatnationallevel): Universign CA hardware

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/PKC*

Service type description *[en]* *A certificate generation service creating and signing non-qualified public key certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats de clés publiques non-qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Universign CA hardware*

Name *[fr]* *AC Matérielle Universign*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *443087468865672937800377456207625919 59*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIEYTCCA0mgAwIBAgIQIVWN4tmvyrr2CIjMBjGC1zANBgkqhkiG9w0BAQsFADB2MQswCQYDVQQG
EwJGUjEgMB4GA1UEChMXQ3J5cHRvbG9nIEludGVybmF0aW9uYWwxHDAaBgNVBAsTEzAwMDIgNDM5
MTI5MTY0MDAwMjYxJzAlBgNVBAMTHlVuaXZlcnNpZ24gUHJpbWFyeSBDQSBoYXJkd2FyZTAeFw0x
MjA2MTUxMjU2MjVaFw0yMjA2MTUxMjU2MjVaMG4xCzAJBgNVBAYTAkZSMSAwHgYDVQQKExdDcnlw
dG9sb2cgSW50ZXJuYXRpb25hbDEcMBoGA1UECxMTMDAwMiA0MzkxMjkxNjQwMDAyNjEfMB0GA1UE
AxMWVW5pdmVyc2lnbiBDQSBoYXJkd2FyZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AKHfv76grtwK9PRFTBq4BDtmmLaaHDAqkj1wd0lHIN2QH1jM6hKWeS4U/wy8QuYtvw0aFxYxiMWz
S/vrj0Sczv5hAt8reE1Eg1uQcx6+aSUBqJ6a+1TbM7PtkHg1ozgbmVXGuiOLyviLhhUo8XmeeGEh
ux+cyRNiYCs37VPN5OVrKks29dspMkvllkexfrxiPfc+gB58EU+iNEcip/YrZLu4ZqErlCePIVBL
yX9skb7QwKXDW8XBIgAzpoBj0U9/4Vxaiyj209xT1Uuz2vKsuT8Hq7I1vt7miYviHg/ovsWXH6yG
cNomxX55l0qWQ4z+mGlVhCLDPMKmspY5D+1kSqsCAwEAAaOB8jCB7zA7BgNVHSAENDAyMDAGBFUd
IAAwKDAmBggrBgEFBQcCARYaaHR0cDovL2RvY3MudW5pdmVyc2lnbi5ldS8wEgYDVR0TAQH/BAgw
BgEB/wIBADBMBgNVHR8ERTBDMEGgP6A9hjtodHRwOi8vY3JsLnVuaXZlcnNpZ24uZXUvdW5pdmVy
c2lnbl9wcmltYXJ5X2NhX2hhcmR3YXJlLmNybDAOBgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFGDk
MN3uetTQfl0l2f07eyFkT927MB8GA1UdIwQYMBaAFE3Z/Kgtx8hapK1fSa5opNyeihIiMA0GCSqG
SIb3DQEBCwUAA4IBAQAQrQJxwn+DBwN+KTt75IuOkaPOnZ+FfmF/1V7zDt3YNz7n1hRXlflbx9wB
Jn30TwyuTuZ/Cq1gEiA+TJMrsdZPKvagY8a/q7oCm6jYw6cBhopErwV/sZ9R3Ic+fphKSxoEnygp
Zs4uKMU2bB7nbul+sdJkP/OrIHKfHydMk3ayeAxnnieOj8EU+Z5w3fpekOGOtb4VUTESWU/xQfDZ
cNaauNRU2DYFi1eDypfVnyD8tORDoFVaAqzdIJuMJ06jJB5fnmNBXU7GOQFLcdK7hy3ZDmPNh5FN
GnaQRrlY2st7lXfV3mu9AgHmjPjxrbAwgo1GzLRY0byI9bfitN0sLT+d

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Universign Primary CA hardware*

Issuer OU: *0002 43912916400026*

Issuer O: *Cryptolog International*

Issuer C: *FR*

Subject CN: *Universign CA hardware*

Subject OU: *0002 43912916400026*

Subject O: *Cryptolog International*

Subject C: *FR*

Valid from: *Fri Jun 15 14:56:25 CEST 2012*

Valid to: *Wed Jun 15 14:56:25 CEST 2022*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:A1:DF:BF:BE:A0:AE:DC:0A:F4:F4:45:4C:1A:B8:04:3B:66:98:B6:9A:1C:30:2A:92:3D:70:77:49:47:20:DD:90:1F:58:CC:EA:12:96:79:2E:14:FF:0C:BC:42:E6:2D:BF:0D:1A:17:16:31:88:C5:B3:4B:FB:EB:8F:44:9C:CE:FE:61:02:DF:2B:78:4D:44:83:5B:90:73:1E:BE:69:25:01:A8:9E:9A:FB:54:DB:33:B3:ED:90:78:35:A3:38:1B:99:55:C6:BA:23:8B:CA:F8:8B:86:15:28:F1:79:9E:78:61:21:BB:1F:9C:C9:13:62:60:2B:37:ED:53:CD:E4:E5:6B:2A:4B:36:F5:DB:29:32:4B:E5:96:47:B1:7E:BC:62:3D:F7:3E:80:1E:7C:11:4F:A2:34:47:22:A7:F6:2B:64:BB:B8:66:A1:2B:94:27:8F:21:50:4B:C9:7F:6C:91:BE:D0:C0:A5:C3:5B:C5:C1:22:00:33:A6:80:63:D1:4F:7F:E1:5C:5A:8B:28:F6:D3:DC:53:D5:4B:B3:DA:F2:AC:B9:3F:07:AB:B2:35:BE:DE:E6:89:8B:E2:1E:0F:E8:BE:C5:97:1F:AC:86:70:DA:26:C5:7E:79:97:4A:96:43:8C:FE:98:69:55:84:22:C3:3C:C2:A6:B2:96:39:0F:ED:64:4A:AB:02:03:01:00:01

Certificate Policies *Policy OID: 2.5.29.32.0*

CPS pointer: http://docs.universign.eu/

Basic Constraints *IsCA: true - Path length: 0*

CRL Distribution Points *http://crl.universign.eu/universign_primary_ca_hardware.crl*

Subject Key Identifier *60:E4:30:DD:EE:7A:D4:D0:7E:5D:25:D9:FD:3B:7B:21:64:4F:DD:BB*

Authority Key Identifier *4D:D9:FC:A8:2D:C7:C8:5A:A4:AD:5F:49:AE:68:A4:DC:9E:8A:12:22*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *2C:72:B1:2D:77:DF:A1:0E:DD:D4:78:D9:67:EB:80:FB:31:4D:EA:1F:7D:96:2D:DC:81:65:24:1E:96:31:77:AC*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/recognisedatnationallevel*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS102042/NCP*

TSP Service Definition URI

URI *[en]* *https://www.universign.eu/en/documents/universign-sub_ca_pc_dpc_en.pdf*

URI *[fr]* *https://www.universign.eu/en/documents/universign-sub_ca_cp_cps_fr.pdf*

7.3.1 - History instance n.1 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/PKC*

Service Name

Name *[en]* *Universign CA hardware*

Name *[fr]* *AC Matérielle Universign*

Service digital identities

X509SubjectName

Subject CN: *Universign CA hardware*

Subject OU: *0002 43912916400026*

Subject O: *Cryptolog International*

Subject C: *FR*

X509SKI

X509 SK I *YOQw3e561NB+XSXZ/Tt7IWRP3bs=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2012-06-14T22:00:00Z*

7.4 - Service (recognisedatnationallevel): Universign Software Primary CA

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/PKC*

Service type description *[en]* *A certificate generation service creating and signing non-qualified public key certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats de clés publiques non-qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Universign Software Primary CA*

Name *[fr]* *AC Logicielle Universign Primaire*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *889410933006147456136521296717061492*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIDuDCCAqCgAwIBAgIQAKtLWDg3Yomlb5h2MRiddDANBgkqhkiG9w0BAQsFADB2MQswCQYDVQQG
EwJGUjEgMB4GA1UEChMXQ3J5cHRvbG9nIEludGVybmF0aW9uYWwxHDAaBgNVBAsTEzAwMDIgNDM5
MTI5MTY0MDAwMjYxJzAlBgNVBAMTHlVuaXZlcnNpZ24gUHJpbWFyeSBDQSBzb2Z0d2FyZTAeFw0x
MjA2MjUxMDUyNDBaFw00MjA2MjUxMDUyNDBaMHYxCzAJBgNVBAYTAkZSMSAwHgYDVQQKExdDcnlw
dG9sb2cgSW50ZXJuYXRpb25hbDEcMBoGA1UECxMTMDAwMiA0MzkxMjkxNjQwMDAyNjEnMCUGA1UE
AxMeVW5pdmVyc2lnbiBQcmltYXJ5IENBIHNvZnR3YXJlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEAsJo3w5cP43mqsU9t627UeAC1TDYH3aMpxqynhX+KYhYY595T2lohT2Secgi7zW+Y
8hzVtM+u5TJqeOdeLYqkpDCsix7QcgCCPPwXhA794WOJPgqVVp/fYLdiShiklbdyB/D7vutFF5k4
YQpH6Bw5xJjnKRgYo0m5KT+0OuTmhuSWINPMfecmHI+rGSM7r7s+k+OuW4BwHODWAw9eKB7HmMVN
0wLiAFVTkVRmL9dcA63ocgoFBmdXjQxe/axDrzwAC5P+rqNBt0Sttzu0gcbvRbT68XxO96cuGXRS
20EbKcGl0tF4u1iGL1jU01meS7+VZUjEpomYeDp9HPh5QJeOyQIDAQABo0IwQDAPBgNVHRMBAf8E
BTADAQH/MA4GA1UdDwEB/wQEAwIBBjAdBgNVHQ4EFgQUoReMYhpBGShkdsHutHXfGm0BAjUwDQYJ
KoZIhvcNAQELBQADggEBAKrZ0GNHpgkmzrPysZsMGMvPrMj8y2v7d7pSDyphsqajiiMCr/j52N48
JK93cTeRkGk7piyhMsm5UZXYW14JkwW61a9dRpgllmtGDb9B/GUKM36x1XxzybWV9jRnLjXkklMm
J/aDdROBLtcNQQobJ8wZnf+6WY2P3fHOOP1HZ1DBAqgj/1XOlyXegQxqV3R3zdpNtZelkntohRI1
EwxEGj7XuTlw+vh89LcAZ0XuBepdvGFyZcYBn0zQyzgQPs/ki9d7LKFG8auM8GZTP4uKSQNtRlCS
JtxST+glaJt3JW06XmB02Ebfsat/ITLa0m8kQyY8PX4/qyvOABa5tbmDl7Y=

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Universign Primary CA software*

Issuer OU: *0002 43912916400026*

Issuer O: *Cryptolog International*

Issuer C: *FR*

Subject CN: *Universign Primary CA software*

Subject OU: *0002 43912916400026*

Subject O: *Cryptolog International*

Subject C: *FR*

Valid from: *Mon Jun 25 12:52:40 CEST 2012*

Valid to: *Wed Jun 25 12:52:40 CEST 2042*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:B0:9A:37:C3:97:0F:E3:79:AA:B1:4F:6D:EB:6E:D4:78:
00:B5:4C:36:07:DD:A3:29:C6:AC:A7:85:7F:8A:62:16:18:E7:DE:53:DA:5A:21:4F:64:9E:72:08:BB:CD:6F:98:F2:1C:D5:B4:CF:AE:E5:32:6A:78:E7:5E:2D:8A:A4:A4:3
0:AC:8B:1E:D0:72:00:82:3C:FC:17:84:0E:FD:E1:63:89:3E:0A:95:56:9F:DF:60:B7:62:4A:18:A4:95:B7:72:07:F0:FB:BE:EB:45:17:99:38:61:0A:47:E8:1C:39:C4:98:E
7:29:18:18:A3:49:B9:29:3F:B4:3A:E4:E6:86:E4:96:20:D3:CC:7D:E7:26:1C:8F:AB:19:23:3B:AF:BB:3E:93:E3:AE:5B:80:70:1C:E0:D6:03:0F:5E:28:1E:C7:98:C5:4D:
D3:02:E2:00:55:53:91:54:66:2F:D7:5C:03:AD:E8:72:0A:05:06:67:57:8D:0C:5E:FD:AC:43:AF:3C:00:0B:93:FE:AE:A3:41:B7:44:AD:B7:3B:B4:81:C6:EF:45:B4:FA:F1

:7C:4E:F7:A7:2E:19:74:52:DB:41:1B:29:C1:A5:D2:D1:78:BB:58:86:2F:58:D4:D3:59:9E:4B:BF:95:65:48:C4:A6:89:98:78:3A:7D:1C:F8:79:40:97:8E:C9:02:03:01:00:01

Basic Constraints *IsCA: true*

Subject Key Identifier *A1:17:8C:62:1A:41:19:28:64:76:C1:EE:B4:75:DF:1A:6D:01:02:35*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *6B:A3:80:62:1B:33:61:97:28:0B:A1:5C:02:E5:97:3A:6E:7B:48:D2:F8:1B:45:DC:90:8B:90:B5:6F:3C:F4:DF*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/recognisedatnationallevel*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS102042/NCP*

TSP Service Definition URI

URI *[en]* *https://www.universign.eu/en/documents/universign-root_ca_cp_cps_en.pdf*

URI *[fr]* *https://www.universign.eu/en/documents/universign-root_ca_cp_cps_fr.pdf*

7.4.1 - History instance n.1 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/PKC*

Service Name

Name *[en]* *Universign Software Primary CA*

Name *[fr]* *AC Logicielle Universign Primaire*

Service digital identities

X509SubjectName

Subject CN: *Universign Primary CA software*

Subject OU: *0002 43912916400026*

Subject O: *Cryptolog International*

Subject C: *FR*

X509SKI

X509 SK I *oReMYhpBGShkdsHutHXfGm0BAjU=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2012-06-14T22:00:00Z*

7.5 - Service (recognisedatnationallevel): Universign Hardware Primary CA

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/PKC*

Service type description

[en] *A certificate generation service creating and signing non-qualified public key certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats de clés publiques non-qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Universign Hardware Primary CA*

Name *[fr]* *AC Matérielle Universign Primaire*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *259438482142957653826574432754588014580*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIDuTCCAqGgAwIBAgIRAMMuCL31l3GyxK1mYwBZV/QwDQYJKoZIhvcNAQELBQAwdjELMAkGA1UE
BhMCRlIxIDAeBgNVBAoTF0NyeXB0b2xvZyBJbnRlcm5hdGlvbmFsMRwwGgYDVQQLExMwMDAyIDQz
OTEyOTE2NDAwMDI2MScwJQYDVQQDEx5Vbml2ZXJzaWduIFByaW1hcnkgQ0EgaGFyZHdhcmUwHhcN
MTIwNTI5MTY1ODA3WhcNNDIwNTI5MTY1ODA3WjB2MQswCQYDVQQGEwJGUjEgMB4GA1UEChMXQ3J5
cHRvbG9nIEludGVybmF0aW9uYWwxHDAaBgNVBAsTEzAwMDIgNDM5MTI5MTY0MDAwMjYxJzAlBgNV
BAMTHlVuaXZlcnNpZ24gUHJpbWFyeSBDQSBoYXJkd2FyZTCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBANmadE1N1cZBcDXE229NXXGngVJgy8DHoB3vVT2k16NHHI9AtynXWo+xtiaSEi3I
U6uoT85iPv+8IXb7pc7Kws7usrxoSkQkauqD10JGezozwU26+MIS96XZnWtxLieW7L7ibMnRyrH8
eCQXA1VZox/QX5tM+fCL2cPLWbzDlVoh9Kkg7OmIMPteTb6G5mTTBUzon7oAlEi3NRxpqsSMi2XM
qYnqpP6w2hX/Yyjw3c+rZbjpFyxCpPxC1EvtkTP2znfsszmLwgvwO1wF47fJuhts4FgIZmTfAOKr
VLzW7wC3JW58/gUQXskc1i51TueF87X/2G4Wq4rXnz5Dn0k+Vb0CAwEAAaNCMEAwDwYDVR0TAQH/
BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFE3Z/Kgtx8hapK1fSa5opNyeihIiMA0G
CSqGSIb3DQEBCwUAA4IBAQAww+NfjmXYX/dQ6l6woSclAhPBZIGsfQ3mRTAsKsrvaEZvjhr+kM+b
tAVzG6UbDIRrp4JmeZId/teMYKo72hrT68x6ZOkyFfIsv1oD0TGjEFYbX8JRfFd0xRm6vLJZfP6J
dRIOH5vHsbid1P7Q6DbWO2c7orwAM5PYQpnmf0dXvZ8DcxMajxtoSWGVw/gZRKQLm0x1Y3Hy6laH
lzr6HBrPX5oVL8AGGCythlO4SjO8c6nCa+gD6khN2PfC09NnoM6hma2xMtyiuv2yxpX9qCdQUJsP
oMYrphXqLU9uos/nNY4w+h0LSEBC3BOa6jH6sZZzoPuQXJR+CLgJaJ9te3gs

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Universign Primary CA hardware*

Issuer OU: *0002 43912916400026*

Issuer O: *Cryptolog International*

Issuer C: *FR*

Subject CN: *Universign Primary CA hardware*

Subject OU: *0002 43912916400026*

Subject O: *Cryptolog International*

Subject C: *FR*

Valid from: *Tue May 29 18:58:07 CEST 2012*

Valid to: *Thu May 29 18:58:07 CEST 2042*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:D9:9A:74:4D:4D:D5:C6:41:70:35:C4:DB:6F:4D:5D:71:A7:81:52:60:CB:C0:C7:A0:1D:EF:55:3D:A4:D7:A3:47:1C:8F:40:B7:29:D7:5A:8F:B1:B6:26:92:12:2D:C8:53:AB:A8:4F:CE:62:3E:FF:BC:21:76:FB:A5:CE:CA:C2:CE:EE:B2:BC:68:4A:44:0A:6A:EA:83:D7:42:46:7B:3A:33:C1:4D:BA:F8:C2:12:F7:A5:D9:9D:6B:71:2E:27:96:EC:BE:E2:6C:C9:D1:CA:B1:FC:78:24:17:03:55:59:A3:1F:D0:5F:9B:4C:F9:F0:8B:D9:C3:CB:59:BC:C3:95:5A:21:F4:A9:20:EC:E9:88:30:FB:5E:4D:BE:86:E6:64:D3:05:4C:E8:9F:BA:00:94:48:B7:35:1C:69:AA:C4:8C:8B:65:CC:A9:89:EA:A4:FE:B0:DA:15:FF:63:28:F0:DD:CF:AB:65:B8:E9:17:2C:42:A4:FC:42:D4:4B:ED:91:33:F6:CE:77:EC:B3:39:8B:C2:0B:F0:3B:5C:05:E3:B7:C9:BA:1B:6C:E0:58:08:66:64:DF:00:E2:AB:54:BC:D6:EF:00:B7:25:6E:7C:FE:05:10:5E:C9:1C:D6:2E:75:4E:E7:85:F3:B5:FF:D8:6E:16:AB:8A:D7:9F:3E:43:9F:49:3E:55:BD:02:03:01:00:01

Basic Constraints *IsCA: true*

Subject Key Identifier *4D:D9:FC:A8:2D:C7:C8:5A:A4:AD:5F:49:AE:68:A4:DC:9E:8A:12:22*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *0A:37:32:29:42:6E:85:A6:00:0B:07:E1:18:55:DA:86:68:BD:13:79:06:A2:BF:79:1F:4D:60:B8:FF:75:30:DD*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/recognisedatnationallevel*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS102042/NCP+*

TSP Service Definition URI

URI	*[en]*	*https://www.universign.eu/en/documents/universign-root_ca_cp_cps_en.pdf*
URI	*[fr]*	*https://www.universign.eu/en/documents/universign-root_ca_cp_cps_fr.pdf*

7.5.1 - History instance n.1 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/PKC*

Service Name

Name	*[en]*	*Universign Hardware Primary CA*
Name	*[fr]*	*AC Matérielle Universign Primaire*

Service digital identities

X509SubjectName

Subject CN:	*Universign Primary CA hardware*
Subject OU:	*0002 43912916400026*
Subject O:	*Cryptolog International*
Subject C:	*FR*

X509SKI

X509 SK I	*Tdn8qC3HyFqkrV9Jrmik3J6KEiI=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2012-06-14T22:00:00Z*

7.6 - Service (granted): Universign Time Stamping

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description	*[en]*	*A time-stamping generation service creating and signing qualified time-stamps tokens.*
	[fr]	*Un service de génération horodatage création et la signature temps timbres jetons qualifiés.*

Service Name

Name	*[en]*	*Universign Time Stamping*

Name *[fr]* *Horodatage Universign*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *311583423277221956465219911797114909 84*

X509 Certificate -----BEGIN CERTIFICATE-----

MIID9TCCAt2gAwIBAgIQF3Dg4iQuLQxzMPFRPs8rqDANBgkqhkiG9w0BAQsFADByMSMwIQYDVQQD
ExpVbml2ZXJzaWduIFRpbWVzdGFtcGluZyBDQTEcMBoGA1UECxMTMDAwMiA0MzkxMjkxNjQwMDAy
NjEgMB4GA1UEChMXQ3J5cHRvbG9nIEludGVybmF0aW9uYWwxCzAJBgNVBAYTAkZSMB4XDTEwMDUw
NjA5MzA1OVoXDTIwMDUwNjA5MzA1OVowcjEjMCEGA1UEAxMaVW5pdmVyc2lnbiBUaW1lc3RhbXBp
bmcgQ0ExHDAaBgNVBAsTEzAwMDIgNDM5MTI5MTY0MDAwMjYxIDAeBgNVBAoTF0NyeXB0b2xvZyBJ
bnRlcm5hdGlvbmFsMQswCQYDVQQGEwJGUjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AMF2r8Q+dqh3iA6fPMn0bOw50sKTsCPCocGVNPf75b6dERmkuiXj48/M6poFaPxV96Y01B8LjTUF
YGQr6Vbf/15HvVskV6ZSTb8PXNZef6vv7681qnMp7NZVyrWO9zjg4NcZ9qVKFlzZe2NCGHAZi+5z
7Y4Phnvg7XdLu0B92oERAIoconTcsHO6BSg9nhv0c+xDsUNdRKF1groYZtAwNO1L1j5kLY3PukPP
Ka0+uyrJ8j56mGGUGWKaZxLuKafn5M3tYMousgKxQ/5cDHnjntTFBXfm7+Jg0PeiJP6boM2nZDTc
nPBt+wvXzo27L4GV0GvZfoi0CVa27hkURRSnsJcCAwEAAaOBhjCBgzAPBgNVHRMBAf8EBTADAQH/
MA4GA1UdDwEB/wQEAwIBBjBBBgNVHSAEOjA4MDYGCisGAQQB+0sFAQEwKDAmBggrBgEFBQcCARYa
aHR0cDovL2RvY3MudW5pdmVyc2lnbi5ldS8wHQYDVR0OBBYEFOzknxQd8GYKOfVELMDFf8PMwaW1
MA0GCSqGSIb3DQEBCwUAA4IBAQAySgYJxVNszlupDmOTfKcSXRohKwxfgv/wVJhH7ypgqX9z+KM8
sh0FDrO2TbEyU/rnpJwauTUwPoa40plvLcBV3zcsA72mzG9fgjmftj0D5LxhkqsN7B13YOP/tlqo
e4f1jyfysxc/JpoBKXklJIBMW5DAbPxZPehVRpBJqrd0ZJNhKZFbBZvVIZ7KO5PX10k1016yiB8L
IuASeJfGMHlzvX0qorvl+98g868vQQB6xyMC8WcikEVsVrTBXnNsdD2F6EkC+HJ88qT5XfUGMxq8
8hvufpwfD3kTkqDm5RDhn0a0o8eIRlze2XopYWz17GWyUVyawoZcEfFYlDxjbo1p

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer C: *FR*

Issuer O: *Cryptolog International*

Issuer OU: *0002 43912916400026*

Issuer CN: *Universign Timestamping CA*

Subject C: *FR*

Subject O: *Cryptolog International*

Subject OU: *0002 43912916400026*

Subject CN: *Universign Timestamping CA*

Valid from: *Thu May 06 11:30:59 CEST 2010*

Valid to: *Wed May 06 11:30:59 CEST 2020*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C1:76:AF:C4:3E:76:A8:77:88:0E:9F:3C:C9:F4:6C:EC:39:D2:C2:93:B0:23:C2:A1:C1:95:34:F7:FB:E5:BE:9D:11:19:A4:BA:25:E3:E3:CF:CC:EA:9A:05:68:FC:55:F7:A6:34:D4:1F:0B:8D:35:05:60:64:2B:E9:56:DF:FF:5E:47:BD:5B:24:57:A6:52:4D:BF:0F:5C:D6:5E:7F:AB:EF:EF:AF:35:AA:73:29:EC:D6:55:CA:B5:8E:F7:38:E0:E0:D7:19:F6:A5:4A:16:5C:D9:7B:63:42:18:70:19:8B:EE:73:ED:8E:0F:86:7B:E0:ED:77:4B:BB:40:7D:DA:81:11:00:8A:1C:A2:74:DC:B0:73:BA:05:28:3D:9E:1B:F4:73:EC:43:B1:43:5D:44:A1:75:82:BA:18:66:D0:30:34:ED:4B:D6:3E:64:2D:8D:CF:BA:43:CF:29:AD:3E:BB:2A:C9:F2:3E:7A:98:61:94:19:62:9A:67:12:EE:29:A7:E7:E4:CD:ED:60:CA:2E:B2:02:B1:43:FE:5C:0C:79:E3:9E:D4:C5:05:77:E6:EF:E2:60:D0:F7:A2:24:FE:9B:A0:CD:A7:64:34:DC:9
C:F0:6D:FB:0B:D7:CE:8D:BB:2F:81:95:D0:6B:D9:7E:88:B4:09:56:B6:EE:19:14:45:14:A7:B0:97:02:03:01:00:01

Basic Constraints *IsCA: true*

Certificate Policies *Policy OID: 1.3.6.1.4.1.15819.5.1.1*
CPS pointer:
http://docs.universign.eu/

Subject Key Identifier *EC:E4:9F:14:1D:F0:66:0A:39:F5:44:2C:C0:C5:7F:C3:CC:C1:A5:B5*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *4F:60:07:66:6E:1C:29:A2:01:B1:45:DE:7F:9B:BE:16:0E:10:B3:C6:07:43:77:3A:2E:83:8E:AC:0F:C4:D7:9A*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*
[fr] *undefined.*

Status Starting Time *2016-12-01T01:00:00Z*

Scheme Service Definition URI

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Time-Stamping*

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS102023/LCP*

TSP Service Definition URI

URI *[en]* *https://www.universign.eu/en/documents/universign-pc_en.pdf*

URI *[fr]* *https://www.universign.eu/fr/documents/universign-pc_fr.pdf*

7.6.1 - History instance n.1 - Status: withdrawn

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service Name

Name *[en]* *Universign Time Stamping*

Name *[fr]* *Horodatage Universign*

Service digital identities

X509SubjectName

Subject C: *FR*

Subject O: *Cryptolog International*

Subject OU: *0002 43912916400026*

Subject CN: *Universign Timestamping CA*

X509SKI

X509 SK I *7OSfFB3wZgo59UQswMV/w8zBpbU=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Status Starting Time *2016-06-30T22:00:00Z*

7.6.2 - History instance n.2 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service Name

Name *[en]* *Universign Time Stamping*

Name *[fr]* *Horodatage Universign*

Service digital identities

X509SubjectName

Subject C: *FR*

Subject O: *Cryptolog International*

Subject OU: *0002 43912916400026*

Subject CN: *Universign Timestamping CA*

X509SKI

X509 SK I *7OSfFB3wZgo59UQswMV/w8zBpbU=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2010-05-05T22:00:00Z*

7.7 - Service (recognisedatnationallevel): Certification Authority for Universign Time Stamping 2015

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/PKC*

Service type description *[en]* *A certificate generation service creating and signing non-qualified public key certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats de clés publiques non-qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Certification Authority for Universign Time Stamping 2015*

Name *[fr]* *Autorité de certification pour l'horodatage Universign 2015*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *847987684037504690966020402803548919 40*

X509 Certificate -----BEGIN CERTIFICATE-----

MIID/zCCAuegAwIBAgIQP8umE0YUpE/yhLiMgaeopDANBgkqhkiG9w0BAQsFADB3MQswCQYDVQQG
EwJGUjEgMB4GA1UEChMXQ3J5cHRvbG9nIEludGVybmF0aW9uYWwxHDAaBgNVBAsTEzAwMDIgNDM5
MTI5MTY0MDAwMjYxKDAmBgNVBAMTH1VuaXZlcnNpZ24gVGltZXN0YW1waW5nIENBIDIwMTUwHhcN
MTUwMTI5MTQwMzE1WhcNMjUwMTI5MTQwMzE1WjB3MQswCQYDVQQGEwJGUjEgMB4GA1UEChMXQ3J5
cHRvbG9nIEludGVybmF0aW9uYWwxHDAaBgNVBAsTEzAwMDIgNDM5MTI5MTY0MDAwMjYxKDAmBgNV
BAMTH1VuaXZlcnNpZ24gVGltZXN0YW1waW5nIENBIDIwMTUwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQDYc1VJ69W70ojewtKbCLZ+P8bDAVJ1qujzgIZEvm15GYX7Jp+Hl9rwxBdswSZ8
S5A/x+0j6YMOHH0Z+iGl649+0GGX1gdAuovQKShsvLSzD/waINxkXXTVXpAW3V4dnCgcb3qaV/pO
9NTk/sdRJxM8lUtWuD7TEAfLzz7Ucl6gBjDTA0Gz+AtUkNWPcofCWuDfiSDOOpyKwSxovde6SRwH
dTXXIiC2Dphffjrr74MvLb0La5JAUwmJLIH42j/frgZeWk148wLMwBW+lvrIJtPz7eHNtTlNfQLr
mmJHW4l+yvTsdJJDs7QYtfzBTNg1zqV8eo/hHxFTFJ8/T9wTmENJAgMBAAGjgYYwgYMwDwYDVR0T
AQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYwQQYDVR0gBDowODA2BgorBgEEAftLBQEBMCgwJgYI
KwYBBQUHAgEWGmh0dHA6Ly9kb2NzLnVuaXZlcnNpZ24uZXUvMB0GA1UdDgQWBBT6Te1XO70/85Ez
mgs5pH9dEt0HRjANBgkqhkiG9w0BAQsFAAOCAQEAc7ud6793wgdjR8Xc1L47ufdVTamI5SHfOTht
ROfn8JL0HuNHKdRgv6COpdjtt6RwQEUUX/km7Q+Pn+A2gA/XoPfqD0iMfP63kMMyqgalEPRv+lXb
Fw3GSC9BQ9s2FL7ScvSuPm7VDZhpYN5xN6H72y4z7BgsDVNhkMu5AiWwbaWF+BHzZeiuvYHX0z/O
gY2oH0hluovuRAanQd4dOa73bbZhTJPFUzkgeIzOiuYS421IiAqsjkFwu3+k4dMDqYfDKUSITbMy
mkRDszR0WGNzIIy2NsTBcKYCHmbIV9S+165i8YjekraBjTTSbpfbty87A1S53CzA2EN1qn mQPwqF
fg==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Universign Timestamping CA 2015*

Issuer OU: *0002 43912916400026*

Issuer O: *Cryptolog International*

Issuer C: *FR*

Subject CN: *Universign Timestamping CA 2015*

Subject OU: *0002 43912916400026*

Subject O: *Cryptolog International*

Subject C: *FR*

Valid from: *Thu Jan 29 15:03:15 CET 2015*

Valid to: *Wed Jan 29 15:03:15 CET 2025*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:D8:73:55:49:EB:D5:BB:D2:88:DE:C2:D2:9B:08:B6:7E:3F:C6:C3:01:52:75:AA:E8:F3:80:86:44:BE:6D:79:19:85:FB:26:9F:87:97:DA:F0:C4:17:6C:C1:26:7C:4B:90:3F:C7:ED:23:E9:83:0E:1C:7D:19:FA:21:A5:EB:8F:7E:D0:61:97:D6:07:40:BA:8B:D0:29:28:6C:BC:B4:B3:0F:FC:1A:20:DC:64:5D:74:D5:5E:90:16:DD:5E:1D:9C:28:1C:6F:7A:9A:57:FA:4E:F4:D4:E4:FE:C7:51:27:13:3C:95:4B:56:B8:3E:D3:10:07:CB:CF:3E:D4:72:5E:A0:06:30:D3:03:41:B3:F8:0B:54:90:D5:8F:72:87:C2:5A:E0:DF:89:20:CE:3A:9C:8A:C1:2C:68:BD:D7:BA:49:1C:07:75:35:D7:22:20:B6:0E:98:5F:7E:3A:EB:EF:83:2F:2D:BD:0B:6B:92:40:53:09:89:2C:81:F8:DA:3F:DF:AE:06:5E:5A:4D:78:F3:02:CC:C0:15:BE:96:FA:C8:26:D3:F3:ED:E1:CD:B5:39:4D:7D:02:EB:9A:62:47:5B:89:7E:CA:F4:EC:74:92:43:B3:B4:18:B5:FC:C1:4C:D8:35:CE:A5:7C:7A:8F:E1:1F:11:53:14:9F:3F:4F:DC:13:98:43:49:02:03:01:00:01

Basic Constraints *IsCA: true*

Certificate Policies *Policy OID: 1.3.6.1.4.1.15819.5.1.1*
CPS pointer:
http://docs.universign.eu/

Subject Key Identifier *FA:4D:ED:57:3B:BD:3F:F3:91:33:9A:0B:39:A4:7F:5D:12:DD:07:46*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *9C:F3:C9:66:97:B7:20:58:9B:10:CC:13:B8:A2:BD:35:FF:BC:41:7B:70:50:A3:82:0A:F5:99:A4:39:DE:75:E5*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/recognisedatnationallevel*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Server-Stamp-1-Star*

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Server-Stamp-1-Star*

TSP Service Definition URI

URI	*[en]*	*https://www.universign.eu/en/documents/universign-pc_en.pdf*
URI	*[fr]*	*https://www.universign.eu/fr/documents/universign-pc_fr.pdf*

7.7.1 - History instance n.1 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/PKC*

Service Name

Name	*[en]*	*Certification Authority for Universign Time Stamping 2015*
Name	*[fr]*	*Autorité de certification pour l'horodatage Universign 2015*

Service digital identities

X509SubjectName

Subject CN:	*Universign Timestamping CA 2015*
Subject OU:	*0002 43912916400026*
Subject O:	*Cryptolog International*
Subject C:	*FR*

X509SKI

X509 SK I	*+k3tVzu9P/ORM5oLOaR/XRLdB0Y=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2015-04-13T22:00:00Z*

7.8 - Service (granted): Universign Time Stamping 2015

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description	*[en]*	*A time-stamping generation service creating and signing qualified time-stamps tokens.*
	[fr]	*Un service de génération horodatage création et la signature temps timbres jetons qualifiés.*

Service Name

Name	*[en]*	*Universign Time Stamping 2015*

Name *[fr]* *Horodatage Universign 2015*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *847987684037504690966020402803548919 40*

X509 Certificate -----BEGIN CERTIFICATE-----

MIID/zCCAuegAwIBAgIQP8umE0YUpE/yhLiMgaeopDANBgkqhkiG9w0BAQsFADB3MQswCQYDVQQG
EwJGUjEgMB4GA1UEChMXQ3J5cHRvbG9nIEludGVybmF0aW9uYWwxHDAaBgNVBAsTEzAwMDIgNDM5
MTI5MTY0MDAwMjYxKDAmBgNVBAMTH1VuaXZlcnNpZ24gVGltZXN0YW1waW5nIENBIDIwMTUwHhcN
MTUwMTI5MTQwMzE1WhcNMjUwMTI5MTQwMzE1WjB3MQswCQYDVQQGEwJGUjEgMB4GA1UEChMXQ3J5
cHRvbG9nIEludGVybmF0aW9uYWwxHDAaBgNVBAsTEzAwMDIgNDM5MTI5MTY0MDAwMjYxKDAmBgNV
BAMTH1VuaXZlcnNpZ24gVGltZXN0YW1waW5nIENBIDIwMTUwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQDYc1VJ69W70ojewtKbCLZ+P8bDAVJ1qujzgIZEvm15GYX7Jp+Hl9rwxBdswSZ8
S5A/x+0j6YMOHH0Z+iGl649+0GGX1gdAuovQKShsvLSzD/waINxkXXTVXpAW3V4dnCgcb3qaV/pO
9NTk/sdRJxM8lUtWuD7TEAfLzz7Ucl6gBjDTA0Gz+AtUkNWPcofCWuDfiSDOOpyKwSxovde6SRwH
dTXXIiC2Dphffjrr74MvLb0La5JAUwmJLIH42j/frgZeWk148wLMwBW+lvrIJtPz7eHNtTlNfQLr
mmJHW4l+yvTsdJJDs7QYtfzBTNg1zqV8eo/hHxFTFJ8/T9wTmENJAgMBAAGjgYYwgYMwDwYDVR0T
AQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYwQQYDVR0gBDowODA2BgorBgEEAftLBQEBMCgwJgYI
KwYBBQUHAgEWGmh0dHA6Ly9kb2NzLnVuaXZlcnNpZ24uZXUvMB0GA1UdDgQWBBT6Te1XO70/85Ez
mgs5pH9dEt0HRjANBgkqhkiG9w0BAQsFAAOCAQEAc7ud6793wgdjR8Xc1L47ufdVTamI5SHfOTht
ROfn8JL0HuNHKdRgv6COpdjtt6RwQEUUX/km7Q+Pn+A2gA/XoPfqD0iMfP63kMMyqgalEPRv+lXb
Fw3GSC9BQ9s2FL7ScvSuPm7VDZhpYN5xN6H72y4z7BgsDVNhkMu5AiWwbaWF+BHzZeiuvYHX0z/O
gY2oH0hluovuRAanQd4dOa73bbZhTJPFUzkgeIzOiuYS421IiAqsjkFwu3+k4dMDqYfDKUSITbMy
mkRDszR0WGNzIIy2NsTBcKYCHmbIV9S+165i8YjekraBjTTSbpfbty87A1S53CzA2EN1qnmQPwqF
fg==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Universign Timestamping CA 2015*

Issuer OU: *0002 43912916400026*

Issuer O: *Cryptolog International*

Issuer C: *FR*

Subject CN: *Universign Timestamping CA 2015*

Subject OU: *0002 43912916400026*

Subject O: *Cryptolog International*

Subject C: *FR*

Valid from: *Thu Jan 29 15:03:15 CET 2015*

Valid to: *Wed Jan 29 15:03:15 CET 2025*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:D8:73:55:49:EB:D5:BB:D2:88:DE:C2:D2:9B:08:B6:7E:3F:C6:C3:01:52:75:AA:E8:F3:80:86:44:BE:6D:79:19:85:FB:26:9F:87:97:DA:F0:C4:17:6C:C1:26:7C:4B:90:3F:C7:ED:23:E9:83:0E:1C:7D:19:FA:21:A5:EB:8F:7E:D0:61:97:D6:07:40:BA:8B:D0:29:28:6C:BC:B4:B3:0F:FC:1A:20:DC:64:5D:74:D5:5E:90:16:DD:5E:1D:9C:28:1C:6F:7A:9A:57:FA:4E:F4:D4:E4:FE:C7:51:27:13:3C:95:4B:56:B8:3E:D3:10:07:CB:CF:3E:D4:72:5E:A0:06:30:D3:03:41:B3:F8:0B:54:90:D5:8F:72:87:C2:5A:E0:DF:89:20:CE:3A:9C:8A:C1:2C:68:BD:D7:BA:49:1C:07:75:35:D7:22:20:B6:0E:98:5F:7E:3A:EB:EF:83:2F:2D:BD:0B:6B:92:40:53:09:89:2C:81:F8:DA:3F:DF:AE:06:5E:5A:4D:78:F3:02:CC:C0:15:BE:96:FA:C8:26:D3:F3:ED:E1:CD:B5:39:4D:7D:02:EB:9A:62:47:5B:89:7E:CA:F4:EC:74:92:43:B3:B4:18:B5:FC:C1:4C:D8:35:CE:A5:7C:7A:8F:E1:1F:11:53:14:9F:3F:4F:DC:13:98:43:49:02:03:01:00:01

Basic Constraints *IsCA: true*

Certificate Policies *Policy OID: 1.3.6.1.4.1.15819.5.1.1*
CPS pointer:
http://docs.universign.eu/

Subject Key Identifier *FA:4D:ED:57:3B:BD:3F:F3:91:33:9A:0B:39:A4:7F:5D:12:DD:07:46*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *9C:F3:C9:66:97:B7:20:58:9B:10:CC:13:B8:A2:BD:35:FF:BC:41:7B:70:50:A3:82:0A:F5:99:A4:39:DE:75:E5*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*
[fr] *undefined.*

Status Starting Time *2016-12-01T01:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS102023/LCP*

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Time-Stamping*

TSP Service Definition URI

URI *[en]* *https://www.universign.eu/en/documents/universign-pc_en.pdf*

URI *[fr]* *https://www.universign.eu/fr/documents/universign-pc_fr.pdf*

7.8.1 - History instance n.1 - Status: withdrawn

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service Name

Name *[en]* *Universign Time Stamping 2015*

Name *[fr]* *Horodatage Universign 2015*

Service digital identities

X509SubjectName

Subject CN: *Universign Timestamping CA 2015*

Subject OU: *0002 43912916400026*

Subject O: *Cryptolog International*

Subject C: *FR*

X509SKI

X509 SK I *+k3tVzu9P/ORM5oLOaR/XRLdB0Y=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Status Starting Time *2016-06-30T22:00:00Z*

7.8.2 - History instance n.2 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service Name

Name *[en]* *Universign Time Stamping 2015*

Name *[fr]* *Horodatage Universign 2015*

Service digital identities

X509SubjectName

Subject CN: *Universign Timestamping CA 2015*

Subject OU: *0002 43912916400026*

Subject O: *Cryptolog International*

Subject C: *FR*

X509SKI

X509 SK I *+k3tVzu9P/ORM5oLOaR/XRLdB0Y=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2015-04-13T22:00:00Z*

7.9 - Service (recognisedatnationallevel): Universign Time Stamping

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA*

Service type description

[en] *A time-stamping generation service creating and signing time-stamps tokens.*

[fr] *Un service de génération horodatage création et la signature des jetons temps timbres.*

Service Name

Name *[en]* *Universign Time Stamping*

Name *[fr]* *Horodatage Universign*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *311583423277221956465219911797114909 84*

X509 Certificate -----BEGIN CERTIFICATE-----

MIID9TCCAt2gAwIBAgIQF3Dg4iQuLQxzMPFRPs8rqDANBgkqhkiG9w0BAQsFADByMSMwIQYDVQQD
ExpVbml2ZXJzaWduIFRpbWVzdGFtcGluZyBDQTEcMBoGA1UECxMTMDAwMiA0MzkxMjkxNjQwMDAy
NjEgMB4GA1UEChMXQ3J5cHRvbG9nIEludGVybmF0aW9uYWwxCzAJBgNVBAYTAkZSMB4XDTEwMDUw
NjA5MzA1OVoXDTIwMDUwNjA5MzA1OVowcjEjMCEGA1UEAxMaVW5pdmVyc2lnbiBUaW1lc3RhbXBp
bmcgQ0ExHDAaBgNVBAsTEzAwMDIgNDM5MTI5MTY0MDAwMjYxIDAeBgNVBAoTF0NyeXB0b2xvZyBJ
bnRlcm5hdGlvbmFsMQswCQYDVQQGEwJGUjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AMF2r8Q+dqh3iA6fPMn0bOw50sKTsCPCocGVNPf75b6dERmkuiXj48/M6poFaPxV96Y01B8LjTUF
YGQr6Vbf/15HvVskV6ZSTb8PXNZef6vv7681qnMp7NZVyrWO9zjg4NcZ9qVKFlzZe2NCGHAZi+5z
7Y4Phnvg7XdLu0B92oERAIoconTcsHO6BSg9nhv0c+xDsUNdRKF1groYZtAwNO1L1j5kLY3PukPP
Ka0+uyrJ8j56mGGUGWKaZxLuKafn5M3tYMousgKxQ/5cDHnjntTFBXfm7+Jg0PeiJP6boM2nZDTc
nPBt+wvXzo27L4GV0GvZfoi0CVa27hkURRSnsJcCAwEAAaOBhjCBgzAPBgNVHRMBAf8EBTADAQH/
MA4GA1UdDwEB/wQEAwIBBjBBBgNVHSAEOjA4MDYGCisGAQQB+0sFAQEwKDAmBggrBgEFBQcCARYa
aHR0cDovL2RvY3MudW5pdmVyc2lnbi5ldS8wHQYDVR0OBBYEFOzknxQd8GYKOfVELMDFf8PMwaW1
MA0GCSqGSIb3DQEBCwUAA4IBAQAySgYJxVNszlupDmOTfKcSXRohKwxfgv/wVJhH7ypgqX9z+KM8
sh0FDrO2TbEyU/rnpJwauTUwPoa40plvLcBV3zcsA72mzG9fgjmftj0D5LxhkqsN7B13YOP/tlqo
e4f1jyfysxc/JpoBKXklJIBMW5DAbPxZPehVRpBJqrd0ZJNhKZFbBZvVIZ7KO5PX10k1016yiB8L
IuASeJfGMHlzvX0qorvl+98g868vQQB6xyMC8WcikEVsVrTBXnNsdD2F6EkC+HJ88qT5XfUGMxq8
8hvufpwfD3kTkqDm5RDhn0a0o8eIRlze2XopYWz17GWyUVyawoZcEfFYlDxjbo1p

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer C: *FR*

Issuer O: *Cryptolog International*

Issuer OU: *0002 43912916400026*

Issuer CN: *Universign Timestamping CA*

Subject C: *FR*

Subject O: *Cryptolog International*

Subject OU: *0002 43912916400026*

Subject CN: *Universign Timestamping CA*

Valid from: *Thu May 06 11:30:59 CEST 2010*

Valid to: *Wed May 06 11:30:59 CEST 2020*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C1:76:AF:C4:3E:76:A8:77:88:0E:9F:3C:C9:F4:6C:EC:39:D2:C2:93:B0:23:C2:A1:C1:95:34:F7:FB:E5:BE:9D:11:19:A4:BA:25:E3:E3:CF:CC:EA:9A:05:68:FC:55:F7:A6:34:D4:1F:0B:8D:35:05:60:64:2B:E9:56:DF:FF:5E:47:BD:5B:24:57:A6:52:4D:BF:0F:5C:D6:5E:7F:AB:EF:EF:AF:35:AA:73:29:EC:D6:55:CA:B5:8E:F7:38:E0:E0:D7:19:F6:A5:4A:16:5C:D9:7B:63:42:18:70:19:8B:EE:73:ED:8E:0F:86:7B:E0:ED:77:4B:BB:40:7D:DA:81:11:00:8A:1C:A2:74:DC:B0:73:BA:05:28:3D:9E:1B:F4:73:EC:43:B1:43:5D:44:A1:75:82:BA:18:66:D0:30:34:ED:4B:D6:3E:64:2D:8D:CF:BA:43:CF:29:AD:3E:BB:2A:C9:F2:3E:7A:98:61:94:19:62:9A:67:12:EE:29:A7:E7:E4:CD:ED:60:CA:2E:B2:02:B1:43:FE:5C:0C:79:E3:9E:D4:C5:05:77:E6:EF:E2:60:D0:F7:A2:24:FE:9B:A0:CD:A7:64:34:DC:9
C:F0:6D:FB:0B:D7:CE:8D:BB:2F:81:95:D0:6B:D9:7E:88:B4:09:56:B6:EE:19:14:45:14:A7:B0:97:02:03:01:00:01

Basic Constraints *IsCA: true*

Certificate Policies *Policy OID: 1.3.6.1.4.1.15819.5.1.1*
CPS pointer:
http://docs.universign.eu/

Subject Key Identifier *EC:E4:9F:14:1D:F0:66:0A:39:F5:44:2C:C0:C5:7F:C3:CC:C1:A5:B5*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *4F:60:07:66:6E:1C:29:A2:01:B1:45:DE:7F:9B:BE:16:0E:10:B3:C6:07:43:77:3A:2E:83:8E:AC:0F:C4:D7:9A*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/recognisedatnationallevel*

Service status description
[en] *undefined.*
[fr] *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

Scheme Service Definition URI

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Time-Stamping*

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS102023/LCP*

TSP Service Definition URI

URI *[en]* *https://www.universign.eu/en/documents/universign-pc_en.pdf*

URI *[fr]* *https://www.universign.eu/fr/documents/universign-pc_fr.pdf*

7.10 - Service (recognisedatnationallevel): Universign Time Stamping 2015

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA*

Service type description *[en]* *A time-stamping generation service creating and signing time-stamps tokens.*

[fr] *Un service de génération horodatage création et la signature des jetons temps timbres.*

Service Name

Name *[en]* *Universign Time Stamping 2015*

Name *[fr]* *Horodatage Universign 2015*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *847987684037504690966020402803548919 40*

X509 Certificate -----BEGIN CERTIFICATE-----

MIID/zCCAuegAwIBAgIQP8umE0YUpE/yhLiMgaeopDANBgkqhkiG9w0BAQsFADB3MQswCQYDVQQG
EwJGUjEgMB4GA1UEChMXQ3J5cHRvbG9nIEludGVybmF0aW9uYWwxHDAaBgNVBAsTEzAwMDIgNDM5
MTI5MTY0MDAwMjYxKDAmBgNVBAMTH1VuaXZlcnNpZ24gVGltZXN0YW1waW5nIENBIDIwMTUwHhcN
MTUwMTI5MTQwMzE1WhcNMjUwMTI5MTQwMzE1WjB3MQswCQYDVQQGEwJGUjEgMB4GA1UEChMXQ3J5
cHRvbG9nIEludGVybmF0aW9uYWwxHDAaBgNVBAsTEzAwMDIgNDM5MTI5MTY0MDAwMjYxKDAmBgNV
BAMTH1VuaXZlcnNpZ24gVGltZXN0YW1waW5nIENBIDIwMTUwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQDYc1VJ69W70ojewtKbCLZ+P8bDAVJ1qujzgIZEvm15GYX7Jp+Hl9rwxBdswSZ8
S5A/x+0j6YMOHH0Z+iGl649+0GGX1gdAuovQKShsvLSzD/waINxkXXTVXpAW3V4dnCgcb3qaV/pO
9NTk/sdRJxM8lUtWuD7TEAfLzz7Ucl6gBjDTA0Gz+AtUkNWPcofCWuDfiSDOOpyKwSxovde6SRwH
dTXXIiC2Dphffjrr74MvLb0La5JAUwmJLIH42j/frgZeWk148wLMwBW+lvrIJtPz7eHNtTlNfQLr
mmJHW4l+yvTsdJJDs7QYtfzBTNg1zqV8eo/hHxFTFJ8/T9wTmENJAgMBAAGjgYYwgYMwDwYDVR0T
AQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYwQQYDVR0gBDowODA2BgorBgEEAftLBQEBMCgwJgYI
KwYBBQUHAgEWGmh0dHA6Ly9kb2NzLnVuaXZlcnNpZ24uZXUvMB0GA1UdDgQWBBT6Te1XO70/85Ez
mgs5pH9dEt0HRjANBgkqhkiG9w0BAQsFAAOCAQEAc7ud6793wgdjR8Xc1L47ufdVTamI5SHfOTht
ROfn8JL0HuNHKdRgv6COpdjtt6RwQEUUX/km7Q+Pn+A2gA/XoPfqD0iMfP63kMMyqgalEPRv+lXb
Fw3GSC9BQ9s2FL7ScvSuPm7VDZhpYN5xN6H72y4z7BgsDVNhkMu5AiWwbaWF+BHzZeiuvYHX0z/O
gY2oH0hluovuRAanQd4dOa73bbZhTJPFUzkgeIzOiuYS421IiAqsjkFwu3+k4dMDqYfDKUSITbMy
mkRDszR0WGNzIIy2NsTBcKYCHmbIV9S+165i8YjekraBjTTSbpfbty87A1S53CzA2EN1qnmQPwqF
fg==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Universign Timestamping CA 2015*

Issuer OU: *0002 43912916400026*

Issuer O: *Cryptolog International*

Issuer C: *FR*

Subject CN: *Universign Timestamping CA 2015*

Subject OU: *0002 43912916400026*

Subject O: *Cryptolog International*

Subject C: *FR*

Valid from: *Thu Jan 29 15:03:15 CET 2015*

Valid to: *Wed Jan 29 15:03:15 CET 2025*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:D8:73:55:49:EB:D5:BB:D2:88:DE:C2:D2:9B:08:B6:7E:3F:C6:C3:01:52:75:AA:E8:F3:80:86:44:BE:6D:79:19:85:FB:26:9F:87:97:DA:F0:C4:17:6C:C1:26:7C:4B:90:3F:C7:ED:23:E9:83:0E:1C:7D:19:FA:21:A5:EB:8F:7E:D0:61:97:D6:07:40:BA:8B:D0:29:28:6C:BC:B4:B3:0F:FC:1A:20:DC:64:5D:74:D5:5E:90:16:DD:5E:1D:9C:28:1C:6F:7A:9A:57:FA:4E:F4:D4:E4:FE:C7:51:27:13:3C:95:4B:56:B8:3E:D3:10:07:CB:CF:3E:D4:72:5E:A0:06:30:D3:03:41:B3:F8:0B:54:90:D5:8F:72:87:C2:5A:E0:DF:89:20:CE:3A:9C:8A:C1:2C:68:BD:D7:BA:49:1C:07:75:35:D7:22:20:B6:0E:98:5F:7E:3A:EB:EF:83:2F:2D:BD:0B:6B:92:40:53:09:89:2C:81:F8:DA:3F:DF:AE:06:5E:5A:4D:78:F3:02:CC:C0:15:BE:96:FA:C8:26:D3:F3:ED:E1:CD:B5:39:4D:7D:02:EB:9A:62:47:5B:89:7E:CA:F4:EC:74:92:43:B3:B4:18:B5:FC:C1:4C:D8:35:CE:A5:7C:7A:8F:E1:1F:11:53:14:9F:3F:4F:DC:13:98:43:49:02:03:01:00:01

Basic Constraints *IsCA: true*

Certificate Policies *Policy OID: 1.3.6.1.4.1.15819.5.1.1*
CPS pointer:
http://docs.universign.eu/

Subject Key Identifier *FA:4D:ED:57:3B:BD:3F:F3:91:33:9A:0B:39:A4:7F:5D:12:DD:07:46*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *9C:F3:C9:66:97:B7:20:58:9B:10:CC:13:B8:A2:BD:35:FF:BC:41:7B:70:50:A3:82:0A:F5:99:A4:39:DE:75:E5*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/recognisedatnationallevel*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS102023/LCP*

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Time-Stamping*

TSP Service Definition URI

URI *[en]* *https://www.universign.eu/en/documents/universign-pc_en.pdf*

URI *[fr]* *https://www.universign.eu/fr/documents/universign-pc_fr.pdf*

8 - TSP: Dhimyotis

TSP Name

Name *[en]* *Dhimyotis*

Name *[fr]* *Dhimyotis*

TSP Trade Name

Name *[en]* *VATFR-85481463081*

Name *[fr]* *VATFR-85481463081*

PostalAddress

Street Address *[en]* *Zone de la plaine - 20, allée de la râperie*

Locality *[en]* *Villeneuve d'Ascq*

Postal Code *[en]* *59650*

Country Name *[en]* *FR*

PostalAddress

Street Address *[fr]* *Zone de la plaine - 20, allée de la râperie*

Locality *[fr]* *Villeneuve d'Ascq*

Postal Code *[fr]* *59650*

Country Name *[fr]* *FR*

ElectronicAddress

URI *http://www.dhimyotis.com/*

URI *mailto:contact@certigna.fr*

URI *mailto:contact@certigna.fr*

URI *http://www.dhimyotis.com/*

URI *http://www.certigna.fr*

URI *http://www.certigna.fr*

TSP Information URI

URI *[fr]* *https://www.certigna.fr/Certigna/autorites*

URI *[en]* *https://www.certigna.fr/Certigna/autorites*

8.1 - Service (withdrawn): Certigna ID PRIS *** PRO

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Certigna ID PRIS *** PRO*

Name *[fr]* *Certigna ID PRIS *** PRO*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *24*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIEhzCCA2+gAwIBAgIBGDANBgkqhkiG9w0BAQsFADA0MQswCQYDVQQGEwJGUjESMBAGA1UECgwJ
RGhpbXlvdGlzMREwDwYDVQQDDAhDZXJ0aWduYTAeFw0wODExMTkxMzI2MzFaFw0xODExMTcxMzI2
MzFaMGkxCzAJBgNVBAYTAkZSMRIwEAYDVQQKDAlEaGlteW90aXMxFzAVBgNVBAsMDjAwMDIgNDgx
NDYzMDgxMSAwHgYDVQQDDBdDZXJ0aWduYSBJRCBQUklTKioqIFBybzELMAkGA1UEBRMCMjQwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC9D8Oo93NtsdlJMXpVIzaKIctVPdlz3z9BLDbj
wfRo1S1OVHrZAL1jw832q91l9lHRR/WuVMrSd9SVBLtaeDTUEkHodr6l3E9cD1prGoUCykYcFmYC
JWhBCUKLqyX1UGXQdAJCN7G+PyEjh9OBmTc49P3lkeSzc4o/L3HJ2bMUJMI109aqGrHGj/F2pzE3
+7/or5LwgkafSa6TpBeMApMVvZltR0uSpWnOCecLIxUI73vq83Dq28Gv+5C+W5UesPPM42cwaEMr
E9/QhLjU3n7n6bY4yBzuZAnfhxrrFGi66nJqluAzVjjHc9Iw1IkiKr+GYRuonwbmhM9skrsTlEYr
AgMBAAGjggFtMIIBaTAPBgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBBjARBglghkgBhvhC
AQEEBAMCAAMwFwYDVR0gBBAwDjAMBgoqgXoBgTEBAAEBMB0GA1UdDgQWBBS6PWIwUB7DTGNFW1M2
Fdxpktj/WjBkBgNVHSMEXTBbgBQa7f5BOZC0JFm+AfJS1UX2WjncEaE4pDYwNDELMAkGA1UEBhMC
RlIxEjAQBgNVBAoMCURoaW15b3RpczERMA8GA1UEAwwIQ2VydGlnbmGCCQD+3OMBD8ll/zAyBglg
hkgBhvhCAQQEJRYjaHR0cDovL2NybC5jZXJ0aWduYS5mci9jZXJ0aWduYS5jcmwwYQYDVR0fBFow
WDApoCegJYYjaHR0cDovL2NybC5jZXJ0aWduYS5mci9jZXJ0aWduYS5jcmwwK6ApoCeGJWh0dHA6
Ly9jcmwuZGhpbXlvdGlzLmNvbS9jZXJ0aWduYS5jcmwwDQYJKoZIhvcNAQELBQADggEBABrjE6p0

pUDt4ykUmVuikPquMeBcsDvSA8MrspNMx676ATc6Fm5YSz6b8wnKKzAzoJDw1fT85HhaylHH8JMZ
ytvY38Hdshu3eeKaZZ9GoW3s9i1mN/S7E6ZejTmqI4M6ld1y4v5C4c0sWyJBE661xCKOLOoRX2Li
ujHlyDc6TsO86/i09AdcVEwNiRv6vDgllYhfWgWON2LFLW5pERtN3EjmxmYdRfv5Bnsl/SLMOn0d
J8DNSR3TMJvhyPqqRW/deqXqDeRDd6oM3+kOtl+aNK8TYSr/pmZqlXpIkikREn+RPwVTm3TZKs99
HhlOJ1kkrNpnz5cIrDWYD5s7JQw9D+8=

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Certigna*

Issuer O: *Dhimyotis*

Issuer C: *FR*

Subject SERIAL NUMBER: *24*

Subject CN: *Certigna ID PRIS*** Pro*

Subject OU: *0002 481463081*

Subject O: *Dhimyotis*

Subject C: *FR*

Valid from: *Wed Nov 19 14:26:31 CET 2008*

Valid to: *Sat Nov 17 14:26:31 CET 2018*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:BD:0F:C3:A8:F7:73:6D:B1:D9:49:31:7A:55:23:36:8A:
21:CB:55:3D:D9:73:DF:3F:41:2C:36:E3:C1:F4:68:D5:2D:4E:54:7A:D9:00:BD:63:C3:CD:F6:AB:DD:65:F6:51:D1:47:F5:AE:54:CA:D2:77:D4:95:04:BB:5A:78:34:D4:
12:41:E8:76:BE:A5:DC:4F:5C:0F:5A:6B:1A:85:02:CA:46:1C:16:66:02:25:68:41:09:42:8B:AB:25:F5:50:65:D0:74:02:42:37:B1:BE:3F:21:23:87:D3:81:99:37:38:F4:
FD:E5:91:E4:B3:73:8A:3F:2F:71:C9:D9:B3:14:24:C2:35:D3:D6:AA:1A:B1:C6:8F:F1:76:A7:31:37:FB:BF:E8:AF:92:F0:82:46:9F:49:AE:93:A4:17:8C:02:93:15:BD:99:
6D:47:4B:92:A5:69:CE:09:E7:0B:23:15:08:EF:7B:EA:F3:70:EA:DB:C1:AF:FB:90:BE:5B:95:1E:B0:F3:CC:E3:67:30:68:43:2B:13:DF:D0:84:B8:D4:DE:7E:E7:E9:B6:38
:C8:1C:EE:64:09:DF:87:1A:EB:14:68:BA:EA:72:6A:96:E0:33:56:38:C7:73:D2:30:D4:89:22:2A:BF:86:61:1B:A8:9F:06:E6:84:CF:6C:92:BB:13:94:46:2B:02:03:01:00
:01

Basic Constraints *IsCA: true*

Certificate Policies *Policy OID: 1.2.250.1.177.1.0.1.1*

Subject Key Identifier *BA:3D:62:30:50:1E:C3:4C:63:45:5B:53:36:15:DC:69:92:D8:FF:5A*

Authority Key Identifier *1A:ED:FE:41:39:90:B4:24:59:BE:01:F2:52:D5:45:F6:5A:39:DC:11*

CRL Distribution Points *http://crl.certigna.fr/certigna.crl*

http://crl.dhimyotis.com/certigna.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *34:1F:7C:F4:30:E3:33:54:4B:DF:43:8C:0C:8F:05:8A:F3:51:0C:59:F7:F3:E1:BE:A8:F8:A6:33:F6:EA:CE:02*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2018-01-30T01:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS101456/QCPPublic*

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Signature-3-Stars/Referenced/*

TSP Service Definition URI

URI *[en]* *http://politique.certigna.fr/en/PCcertignaidpris3pro.pdf*

URI *[fr]* *http://politique.certigna.fr/PCcertignaidpris3pro.pdf*

8.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

8.1.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Certigna ID PRIS *** PRO*

Name *[fr]* *Certigna ID PRIS *** PRO*

Service digital identities

X509SubjectName

Subject SERIAL NUMBER: *24*

Subject CN: *Certigna ID PRIS*** Pro*

Subject OU: *0002 481463081*

Subject O: *Dhimyotis*

Subject C: *FR*

X509SKI

X509 SK I *uj1iMFAew0xjRVtTNhXcaZLY/1o=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

8.1.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

8.1.3 - History instance n.2 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Certigna ID PRIS *** PRO*

Name *[fr]* *Certigna ID PRIS *** PRO*

Service digital identities

X509SubjectName

Subject SERIAL NUMBER: *24*

Subject CN: *Certigna ID PRIS*** Pro*

Subject OU: *0002 481463081*

Subject O: *Dhimyotis*

Subject C: *FR*

X509SKI

X509 SK I *uj1iMFAew0xjRVtTNhXcaZLY/1o=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2008-11-18T23:00:00Z*

8.2 - Service (withdrawn): Certigna ID PRIS ***

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Certigna ID PRIS ****

Name *[fr]* *Certigna ID PRIS ****

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *23*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIEgzCCA2ugAwIBAgIBFzANBgkqhkiG9w0BAQsFADA0MQswCQYDVQQGEwJGUjESMBAGA1UECgwJ
RGhpbXlvdGlzMREwDwYDVQQDDAhDZXJ0aWduYTAeFw0wODExMTkxMzAzNDBaFw0xODExMTcxMzAz
NDBaMGUxCzAJBgNVBAYTAkZSMRIwEAYDVQQKDAlEaGlteW90aXMxFzAVBgNVBAsMDjAwMDIgNDgx
NDYzMDgxMRwwGgYDVQQDDBNDZXJ0aWduYSBJRCBQUklTKioqMQswCQYDVQQFEwIyMzCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBAMSZdSYGAl3ELDEiiuVT59lGKBd0KqI1v4aELLROksaL
Asn5NxRtuvmRmNqXpD5eoZzynMZe/pLB7PC2O6TmbHYcadYirX/CKeDirSFZM0Lf40/5Iji1idWe
3jDZuR4NIXTiflJUJ6S7rEHjojW1amPAqnkinv9VDUvD2rSGHvBSXLFvl6HyRMA0uNg5BxZLBSQr
A+66kTLkbNtAYwpYU7L6mMw93m3V/8aMag81idOvymjJWO1iXQnCxyr7b6I73sFGAjtQ20TFCiiO
3rJDdPDTc1eAJLesKjYq5PiX1uBU3ViOGSnwQA8ezZ8tv8Xk6VmDqzxSAs8Pm2srBRPnyncCAwEA
AaOCAW0wggFpMA8GA1UdEwEB/wQFMAMBAf8wDgYDVR0PAQH/BAQDAgEGMBEGCWCGSAGG+EIBAQQE
AwIAAzAXBgNVHSAEEDAOMAwGCiqBegGBMQEAAQEwHQYDVR0OBBYEFBOAp8XAJEr6sNxz9FuuGsLd
RV1tMGQGA1UdIwRdMFuAFBrt/kE5kLQkWb4B8lLVRfZaOdwRoTikNjA0MQswCQYDVQQGEwJGUjES
MBAGA1UECgwJRGhpbXlvdGlzMREwDwYDVQQDDAhDZXJ0aWduYYIJAP7c4wEPyUj/MDIGCWCGSAGG
+EIBBAQlFiNodHRwOi8vY3JsLmNlcnRpZ25hLmZyL2NlcnRpZ25hLmNybDBhBgNVHR8EWjBYMCmg
J6AlhiNodHRwOi8vY3JsLmNlcnRpZ25hLmZyL2NlcnRpZ25hLmNybDAroCmgJ4YlaHR0cDovL2Ny
bC5kaGlteW90aXMuY29tL2NlcnRpZ25hLmNybDANBgkqhkiG9w0BAQsFAAOCAQEACXBoGcUC1ScM
3WJFs2sW12OJVLKP2Wl4Efm33imvChq5xWUNdFPE+Z83/JA4EnqvsQF3ojfZRQqm7A6pctvtw1u2
XHAL0KyzGlxUYUiw3q5PHoxuRLw3bN9RHJaS/2eiZW6eHWkEW0apgDFwhnVNcP81zgKSXzu5VYwo
5sPbLIHndYM8fT2koCZzybMAJUJaIYugxxekce2InKcvBOZ0TJYpblTBissmMNREvJXXM87Y80L0
/JFhGs4n9WkRvyN8FWz+J8MJ9Qg8t7wl134O2fm6ESBMDXJ++3wKvGY6JzT3NYhs9zFC+9JMCGNW
HHUDyXqEYsJicxJ7XBdrEeTiSA==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Certigna*

Issuer O: *Dhimyotis*

Issuer C: *FR*

Subject SERIAL NUMBER: *23*

Subject CN: *Certigna ID PRIS****

Subject OU: *0002 481463081*

Subject O: *Dhimyotis*

Subject C: *FR*

Valid from: *Wed Nov 19 14:03:40 CET 2008*

Valid to: *Sat Nov 17 14:03:40 CET 2018*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C4:99:75:26:06:02:5D:C4:2C:31:22:8A:E5:53:E7:D9:
46:28:17:74:2A:A2:35:BF:86:84:2C:B4:4E:92:C6:8B:02:C9:F9:37:14:6D:BA:F9:91:98:DA:97:A4:3E:5E:A1:9C:F2:9C:C6:5E:FE:92:C1:EC:F0:B6:3B:A4:E6:6C:76:1C:
69:D6:22:AD:7F:C2:29:E0:E2:AD:21:59:33:42:DF:E3:4F:F9:22:38:B5:89:D5:9E:DE:30:D9:B9:1E:0D:21:74:E2:7E:52:54:27:A4:BB:AC:41:E3:A2:35:B5:6A:63:C0:A
A:79:22:9E:FF:55:0D:4B:C3:DA:B4:86:1E:F0:52:5C:B1:6F:97:A1:F2:44:C0:34:B8:D8:39:07:16:4B:05:24:2B:03:EE:BA:91:32:E4:6C:DB:40:63:0A:58:53:B2:FA:98:
CC:3D:DE:6D:D5:FF:C6:8C:6A:0F:35:89:D3:AF:CA:68:C9:58:ED:62:5D:09:C2:C7:2A:FB:6F:A2:3B:DE:C1:46:02:3B:50:DB:44:C5:0A:28:8E:DE:B2:43:74:F0:D3:73:5
7:80:24:B7:AC:2A:36:2A:E4:F8:97:D6:E0:54:DD:58:8E:19:29:F
0:40:0F:1E:CD:9F:2D:BF:C5:E4:E9:59:83:AB:3C:52:02:CF:0F:9B:6B:2B:05:13:E7:CA:77:02:03:01:00:01

Basic Constraints *IsCA: true*

Certificate Policies *Policy OID: 1.2.250.1.177.1.0.1.1*

Subject Key Identifier *13:80:A7:C5:C0:24:4A:FA:B0:DC:73:F4:5B:AE:1A:C2:DD:45:5D:6D*

Authority Key Identifier *1A:ED:FE:41:39:90:B4:24:59:BE:01:F2:52:D5:45:F6:5A:39:DC:11*

CRL Distribution Points *http://crl.certigna.fr/certigna.crl*

http://crl.dhimyotis.com/certigna.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *D0:DC:19:9F:E7:CE:45:62:E4:73:28:CD:0D:6E:E9:CE:10:6C:38:4B:AB:E3:76:41:FE:33:24:2A:22:A1:BB:A6*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description

[en] *undefined.*

[fr] *undefined.*

Status Starting Time *2017-05-01T00:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS101456/QCPPublic*

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Signature-3-Stars/Referenced/*

TSP Service Definition URI

URI *[en]* *http://politique.certigna.fr/en/PCcertignaidpris3.pdf*

URI *[fr]* *http://politique.certigna.fr/PCcertignaidpris3.pdf*

8.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

8.2.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Certigna ID PRIS ****

Name *[fr]* *Certigna ID PRIS ****

Service digital identities

X509SubjectName

Subject SERIAL NUMBER: *23*

Subject CN: *Certigna ID PRIS****

Subject OU: *0002 481463081*

Subject O: *Dhimyotis*

Subject C: *FR*

X509SKI

X509 SK I *E4CnxcAkSvqw3HP0W64awt1FXW0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

8.2.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

8.2.3 - History instance n.2 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Certigna ID PRIS ****

Name *[fr]* *Certigna ID PRIS ****

Service digital identities

X509SubjectName

Subject SERIAL NUMBER: *23*

Subject CN: *Certigna ID PRIS****

Subject OU: *0002 481463081*

Subject O: *Dhimyotis*

Subject C: *FR*

X509SKI

X509 SK I *E4CnxcAkSvqw3HP0W64awt1FXW0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2008-11-18T23:00:00Z*

8.3 - Service (granted): Certigna Identity Plus CA - ID *** - 1.2.250.1.177.2.4.1.6.1

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Certigna Identity Plus CA - ID *** - 1.2.250.1.177.2.4.1.6.1*

Name *[fr]* *Certigna Identity Plus CA - ID *** - 1.2.250.1.177.2.4.1.6.1*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *625768101432799552817853009833909090 51*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIGHDCCBQSgAwIBAgIQLxPa8YcM1DOPGNv8N2uyezANBgkqhkiG9w0BAQsFADA0MQswCQYDVQQG
EwJGUjESMBAGA1UECgwJRGhpbXlvdGlzMREwDwYDVQQDDAhDZXJ0aWduYTAeFw0xNTExMjUwOTIz
MjVaFw0yNTExMjIwOTIzMjVaMIGCMQswCQYDVQQGEwJGUjESMBAGA1UECgwJREhJTVlPVElTMRww
GgYDVQQLDBMwMDAyIDQ4MTQ2MzA4MTAwMDM2MR0wGwYDVQRhDBROVFJGUi00ODE0NjMwODEwMDAz
NjEiMCAGA1UEAwwZQ2VydGlnbmEgSWRlbnRpdHkgUGx1cyBDQTCCAiIwDQYJKoZIhvcNAQEBBQAD
ggIPADCCAgoCggIBAMfolTzFjsvedPYwvO3ph5U+t8tmXWjPCSg7pRdR7Ip5dhBqmdENIQ2THhBQ
KzjEX9fdwHQr9EUxUtZMWF93HAlj03o2ZgNtLUblObru+LwA/DObWQVndKMGmd6NKFUA23YcaLwe
2/nNUdjV7caK0o95Ret5UZ4nVoeP9JBgTtwiPHu09x3npsSJ3mlOB754RKbKJdbDkJOFAiJOxfBi
GuLsztrwHtPDWHP3JkAg87gNMl9WyWGdnOnrexcbqUgG10Gufh5L7WuKmKogU6UEK2Fsu6pUbc8M
90x6Ft26UeRPgbC3cI0quO66dm/zi06zXsefWcjee7QfwLbSALJBBXO3IfbRnhknphhMhHR4IsHZ
YiUMzvrn35iOGawPv82fBHJj9IlXH42IwMALW82559r4nXT/mGg3yR7NFqJ9JUwvJVSKZIgDQXBM
2i5qjw0vq6qu9w3+2nWZ9XmGEYDuqPswy8C9LGCN27teASRFuL2J6+yJDmvXsXjl3AWibJG9Q4xE
Yu+H2N4fh1XEFfctgPNnOGcs85t3PAO6zJOxPeESljc/8sFxZ3N1LSzUOJYQphDNevIB91WGF27v
1siGHlEJB+lwfuumx9I2/+YF8M8S1UFhHpJi/nz9mvkeFKz/Y01tr7Xyn/JL/i3rRX9oqdDwgzZq
MF2KneQAzxf6CtstAgMBAAGjggHZMIIB1TASBgNVHRMBAf8ECDAGAQH/AgEAMA4GA1UdDwEB/wQE
AwIBBjAdBgNVHQ4EFgQUZjjzwlqN3683rWHZPBodPhdnB3UwZAYDVR0jBF0wW4AUGu3+QTmQtCRZ
vgHyUtVF9lo53BGhOKQ2MDQxCzAJBgNVBAYTAkZSMRIwEAYDVQQKDAlEaGlteW90aXMxETAPBgNV
BAMMCENlcnRpZ25hggkA/tzjAQ/JSP8wSQYDVR0gBEIwQDA+BgoqgXoBgTEBAAECMDAwLgYIKwYB
BQUHAgEWImh0dHBzOi8vd3d3LmNlcnRpZ25hLmZyL2F1dG9yaXRlcy8wfAYIKwYBBQUHAQEEcDBu
MDQGCCsGAQUFBzAChihodHRwOi8vYXV0b3JpdGUuY2VydGlnbmEuZnlvY2VydGlnbmEuZGVyMDYG
CCsGAQUFBzAChipodHRwOi8vYXV0b3JpdGUuZGhpbXlvdGlzLmNvbS9jZXJ0aWduYS5kZXIwYQYD
VR0fBFowWDApoCegJYYjaHR0cDovL2NybC5jZXJ0aWduYS5mci9jZXJ0aWduYS5jcmwwK6ApoCeG
JWh0dHA6Ly9jcmwuZGhpbXlvdGlzLmNvbS9jZXJ0aWduYS5jcmwwDQYJKoZIhvcNAQELBQADggEB
AK05XoyuwD1xY8gklri3eb/mk0rVyRp6Pa9VA8hDNiZqz2ZaVAOKZYP3tvRXTz/vOMlDVO9i66MB
qADiG9smLFB2dWQVojALSbX52V5gyKPglfqY99YPLwuihlrOYSDsuooEc6qZ3RKgK3HnbLAlhTNR
ljgcOkKFYmnMXggsUA5ZhL0fntu+b89FCSbtth3nhoL1gVYZg54ZtyzMi8VmJTMUDk/2nXuzIan6
dZByWdcUfwHj5iGyAnXs09+iQA0q+EyqxKG/7ovWpOndOJIZ576bEy3+WcnxWAdYiBV8tA1Snjit
91RkThbjIz+nzuVJOvYwQwJdBp9lBJoFK2zKHy4=

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Certigna*

Issuer O: *Dhimyotis*

Issuer C: *FR*

Subject CN: *Certigna Identity Plus CA*

Subject 2.5.4.97: *NTRFR-48146308100036*

Subject OU: *0002 48146308100036*

Subject O: *DHIMYOTIS*

Subject C: *FR*

Valid from: *Wed Nov 25 10:23:25 CET 2015*

Valid to: *Sat Nov 22 10:23:25 CET 2025*

Public Key:

:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:C7:E8:95:3C:C5:8E:CB:DE:74:F6:30:BC:ED:E9:87:95:3E:B7:CB:66:5D:68:CF:09:28:3B:A5:17:51:EC:8A:79:76:10:306A:99:D1:0D:21:0D:93:1E:10:50:2B:38:C4:5F:D7:DD:C0:74:2B:F4:45:31:52:D6:4C:58:5F:77:1C:09:63:D3:7A:36:66:03:6D:2D:46:E5:39:BA:EE:F8:BC:00:FC:33:9B:59:05:67:74:A3:06:99:DE:8D:28:55:00:DB:76:1C:68:BC:1E:DB:F9:CD:51:D8:D5:ED:C6:8A:D2:8F:79:45:EB:79:51:9E:27:56:87:8F:F4:90:60:4E:DC:22:3C:7B:B4:F7:1D:E7:A6:C4:89:DE:69:4E:07:BE:78:44:A6:CA:25:D6:C3:90:93:85:02:22:4E:C5:F0:62:1A:E2:EC:CE:DA:F0:1E:D3:C3:58:73:F7:26:40:20:F3:B8:0D:32:5F:56:C9:61:9D:9C:E9:EB:7B:17:1B:A9:48:06:D7:41:AE:7E:1E:4B:ED:6B:8A:98:AA:20:53:A5:04:2B:61:6C:BB:AA:54:6D:CF:0C:F7:4C:7A:16:DD:BA:51:E4:4F:81:B0:B7:70:8D:2A:B8:EE:BA:76:6F:F3:8B:4E:B3:5E:C7:9F:59:C8:DE:7B:B4:1F:C0:B6:D2:00:B2:41:05:73:B7:21:F6:D1:9E:19:27:A6:18:4C:84:74:78:22:C1:D9:62:25:0C:CE:FA:E7:DF:98:8E:19:AC:0F:BF:CD:9F:04:72:63:F4:89:57:1F:8D:88:C0:C0:0B:5B:CD:B9:E7:DA:F8:9D:74:FF:98:68:37:C9:1E:CD:16:A2:7D:25:4C:2F:25:54:8A:64:88:03:41:70:4C:DA:2E:6A:8F:0D:2F:AB:AA:AE:F7:0D:FE:DA:75:99:F5:79:86:11:80:EE:A8:FB:30:CB:C0:BD:2C:60:8
D:DB:BB:5E:01:24:45:B8:BD:89:EB:EC:89:0E:6B:D7:B1:78:E5:DC:05:A2:6C:91:BD:43:8C:44:62:EF:87:D8:DE:1F:87:55:C4:15:F7:2D:80:F3:67:38:67:2C:F3:9B:77:3C:03:BA:CC:93:B1:3D:E1:12:96:37:3F:F2:C1:71:67:73:75:2D:2C:D4:38:96:10:A6:10:CD:7A:F2:01:F7:55:86:17:6E:EF:D6:C8:86:1E:51:09:07:E9:70:7E:EB:A6:C7:D2:36:FF:E6:05:F0:CF:12:D5:41:61:1E:92:62:FE:7C:FD:9A:F9:1E:14:AC:FF:63:4D:6D:AF:B5:F2:9F:F2:4B:FE:2D:EB:45:7F:68:A9:D0:F0:83:36:6A:30:5D:8A:9D:E4:00:CF:17:FA:0A:DB:2D:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *66:38:F3:C2:5A:8D:DF:AF:37:AD:61:D9:3C:1A:1D:3E:17:67:07:75*

Authority Key Identifier *1A:ED:FE:41:39:90:B4:24:59:BE:01:F2:52:D5:45:F6:5A:39:DC:11*

Certificate Policies *Policy OID: 1.2.250.1.177.1.0.1.2*

CPS pointer: https://www.certigna.fr/autorites/

Authority Info Access *http://autorite.certigna.fr/certigna.der*

http://autorite.dhimyotis.com/certigna.der

CRL Distribution Points *http://crl.certigna.fr/certigna.crl*

http://crl.dhimyotis.com/certigna.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *02:C4:A3:00:A0:9C:1B:89:3B:11:F9:56:76:59:AF:95:BB:B9:BB:E7:95:38:93:E3:6C:5B:AF:17:B5:55:CE:E3*

Certificate fields details

Version: *3*

Serial Number: *263614261279511986064484843886564435021*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIHFzCCBP+gAwIBAgIRAMZSQoyDlJwTf12f6/JxZE0wDQYJKoZIhvcNAQELBQAwWjELMAkGA1UE
BhMCRlIxEjAQBgNVBAoMCUNoaW15b3RpczEcMBoGA1UECwwTMDAwMiA0ODE0NjMwODEwMDAzNjEZ
MBcGA1UEAwwQQ2VydGlnbmEgUm9vdCBDQTAeFw0xNTExMjUwOTMwNTFaFw0zMzA2MDMwOTMwNTFa
MIGCMQswCQYDVQQGEwJGUjESMBAGA1UECgwJREhJTVlPVElTMRwwGgYDVQQLDBMwMDAyIDQ4MTQ2
MzA4MTAwMDM2MR0wGwYDVQRhDBROVFJGUi00ODE0NjMwODEwMDAzNjEiMCAGA1UEAwwZQ2VydGln
bmEgSWRlbnRpdHkgUGx1cyBDQTCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAMfolTzF
jsvedPYwvO3ph5U+t8tmXWjPCSg7pRdR7Ip5dhBqmdENIQ2THhBQKzjEX9fdwHQr9EUxUtZMWF93
HAlj03o2ZgNtLUblObru+LwA/DObWQVndKMGmd6NKFUA23YcaLwe2/nNUdjV7caK0o95Ret5UZ4n
VoeP9JBgTtwiPHu09x3npsSJ3mlOB754RKbKJdbDkJOFAiJOxfBiGuLsztrwHtPDWHP3JkAg87gN
Ml9WyWGdnOnrexcbqUgG10Gufh5L7WuKmKogU6UEK2Fsu6pUbc8M90x6Ft26UeRPgbC3cI0quO66
dm/zi06zXsefWcjee7QfwLbSALJBBXO3IfbRnhknphhMhHR4IsHZYiUMzvrn35iOGawPv82fBHJj
9llXH42IwMALW82559r4nXT/mGg3yR7NFqJ9JUwvJVSKZIgDQXBM2i5qjw0vq6qu9w3+2nWZ9XmG
EYDuqPswy8C9LGCN27teASRFuL2J6+yJDmvXsXjl3AWibJG9Q4xEYu+H2N4fh1XEFfctgPNnOGcs
85t3PAO6zJOxPeESljc/8sFxZ3N1LSzUOJYQphDNevIB91WGF27v1siGHlEJB+lwfuumx9I2/+YF
8M8S1UFhHpJi/nz9mvkeFKz/Y01tr7Xyn/JL/i3rRX9oqdDwgzZqMF2KneQAzxf6CtstAgMBAAGj
ggGtMIIBqTASBgNVHRMBAf8ECDAGAQH/AgEAMA4GA1UdDwEB/wQEAwIBBjAdBgNVHQ4EFgQUZjjz
wlqN3683rWHZPBodPhdnB3UwHwYDVR0jBBgwFoAUGIdW4G537iQ1PE5zmh/W4eJ5fiswSQYDVR0g
BEIwQDA+BgoqgXoBgTECAAEBMDAwLgYIKwYBBQUHAgEWImh0dHBzOi8vd3d3LmNlcnRpZ25hLmZy
L2F1dG9yaXRlcy8wgYgGCCsGAQUFBwEBBHwwejA6BggrBgEFBQcwAoYuaHR0cDovL2F1dG9yaXRl
LmNlcnRpZ25hLmZyL2NlcnRpZ25hcm9vdGNhLmRlcjA8BggrBgEFBQcwAoYwaHR0cDovL2F1dG9y
aXRlLmRoaW15b3Rpcy5jb20vY2VydGlnbmFyb290Y2EuZGVyMG0GA1UdHwRmMGQwL6AtoCuGKWh0
dHA6Ly9jcmwuY2VydGlnbmEuZnIvY2VydGlnbmFyb290Y2EuY3JsMDGgL6AthitodHRwOi8vY3Js
LmRoaW15b3Rpcy5jb20vY2VydGlnbmFyb290Y2EuY3JsMA0GCSqGSIb3DQEBCwUAA4ICAQC75ZUB
BzkUGAgcPanEMIYXFQaMMbdkRqW2jnGZTCKn7ahguFGl4/VwDN7oT9Yw7LqFLNZumbKFR+QUOlFi
4DiqWUqFbYle8ir3gZBLMiGpD8fO4qbhDfMRLJytJ1UWZN0zHov5KC6w14SQVoyUH6tbq7FYX99K
qQ5Twjq2Z8+pVQGiz7cay107Hod/86gl9SAEq+YIdKlgfax+GKi6wo18m1Z6NuGQp1SYfVnO1eWd
PyNRAIv9Y4N/vZkxV6ct9KuNAv1DB4CSjuYJVyO1UIk2LNqYTZUQPEXUpdgXFoiLKqWgvysgxh0n
r+IrzblClUusEpOOIPVCRTlkLQNKLXh6rTglltjeqIF16ksYjag0Km7qSP4dLK9+vQ6y38YfTE3Z
PjH6inK5o9jU+3bgch7sY8whZzm57768SZXSndRS4DSaMlUieZV4flCAKQ0I85Bu7tSAIPtdT0XO
5gquusAW1fTclq2Z7JBOBdlMjsRG9ZIq9cZ9tCt1Pty43D6I/GGQXAP/hri47oquz2pSqDwOqt7t
GvPP+pSYDEgRFJ5WcrwAAl/j9kIBteCSveZMaRo5esXgFbzafIXDPh0pPpUGdp8Q2opiWv4OpIBX
PnQZXI1iMnOFBLQyzO+oYV1u3Gbjul8Y3xlst/mB/3KXXEVWUaKp9OXNa2MZkHqEkHinHQ==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Certigna Root CA*

Issuer OU: *0002 48146308100036*

Issuer O: *Dhimyotis*

Issuer C: *FR*

Subject CN: *Certigna Identity Plus CA*

Subject 2.5.4.97: *NTRFR-48146308100036*

Subject OU: *0002 48146308100036*

Subject O: *DHIMYOTIS*

Subject C: *FR*

Valid from: *Wed Nov 25 10:30:51 CET 2015*

Valid to: *Fri Jun 03 11:30:51 CEST 2033*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:C7:E8:95:3C:C5:8E:CB:DE:74:F6:30:BC:ED:E9:87:95:3E:B7:CB:66:5D:68:CF:09:28:3B:A5:17:51:EC:8A:79:76:10:6A:99:D1:0D:21:0D:93:1E:10:50:2B:38:C4:5F:D7:DD:C0:74:2B:F4:45:31:52:D6:4C:58:5F:77:1C:09:63:D3:7A:36:66:03:6D:2D:46:E5:39:BA:EE:F8:BC:00:FC:33:9B:59:05:67:74:A3:06:99:DE:8D:28:55:00:DB:76:1C:68:BC:1E:DB:F9:CD:51:D8:D5:ED:C6:8A:D2:8F:79:45:EB:79:51:9E:27:56:87:8F:F4:90:60:4E:DC:22:3C:7B:B4:F7:1D:E7:A6:C4:89:DE:69:4E:07:BE:78:44:A6:CA:25:D6:C3:90:93:85:02:22:4E:C5:F0:62:1A:E2:EC:CE:DA:F0:1E:D3:C3:58:73:F7:26:40:20:F3:B8:0D:32:5F:56:C9:61:9D:9C:E9:EB:7B:17:1B:A9:48:06:D7:41:AE:7E:1E:4B:ED:6B:8A:98:AA:20:53:A5:04:2B:61:6C:BB:AA:54:6D:CF:0C:F7:4C:7A:16:DD:BA:51:E4:4F:81:B0:B7:70:8D:2A:B8:EE:BA:76:6F:F3:8B:4E:B3:5E:C7:9F:59:C8:DE:7B:B4:1F:C0:B6:D2:00:B2:41:05:73:B7:21:F6:D1:9E:19:27:A6:18:4C:84:74:78:22:C1:D9:62:25:0C:CE:FA:E7:DF:98:8E:19:AC:0F:BF:CD:9F:04:72:63:F4:89:57:1F:8D:88:C0:C0:0B:5B:CD:B9:E7:DA:F8:9D:74:FF:98:68:37:C9:1E:CD:16:A2:7D:25:4C:2F:25:54:8A:64:88:03:41:70:4C:DA:2E:6A:8F:0D:2F:AB:AA:AE:F7:0D:FE:DA:75:99:F5:79:86:11:80:EE:A8:FB:30:CB:C0:BD:2C:60:8
D:DB:BB:5E:01:24:45:B8:BD:89:EB:EC:89:0E:6B:D7:B1:78:E5:DC:05:A2:6C:91:BD:43:8C:44:62:EF:87:D8:DE:1F:87:55:C4:15:F7:2D:80:F3:67:38:67:2C:F3:9B:77:3C:03:BA:CC:93:B1:3D:E1:12:96:37:3F:F2:C1:71:67:73:75:2D:2C:D4:38:96:10:A6:10:CD:7A:F2:01:F7:55:86:17:6E:EF:D6:C8:86:1E:51:09:07:E9:70:7E:EB:A6:C7:D2:36:FF:E6:05:F0:CF:12:D5:41:61:1E:92:62:FE:7C:FD:9A:F9:1E:14:AC:FF:63:4D:6D:AF:B5:F2:9F:F2:4B:FE:2D:EB:45:7F:68:A9:D0:F0:83:36:6A:30:5D:8A:9D:E4:00:CF:17:FA:0A:DB:2D:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *66:38:F3:C2:5A:8D:DF:AF:37:AD:61:D9:3C:1A:1D:3E:17:67:07:75*

Authority Key Identifier *18:87:56:E0:6E:77:EE:24:35:3C:4E:73:9A:1F:D6:E1:E2:79:7E:2B*

Certificate Policies *Policy OID: 1.2.250.1.177.2.0.1.1*

CPS pointer: https://www.certigna.fr/autorites/

Authority Info Access *http://autorite.certigna.fr/certignarootca.der*

http://autorite.dhimyotis.com/certignarootca.der

CRL Distribution Points *http://crl.certigna.fr/certignarootca.crl*

http://crl.dhimyotis.com/certignarootca.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *73:6B:99:6D:33:96:84:72:9C:43:CB:39:7D:1B:B2:B2:F3:F4:A7:81:6A:5E:3C:5D:58:92:03:F8:85:C5:D4:7C*

X509SubjectName

Subject CN: *Certigna Identity Plus CA*

Subject 2.5.4.97: *NTRFR-48146308100036*

Subject OU: *0002 48146308100036*

Subject O: *DHIMYOTIS*

Subject C: *FR*

X509SKI

X509 SK I *ZjjzwlqN3683rWHZPBodPhdnB3U=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2017-04-30T22:00:00Z*

TSP Service Definition URI

URI *[en]* *http://politique.certigna.fr/en/PCcertignaidentityplusca.pdf*

URI *[fr]* *http://politique.certigna.fr/PCcertignaidentityplusca.pdf*

8.3.1 - Extension (critical): Qualifiers [QCWithQSCD]

Qualifier type description *[en]* *undefined.*

[fr] *undefined.*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithQSCD*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Policy Identifier nodes:

Identifier *1.2.250.1.177.2.4.1.6.1*

8.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

8.4 - Service (granted): Certigna Identity Plus CA - ID ** Pro - 1.2.250.1.177.2.4.1.1.1

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Certigna Identity Plus CA - ID ** Pro - 1.2.250.1.177.2.4.1.1.1*

Name *[fr]* *Certigna Identity Plus CA - ID ** Pro - 1.2.250.1.177.2.4.1.1.1*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *263614261279511986064484843886564435021*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIHFzCCBP+gAwIBAgIRAMZSQoyDlJwTf12f6/JxZE0wDQYJKoZIhvcNAQELBQAwWjELMAkGA1UE
BhMCRlIxEjAQBgNVBAoMCUNoaW15b3RpczEcMBoGA1UECwwTMDAwMiA0ODE0NjMwODEwMDAzNjEZ
MBcGA1UEAwwQQ2VydGlnbmEgUm9vdCBDQTAeFw0xNTExMjUwOTMwNTFaFw0zMzA2MDMwOTMwNTFa
MIGCMQswCQYDVQQGEwJGUjESMBAGA1UECgwJREhJTVlPVElTMRwwGgYDVQQLDBMwMDAyIDQ4MTQ2
MzA4MTAwMDM2MR0wGwYDVQRhDBROVFJGUi00ODE0NjMwODEwMDAzNjEiMCAGA1UEAwwZQ2VydGln
bmEgSWRlbnRpdHkgUGx1cyBDQTCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAMfolTzF
jsvedPYwvO3ph5U+t8tmXWjPCSg7pRdR7Ip5dhBqmdENIQ2THhBQKzjEX9fdwHQr9EUxUtZMWF93
HAlj03o2ZgNtLUblObru+LwA/DObWQVndKMGmd6NKFUA23YcaLwe2/nNUdjV7caK0o95Ret5UZ4n
VoeP9JBgTtwiPHu09x3npsSJ3mlOB754RKbKJdbDkJOFAiJOxfBiGuLsztrwHtPDWHP3JkAg87gN
Ml9WyWGdnOnrexcbqUgG10Gufh5L7WuKmKogU6UEK2Fsu6pUbc8M90x6Ft26UeRPgbC3cI0quO66
dm/zi06zXsefWcjee7QfwLbSALJBBXO3IfbRnhknphhMhHR4IsHZYiUMzvrn35iOGawPv82fBHJj
9llXH42IwMALW82559r4nXT/mGg3yR7NFqJ9JUwvJVSKZIgDQXBM2i5qjw0vq6qu9w3+2nWZ9XmG
EYDuqPswy8C9LGCN27teASRFuL2J6+yJDmvXsXjl3AWibJG9Q4xEYu+H2N4fh1XEFfctgPNnOGcs
85t3PAO6zJOxPeESljc/8sFxZ3N1LSzUOJYQphDNevIB91WGF27v1siGHlEJB+lwfuumx9I2/+YF
8M8S1UFhHpJi/nz9mvkeFKz/Y01tr7Xyn/JL/i3rRX9oqdDwgzZqMF2KneQAzxf6CtstAgMBAAGj
ggGtMIIBqTASBgNVHRMBAf8ECDAGAQH/AgEAMA4GA1UdDwEB/wQEAwIBBjAdBgNVHQ4EFgQUZjjz
wlqN3683rWHZPBodPhdnB3UwHwYDVR0jBBgwFoAUGIdW4G537iQ1PE5zmh/W4eJ5fiswSQYDVR0g
BEIwQDA+BgoqgXoBgTECAAEBMDAwLgYIKwYBBQUHAgEWImh0dHBzOi8vd3d3LmNlcnRpZ25hLmZy
L2F1dG9yaXRlcy8wgYgGCCsGAQUFBwEBBHwwejA6BggrBgEFBQcwAoYuaHR0cDovL2F1dG9yaXRl
LmNlcnRpZ25hLmZyL2NlcnRpZ25hcm9vdGNhLmRlcjA8BggrBgEFBQcwAoYwaHR0cDovL2F1dG9y
aXRlLmRoaW15b3Rpcy5jb20vY2VydGlnbmFyb290Y2EuZGVyMG0GA1UdHwRmMGQwL6AtoCuGKWh0
dHA6Ly9jcmwuY2VydGlnbmEuZnIvY2VydGlnbmFyb290Y2EuY3JsMDGgL6AthitodHRwOi8vY3Js
LmRoaW15b3Rpcy5jb20vY2VydGlnbmFyb290Y2EuY3JsMA0GCSqGSIb3DQEBCwUAA4ICAQC75ZUB
BzkUGAgcPanEMIYXFQaMMbdkRqW2jnGZTCKn7ahguFGl4/VwDN7oT9Yw7LqFLNZumbKFR+QUOlFi
4DiqWUqFbYle8ir3gZBLMiGpD8fO4qbhDfMRLJytJ1UWZN0zHov5KC6w14SQVoyUH6tbq7FYX99K
qQ5Twjq2Z8+pVQGiz7cay107Hod/86gl9SAEq+YIdKlgfax+GKi6wo18m1Z6NuGQp1SYfVnO1eWd
PyNRAIv9Y4N/vZkxV6ct9KuNAv1DB4CSjuYJVyO1UIk2LNqYTZUQPEXUpdgXFoiLKqWgvysgxh0n
r+IrzblClUusEpOOIPVCRTlkLQNKLXh6rTgltjeqIF16ksYjag0Km7qSP4dLK9+vQ6y38YfTE3Z
PjH6inK5o9jU+3bgch7sY8whZzm57768SZXSndRS4DSaMlUieZV4flCAKQ0l85Bu7tSAIPtdT0XO
5gquusAW1fTclq2Z7JBOBdlMjsRG9Zlq9cZ9tCt1Pty43D6I/GGQXAP/hri47oquz2pSqDwOqt7t
GvPP+pSYDEgRFJ5WcrwAAl/j9kIBteCSveZMaRo5esXgFbzafIXDPh0pPpUGdp8Q2opiWv4OpIBX
PnQZXI1iMnOFBLQyzO+oYV1u3Gbjul8Y3xlst/mB/3KXXEVWUaKp9OXNa2MZkHqEkHinHQ==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Certigna Root CA*

Issuer OU: *0002 48146308100036*

Issuer O: *Dhimyotis*

Issuer C: *FR*

Subject CN: *Certigna Identity Plus CA*

Subject 2.5.4.97: *NTRFR-48146308100036*

Subject OU: *0002 48146308100036*

Subject O: *DHIMYOTIS*

Subject C: *FR*

Valid from: *Wed Nov 25 10:30:51 CET 2015*

Valid to: *Fri Jun 03 11:30:51 CEST 2033*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:C7:E8:95:3C:C5:8E:CB:DE:74:F6:30:BC:ED:E9:87:95:3E:B7:CB:66:5D:68:CF:09:28:3B:A5:17:51:EC:8A:79:76:10:6A:99:D1:0D:21:0D:93:1E:10:50:2B:38:C4:5F:D7:DD:C0:74:2B:F4:45:31:52:D6:4C:58:5F:77:1C:09:63:D3:7A:36:66:03:6D:2D:46:E5:39:BA:EE:F8:BC:00:FC:33:9B:59:05:67:74:A3:06:99:DE:8D:28:55:00:DB:76:1C:68:BC:1E:DB:F9:CD:51:D8:D5:ED:C6:8A:D2:8F:79:45:EB:79:51:9E:27:56:87:8F:F4:90:60:4E:DC:22:3C:7B:B4:F7:1D:E7:A6:C4:89:DE:69:4E:07:BE:78:44:A6:CA:25:D6:C3:90:93:85:02:22:4E:C5:F0:62:1A:E2:EC:CE:DA:F0:1E:D3:C3:58:73:F7:26:40:20:F3:B8:0D:32:5F:56:C9:61:9D:9C:E9:EB:7B:17:1B:A9:48:06:D7:41:AE:7E:1E:4B:ED:6B:8A:98:AA:20:53:A5:04:2B:61:6C:BB:AA:54:6D:CF:0C:F7:4C:7A:16:DD:BA:51:E4:4F:81:B0:B7:70:8D:2A:B8:EE:BA:76:6F:F3:8B:4E:B3:5E:C7:9F:59:C8:DE:7B:B4:1F:C0:B6:D2:00:B2:41:05:73:B7:21:F6:D1:9E:19:27:A6:18:4C:84:74:78:22:C1:D9:62:25:0C:CE:FA:E7:DF:98:8E:19:AC:0F:BF:CD:9F:04:72:63:F4:89:57:1F:8D:88:C0:C0:0B:5B:CD:B9:E7:DA:F8:9D:74:FF:98:68:37:C9:1E:CD:16:A2:7D:25:4C:2F:25:54:8A:64:88:03:41:70:4C:DA:2E:6A:8F:0D:2F:AB:AA:AE:F7:0D:FE:DA:75:99:F5:79:86:11:80:EE:A8:FB:30:CB:C0:BD:2C:60:8
D:DB:BB:5E:01:24:45:B8:BD:89:EB:EC:89:0E:6B:D7:B1:78:E5:DC:05:A2:6C:91:BD:43:8C:44:62:EF:87:D8:DE:1F:87:55:C4:15:F7:2D:80:F3:67:38:67:2C:F3:9B:77:3C:03:BA:CC:93:B1:3D:E1:12:96:37:3F:F2:C1:71:67:73:75:2D:2C:D4:38:96:10:A6:10:CD:7A:F2:01:F7:55:86:17:6E:EF:D6:C8:86:1E:51:09:07:E9:70:7E:EB:A6:C7:D2:36:FF:E6:05:F0:CF:12:D5:41:61:1E:92:62:FE:7C:FD:9A:F9:1E:14:AC:FF:63:4D:6D:AF:B5:F2:9F:F2:4B:FE:2D:EB:45:7F:68:A9:D0:F0:83:36:6A:30:5D:8A:9D:E4:00:CF:17:FA:0A:DB:2D:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *66:38:F3:C2:5A:8D:DF:AF:37:AD:61:D9:3C:1A:1D:3E:17:67:07:75*

Authority Key Identifier *18:87:56:E0:6E:77:EE:24:35:3C:4E:73:9A:1F:D6:E1:E2:79:7E:2B*

Certificate Policies *Policy OID: 1.2.250.1.177.2.0.1.1*

CPS pointer: https://www.certigna.fr/autorites/

Authority Info Access *http://autorite.certigna.fr/certignarootca.der*

http://autorite.dhimyotis.com/certignarootca.der

CRL Distribution Points *http://crl.certigna.fr/certignarootca.crl*

http://crl.dhimyotis.com/certignarootca.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *73:6B:99:6D:33:96:84:72:9C:43:CB:39:7D:1B:B2:B2:F3:F4:A7:81:6A:5E:3C:5D:58:92:03:F8:85:C5:D4:7C*

Certificate fields details

Version: *3*

Serial Number: *625768101432799552817853009833909090 51*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIGHDCCBQSgAwIBAgIQLxPa8YcM1DOPGNv8N2uyezANBgkqhkiG9w0BAQsFADA0MQswCQYDVQQG
EwJGUjESMBAGA1UECgwJRGhpbXlvdGlzMREwDwYDVQQDDAhDZXJ0aWduYTAeFw0xNTExMjUwOTIz
MjVaFw0yNTExMjIwOTIzMjVaMIGCMQswCQYDVQQGEwJGUjESMBAGA1UECgwJREhJTVlPVElTMRww
GgYDVQQLDBMwMDAyIDQ4MTQ2MzA4MTAwMDM2MR0wGwYDVQRhDBROVFJGUi00ODE0NjMwODEwMDAz
NjEiMCAGA1UEAwwZQ2VydGlnbmEgSWRlbnRpdHkgUGx1cyBDQTCCAiIwDQYJKoZIhvcNAQEBBQAD
ggIPADCCAgoCggIBAMfolTzFjsvedPYwvO3ph5U+t8tmXWjPCSg7pRdR7Ip5dhBqmdENIQ2THhBQ
KzjEX9fdwHQr9EUxUtZMWF93HAlj03o2ZgNtLUblObru+LwA/DObWQVndKMGmd6NKFUA23YcaLwe
2/nNUdjV7caK0o95Ret5UZ4nVoeP9JBgTtwiPHu09x3npsSJ3mlOB754RKbKJdbDkJOFAiJOxfBi
GuLsztrwHtPDWHP3JkAg87gNMl9WyWGdnOnrexcbqUgG10Gufh5L7WuKmKogU6UEK2Fsu6pUbc8M
90x6Ft26UeRPgbC3cI0quO66dm/zi06zXsefWcjee7QfwLbSALJBBXO3IfbRnhknphhMhHR4IsHZ
YiUMzvrn35iOGawPv82fBHJj9llXH42IwMALW82559r4nXT/mGg3yR7NFqJ9JUwvJVSKZIgDQXBM
2i5qjw0vq6qu9w3+2nWZ9XmGEYDuqPswy8C9LGCN27teASRFuL2J6+yJDmvXsXjl3AWibJG9Q4xE
Yu+H2N4fh1XEFfctgPNnOGcs85t3PAO6zJOxPeESljc/8sFxZ3N1LSzUOJYQphDNevIB91WGF27v
1siGHlEJB+lwfuumx9I2/+YF8M8S1UFhHpJi/nz9mvkeFKz/Y01tr7Xyn/JL/i3rRX9oqdDwgzZq
MF2KneQAzxf6CtstAgMBAAGjggHZMIIB1TASBgNVHRMBAf8ECDAGAQH/AgEAMA4GA1UdDwEB/wQE
AwIBBjAdBgNVHQ4EFgQUZjjzwlqN3683rWHZPBodPhdnB3UwZAYDVR0jBF0wW4AUGu3+QTmQtCRZ
vgHyUtVF9lo53BGhOKQ2MDQxCzAJBgNVBAYTAkZSMRIwEAYDVQQKDAlEaGlteW90aXMxETAPBgNV
BAMMCENlcnRpZ25hggkA/tzjAQ/JSP8wSQYDVR0gBEIwQDA+BgoqgXoBgTEBAAECMDAwLgYIKwYB
BQUHAgEWImh0dHBzOi8vd3d3LmNlcnRpZ25hLmZyL2F1dG9yaXRlcy8wfAYIKwYBBQUHAQEEcDBu
MDQGCCsGAQUFBzAChihodHRwOi8vYXV0b3JpdGUuY2VydGlnbmEuZnlvY2VydGlnbmEuZGVyMDYG
CCsGAQUFBzAChipodHRwOi8vYXV0b3JpdGUuZGhpbXlvdGlzLmNvbS9jZXJ0aWduYS5kZXIwYQYD
VR0fBFowWDApoCegJYYjaHR0cDovL2NybC5jZXJ0aWduYS5mci9jZXJ0aWduYS5jcmwwK6ApoCeG
JWh0dHA6Ly9jcmwuZGhpbXlvdGlzLmNvbS9jZXJ0aWduYS5jcmwwDQYJKoZIhvcNAQELBQADggEB
AK05XoyuwD1xY8gkIri3eb/mk0rVyRp6Pa9VA8hDNiZqz2ZaVAOKZYP3tvRXTz/vOMlDVO9i66MB
qADiG9smLFB2dWQVojALSbX52V5gyKPglfqY99YPLwuihlrOYSDsuooEc6qZ3RKgK3HnbLAlhTNR
ljgcOkKFYmnMXggsUA5ZhL0fntu+b89FCSbtth3nhoL1gVYZg54ZtyzMi8VmJTMUDk/2nXuzIan6
dZByWdcUfwHj5iGyAnXs09+iQA0q+EyqxKG/7ovWpOndOJIZ576bEy3+WcnxWAdYiBV8tA1Snjit
91RkThbjlz+nzuVJOvYwQwJdBp9lBJoFK2zKHy4=

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Certigna*

Issuer O: *Dhimyotis*

Issuer C: *FR*

Subject CN: *Certigna Identity Plus CA*

Subject 2.5.4.97: *NTRFR-48146308100036*

Subject OU: *0002 48146308100036*

Subject O: *DHIMYOTIS*

Subject C: *FR*

Valid from: *Wed Nov 25 10:23:25 CET 2015*

Valid to: *Sat Nov 22 10:23:25 CET 2025*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:C7:E8:95:3C:C5:8E:CB:DE:74:F6:30:BC:ED:E9:87:95:3E:B7:CB:66:5D:68:CF:09:28:3B:A5:17:51:EC:8A:79:76:10:6A:99:D1:0D:21:0D:93:1E:10:50:2B:38:C4:5F:D7:DD:C0:74:2B:F4:45:31:52:D6:4C:58:5F:77:1C:09:63:D3:7A:36:66:03:6D:2D:46:E5:39:BA:EE:F8:BC:00:FC:33:9B:59:05:67:74:A3:06:99:DE:8D:28:55:00:DB:76:1C:68:BC:1E:DB:F9:CD:51:D8:D5:ED:C6:8A:D2:8F:79:45:EB:79:51:9E:27:56:87:8F:F4:90:60:4E:DC:22:3C:7B:B4:F7:1D:E7:A6:C4:89:DE:69:4E:07:BE:78:44:A6:CA:25:D6:C3:90:93:85:02:22:4E:C5:F0:62:1A:E2:EC:CE:DA:F0:1E:D3:C3:58:73:F7:26:40:20:F3:B8:0D:32:5F:56:C9:61:9D:9C:E9:EB:7B:17:1B:A9:48:06:D7:41:AE:7E:1E:4B:ED:6B:8A:98:AA:20:53:A5:04:2B:61:6C:BB:AA:54:6D:CF:0C:F7:4C:7A:16:DD:BA:51:E4:4F:81:B0:B7:70:8D:2A:B8:EE:BA:76:6F:F3:8B:4E:B3:5E:C7:9F:59:C8:DE:7B:B4:1F:C0:B6:D2:00:B2:41:05:73:B7:21:F6:D1:9E:19:27:A6:18:4C:84:74:78:22:C1:D9:62:25:0C:CE:FA:E7:DF:98:8E:19:AC:0F:BF:CD:9F:04:72:63:F4:89:57:1F:8D:88:C0:C0:0B:5B:CD:B9:E7:DA:F8:9D:74:FF:98:68:37:C9:1E:CD:16:A2:7D:25:4C:2F:25:54:8A:64:88:03:41:70:4C:DA:2E:6A:8F:0D:2F:AB:AA:AE:F7:0D:FE:DA:75:99:F5:79:86:11:80:EE:A8:FB:30:CB:C0:BD:2C:60:8
D:DB:BB:5E:01:24:45:B8:BD:89:EB:EC:89:0E:6B:D7:B1:78:E5:DC:05:A2:6C:91:BD:43:8C:44:62:EF:87:D8:DE:1F:87:55:C4:15:F7:2D:80:F3:67:38:67:2C:F3:9B:77:3C:03:BA:CC:93:B1:3D:E1:12:96:37:3F:F2:C1:71:67:73:75:2D:2C:D4:38:96:10:A6:10:CD:7A:F2:01:F7:55:86:17:6E:EF:D6:C8:86:1E:51:09:07:E9:70:7E:EB:A6:C7:D2:36:FF:E6:05:F0:CF:12:D5:41:61:1E:92:62:FE:7C:FD:9A:F9:1E:14:AC:FF:63:4D:6D:AF:B5:F2:9F:F2:4B:FE:2D:EB:45:7F:68:A9:D0:F0:83:36:6A:30:5D:8A:9D:E4:00:CF:17:FA:0A:DB:2D:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *66:38:F3:C2:5A:8D:DF:AF:37:AD:61:D9:3C:1A:1D:3E:17:67:07:75*

Authority Key Identifier *1A:ED:FE:41:39:90:B4:24:59:BE:01:F2:52:D5:45:F6:5A:39:DC:11*

Certificate Policies *Policy OID: 1.2.250.1.177.1.0.1.2*

CPS pointer: https://www.certigna.fr/autorites/

Authority Info Access *http://autorite.certigna.fr/certigna.der*

http://autorite.dhimyotis.com/certigna.der

CRL Distribution Points *http://crl.certigna.fr/certigna.crl*

http://crl.dhimyotis.com/certigna.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *02:C4:A3:00:A0:9C:1B:89:3B:11:F9:56:76:59:AF:95:BB:B9:BB:E7:95:38:93:E3:6C:5B:AF:17:B5:55:CE:E3*

X509SubjectName

Subject CN: *Certigna Identity Plus CA*

Subject 2.5.4.97: *NTRFR-48146308100036*

Subject OU: *0002 48146308100036*

Subject O: *DHIMYOTIS*

Subject C: *FR*

X509SKI

X509 SK I *ZjjzwlqN3683rWHZPBodPhdnB3U=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2017-04-30T22:00:00Z*

TSP Service Definition URI

URI *[en]* *http://politique.certigna.fr/en/PCcertignaidentityplusca.pdf*

URI *[fr]* *http://politique.certigna.fr/PCcertignaidentityplusca.pdf*

8.4.1 - Extension (critical): Qualifiers [QCWithQSCD]

Qualifier type description *[en]* *undefined.*

[fr] *undefined.*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithQSCD*

Criteria list assert=all

Key Usage *[digitalSignature]* *true*

Key Usage *[nonRepudiation]* *true*

Policy Identifier nodes:

Identifier *1.2.250.1.177.2.4.1.1.1*

8.4.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

8.5 - Service (granted): Certigna Identity Plus CA - ID *** Pro - 1.2.250.1.177.2.4.1.3.1

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Certigna Identity Plus CA - ID *** Pro - 1.2.250.1.177.2.4.1.3.1*

Name *[fr]* *Certigna Identity Plus CA - ID *** Pro - 1.2.250.1.177.2.4.1.3.1*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *263614261279511986064484843886564435021*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIHFzCCBP+gAwIBAgIRAMZSQoyDlJwTf12f6/JxZE0wDQYJKoZIhvcNAQELBQAwWjELMAkGA1UE
BhMCRlIxEjAQBgNVBAoMCUNoaW15b3RpczEcMBoGA1UECwwTMDAwMiA0ODE0NjMwODEwMDAzNjEZ
MBcGA1UEAwwQQ2VydGlnbmEgUm9vdCBDQTAeFw0xNTExMjUwOTMwNTFaFw0zMzA2MDMwOTMwNTFa
MIGCMQswCQYDVQQGEwJGUjESMBAGA1UECgwJREhJTVlPVElTMRwwGgYDVQQLDBMwMDAyIDQ4MTQ2
MzA4MTAwMDM2MR0wGwYDVQRhDBROVFJGUi00ODE0NjMwODEwMDAzNjEiMCAGA1UEAwwZQ2VydGln
bmEgSWRlbnRpdHkgUGx1cyBDQTCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAMfolTzF
jsvedPYwvO3ph5U+t8tmXWjPCSg7pRdR7Ip5dhBqmdENIQ2THhBQKzjEX9fdwHQr9EUxUtZMWF93
HAlj03o2ZgNtLUblObru+LwA/DObWQVndKMGmd6NKFUA23YcaLwe2/nNUdjV7caK0o95Ret5UZ4n
VoeP9JBgTtwiPHu09x3npsSJ3mlOB754RKbKJdbDkJOFAiJOxfBiGuLsztrwHtPDWHP3JkAg87gN
Ml9WyWGdnOnrexcbqUgG10Gufh5L7WuKmKogU6UEK2Fsu6pUbc8M90x6Ft26UeRPgbC3cI0quO66
dm/zi06zXsefWcjee7QfwLbSALJBBXO3IfbRnhknphhMhHR4IsHZYiUMzvrn35iOGawPv82fBHJj
9IlXH42IwMALW82559r4nXT/mGg3yR7NFqJ9JUwvJVSKZIgDQXBM2i5qjw0vq6qu9w3+2nWZ9XmG
EYDuqPswy8C9LGCN27teASRFuL2J6+yJDmvXsXjl3AWibJG9Q4xEYu+H2N4fh1XEFfctgPNnOGcs
85t3PAO6zJOxPeESljc/8sFxZ3N1LSzUOJYQphDNevIB91WGF27v1siGHlEJB+lwfuumx9I2/+YF
8M8S1UFhHpJi/nz9mvkeFKz/Y01tr7Xyn/JL/i3rRX9oqdDwgzZqMF2KneQAzxf6CtstAgMBAAGj
ggGtMIIBqTASBgNVHRMBAf8ECDAGAQH/AgEAMA4GA1UdDwEB/wQEAwIBBjAdBgNVHQ4EFgQUZjjz
wlqN3683rWHZPBodPhdnB3UwHwYDVR0jBBgwFoAUGldW4G537iQ1PE5zmh/W4eJ5fiswSQYDVR0g
BEIwQDA+BgoqgXoBgTECAAEBMDAwLgYIKwYBBQUHAgEWImh0dHBzOi8vd3d3LmNlcnRpZ25hLmZy
L2F1dG9yaXRlcy8wgYgGCCsGAQUFBwEBBHwwejA6BggrBgEFBQcwAoYuaHR0cDovL2F1dG9yaXRl
LmNlcnRpZ25hLmZyL2NlcnRpZ25hcm9vdGNhLmRlcjA8BggrBgEFBQcwAoYwaHR0cDovL2F1dG9y
aXRlLmRoaW15b3Rpcy5jb20vY2VydGlnbmFyb290Y2EuZGVyMG0GA1UdHwRmMGQwL6AtoCuGKWh0
dHA6Ly9jcmwuY2VydGlnbmEuZnIvY2VydGlnbmFyb290Y2EuY3JsMDGgL6AthitodHRwOi8vY3Js
LmRoaW15b3Rpcy5jb20vY2VydGlnbmFyb290Y2EuY3JsMA0GCSqGSIb3DQEBCwUAA4ICAQC75ZUB
BzkUGAgcPanEMIYXFQaMMbdkRqW2jnGZTCKn7ahguFGl4/VwDN7oT9Yw7LqFLNZumbKFR+QUOlFi
4DiqWUqFbYle8ir3gZBLMiGpD8fO4qbhDfMRLJytJ1UWZN0zHov5KC6w14SQVoyUH6tbq7FYX99K
qQ5Twjq2Z8+pVQGiz7cay107Hod/86gl9SAEq+YIdKlgfax+GKi6wo18m1Z6NuGQp1SYfVnO1eWd
PyNRAIv9Y4N/vZkxV6ct9KuNAv1DB4CSjuYJVyO1UIk2LNqYTZUQPEXUpdgXFoiLKqWgvysgxh0n
r+IrzblClUusEpOOIPVCRTlkLQNKLXh6rTgIltjeqIF16ksYjag0Km7qSP4dLK9+vQ6y38YfTE3Z
PjH6inK5o9jU+3bgch7sY8whZzm57768SZXSndRS4DSaMlUieZV4flCAKQ0I85Bu7tSAIPtdT0XO
5gquusAW1fTclq2Z7JBOBdlMjsRG9ZIq9cZ9tCt1Pty43D6I/GGQXAP/hri47oquz2pSqDwOqt7t
GvPP+pSYDEgRFJ5WcrwAAl/j9kIBteCSveZMaRo5esXgFbzafIXDPh0pPpUGdp8Q2opiWv4OpIBX
PnQZXI1iMnOFBLQyzO+oYV1u3Gbjul8Y3xlst/mB/3KXXEVWUaKp9OXNa2MZkHqEkHinHQ==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Certigna Root CA*

Issuer OU: *0002 48146308100036*

Issuer O: *Dhimyotis*

Issuer C: *FR*

Subject CN: *Certigna Identity Plus CA*

Subject 2.5.4.97: *NTRFR-48146308100036*

Subject OU: *0002 48146308100036*

Subject O: *DHIMYOTIS*

Subject C: *FR*

Valid from: *Wed Nov 25 10:30:51 CET 2015*

Valid to: *Fri Jun 03 11:30:51 CEST 2033*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:C7:E8:95:3C:C5:8E:CB:DE:74:F6:30:BC:ED:E9:87:95:3E:B7:CB:66:5D:68:CF:09:28:3B:A5:17:51:EC:8A:79:76:10:6A:99:D1:0D:21:0D:93:1E:10:50:2B:38:C4:5F:D7:DD:C0:74:2B:F4:45:31:52:D6:4C:58:5F:77:1C:09:63:D3:7A:36:66:03:6D:2D:46:E5:39:BA:EE:F8:BC:00:FC:33:9B:59:05:67:74:A3:06:99:DE:8D:28:55:00:DB:76:1C:68:BC:1E:DB:F9:CD:51:D8:D5:ED:C6:8A:D2:8F:79:45:EB:79:51:9E:27:56:87:8F:F4:90:60:4E:DC:22:3C:7B:B4:F7:1D:E7:A6:C4:89:DE:69:4E:07:BE:78:44:A6:CA:25:D6:C3:90:93:85:02:22:4E:C5:F0:62:1A:E2:EC:CE:DA:F0:1E:D3:C3:58:73:F7:26:40:20:F3:B8:0D:32:5F:56:C9:61:9D:9C:E9:EB:7B:17:1B:A9:48:06:D7:41:AE:7E:1E:4B:ED:6B:8A:98:AA:20:53:A5:04:2B:61:6C:BB:AA:54:6D:CF:0C:F7:4C:7A:16:DD:BA:51:E4:4F:81:B0:B7:70:8D:2A:B8:EE:BA:76:6F:F3:8B:4E:B3:5E:C7:9F:59:C8:DE:7B:B4:1F:C0:B6:D2:00:B2:41:05:73:B7:21:F6:D1:9E:19:27:A6:18:4C:84:74:78:22:C1:D9:62:25:0C:CE:FA:E7:DF:98:8E:19:AC:0F:BF:CD:9F:04:72:63:F4:89:57:1F:8D:88:C0:C0:0B:5B:CD:B9:E7:DA:F8:9D:74:FF:98:68:37:C9:1E:CD:16:A2:7D:25:4C:2F:25:54:8A:64:88:03:41:70:4C:DA:2E:6A:8F:0D:2F:AB:AA:AE:F7:0D:FE:DA:75:99:F5:79:86:11:80:EE:A8:FB:30:CB:C0:BD:2C:60:8
D:DB:BB:5E:01:24:45:B8:BD:89:EB:EC:89:0E:6B:D7:B1:78:E5:DC:05:A2:6C:91:BD:43:8C:44:62:EF:87:D8:DE:1F:87:55:C4:15:F7:2D:80:F3:67:38:67:2C:F3:9B:77:3C:03:BA:CC:93:B1:3D:E1:12:96:37:3F:F2:C1:71:67:73:75:2D:2C:D4:38:96:10:A6:10:CD:7A:F2:01:F7:55:86:17:6E:EF:D6:C8:86:1E:51:09:07:E9:70:7E:EB:A6:C7:D2:36:FF:E6:05:F0:CF:12:D5:41:61:1E:92:62:FE:7C:FD:9A:F9:1E:14:AC:FF:63:4D:6D:AF:B5:F2:9F:F2:4B:FE:2D:EB:45:7F:68:A9:D0:F0:83:36:6A:30:5D:8A:9D:E4:00:CF:17:FA:0A:DB:2D:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *66:38:F3:C2:5A:8D:DF:AF:37:AD:61:D9:3C:1A:1D:3E:17:67:07:75*

Authority Key Identifier *18:87:56:E0:6E:77:EE:24:35:3C:4E:73:9A:1F:D6:E1:E2:79:7E:2B*

Certificate Policies *Policy OID: 1.2.250.1.177.2.0.1.1*

CPS pointer: https://www.certigna.fr/autorites/

Authority Info Access *http://autorite.certigna.fr/certignarootca.der*

http://autorite.dhimyotis.com/certignarootca.der

CRL Distribution Points *http://crl.certigna.fr/certignarootca.crl*

http://crl.dhimyotis.com/certignarootca.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *73:6B:99:6D:33:96:84:72:9C:43:CB:39:7D:1B:B2:B2:F3:F4:A7:81:6A:5E:3C:5D:58:92:03:F8:85:C5:D4:7C*

Certificate fields details

Version: *3*

Serial Number: *625768101432799552817853009833909090 51*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIGHDCCBQSgAwIBAgIQLxPa8YcM1DOPGNv8N2uyezANBgkqhkiG9w0BAQsFADA0MQswCQYDVQQG
EwJGUjESMBAGA1UECgwJRGhpbXlvdGlzMREwDwYDVQQDDAhDZXJ0aWduYTAeFw0xNTExMjUwOTIz
MjVaFw0yNTExMjIwOTIzMjVaMIGCMQswCQYDVQQGEwJGUjESMBAGA1UECgwJREhJTVlPVElTMRww
GgYDVQQLDBMwMDAyIDQ4MTQ2MzA4MTAwMDM2MR0wGwYDVQRhDBROVFJGUi00ODE0NjMwODEwMDAz
NjEiMCAGA1UEAwwZQ2VydGlnbmEgSWRlbnRpdHkgUGx1cyBDQTCCAiIwDQYJKoZIhvcNAQEBBQAD
ggIPADCCAgoCggIBAMfolTzFjsvedPYwvO3ph5U+t8tmXWjPCSg7pRdR7Ip5dhBqmdENIQ2THhBQ
KzjEX9fdwHQr9EUxUtZMWF93HAlj03o2ZgNtLUblObru+LwA/DObWQVndKMGmd6NKFUA23YcaLwe
2/nNUdjV7caK0o95Ret5UZ4nVoeP9JBgTtwiPHu09x3npsSJ3mlOB754RKbKJdbDkJOFAiJOxfBi
GuLsztrwHtPDWHP3JkAg87gNMl9WyWGdnOnrexcbqUgG10Gufh5L7WuKmKogU6UEK2Fsu6pUbc8M
90x6Ft26UeRPgbC3cI0quO66dm/zi06zXsefWcjee7QfwLbSALJBBXO3IfbRnhknphhMhHR4IsHZ
YiUMzvrn35iOGawPv82fBHJj9llXH42IwMALW82559r4nXT/mGg3yR7NFqJ9JUwvJVSKZIgDQXBM
2i5qjw0vq6qu9w3+2nWZ9XmGEYDuqPswy8C9LGCN27teASRFuL2J6+yJDmvXsXjl3AWibJG9Q4xE
Yu+H2N4fh1XEFfctgPNnOGcs85t3PAO6zJOxPeESljc/8sFxZ3N1LSzUOJYQphDNevIB91WGF27v
1siGHlEJB+lwfuumx9I2/+YF8M8S1UFhHpJi/nz9mvkeFKz/Y01tr7Xyn/JL/i3rRX9oqdDwgzZq
MF2KneQAzxf6CtstAgMBAAGjggHZMIIB1TASBgNVHRMBAf8ECDAGAQH/AgEAMA4GA1UdDwEB/wQE
AwIBBjAdBgNVHQ4EFgQUZjjzwlqN3683rWHZPBodPhdnB3UwZAYDVR0jBF0wW4AUGu3+QTmQtCRZ
vgHyUtVF9lo53BGhOKQ2MDQxCzAJBgNVBAYTAkZSMRIwEAYDVQQKDAlEaGlteW90aXMxETAPBgNV
BAMMCENlcnRpZ25hggkA/tzjAQ/JSP8wSQYDVR0gBEIwQDA+BgoqgXoBgTEBAAECMDAwLgYIKwYB
BQUHAgEWImh0dHBzOi8vd3d3LmNlcnRpZ25hLmZyL2F1dG9yaXRlcy8wfAYIKwYBBQUHAQEEcDBu
MDQGCCsGAQUFBzAChihodHRwOi8vYXV0b3JpdGUuY2VydGlnbmEuZnlvY2VydGlnbmEuZGVyMDYG
CCsGAQUFBzAChipodHRwOi8vYXV0b3JpdGUuZGhpbXlvdGlzLmNvbS9jZXJ0aWduYS5kZXIwYQYD
VR0fBFowWDApoCegJYYjaHR0cDovL2NybC5jZXJ0aWduYS5mci9jZXJ0aWduYS5jcmwwK6ApoCeG
JWh0dHA6Ly9jcmwuZGhpbXlvdGlzLmNvbS9jZXJ0aWduYS5jcmwwDQYJKoZIhvcNAQELBQADggEB
AK05XoyuwD1xY8gkIri3eb/mk0rVyRp6Pa9VA8hDNiZqz2ZaVAOKZYP3tvRXTz/vOMlDVO9i66MB
qADiG9smLFB2dWQVojALSbX52V5gyKPglfqY99YPLwuihlrOYSDsuooEc6qZ3RKgK3HnbLAlhTNR
ljgcOkKFYmnMXggsUA5ZhL0fntu+b89FCSbtth3nhoL1gVYZg54ZtyzMi8VmJTMUDk/2nXuzIan6
dZByWdcUfwHj5iGyAnXs09+iQA0q+EyqxKG/7ovWpOndOJIZ576bEy3+WcnxWAdYiBV8tA1Snjit
91RkThbjIz+nzuVJOvYwQwJdBp9lBJoFK2zKHy4=

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Certigna*

Issuer O: *Dhimyotis*

Issuer C: *FR*

Subject CN: *Certigna Identity Plus CA*

Subject 2.5.4.97: *NTRFR-48146308100036*

Subject OU: *0002 48146308100036*

Subject O: *DHIMYOTIS*

Subject C: *FR*

Valid from: *Wed Nov 25 10:23:25 CET 2015*

Valid to: *Sat Nov 22 10:23:25 CET 2025*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:C7:E8:95:3C:C5:8E:CB:DE:74:F6:30:BC:ED:E9:87:95:3E:B7:CB:66:5D:68:CF:09:28:3B:A5:17:51:EC:8A:79:76:10:6A:99:D1:0D:21:0D:93:1E:10:50:2B:38:C4:5F:D7:DD:C0:74:2B:F4:45:31:52:D6:4C:58:5F:77:1C:09:63:D3:7A:36:66:03:6D:2D:46:E5:39:BA:EE:F8:BC:00:FC:33:9B:59:05:67:74:A3:06:99:DE:8D:28:55:00:DB:76:1C:68:BC:1E:DB:F9:CD:51:D8:D5:ED:C6:8A:D2:8F:79:45:EB:79:51:9E:27:56:87:8F:F4:90:60:4E:DC:22:3C:7B:B4:F7:1D:E7:A6:C4:89:DE:69:4E:07:BE:78:44:A6:CA:25:D6:C3:90:93:85:02:22:4E:C5:F0:62:1A:E2:EC:CE:DA:F0:1E:D3:C3:58:73:F7:26:40:20:F3:B8:0D:32:5F:56:C9:61:9D:9C:E9:EB:7B:17:1B:A9:48:06:D7:41:AE:7E:1E:4B:ED:6B:8A:98:AA:20:53:A5:04:2B:61:6C:BB:AA:54:6D:CF:0C:F7:4C:7A:16:DD:BA:51:E4:4F:81:B0:B7:70:8D:2A:B8:EE:BA:76:6F:F3:8B:4E:B3:5E:C7:9F:59:C8:DE:7B:B4:1F:C0:B6:D2:00:B2:41:05:73:B7:21:F6:D1:9E:19:27:A6:18:4C:84:74:78:22:C1:D9:62:25:0C:CE:FA:E7:DF:98:8E:19:AC:0F:BF:CD:9F:04:72:63:F4:89:57:1F:8D:88:C0:C0:0B:5B:CD:B9:E7:DA:F8:9D:74:FF:98:68:37:C9:1E:CD:16:A2:7D:25:4C:2F:25:54:8A:64:88:03:41:70:4C:DA:2E:6A:8F:0D:2F:AB:AA:AE:F7:0D:FE:DA:75:99:F5:79:86:11:80:EE:A8:FB:30:CB:C0:BD:2C:60:8
D:DB:BB:5E:01:24:45:B8:BD:89:EB:EC:89:0E:6B:D7:B1:78:E5:DC:05:A2:6C:91:BD:43:8C:44:62:EF:87:D8:DE:1F:87:55:C4:15:F7:2D:80:F3:67:38:67:2C:F3:9B:77:3C:03:BA:CC:93:B1:3D:E1:12:96:37:3F:F2:C1:71:67:73:75:2D:2C:D4:38:96:10:A6:10:CD:7A:F2:01:F7:55:86:17:6E:EF:D6:C8:86:1E:51:09:07:E9:70:7E:EB:A6:C7:D2:36:FF:E6:05:F0:CF:12:D5:41:61:1E:92:62:FE:7C:FD:9A:F9:1E:14:AC:FF:63:4D:6D:AF:B5:F2:9F:F2:4B:FE:2D:EB:45:7F:68:A9:D0:F0:83:36:6A:30:5D:8A:9D:E4:00:CF:17:FA:0A:DB:2D:02:03:01:00:01

Basic Constraints	*IsCA: true - Path length: 0*
Subject Key Identifier	*66:38:F3:C2:5A:8D:DF:AF:37:AD:61:D9:3C:1A:1D:3E:17:67:07:75*
Authority Key Identifier	*1A:ED:FE:41:39:90:B4:24:59:BE:01:F2:52:D5:45:F6:5A:39:DC:11*
Certificate Policies	*Policy OID: 1.2.250.1.177.1.0.1.2* *CPS pointer: https://www.certigna.fr/autorites/*
Authority Info Access	*http://autorite.certigna.fr/certigna.der* *http://autorite.dhimyotis.com/certigna.der*
CRL Distribution Points	*http://crl.certigna.fr/certigna.crl* *http://crl.dhimyotis.com/certigna.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*02:C4:A3:00:A0:9C:1B:89:3B:11:F9:56:76:59:AF:95:BB:B9:BB:E7:95:38:93:E3:6C:5B:AF:17:B5:55:CE:E3*

X509SubjectName

Subject CN:	*Certigna Identity Plus CA*
Subject 2.5.4.97:	*NTRFR-48146308100036*
Subject OU:	*0002 48146308100036*
Subject O:	*DHIMYOTIS*
Subject C:	*FR*
X509 SK I	*ZjjzwlqN3683rWHZPBodPhdnB3U=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2017-04-30T22:00:00Z*

TSP Service Definition URI

URI *[en]* *http://politique.certigna.fr/en/PCcertignaidentityplusca.pdf*

URI *[fr]* *http://politique.certigna.fr/PCcertignaidentityplusca.pdf*

8.5.1 - Extension (critical): Qualifiers [QCWithQSCD]

Qualifier type description *[en]* *undefined.*

[fr] *undefined.*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithQSCD*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Policy Identifier nodes:

Identifier *1.2.250.1.177.2.4.1.3.1*

8.5.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

8.6 - Service (granted): Certigna Identity Plus CA - ID ** - 1.2.250.1.177.2.4.1.4.1

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Certigna Identity Plus CA - ID ** - 1.2.250.1.177.2.4.1.4.1*

Name *[fr]* *Certigna Identity Plus CA - ID ** - 1.2.250.1.177.2.4.1.4.1*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *263614261279511986064484843886564435021*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIHFzCCBP+gAwIBAgIRAMZSQoyDlJwTf12f6/JxZE0wDQYJKoZIhvcNAQELBQAwWjELMAkGA1UE
BhMCRlIxEjAQBgNVBAoMCURoaW15b3RpczEcMBoGA1UECwwTMDAwMiA0ODE0NjMwODEwMDAzNjEZ
MBcGA1UEAwwQQ2VydGlnbmEgUm9vdCBDQTAeFw0xNTExMjUwOTMwNTFaFw0zMzA2MDMwOTMwNTFa
MIGCMQswCQYDVQQGEwJGUjESMBAGA1UECgwJREhJTVlPVElTMRwwGgYDVQQLDBMwMDAyIDQ4MTQ2
MzA4MTAwMDM2MR0wGwYDVQRhDBROVFJGUi00ODE0NjMwODEwMDAzNjEiMCAGA1UEAwwZQ2VydGln
bmEgSWRlbnRpdHkgUGx1cyBDQTCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAMfolTzF
jsvedPYwvO3ph5U+t8tmXWjPCSg7pRdR7Ip5dhBqmdENIQ2THhBQKzjEX9fdwHQr9EUxUtZMWF93
HAlj03o2ZgNtLUblObru+LwA/DObWQVndKMGmd6NKFUA23YcaLwe2/nNUdjV7caK0o95Ret5UZ4n
VoeP9JBgTtwiPHu09x3npsSJ3mlOB754RKbKJdbDkJOFAiJOxfBiGuLsztrwHtPDWHP3JkAg87gN
Ml9WyWGdnOnrexcbqUgG10Gufh5L7WuKmKogU6UEK2Fsu6pUbc8M90x6Ft26UeRPgbC3cI0quO66
dm/zi06zXsefWcjee7QfwLbSALJBBXO3IfbRnhknphhMhHR4IsHZYiUMzvrn35iOGawPv82fBHJj
9llXH42IwMALW82559r4nXT/mGg3yR7NFqJ9JUwvJVSKZIgDQXBM2i5qjw0vq6qu9w3+2nWZ9XmG
EYDuqPswy8C9LGCN27teASRFuL2J6+yJDmvXsXjl3AWibJG9Q4xEYu+H2N4fh1XEFfctgPNnOGcs
85t3PAO6zJOxPeESljc/8sFxZ3N1LSzUOJYQphDNevIB91WGF27v1siGHlEJB+lwfuumx9I2/+YF
8M8S1UFhHpJi/nz9mvkeFKz/Y01tr7Xyn/JL/i3rRX9oqdDwgzZqMF2KneQAzxf6CtstAgMBAAGj
ggGtMIIBqTASBgNVHRMBAf8ECDAGAQH/AgEAMA4GA1UdDwEB/wQEAwIBBjAdBgNVHQ4EFgQUZjjz
wlqN3683rWHZPBodPhdnB3UwHwYDVR0jBBgwFoAUGIdW4G537iQ1PE5zmh/W4eJ5fiswSQYDVR0g
BEIwQDA+BgoqgXoBgTECAAEBMDAwLgYIKwYBBQUHAgEWImh0dHBzOi8vd3d3LmNlcnRpZ25hLmZy
L2F1dG9yaXRlcy8wgYgGCCsGAQUFBwEBBHwwejA6BggrBgEFBQcwAoYuaHR0cDovL2F1dG9yaXRl
LmNlcnRpZ25hLmZyL2NlcnRpZ25hcm9vdGNhLmRlcjA8BggrBgEFBQcwAoYwaHR0cDovL2F1dG9y
aXRlLmRoaW15b3Rpcy5jb20vY2VydGlnbmFyb290Y2EuZGVyMG0GA1UdHwRmMGQwL6AtoCuGKWh0
dHA6Ly9jcmwuY2VydGlnbmEuZnIvY2VydGlnbmFyb290Y2EuY3JsMDGgL6AthitodHRwOi8vY3Js
LmRoaW15b3Rpcy5jb20vY2VydGlnbmFyb290Y2EuY3JsMA0GCSqGSIb3DQEBCwUAA4ICAQC75ZUB
BzkUGAgcPanEMIYXFQaMMbdkRqW2jnGZTCKn7ahguFGl4/VwDN7oT9Yw7LqFLNZumbKFR+QUOlFi
4DiqWUqFbYle8ir3gZBLMiGpD8fO4qbhDfMRLJytJ1UWZN0zHov5KC6w14SQVoyUH6tbq7FYX99K
qQ5Twjq2Z8+pVQGiz7cay107Hod/86gl9SAEq+YIdKlgfax+GKi6wo18m1Z6NuGQp1SYfVnO1eWd
PyNRAIv9Y4N/vZkxV6ct9KuNAv1DB4CSjuYJVyO1UIk2LNqYTZUQPEXUpdgXFoiLKqWgvysgxh0n
r+IrzblClUusEpOOIPVCRTlkLQNKLXh6rTglltjeqIF16ksYjag0Km7qSP4dLK9+vQ6y38YfTE3Z
PjH6inK5o9jU+3bgch7sY8whZzm57768SZXSndRS4DSaMlUieZV4flCAKQ0I85Bu7tSAIPtdT0XO
5gquusAW1fTclq2Z7JBOBdlMjsRG9ZIq9cZ9tCt1Pty43D6I/GGQXAP/hri47oquz2pSqDwOqt7t
GvPP+pSYDEgRFJ5WcrwAAl/j9kIBteCSveZMaRo5esXgFbzafIXDPh0pPpUGdp8Q2opiWv4OpIBX
PnQZXI1iMnOFBLQyzO+oYV1u3Gbjul8Y3xlst/mB/3KXXEVWUaKp9OXNa2MZkHqEkHinHQ==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Certigna Root CA*

Issuer OU: *0002 48146308100036*

Issuer O: *Dhimyotis*

Issuer C: *FR*

Subject CN: *Certigna Identity Plus CA*

Subject 2.5.4.97: *NTRFR-48146308100036*

Subject OU: *0002 48146308100036*

Subject O: *DHIMYOTIS*

Subject C: *FR*

Valid from: *Wed Nov 25 10:30:51 CET 2015*

Valid to: *Fri Jun 03 11:30:51 CEST 2033*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:C7:E8:95:3C:C5:8E:CB:DE:74:F6:30:BC:ED:E9:87:95:3E:B7:CB:66:5D:68:CF:09:28:3B:A5:17:51:EC:8A:79:76:10:6A:99:D1:0D:21:0D:93:1E:10:50:2B:38:C4:5F:D7:DD:C0:74:2B:F4:45:31:52:D6:4C:58:5F:77:1C:09:63:D3:7A:36:66:03:6D:2D:46:E5:39:BA:EE:F8:BC:00:FC:33:9B:59:05:67:74:A3:06:99:DE:8D:28:55:00:DB:76:1C:68:BC:1E:DB:F9:CD:51:D8:D5:ED:C6:8A:D2:8F:79:45:EB:79:51:9E:27:56:87:8F:F4:90:60:4E:DC:22:3C:7B:B4:F7:1D:E7:A6:C4:89:DE:69:4E:07:BE:78:44:A6:CA:25:D6:C3:90:93:85:02:22:4E:C5:F0:62:1A:E2:EC:CE:DA:F0:1E:D3:C3:58:73:F7:26:40:20:F3:B8:0D:32:5F:56:C9:61:9D:9C:E9:EB:7B:17:1B:A9:48:06:D7:41:AE:7E:1E:4B:ED:6B:8A:98:AA:20:53:A5:04:2B:61:6C:BB:AA:54:6D:CF:0C:F7:4C:7A:16:DD:BA:51:E4:4F:81:B0:B7:70:8D:2A:B8:EE:BA:76:6F:F3:8B:4E:B3:5E:C7:9F:59:C8:DE:7B:B4:1F:C0:B6:D2:00:B2:41:05:73:B7:21:F6:D1:9E:19:27:A6:18:4C:84:74:78:22:C1:D9:62:25:0C:CE:FA:E7:DF:98:8E:19:AC:0F:BF:CD:9F:04:72:63:F4:89:57:1F:8D:88:C0:C0:0B:5B:CD:B9:E7:DA:F8:9D:74:FF:98:68:37:C9:1E:CD:16:A2:7D:25:4C:2F:25:54:8A:64:88:03:41:70:4C:DA:2E:6A:8F:0D:2F:AB:AA:AE:F7:0D:FE:DA:75:99:F5:79:86:11:80:EE:A8:FB:30:CB:C0:BD:2C:60:8
D:DB:BB:5E:01:24:45:B8:BD:89:EB:EC:89:0E:6B:D7:B1:78:E5:DC:05:A2:6C:91:BD:43:8C:44:62:EF:87:D8:DE:1F:87:55:C4:15:F7:2D:80:F3:67:38:67:2C:F3:9B:77:3C:03:BA:CC:93:B1:3D:E1:12:96:37:3F:F2:C1:71:67:73:75:2D:2C:D4:38:96:10:A6:10:CD:7A:F2:01:F7:55:86:17:6E:EF:D6:C8:86:1E:51:09:07:E9:70:7E:EB:A6:C7:D2:36:FF:E6:05:F0:CF:12:D5:41:61:1E:92:62:FE:7C:FD:9A:F9:1E:14:AC:FF:63:4D:6D:AF:B5:F2:9F:F2:4B:FE:2D:EB:45:7F:68:A9:D0:F0:83:36:6A:30:5D:8A:9D:E4:00:CF:17:FA:0A:DB:2D:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *66:38:F3:C2:5A:8D:DF:AF:37:AD:61:D9:3C:1A:1D:3E:17:67:07:75*

Authority Key Identifier *18:87:56:E0:6E:77:EE:24:35:3C:4E:73:9A:1F:D6:E1:E2:79:7E:2B*

Certificate Policies *Policy OID: 1.2.250.1.177.2.0.1.1*

CPS pointer: https://www.certigna.fr/autorites/

Authority Info Access *http://autorite.certigna.fr/certignarootca.der*

http://autorite.dhimyotis.com/certignarootca.der

CRL Distribution Points *http://crl.certigna.fr/certignarootca.crl*

http://crl.dhimyotis.com/certignarootca.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *73:6B:99:6D:33:96:84:72:9C:43:CB:39:7D:1B:B2:B2:F3:F4:A7:81:6A:5E:3C:5D:58:92:03:F8:85:C5:D4:7C*

Certificate fields details

Version: *3*

Serial Number: *625768101432799552817853009833909090 51*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIGHDCCBQSgAwIBAgIQLxPa8YcM1DOPGNv8N2uyezANBgkqhkiG9w0BAQsFADA0MQswCQYDVQQG
EwJGUjESMBAGA1UECgwJRGhpbXlvdGlzMREwDwYDVQQDDAhDZXJ0aWduYTAeFw0xNTExMjUwOTIz
MjVaFw0yNTExMjIwOTIzMjVaMIGCMQswCQYDVQQGEwJGUjESMBAGA1UECgwJREhJTVlPVElTMRww
GgYDVQQLDBMwMDAyIDQ4MTQ2MzA4MTAwMDM2MR0wGwYDVQRhDBROVFJGUi00ODE0NjMwODEwMDAz
NjEiMCAGA1UEAwwZQ2VydGlnbmEgSWRlbnRpdHkgUGx1cyBDQTCCAiIwDQYJKoZIhvcNAQEBBQAD
ggIPADCCAgoCggIBAMfolTzFjsvedPYwvO3ph5U+t8tmXWjPCSg7pRdR7Ip5dhBqmdENIQ2THhBQ
KzjEX9fdwHQr9EUxUtZMWF93HAlj03o2ZgNtLUblObru+LwA/DObWQVndKMGmd6NKFUA23YcaLwe
2/nNUdjV7caK0o95Ret5UZ4nVoeP9JBgTtwiPHu09x3npsSJ3mlOB754RKbKJdbDkJOFAiJOxfBi
GuLsztrwHtPDWHP3JkAg87gNMl9WyWGdnOnrexcbqUgG10Gufh5L7WuKmKogU6UEK2Fsu6pUbc8M
90x6Ft26UeRPgbC3cI0quO66dm/zi06zXsefWcjee7QfwLbSALJBBXO3IfbRnhknphhMhHR4IsHZ
YiUMzvrn35iOGawPv82fBHJj9llXH42IwMALW82559r4nXT/mGg3yR7NFqJ9JUwvJVSKZIgDQXBM
2i5qjw0vq6qu9w3+2nWZ9XmGEYDuqPswy8C9LGCN27teASRFuL2J6+yJDmvXsXjl3AWibJG9Q4xE
Yu+H2N4fh1XEFfctgPNnOGcs85t3PAO6zJOxPeESljc/8sFxZ3N1LSzUOJYQphDNevIB91WGF27v
1siGHlEJB+lwfuumx9I2/+YF8M8S1UFhHpJi/nz9mvkeFKz/Y01tr7Xyn/JL/i3rRX9oqdDwgzZq
MF2KneQAzxf6CtstAgMBAAGjggHZMIIB1TASBgNVHRMBAf8ECDAGAQH/AgEAMA4GA1UdDwEB/wQE
AwIBBjAdBgNVHQ4EFgQUZjjzwlqN3683rWHZPBodPhdnB3UwZAYDVR0jBF0wW4AUGu3+QTmQtCRZ
vgHyUtVF9lo53BGhOKQ2MDQxCzAJBgNVBAYTAkZSMRIwEAYDVQQKDAlEaGlteW90aXMxETAPBgNV
BAMMCENlcnRpZ25hggkA/tzjAQ/JSP8wSQYDVR0gBEIwQDA+BgoqgXoBgTEBAAECMDAwLgYIKwYB
BQUHAgEWImh0dHBzOi8vd3d3LmNlcnRpZ25hLmZyL2F1dG9yaXRlcy8wfAYIKwYBBQUHAQEEcDBu
MDQGCCsGAQUFBzAChihodHRwOi8vYXV0b3JpdGUuY2VydGlnbmEuZnlvY2VydGlnbmEuZGVyMDYG
CCsGAQUFBzAChipodHRwOi8vYXV0b3JpdGUuZGhpbXlvdGlzLmNvbS9jZXJ0aWduYS5kZXIwYQYD
VR0fBFowWDApoCegJYYjaHR0cDovL2NybC5jZXJ0aWduYS5mci9jZXJ0aWduYS5jcmwwK6ApoCeG
JWh0dHA6Ly9jcmwuZGhpbXlvdGlzLmNvbS9jZXJ0aWduYS5jcmwwDQYJKoZIhvcNAQELBQADggEB
AK05XoyuwD1xY8gkIri3eb/mk0rVyRp6Pa9VA8hDNiZqz2ZaVAOKZYP3tvRXTz/vOMlDVO9i66MB
qADiG9smLFB2dWQVojALSbX52V5gyKPglfqY99YPLwuihlrOYSDsuooEc6qZ3RKgK3HnbLAlhTNR
ljgcOkKFYmnMXggsUA5ZhL0fntu+b89FCSbtth3nhoL1gVYZg54ZtyzMi8VmJTMUDk/2nXuzIan6
dZByWdcUfwHj5iGyAnXs09+iQA0q+EyqxKG/7ovWpOndOJIZ576bEy3+WcnxWAdYiBV8tA1Snjit
91RkThbjIz+nzuVJOvYwQwJdBp9lBJoFK2zKHy4=

-----END CERTIFICATE-----

Signature algorithm:	*SHA256withRSA*
Issuer CN:	*Certigna*
Issuer O:	*Dhimyotis*
Issuer C:	*FR*
Subject CN:	*Certigna Identity Plus CA*
Subject 2.5.4.97:	*NTRFR-48146308100036*
Subject OU:	*0002 48146308100036*
Subject O:	*DHIMYOTIS*
Subject C:	*FR*
Valid from:	*Wed Nov 25 10:23:25 CET 2015*
Valid to:	*Sat Nov 22 10:23:25 CET 2025*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:C7:E8:95:3C:C5:8E:CB:DE:74:F6:30:BC:ED:E9:87:95:
3E:B7:CB:66:5D:68:CF:09:28:3B:A5:17:51:EC:8A:79:76:10:6A:99:D1:0D:21:0D:93:1E:10:50:2B:38:C4:5F:D7:DD:C0:74:2B:F4:45:31:52:D6:4C:58:5F:77:1C:09:6
3:D3:7A:36:66:03:6D:2D:46:E5:39:BA:EE:F8:BC:00:FC:33:9B:59:05:67:74:A3:06:99:DE:8D:28:55:00:DB:76:1C:68:BC:1E:DB:F9:CD:51:D8:D5:ED:C6:8A:D2:8F:79

:45:EB:79:51:9E:27:56:87:8F:F4:90:60:4E:DC:22:3C:7B:B4:F7:1D:E7:A6:C4:89:DE:69:4E:07:BE:78:44:A6:CA:25:D6:C3:90:93:85:02:22:4E:C5:F0:62:1A:E2:EC:CE
:DA:F0:1E:D3:C3:58:73:F7:26:40:20:F3:B8:0D:32:5F:56:C9:61:9D:9C:E9:EB:7B:17:1B:A9:48:06:D7:41:AE:7E:1E:4B:ED:6B:8A:98:AA:20:53:A5:04:2B:61:6C:BB:A
A:54:6D:CF:0C:F7:4C:7A:16:DD:BA:51:E4:4F:81:B0:B7:70:8D:2A:B8:EE:BA:76:6F:F3:8B:4E:B3:5E:C7:9F:59:C8:DE:7B:B4:1F:C0:B6:D2:00:B2:41:05:73:B7:21:F6:
D1:9E:19:27:A6:18:4C:84:74:78:22:C1:D9:62:25:0C:CE:FA:E7:DF:98:8E:19:AC:0F:BF:CD:9F:04:72:63:F4:89:57:1F:8D:88:C0:C0:0B:5B:CD:B9:E7:DA:F8:9D:74:FF
:98:68:37:C9:1E:CD:16:A2:7D:25:4C:2F:25:54:8A:64:88:03:41:70:4C:DA:2E:6A:8F:0D:2F:AB:AA:AE:F7:0D:FE:DA:75:99:F5:79:86:11:80:EE:A8:FB:30:CB:C0:BD:2
C:60:8
D:DB:BB:5E:01:24:45:B8:BD:89:EB:EC:89:0E:6B:D7:B1:78:E5:DC:05:A2:6C:91:BD:43:8C:44:62:EF:87:D8:DE:1F:87:55:C4:15:F7:2D:80:F3:67:38:67:2C:F3:9B:77:
3C:03:BA:CC:93:B1:3D:E1:12:96:37:3F:F2:C1:71:67:73:75:2D:2C:D4:38:96:10:A6:10:CD:7A:F2:01:F7:55:86:17:6E:EF:D6:C8:86:1E:51:09:07:E9:70:7E:EB:A6:C7:
D2:36:FF:E6:05:F0:CF:12:D5:41:61:1E:92:62:FE:7C:FD:9A:F9:1E:14:AC:FF:63:4D:6D:AF:B5:F2:9F:F2:4B:FE:2D:EB:45:7F:68:A9:D0:F0:83:36:6A:30:5D:8A:9D:E4:
00:CF:17:FA:0A:DB:2D:02:03:01:00:01

Basic Constraints	*IsCA: true - Path length: 0*
Subject Key Identifier	*66:38:F3:C2:5A:8D:DF:AF:37:AD:61:D9:3C:1A:1D:3E:17:67:07:75*
Authority Key Identifier	*1A:ED:FE:41:39:90:B4:24:59:BE:01:F2:52:D5:45:F6:5A:39:DC:11*
Certificate Policies	*Policy OID: 1.2.250.1.177.1.0.1.2* *CPS pointer: https://www.certigna.fr/autorites/*
Authority Info Access	*http://autorite.certigna.fr/certigna.der* *http://autorite.dhimyotis.com/certigna.der*
CRL Distribution Points	*http://crl.certigna.fr/certigna.crl* *http://crl.dhimyotis.com/certigna.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*02:C4:A3:00:A0:9C:1B:89:3B:11:F9:56:76:59:AF:95:BB:B9:BB:E7:95:38:93:E3:6C:5B:AF:17:B5:55:CE:E3*

X509SubjectName

Subject CN:	*Certigna Identity Plus CA*
Subject 2.5.4.97:	*NTRFR-48146308100036*
Subject OU:	*0002 48146308100036*
Subject O:	*DHIMYOTIS*
Subject C:	*FR*

X509SKI

X509 SK I	*ZjjzwlqN3683rWHZPBodPhdnB3U=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description	*[en]*	*undefined.*
	[fr]	*undefined.*

Status Starting Time *2017-04-30T22:00:00Z*

TSP Service Definition URI

URI *[en]* *http://politique.certigna.fr/en/PCcertignaidentityplusca.pdf*

URI *[fr]* *http://politique.certigna.fr/PCcertignaidentityplusca.pdf*

8.6.1 - Extension (critical): Qualifiers [QCWithQSCD]

Qualifier type description *[en]* *undefined.*

[fr] *undefined.*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithQSCD*

Criteria list assert=all

Key Usage *[digitalSignature]* *true*

Key Usage *[nonRepudiation]* *true*

Policy Identifier nodes:

Identifier *1.2.250.1.177.2.4.1.4.1*

8.6.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

8.7 - Service (granted): Certigna Entity Code Signing CA - Cachet de signature de code ** - 1.2.250.1.177.2.8.1.2.1

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Certigna Entity Code Signing CA - Cachet de signature de code ** - 1.2.250.1.177.2.8.1.2.1*

Name *[fr]* *Certigna Entity Code Signing CA - Cachet de signature de code ** - 1.2.250.1.177.2.8.1.2.1*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *388115030707504881294513929966996241 60*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIHHDCCBQSgAwIBAgIQHTLS1yBHGnaRVupojsVS4DANBgkqhkiG9w0BAQsFADBaMQswCQYDVQQG
EwJGUjESMBAGA1UECgwJRGhpbXlvdGlzMRwwGgYDVQQLDBMwMDAyIDQ4MTQ2MzA4MTAwMDM2MRkw
FwYDVQQDDBBDZXJ0aWduYSBSb290IENBMB4XDTE2MDIwNDExMTA1MFoXDTMzMDgxMzExMTA1MFow
gYgxCzAJBgNVBAYTAkZSMRIwEAYDVQQKDAlESElNWU9USVMxHDAaBgNVBAsMEzAwMDIgNDgxNDYz
MDgxMDAwMzYxHTAbBgNVBGEMFE5UUkZSLTQ4MTQ2MzA4MTAwMDM2MSgwJgYDVQQDDB9DZXJ0aWdu
YSBFbnRpdHkgQ29kZSBTaWduaW5nIENBMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA
w5yYR0QpkhFkNlq6J0LVJt38Ylrq2bTZjPpGkQSzgLuyzjrh6IeBmiPTYYnP2Yy2QMFeVdlPD/nE
q5j11lz1R3CFfP9Cg9jQFhgYdEoVCcQBw9iTao4bCN1xowXwn/dNjagVQxMULCjV6PelU9pu/bsJ
GbdAMujD2Ihu/zhvXhgdc8s80XuHACOO7Sz4MdiN1MhDI3rPYQfV83q0R68JtMLPb+shAsqttjbj
kU1i9q2LGfmkFyv/k8GCx4wQwohWTaU5ALbRxjpr/TCt75KoVA2R4Zb69qOsA//S27oeqwoHPoyE
TeQ7y721gTFMtm0oOJlBe2XKiL5Yg8aRfDA1Dg3g6BVJDYXr//Hui0kuIEvqficqrl9HUEuUgI//
Flug5bwqQ1z9SeCOSvgxnAYoOUM40jLkKK5nN59M7aDENXV4Lpq7TIwQsyOMMAdnhp/gVYQ2eaIn
D7JFURTZ13sZyVS+QNfOorWZOr90UhucqAz6NYA0Mb1domXnlz4OLKag9vCNBmdJtjYUzXVPXJqx
b89Zngle8MPlXE2vjcAp8AXCdFtYaJw6Ae9rR3OhUhWppyq+wzy3Lu8v3913NsU8oo1YhXw0oK9t
3prpUfk19FUNuaXfiKs6P971DJUwoSsx4q2zrsBcWUfZc02pvkjDbPOPRiO5A1CziUcXYG87jG8C
AwEAAaOCAa0wggGpMBIGA1UdEwEB/wQIMAYBAf8CAQAwDgYDVR0PAQH/BAQDAgEGMB0GA1UdDgQW
BBRxkMWZyggSyUDzmNOmsw/J/arH1jAfBgNVHSMEGDAWgBQYh1bgbnfuJDU8TnOaH9bh4nl+KzBJ
BgNVHSAEQjBAMD4GCiqBegGBMQIAAQEwMDAuBggrBgEFBQcCARYiaHR0cHM6Ly93d3cuY2VydGln
bmEuZnIvYXV0b3JpdGVzLzCBiAYIKwYBBQUHAQEEfDB6MDoGCCsGAQUFBzAChi5odHRwOi8vYXV0
b3JpdGUuY2VydGlnbmEuZnIvY2VydGlnbmFyb290Y2EuZGVyMDwGCCsGAQUFBzAChjBodHRwOi8v
YXV0b3JpdGUuZGhpbXlvdGlzLmNvbS9jZXJ0aWduYXJvb3RjYS5kZXIwbQYDVR0fBGYwZDAvoC2g
K4YpaHR0cDovL2NybC5jZXJ0aWduYS5mci9jZXJ0aWduYXJvb3RjYS5jcmwwMaAvoC2GK2h0dHA6
Ly9jcmwuZGhpbXlvdGlzLmNvbS9jZXJ0aWduYXJvb3RjYS5jcmwwDQYJKoZIhvcNAQELBQADggIB
AK1sWN4vvkkxUBYlSl+sVxuF0uPkx3/pHngQXF+fYSubGQ0Z7JPOpWZ8/nWyjE8jV/Ps6qam3UZ1
3G/8EqU1mDvKo9eb76TxxUtJF74mmkZTJDGa6c6MP0fHlcDuZsvCKoZbHOLutItRs7JMz/8WxB9T
5oIZs4Ejv3MNuFrnG2TdVtMc3P/NVMMNrMJ6oYhjS49XVWOVPqgrPx6oAmErulVhVR4JoPpYFRP2
MpHsOfBW2MRJMDa7ZCd5WQfKvbBkb9v107B2htlywYsmZGTo/brwxcU3IUs660xHglnlitaFnZR0
EPDjWAyHFm5qamwrukWqFYYu1MwgmuMvSqGBQZfCCMFsUdvAspnCiCeXkygoYVbWPqoQX7XVquGh
rC1Or8h6ZnysMfHniilKvgwM9mxocTZbg8iK5G7yCEzz6Fw8ZEES3LLcOQV6nYpNnxhbgklEKgJI
pZkdeURL7h6MZsGv2kE+t1Jqpfch3ij6P46A4tCdnPkuSHWSV06Uy8V//s5kf7FmhcvOAQHRciHB
JXSWVFoxPMboPoPtXnp390UUM1FLpW9inQAtcDnTYqB0M/HzAiv36cCuY6TEdvaUHT+RYlzIDMvz
0jEBgcH4kII9pwLbmT0WulrsOhZFwa1xXg014Ga2Htu2W4MPeO9JXTKQClk5IePocjogvR5OgSDK

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Certigna Root CA*

Issuer OU: *0002 48146308100036*

Issuer O: *Dhimyotis*

Issuer C: *FR*

Subject CN: *Certigna Entity Code Signing CA*

Subject 2.5.4.97: *NTRFR-48146308100036*

Subject OU: *0002 48146308100036*

Subject O: *DHIMYOTIS*

Subject C: *FR*

Valid from: *Thu Feb 04 12:10:50 CET 2016*

Valid to: *Sat Aug 13 13:10:50 CEST 2033*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:C3:9C:98:47:44:29:92:11:64:36:5A:BA:27:42:D5:26:
DD:FC:62:5A:EA:D9:B4:D9:8C:FA:46:91:04:B3:80:BB:B2:CE:3A:E1:E8:87:81:9A:23:D3:61:89:CF:D9:8C:B6:40:C1:5E:55:D9:4F:0F:F9:C4:AB:98:F5:D6:5C:F5:47:7
0:85:7C:FF:42:83:D8:D0:16:18:18:74:4A:15:09:C4:01:C3:D8:93:6A:8E:1B:08:DD:71:A3:05:F0:9F:F7:4D:8D:A8:15:43:13:14:2C:28:D5:E8:F7:A5:53:DA:6E:FD:BB:
09:19:B7:40:32:E8:C3:D8:88:6E:FF:38:6F:5E:18:1D:73:CB:3C:D1:7B:87:00:23:8E:ED:2C:F8:31:D8:8D:D4:C8:43:23:7A:CF:61:07:D5:F3:7A:B4:47:AF:09:B4:C2:CF
:6F:EB:21:02:CA:AD:B6:36:E3:91:4D:62:F6:AD:8B:19:F9:A4:17:2B:FF:93:C1:82:C7:8C:10:C2:88:56:4D:A5:39:00:B6:D1:C6:3A:6B:FD:30:AD:EF:92:A8:54:0D:91:
E1:96:FA:F6:A3:AC:03:FF:D2:DB:BA:1E:AB:0A:07:3E:8C:84:4D:E4:3B:CB:BD:B5:81:31:4C:B6:6D:28:38:99:41:7B:65:CA:88:BE:58:83:C6:91:7C:30:35:0E:0D:E0:E
8:15:49:0D:85:EB:FF:F1:EE:8B:49:2E:20:4B:EA:7E:27:2A:AE:5F:47:50:4B:94:80:8F:FF:16:5B:A0:E5:BC:2A:43:5C:FD:49:E0:8E:4A:F8:31:9C:06:28:39:43:38:D2:3
2:E4:28:AE:67:37:9F:4C:ED:A0:C4:35:75:78:2E:9A:BB:4C:8C:10:B3:23:8C:30:07:67:86:9F:E0:55:84:36:79:A2:27:0F:B2:45:51:14:D9:D7:7B:19:C9:54:BE:40:D7:C
E:A2:B5:99:3A:BF:74:52:1B:9C:A8:0C:FA:35:80:34:31:BD:5D:A2:65:E7:97:3E:0E:2C:A6:A0:F6:F0:8D:06:67:49:B6:36:14:CD:75:4F:5C:9A:B1:6F:CF:59:9E:09:5E:F
0:C3:E5:5C:4D:AF:8D:C0:29:F0:05:C2:74:5B:58:68:9C:3A:01:EF:6B:47:73:A1:52:15:A9:A7:2A:BE:C3:3C:B7:2E:EF:2F:DF:DD:77:36:C5:3C:A2:8D:58:85:7C:34:A0:
AF:6D:DE:9A:E9:51:F9:35:F4:55:0D:B9:A5:DF:88:AB:3A:3F:DE:F5:0C:95:30:A1:2B:31:E2:AD:B3:AE:C0:5C:59:47:D9:73:4D:A9:BE:48:C3:6C:F3:8F:46:23:B9:03:5
0:B3:89:47:17:60:6F:3B:8C:6F:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *71:90:C5:99:CA:08:12:C9:40:F3:98:D3:A6:B3:0F:C9:FD:AA:C7:D6*

Authority Key Identifier *18:87:56:E0:6E:77:EE:24:35:3C:4E:73:9A:1F:D6:E1:E2:79:7E:2B*

Certificate Policies *Policy OID: 1.2.250.1.177.2.0.1.1*

CPS pointer: https://www.certigna.fr/autorites/

Authority Info Access *http://autorite.certigna.fr/certignarootca.der*

http://autorite.dhimyotis.com/certignarootca.der

CRL Distribution Points *http://crl.certigna.fr/certignarootca.crl*

http://crl.dhimyotis.com/certignarootca.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *78:1A:CD:20:9D:3B:87:3F:14:8F:5D:B3:1C:68:0A:DA:DC:ED:40:23:8D:8C:1B:F1:A2:D5:53:39:1F:A5:D0:F3*

Certificate fields details

Version: *3*

Serial Number: *156762549197834556994352785380332204247*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIGIjCCBQqgAwIBAgIQde9eZ3B27Q+W+pWi7G7w1zANBgkqhkiG9w0BAQsFADA0MQswCQYDVQQG

EwJGUjESMBAGA1UECgwJRGhpbXlvdGlzMREwDwYDVQQDDAhDZXJ0aWduYTAeFw0xNjAyMDQxMTEz
MzNaFw0yNTEyMTMxMTEzMzNaMIGIMQswCQYDVQQGEwJGUjESMBAGA1UECgwJREhJTVlPVElTMRww
GgYDVQQLDBMwMDAyIDQ4MTQ2MzA4MTAwMDM2MR0wGwYDVQRhDBROVFJGUi00ODE0NjMwODEwMDAz
NjEoMCYGA1UEAwwfQ2VydGlnbmEgRW50aXR5IENvZGUgU2lnbmluZyBDQTCCAiIwDQYJKoZIhvcN
AQEBBQADggIPADCCAgoCggIBAMOcmEdEKZIRZDZauidC1Sbd/GJa6tm02Yz6RpEEs4C7ss464eiH
gZoj02GJz9mMtkDBXlXZTw/5xKuY9dZc9UdwhXz/QoPY0BYYGHRKFQnEAcPYk2qOGwjdcaMF8J/3
TY2oFUMTFCwo1ej3pVPabv27CRm3QDLow9iIbv84b14YHXPLPNF7hwAjju0s+DHYjdTIQyN6z2EH
1fN6tEevCbTCz2/rIQLKrbY245FNYvatixn5pBcr/5PBgseMEMKIVk2lOQC20cY6a/0wre+SqFQN
keGW+vajrAP/0tu6HqsKBz6MhE3kO8u9tYExTLZtKDiZQXtlyoi+WIPGkXwwNQ4N4OgVSQ2F6//x
7otJLiBL6n4nKq5fR1BLlICP/xZboOW8KkNc/Ungjkr4MZwGKDlDONIy5CiuZzefTO2gxDV1eC6a
u0yMELMjjDAHZ4af4FWENnmiJw+yRVEU2dd7GclUvkDXzqK1mTq/dFlbnKgM+jWANDG9XaJl55c+
DiymoPbwjQZnSbY2FM11T1yasW/PWZ4JXvDD5VxNr43AKfAFwnRbWGicOgHva0dzoVlVqacqvsM8
ty7vL9/ddzbFPKKNWlV8NKCvbd6a6VH5NfRVDbml34irOj/e9QyVMKErMeKts67AXFlH2XNNqb5I
w2zzj0YjuQNQs4lHF2BvO4xvAgMBAAGjggHZMIIB1TASBgNVHRMBAf8ECDAGAQH/AgEAMA4GA1Ud
DwEB/wQEAwIBBjAdBgNVHQ4EFgQUcZDFmcoIEslA85jTprMPyf2qx9YwZAYDVR0jBF0wW4AUGu3+
QTmQtCRZvgHyUtVF9lo53BGhOKQ2MDQxCzAJBgNVBAYTAkZSMRIwEAYDVQQKDAlEaGlteW90aXMx
ETAPBgNVBAMMCENlcnRpZ25hggkA/tzjAQ/JSP8wSQYDVR0gBEIwQDA+BgoqgXoBgTEBAAECMDAw
LgYIKwYBBQUHAgEWImh0dHBzOi8vd3d3LmNlcnRpZ25hLmZyL2F1dG9yaXRlcy8wfAYIKwYBBQUH
AQEEcDBuMDQGCCsGAQUFBzAChihodHRwOi8vYXV0b3JpdGUuY2VydGlnbmEuZnIvY2VydGlnbmEu
ZGVyMDYGCCsGAQUFBzAChipodHRwOi8vYXV0b3JpdGUuZGhpbXlvdGlzLmNvbS9jZXJ0aWduYS5k
ZXIwYQYDVR0fBFowWDApoCegJYYjaHR0cDovL2NybC5jZXJ0aWduYS5mci9jZXJ0aWduYS5jcmww
K6ApoCeGJWh0dHA6Ly9jcmwuZGhpbXlvdGlzLmNvbS9jZXJ0aWduYS5jcmwwDQYJKoZIhvcNAQEL
BQADggEBAGYlp9+MguDNmi4/pkAWtjRMYYT95Gwq73YS9SCckEaUDvVwyURgdvuW3Nf3Tv5v54H2
ZNNPRWlVrCyL9dyFZEN+g4DdAAEDUhQw9GzqiELKw0HmqN7XG9Q3YbMZ8sHXu/FWK425pFDBfZJU
pn5MZkiqsDlxCsuunb136TbFU5S3ESsNf6CQlgQUFx/AGYY5DduS92UfaBZMnPKvr6tDK/jsIBS0
otB0nMK6U+wje3M9WkS30r/uFJoTcaVLayk6eWUZxQLvZSCiBQx2rykhds4Ew1vlHgHnKn9RFnPS
u2VwXWTFWBwRCuIYK/66wOo97Snq79/RTkEeVDCFMd62FHI=

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Certigna*

Issuer O: *Dhimyotis*

Issuer C: *FR*

Subject CN: *Certigna Entity Code Signing CA*

Subject 2.5.4.97: *NTRFR-48146308100036*

Subject OU: *0002 48146308100036*

Subject O: *DHIMYOTIS*

Subject C: *FR*

Valid from: *Thu Feb 04 12:13:33 CET 2016*

Valid to: *Sat Dec 13 12:13:33 CET 2025*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:C3:9C:98:47:44:29:92:11:64:36:5A:BA:27:42:D5:26:
DD:FC:62:5A:EA:D9:B4:D9:8C:FA:46:91:04:B3:80:BB:B2:CE:3A:E1:E8:87:81:9A:23:D3:61:89:CF:D9:8C:B6:40:C1:5E:55:D9:4F:0F:F9:C4:AB:98:F5:D6:5C:F5:47:7
0:85:7C:FF:42:83:D8:D0:16:18:18:74:4A:15:09:C4:01:C3:D8:93:6A:8E:1B:08:DD:71:A3:05:F0:9F:F7:4D:8D:A8:15:43:13:14:2C:28:D5:E8:F7:A5:53:DA:6E:FD:BB:
09:19:B7:40:32:E8:C3:D8:88:6E:FF:38:6F:5E:18:1D:73:CB:3C:D1:7B:87:00:23:8E:ED:2C:F8:31:D8:8D:D4:C8:43:23:7A:CF:61:07:D5:F3:7A:B4:47:AF:09:B4:C2:CF
:6F:EB:21:02:CA:AD:B6:36:E3:91:4D:62:F6:AD:8B:19:F9:A4:17:2B:FF:93:C1:82:C7:8C:10:C2:88:56:4D:A5:39:00:B6:D1:C6:3A:6B:FD:30:AD:EF:92:A8:54:0D:91:

E1:96:FA:F6:A3:AC:03:FF:D2:DB:BA:1E:AB:0A:07:3E:8C:84:4D:E4:3B:CB:BD:B5:81:31:4C:B6:6D:28:38:99:41:7B:65:CA:88:BE:58:83:C6:91:7C:30:35:0E:0D:E0:E8:15:49:0D:85:EB:FF:F1:EE:8B:49:2E:20:4B:EA:7E:27:2A:AE:5F:47:50:4B:94:80:8F:FF:16:5B:A0:E5:BC:2A:43:5C:FD:49:E0:8E:4A:F8:31:9C:06:28:39:43:38:D2:32:E4:28:AE:67:37:9F:4C:ED:A0:C4:35:75:78:2E:9A:BB:4C:8C:10:B3:23:8C:30:07:67:86:9F:E0:55:84:36:79:A2:27:0F:B2:45:51:14:D9:D7:7B:19:C9:54:BE:40:D7:CE:A2:B5:99:3A:BF:74:52:1B:9C:A8:0C:FA:35:80:34:31:BD:5D:A2:65:E7:97:3E:0E:2C:A6:A0:F6:F0:8D:06:67:49:B6:36:14:CD:75:4F:5C:9A:B1:6F:CF:59:9E:09:5E:F0:C3:E5:5C:4D:AF:8D:C0:29:F0:05:C2:74:5B:58:68:9C:3A:01:EF:6B:47:73:A1:52:15:A9:A7:2A:BE:C3:3C:B7:2E:EF:2F:DF:DD:77:36:C5:3C:A2:8D:58:85:7C:34:A0:AF:6D:DE:9A:E9:51:F9:35:F4:55:0D:B9:A5:DF:88:AB:3A:3F:DE:F5:0C:95:30:A1:2B:31:E2:AD:B3:AE:C0:5C:59:47:D9:73:4D:A9:BE:48:C3:6C:F3:8F:46:23:B9:03:50:B3:89:47:17:60:6F:3B:8C:6F:02:03:01:00:01

Basic Constraints	*IsCA: true - Path length: 0*
Subject Key Identifier	*71:90:C5:99:CA:08:12:C9:40:F3:98:D3:A6:B3:0F:C9:FD:AA:C7:D6*
Authority Key Identifier	*1A:ED:FE:41:39:90:B4:24:59:BE:01:F2:52:D5:45:F6:5A:39:DC:11*
Certificate Policies	*Policy OID: 1.2.250.1.177.1.0.1.2* *CPS pointer: https://www.certigna.fr/autorites/*
Authority Info Access	*http://autorite.certigna.fr/certigna.der* *http://autorite.dhimyotis.com/certigna.der*
CRL Distribution Points	*http://crl.certigna.fr/certigna.crl* *http://crl.dhimyotis.com/certigna.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*93:50:61:BE:52:C8:EA:88:C0:34:B3:9A:DF:D5:22:BB:31:4C:BF:53:04:E5:A7:06:47:35:DD:BD:A3:24:2A:AF*

X509SubjectName

Subject CN:	*Certigna Entity Code Signing CA*
Subject 2.5.4.97:	*NTRFR-48146308100036*
Subject OU:	*0002 48146308100036*
Subject O:	*DHIMYOTIS*
Subject C:	*FR*

X509SKI

X509 SK I	*cZDFmcoIEslA85jTprMPyf2qx9Y=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description	*[en]*	*undefined.*
	[fr]	*undefined.*

Status Starting Time *2017-04-30T22:00:00Z*

TSP Service Definition URI

URI	*[en]*	*http://politique.certigna.fr/en/PCcertignaentitycsca.pdf*
URI	*[fr]*	*http://politique.certigna.fr/PCcertignaentitycsca.pdf*

8.7.1 - Extension (critical): Qualifiers [QCWithQSCD]

Qualifier type description	*[en]*	*undefined.*
	[fr]	*undefined.*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithQSCD*

Criteria list assert=all

Key Usage	*[digitalSignature]*	*true*

Policy Identifier nodes:

Identifier *1.2.250.1.177.2.8.1.2.1*

8.7.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

8.8 - Service (granted): Certigna Entity CA - Cachet de signature de mails et de documents ** - 1.2.250.1.177.2.6.1.4.1

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[fr]	*Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name	*[en]*	*Certigna Entity CA - Cachet de signature de mails et de documents ** - 1.2.250.1.177.2.6.1.4.1*
Name	*[fr]*	*Certigna Entity CA - Cachet de signature de mails et de documents ** - 1.2.250.1.177.2.6.1.4.1*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *198429372998709978411380447595286256357*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIHDzCCBPegAwIBAgIRAJVIG2zmMiFC/oSZgw58WuUwDQYJKoZIhvcNAQELBQAwWjELMAkGA1UE
BhMCRlIxEjAQBgNVBAoMCURoaW15b3RpczEcMBoGA1UECwwTMDAwMiA0ODE0NjMwODEwMDAzNjEZ
MBcGA1UEAwwQQ2VydGlnbmEgUm9vdCBDQTAeFw0xNTExMjUxMDI3NTRaFw0zMzA2MDMxMDI3NTRa
MHsxCzAJBgNVBAYTAkZSMRIwEAYDVQQKDAlESElNWU9USVMxHDAaBgNVBAsMEzAwMDIgNDgxNDYz
MDgxMDAwMzYxHTAbBgNVBGEMFE5UUkZSLTQ4MTQ2MzA4MTAwMDM2MRswGQYDVQQDDBJDZXJ0aWdu
YSBFbnRpdHkgQ0EwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDSVOsDBho4mm9t5I92
PyXgNVQI/a13lmknpgEROSPQMTJqKubOH5B2iom6wTRs+7sN6K8Zgtoh9k/nd9WL44zz9N+JArrU
HneSDAjW0vWcSF0t3sbwbtKsqzQcZKh+Tooxaqfi3aRWSS+i24flHPFb9OtjIX2RSsG+pwCpSKCk
+02/bDolGYQ3dClhgOMbgHDPgndExEy2rnPpPUXnmFfWEU/sVxq836rgaInqbssyHCLCHucdTvWW
YuFStgcAivKA395ChsKdXweJLEGbR4W2ckNdZR3sp2R0nTYTrtpyVXrblXDPD7Q4ofbRcGo7i07x
jLRO4mdlAZ8D+1LF1+nuHE1aVcUe+RpEZN+P3Lq2/1ZVmuBw1tpdHhzeCMT8a6EYMKq3faiBMq7f
twcwHEJFcKAxYQDLPi0ENVPz9RnMNvIUk57rdquhl2iiEjheQSPnR9hPr4CgSXRShy2zBs/OrU90
jNdv67ySLgVkr/axPAIonGJ+mXOP14Vy/SZwRXJijNU8A/MCjVqSwrX8pZlJ0cHY52jl2EuXKIb8
CZVx0Ds2VAQ+Dp9KQlxtlXmQ2eaQj1uBC/SJUU73LSzUCXN8VwisUltL8DVSwvr7n0fWJ9K5t6GY
PiazwC3zf82PICMQkKztS8gaRIV7niJ9Kch0HTcplrPpycUjA/LtOE9TiQIDAQABo4IBrTCCAakw
EgYDVR0TAQH/BAgwBgEB/wIBADAOBgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFKU/HiRMbPiL0hty
mEZQyuiGVbnYMB8GA1UdIwQYMBaAFBiHVuBud+4kNTxOc5of1uHieX4rMEkGA1UdIARCMEAwPgYK
KoF6AYExAgABATAwMC4GCCsGAQUFBwIBFiJodHRwczovL3d3dy5jZXJ0aWduYS5mci9hdXRvcml0
ZXMvMIGIBggrBgEFBQcBAQR8MHowOgYIKwYBBQUHMAKGLmh0dHA6Ly9hdXRvcml0ZS5jZXJ0aWdu
YS5mci9jZXJ0aWduYXJvb3RjYS5kZXIwPAYIKwYBBQUHMAKGMGh0dHA6Ly9hdXRvcml0ZS5kaGlt
eW90aXMuY29tL2NlcnRpZ25hcm9vdGNhLmRlcjBtBgNVHR8EZjBkMC+gLaArhilodHRwOi8vY3Js
LmNlcnRpZ25hLmZyL2NlcnRpZ25hcm9vdGNhLmNybDAxoC+gLYYraHR0cDovL2NybC5kaGlteW90
aXMuY29tL2NlcnRpZ25hcm9vdGNhLmNybDANBgkqhkiG9w0BAQsFAAOCAgEArfWJJUSj21DuIP7q
021HUkYV6dXH1FN9sEaOD5156JHV7M4FqkyubCjgfswL6NwW0UO2xanxFdcKPfx14M+H6Jgwqilz
W3InAwevKIx8+UivCpV47rDQe4/Yd//xbG0sd7+dMCvCAj7gOtlap/h1VJhwip6YVkaCp+q0nBbO
hEx+azqdc9Urh7eyj3no/4uJogc79vhrZ3QYm0AfAqosjH0IekZblyNOrqKR6NiMqGGNuWRJlg8r
pkEEakeTwIofh2lByrvlKIGcXRdl/oFhxDiC7Q3sCCpwq2VEmNAxg+ZWh4OnJxLx2uC8tDgN6IIH
+4TztUyO+KUG1Xnw1Mlg2dQKqt1B5/xvVKPOG2LNcUCeNAt7QmgkIvefsuxrHcFI2qZ7I9spo89w
je2BCY1ey0lkePGyzX8jy2CLTrFvfGhtw/S28L9oryrW5XS8J5ebAS+w+G2lda4rowb8EOjhXDVY
pA93yAB5SWjwWLzjcVn2WcJGOhEp9iZsVUDni/0b/JL7ovqtcPlY7Z9RtAg1SXY0SUc/CEVCbQM2
5EPcoNryEj7RivjYSZeJdwZ9/UoKq/be9dHqssrr1PusyLptEmUjV9a4d91NHiRwbHboyX77LJXj
9M0jc0WCwSbAyViEXJZx1jLAjakWnh5bTrmipLf7Mc8Fk3xw61zpX9ow1gc=

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Certigna Root CA*

Issuer OU: *0002 48146308100036*

Issuer O: *Dhimyotis*

Issuer C: *FR*

Subject CN: *Certigna Entity CA*

Subject 2.5.4.97: *NTRFR-48146308100036*

Subject OU: *0002 48146308100036*

Subject O: *DHIMYOTIS*

Subject C: *FR*

Valid from: *Wed Nov 25 11:27:54 CET 2015*

Valid to: *Fri Jun 03 12:27:54 CEST 2033*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:D2:54:EB:03:06:1A:38:9A:6F:6D:E4:8F:76:3F:25:E0:
35:54:08:FD:AD:77:96:69:27:A6:01:11:39:23:D0:31:32:6A:2A:E6:CE:1F:90:76:8A:89:BA:C1:34:6C:FB:BB:0D:E8:AF:19:82:DA:21:F6:4F:E7:77:D5:8B:E3:8C:F3:F4
:DF:89:02:BA:D4:1E:77:92:0C:08:D6:D2:F5:9C:48:5D:2D:DE:C6:F0:6E:D2:AC:AB:34:1C:64:A8:7E:4E:8A:31:6A:A7:E2:DD:A4:56:49:2F:A2:DB:87:E5:1C:F1:5B:F4:
EB:63:21:7D:91:4A:C1:BE:A7:00:A9:48:A0:A4:FB:4D:BF:6C:3A:25:19:84:37:74:29:61:80:E3:1B:80:70:CF:82:77:44:C4:4C:B6:AE:73:E9:3D:45:E7:98:57:D6:11:4F
:EC:57:1A:BC:DF:AA:E0:68:89:EA:6E:CB:32:1C:22:C2:1E:E7:1D:4E:F5:96:62:E1:52:B6:07:00:8A:F2:80:DF:DE:42:86:C2:9D:5F:07:89:2C:41:9B:47:85:B6:72:43:5
D:65:1D:EC:A7:64:74:9D:36:13:AE:DA:72:55:7A:DB:95:70:CF:0F:B4:38:A1:F6:D1:70:6A:3B:8B:4E:F1:8C:B4:4E:E2:67:65:01:9F:03:FB:52:C5:D7:E9:EE:1C:4D:5A:
55:C5:1E:F9:1A:44:64:DF:8F:DC:BA:B6:FF:56:55:9A:E0:70:D6:DA:5D:1E:1C:DE:08:C4:FC:6B:A1:18:30:AA:B7:7D:A8:81:32:AE:DF:B7:07:30:1C:42:45:70:A0:31:6
1:00:CB:3E:2D:04:35:53:F3:F5:19:CC:36:F2:14:93:9E:EB:76:AB:A1:97:68:A2:12:38:5E:41:23:E7:47:D8:4F:AF:80:A0:49:74:52:87:2D:B3:06:CF:CE:AD:4F:74:8C:D
7:6F:EB:BC:92:2E:05:64:AF:F6:B1:3C:02:28:9C:62:7E:99:73:8F:D7:85:72:FD:26:70:45:72:62:8C:D5:3C:03:F3:02:8D:5A:92:C2:B5:FC:A5:92:09:D1:C1:D8:E7:68:E
5:D8:4B:97:28:86:FC:09:95:71:D0:3B:36:54:04:3E:0E:9F:4A:42:5C:6D:95:79:90:D9:E6:90:8F:5B:81:0B:F4:89:51:4E:F7:2D:2C:D4:09:73:7C:57:08:AC:50:8B:4B:F
0:35:52:C2:FA:FB:9F:47:D6:27:D2:B9:B7:A1:98:3E:26:B3:C0:2D:F3:7F:CD:8F:20:23:10:90:AC:ED:4B:C8:1A:44:85:7B:9E:22:7D:29:C8:74:1D:37:29:96:B3:E9:C9:
C5:23:03:F2:ED:38:4F:53:89:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *A5:3F:1E:24:4C:6C:F8:8B:D2:1B:72:98:46:50:CA:E8:86:55:B9:D8*

Authority Key Identifier *18:87:56:E0:6E:77:EE:24:35:3C:4E:73:9A:1F:D6:E1:E2:79:7E:2B*

Certificate Policies *Policy OID: 1.2.250.1.177.2.0.1.1*

CPS pointer: https://www.certigna.fr/autorites/

Authority Info Access *http://autorite.certigna.fr/certignarootca.der*

http://autorite.dhimyotis.com/certignarootca.der

CRL Distribution Points *http://crl.certigna.fr/certignarootca.crl*

http://crl.dhimyotis.com/certignarootca.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *1C:C3:58:A6:DF:A0:A7:6B:B5:47:06:60:D7:8F:3B:25:F2:3C:CD:63:95:66:7E:49:CC:FC:82:01:D
A:3D:19:2D*

Certificate fields details

Version: *3*

Serial Number: *331390735146257245090881749240634956198*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIGFTCCBP2gAwIBAgIRAPlPiLTzBzmpCdNvjtZMWaYwDQYJKoZIhvcNAQELBQAwNDELMAkGA1UE
BhMCRlIxEjAQBgNVBAoMCURoaW15b3RpczERMA8GA1UEAwwIQ2VydGlnbmEwHhcNMTUxMTI1MTAy
NDA3WhcNMjUxMTIyMTAyNDA3WjB7MQswCQYDVQQGEwJGUjESMBAGA1UECgwJREhJTVlPVElTMRww
GgYDVQQLDBMwMDAyIDQ4MTQ2MzA4MTAwMDM2MR0wGwYDVQRhDBROVFJGUi00ODE0NjMwODEwMDAz
NjEbMBkGA1UEAwwSQ2VydGlnbmEgRW50aXR5IENBMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIIC

CgKCAgEA0lTrAwYaOJpvbeSPdj8l4DVUCP2td5ZpJ6YBETkj0DEyairmzh+QdoqJusE0bPu7Deiv
GYLaIfZP53fVi+OM8/TfiQK61B53kgwI1tL1nEhdLd7G8G7SrKs0HGSofk6KMWqn4t2kVkkvotuH
5RzxW/TrYyF9kUrBvqcAqUigpPtNv2w6JRmEN3QpYYDjG4Bwz4J3RMRMtq5z6T1F55hX1hFP7Fca
vN+q4GiJ6m7LMhwiwh7nHU71lmLhUrYHAIrygN/eQobCnV8HiSxBm0eFtnJDXWUd7KdkdJ02E67a
clV625Vwzw+0OKH20XBqO4tO8Yy0TuJnZQGfA/tSxdfp7hxNWlXFHvkaRGTfj9y6tv9WVZrgcNba
XR4c3gjE/GuhGDCqt32ogTKu37cHMBxCRXCgMWEAyz4tBDVT8/UZzDbyFJOe63aroZdoohI4XkEj
50fYT6+AoEl0UoctswbPzq1PdIzXb+u8ki4FZK/2sTwCKJxifplzj9eFcv0mcEVyYozVPAPzAo1a
ksK1/KWSCdHB2Odo5dhLlyiG/AmVcdA7NlQEPg6fSkJcbZV5kNnmkI9bgQv0iVFO9y0s1AlzfFcI
rFCLS/A1UsL6+59H1ifSubehmD4ms8At83/NjyAjEJCs7UvIGkSFe54ifSnIdB03KZaz6cnFIwPy
7ThPU4kCAwEAAaOCAdkwggHVMBIGA1UdEwEB/wQIMAYBAf8CAQAwDgYDVR0PAQH/BAQDAgEGMB0G
A1UdDgQWBBSlPx4kTGz4i9IbcphGUMrohlW52DBkBgNVHSMEXTBbgBQa7f5BOZC0JFm+AfJS1UX2
WjncEaE4pDYwNDELMAkGA1UEBhMCRllxEjAQBgNVBAoMCURoaW15b3RpczERMA8GA1UEAwwIQ2Vy
dGlnbmGCCQD+3OMBD8ll/zBJBgNVHSAEQjBAMD4GCiqBegGBMQEAAQIwMDAuBggrBgEFBQcCARYi
aHR0cHM6Ly93d3cuY2VydGlnbmEuZnIvYXV0b3JpdGVzLzB8BggrBgEFBQcBAQRwMG4wNAYIKwYB
BQUHMAKGKGh0dHA6Ly9hdXRvcml0ZS5jZXJ0aWduYS5mci9jZXJ0aWduYS5kZXIwNgYIKwYBBQUH
MAKGKmh0dHA6Ly9hdXRvcml0ZS5kaGlteW90aXMuY29tL2NlcnRpZ25hLmRlcjBhBgNVHR8EWjBY
MCmgJ6AlhiNodHRwOi8vY3JsLmNlcnRpZ25hLmZyL2NlcnRpZ25hLmNybDAroCmgJ4YlaHR0cDov
L2NybC5kaGlteW90aXMuY29tL2NlcnRpZ25hLmNybDANBgkqhkiG9w0BAQsFAAOCAQEAq05OtV0W
mCyLpzxxcw98xPV8OiY56TQch4KEGotY1Dfw7H0nM7lap/6kAZkUwfI4WJt4piRedJHgasQOj+aJ
bpxCYX7Hv7vCnGDKZFC6c/vY3B/stbQRGTl//7+iKB2fgB/FoQOohrZqO77C0tqp1KuTfCSq/XAy
ZNtXoVn+YDaILMUHp2vslSHh131XPGjkloeXTMLf/+RcVVimMyAUjwdfcIUQEGU4Z5suQNWiwCU8
9l1UY7qaWC9As/GqWo3vqQG9ALG+HBFBr1HSPnUjW88J6CYUVxOcTDfAj3eJtvUF/3dFjPl6jM4r AJNeg+LqU6kQ+z/50yhrdgJ/A8cZiQ==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Certigna*

Issuer O: *Dhimyotis*

Issuer C: *FR*

Subject CN: *Certigna Entity CA*

Subject 2.5.4.97: *NTRFR-48146308100036*

Subject OU: *0002 48146308100036*

Subject O: *DHIMYOTIS*

Subject C: *FR*

Valid from: *Wed Nov 25 11:24:07 CET 2015*

Valid to: *Sat Nov 22 11:24:07 CET 2025*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:D2:54:EB:03:06:1A:38:9A:6F:6D:E4:8F:76:3F:25:E0:
35:54:08:FD:AD:77:96:69:27:A6:01:11:39:23:D0:31:32:6A:2A:E6:CE:1F:90:76:8A:89:BA:C1:34:6C:FB:BB:0D:E8:AF:19:82:DA:21:F6:4F:E7:77:D5:8B:E3:8C:F3:F4
:DF:89:02:BA:D4:1E:77:92:0C:08:D6:D2:F5:9C:48:5D:2D:DE:C6:F0:6E:D2:AC:AB:34:1C:64:A8:7E:4E:8A:31:6A:A7:E2:DD:A4:56:49:2F:A2:DB:87:E5:1C:F1:5B:F4:
EB:63:21:7D:91:4A:C1:BE:A7:00:A9:48:A0:A4:FB:4D:BF:6C:3A:25:19:84:37:74:29:61:80:E3:1B:80:70:CF:82:77:44:C4:4C:B6:AE:73:E9:3D:45:E7:98:57:D6:11:4F
:EC:57:1A:BC:DF:AA:E0:68:89:EA:6E:CB:32:1C:22:C2:1E:E7:1D:4E:F5:96:62:E1:52:B6:07:00:8A:F2:80:DF:DE:42:86:C2:9D:5F:07:89:2C:41:9B:47:85:B6:72:43:5
D:65:1D:EC:A7:64:74:9D:36:13:AE:DA:72:55:7A:DB:95:70:CF:0F:B4:38:A1:F6:D1:70:6A:3B:8B:4E:F1:8C:B4:4E:E2:67:65:01:9F:03:FB:52:C5:D7:E9:EE:1C:4D:5A:
55:C5:1E:F9:1A:44:64:DF:8F:DC:BA:B6:FF:56:55:9A:E0:70:D6:DA:5D:1E:1C:DE:08:C4:FC:6B:A1:18:30:AA:B7:7D:A8:81:32:AE:DF:B7:07:30:1C:42:45:70:A0:31:6
1:00:CB:3E:2D:04:35:53:F3:F5:19:CC:36:F2:14:93:9E:EB:76:AB:A1:97:68:A2:12:38:5E:41:23:E7:47:D8:4F:AF:80:A0:49:74:52:87:2D:B3:06:CF:CE:AD:4F:74:8C:D
7:6F:EB:BC:92:2E:05:64:AF:F6:B1:3C:02:28:9C:62:7E:99:73:8F:D7:85:72:FD:26:70:45:72:62:8C:D5:3C:03:F3:02:8D:5A:92:C2:B5:FC:A5:92:09:D1:C1:D8:E7:68:E
5:D8:4B:97:28:86:FC:09:95:71:D0:3B:36:54:04:3E:0E:9F:4A:42:5C:6D:95:79:90:D9:E6:90:8F:5B:81:0B:F4:89:51:4E:F7:2D:2C:D4:09:73:7C:57:08:AC:50:8B:4B:F

0:35:52:C2:FA:FB:9F:47:D6:27:D2:B9:B7:A1:98:3E:26:B3:C0:2D:F3:7F:CD:8F:20:23:10:90:AC:ED:4B:C8:1A:44:85:7B:9E:22:7D:29:C8:74:1D:37:29:96:B3:E9:C9:C5:23:03:F2:ED:38:4F:53:89:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *A5:3F:1E:24:4C:6C:F8:8B:D2:1B:72:98:46:50:CA:E8:86:55:B9:D8*

Authority Key Identifier *1A:ED:FE:41:39:90:B4:24:59:BE:01:F2:52:D5:45:F6:5A:39:DC:11*

Certificate Policies *Policy OID: 1.2.250.1.177.1.0.1.2*

CPS pointer: https://www.certigna.fr/autorites/

Authority Info Access *http://autorite.certigna.fr/certigna.der*

http://autorite.dhimyotis.com/certigna.der

CRL Distribution Points *http://crl.certigna.fr/certigna.crl*

http://crl.dhimyotis.com/certigna.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *EB:BF:4D:C6:00:C1:7D:A0:43:81:DE:FD:CF:C1:19:C3:F3:4E:FB:4A:04:D0:86:09:10:B8:13:C7:79:2D:75:85*

X509SubjectName

Subject CN: *Certigna Entity CA*

Subject 2.5.4.97: *NTRFR-48146308100036*

Subject OU: *0002 48146308100036*

Subject O: *DHIMYOTIS*

Subject C: *FR*

X509SKI

X509 SK I *pT8eJExs+IvSG3KYRlDK6IZVudg=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2017-04-30T22:00:00Z*

TSP Service Definition URI

URI *[en]* *http://politique.certigna.fr/en/PCcertignaentityca.pdf*

URI *[fr]* *http://politique.certigna.fr/PCcertignaentityca.pdf*

8.8.1 - Extension (critical): Qualifiers [QCWithQSCD]

Qualifier type description *[en]* *undefined.*

[fr] *undefined.*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithQSCD*

Criteria list assert=all

Key Usage *[digitalSignature]* *true*

Policy Identifier nodes:

Identifier *1.2.250.1.177.2.6.1.4.1*

8.8.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

8.9 - Service (granted): Certigna Entity CA - Cachet de signature de jetons d'horodatage ** - 1.2.250.1.177.2.6.1.6.1

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Certigna Entity CA - Cachet de signature de jetons d'horodatage ** - 1.2.250.1.177.2.6.1.6.1*

Name *[fr]* *Certigna Entity CA - Cachet de signature de jetons d'horodatage ** - 1.2.250.1.177.2.6.1.6.1*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *198429372998709978411380447595286256357*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIHDzCCBPegAwIBAgIRAJVIG2zmMiFC/oSZgw58WuUwDQYJKoZIhvcNAQELBQAwWjELMAkGA1UE
BhMCRlIxEjAQBgNVBAoMCURoaW15b3RpczEcMBoGA1UECwwTMDAwMiA0ODE0NjMwODEwMDAzNjEZ
MBcGA1UEAwwQQ2VydGlnbmEgUm9vdCBDQTAeFw0xNTExMjUxMDI3NTRaFw0zMzA2MDMxMDI3NTRa
MHsxCzAJBgNVBAYTAkZSMRIwEAYDVQQKDAlESElNWU9USVMxHDAaBgNVBAsMEzAwMDIgNDgxNDYz
MDgxMDAwMzYxHTAbBgNVBGEMFE5UUkZSLTQ4MTQ2MzA4MTAwMDM2MRswGQYDVQQDDBJDZXJ0aWdu
YSBFbnRpdHkgQ0EwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDSVOsDBho4mm9t5I92
PyXgNVQI/a13lmknpgEROSPQMTJqKubOH5B2iom6wTRs+7sN6K8Zgtoh9k/nd9WL44zz9N+JArrU
HneSDAjW0vWcSF0t3sbwbtKsqzQcZKh+TooxaqfI3aRWSS+i24flHPFb9OtjIX2RSsG+pwCpSKCk
+02/bDolGYQ3dClhgOMbgHDPgndExEy2rnPpPUXnmFfWEU/sVxq836rgaInqbssyHCLCHucdTvWW
YuFStgcAivKA395ChsKdXweJLEGbR4W2ckNdZR3sp2R0nTYTrtpyVXrblXDPD7Q4ofbRcGo7i07x
jLRO4mdlAZ8D+1LF1+nuHE1aVcUe+RpEZN+P3Lq2/1ZVmuBw1tpdHhzeCMT8a6EYMKq3faiBMq7f
twcwHEJFcKAxYQDLPi0ENVPz9RnMNvIUk57rdquhl2iiEjheQSPnR9hPr4CgSXRShy2zBs/OrU90
jNdv67ySLgVkr/axPAIonGJ+mXOP14Vy/SZwRXJijNU8A/MCjVqSwrX8pZlJ0cHY52jl2EuXKIb8
CZVx0Ds2VAQ+Dp9KQlxtlXmQ2eaQj1uBC/SJUU73LSzUCXN8VwisUItL8DVSwvr7n0fWJ9K5t6GY
PiazwC3zf82PICMQkKztS8gaRIV7niJ9Kch0HTcplrPpycUjA/LtOE9TiQIDAQABo4IBrTCCAakw
EgYDVR0TAQH/BAgwBgEB/wIBADAOBgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFKU/HiRMbPiL0hty
mEZQyuiGVbnYMB8GA1UdIwQYMBaAFBiHVuBud+4kNTxOc5of1uHieX4rMEkGA1UdIARCMEAwPgYK
KoF6AYExAgABATAwMC4GCCsGAQUFBwIBFiJodHRwczovL3d3dy5jZXJ0aWduYS5mci9hdXRvcml0
ZXMvMIGIBggrBgEFBQcBAQR8MHowOgYIKwYBBQUHMAKGLmh0dHA6Ly9hdXRvcml0ZS5jZXJ0aWdu
YS5mci9jZXJ0aWduYXJvb3RjYS5kZXIwPAYIKwYBBQUHMAKGMGh0dHA6Ly9hdXRvcml0ZS5kaGlt
eW90aXMuY29tL2NlcnRpZ25hcm9vdGNhLmRlcjBtBgNVHR8EZjBkMC+gLaArhilodHRwOi8vY3Js
LmNlcnRpZ25hLmZyL2NlcnRpZ25hcm9vdGNhLmNybDAxoC+gLYYraHR0cDovL2NybC5kaGlteW90
aXMuY29tL2NlcnRpZ25hcm9vdGNhLmNybDANBgkqhkiG9w0BAQsFAAOCAgEArfWJJUSj21DuIP7q
021HUkYV6dXH1FN9sEaOD5156JHV7M4FqkyubCjgfswL6NwW0UO2xanxFdcKPfx14M+H6Jgwqilz
W3InAwevKIx8+UivCpV47rDQe4/Yd//xbG0sd7+dMCvCAj7gOtlap/h1VJhwip6YVkaCp+q0nBbO
hEx+azqdc9Urh7eyj3no/4uJogc79vhrZ3QYm0AfAqosjH0IekZblyNOrqKR6NiMqGGNuWRJlg8r
pkEEakeTwIofh2lByrvlKIGcXRdl/oFhxDiC7Q3sCCpwq2VEmNAxg+ZWh4OnJxLx2uC8tDgN6IIH
+4TztUyO+KUG1Xnw1Mlg2dQKqt1B5/xvVKPOG2LNcUCeNAt7QmgkIvefsuxrHcFI2qZ7I9spo89w
je2BCY1ey0lkePGyzX8jy2CLTrFvfGhtw/S28L9oryrW5XS8J5ebAS+w+G2lda4rowb8EOjhXDVY
pA93yAB5SWjwWLzjcVn2WcJGOhEp9iZsVUDni/0b/JL7ovqtcPlY7Z9RtAg1SXY0SUc/CEVCbQM2
5EPcoNryEj7RivjYSZeJdwZ9/UoKq/be9dHqssrr1PusyLptEmUjV9a4d91NHiRwbHboyX77LJXj
9M0jc0WCwSbAyViEXJZx1jLAjakWnh5bTrmipLf7Mc8Fk3xw61zpX9ow1gc=

-----END CERTIFICATE-----

Signature algorithm:	*SHA256withRSA*
Issuer CN:	*Certigna Root CA*
Issuer OU:	*0002 48146308100036*
Issuer O:	*Dhimyotis*
Issuer C:	*FR*
Subject CN:	*Certigna Entity CA*
Subject 2.5.4.97:	*NTRFR-48146308100036*
Subject OU:	*0002 48146308100036*
Subject O:	*DHIMYOTIS*
Subject C:	*FR*
Valid from:	*Wed Nov 25 11:27:54 CET 2015*
Valid to:	*Fri Jun 03 12:27:54 CEST 2033*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:D2:54:EB:03:06:1A:38:9A:6F:6D:E4:8F:76:3F:25:E0:35:54:08:FD:AD:77:96:69:27:A6:01:11:39:23:D0:31:32:6A:2A:E6:CE:1F:90:76:8A:89:BA:C1:34:6C:FB:BB:0D:E8:AF:19:82:DA:21:F6:4F:E7:77:D5:8B:E3:8C:F3:F4:DF:89:02:BA:D4:1E:77:92:0C:08:D6:D2:F5:9C:48:5D:2D:DE:C6:F0:6E:D2:AC:AB:34:1C:64:A8:7E:4E:8A:31:6A:A7:E2:DD:A4:56:49:2F:A2:DB:87:E5:1C:F1:5B:F4:EB:63:21:7D:91:4A:C1:BE:A7:00:A9:48:A0:A4:FB:4D:BF:6C:3A:25:19:84:37:74:29:61:80:E3:1B:80:70:CF:82:77:44:C4:4C:B6:AE:73:E9:3D:45:E7:98:57:D6:11:4F:EC:57:1A:BC:DF:AA:E0:68:89:EA:6E:CB:32:1C:22:C2:1E:E7:1D:4E:F5:96:62:E1:52:B6:07:00:8A:F2:80:DF:DE:42:86:C2:9D:5F:07:89:2C:41:9B:47:85:B6:72:43:5D:65:1D:EC:A7:64:74:9D:36:13:AE:DA:72:55:7A:DB:95:70:CF:0F:B4:38:A1:F6:D1:70:6A:3B:8B:4E:F1:8C:B4:4E:E2:67:65:01:9F:03:FB:52:C5:D7:E9:EE:1C:4D:5A:55:C5:1E:F9:1A:44:64:DF:8F:DC:BA:B6:FF:56:55:9A:E0:70:D6:DA:5D:1E:1C:DE:08:C4:FC:6B:A1:18:30:AA:B7:7D:A8:81:32:AE:DF:B7:07:30:1C:42:45:70:A0:31:61:00:CB:3E:2D:04:35:53:F3:F5:19:CC:36:F2:14:93:9E:EB:76:AB:A1:97:68:A2:12:38:5E:41:23:E7:47:D8:4F:AF:80:A0:49:74:52:87:2D:B3:06:CF:CE:AD:4F:74:8C:D7:6F:EB:BC:92:2E:05:64:AF:F6:B1:3C:02:28:9C:62:7E:99:73:8F:D7:85:72:FD:26:70:45:72:62:8C:D5:3C:03:F3:02:8D:5A:92:C2:B5:FC:A5:92:09:D1:C1:D8:E7:68:E5:D8:4B:97:28:86:FC:09:95:71:D0:3B:36:54:04:3E:0E:9F:4A:42:5C:6D:95:79:90:D9:E6:90:8F:5B:81:0B:F4:89:51:4E:F7:2D:2C:D4:09:73:7C:57:08:AC:50:8B:4B:F0:35:52:C2:FA:FB:9F:47:D6:27:D2:B9:B7:A1:98:3E:26:B3:C0:2D:F3:7F:CD:8F:20:23:10:90:AC:ED:4B:C8:1A:44:85:7B:9E:22:7D:29:C8:74:1D:37:29:96:B3:E9:C9:C5:23:03:F2:ED:38:4F:53:89:02:03:01:00:01

Basic Constraints	*IsCA: true - Path length: 0*
Subject Key Identifier	*A5:3F:1E:24:4C:6C:F8:8B:D2:1B:72:98:46:50:CA:E8:86:55:B9:D8*
Authority Key Identifier	*18:87:56:E0:6E:77:EE:24:35:3C:4E:73:9A:1F:D6:E1:E2:79:7E:2B*
Certificate Policies	*Policy OID: 1.2.250.1.177.2.0.1.1* *CPS pointer: https://www.certigna.fr/autorites/*
Authority Info Access	*http://autorite.certigna.fr/certignarootca.der* *http://autorite.dhimyotis.com/certignarootca.der*
CRL Distribution Points	*http://crl.certigna.fr/certignarootca.crl* *http://crl.dhimyotis.com/certignarootca.crl*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*1C:C3:58:A6:DF:A0:A7:6B:B5:47:06:60:D7:8F:3B:25:F2:3C:CD:63:95:66:7E:49:CC:FC:82:01:DA:3D:19:2D*

Certificate fields details

Version:	*3*
Serial Number:	*331390735146257245090881749240634956198*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIGFTCCBP2gAwIBAgIRAPlPiLTzBzmpCdNvjtZMWaYwDQYJKoZIhvcNAQELBQAwNDELMAkGA1UE
BhMCRlIxEjAQBgNVBAoMCURoaW15b3RpczERMA8GA1UEAwwIQ2VydGlnbmEwHhcNMTUxMTI1MTAy
NDA3WhcNMjUxMTIyMTAyNDA3WjB7MQswCQYDVQQGEwJGUjESMBAGA1UECgwJREhJTVlPVElTMRww
GgYDVQQLDBMwMDAyIDQ4MTQ2MzA4MTAwMDM2MR0wGwYDVQRhDBROVFJGUi00ODE0NjMwODEwMDAz
NjEbMBkGA1UEAwwSQ2VydGlnbmEgRW50aXR5IENBMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIIC
CgKCAgEA0lTrAwYaOJpvbeSPdj8l4DVUCP2td5ZpJ6YBETkj0DEyairmzh+QdoqJusE0bPu7Deiv
GYLaIfZP53fVi+OM8/TfiQK61B53kgwI1tL1nEhdLd7G8G7SrKs0HGSofk6KMWqn4t2kVkkvotuH
5RzxW/TrYyF9kUrBvqcAqUigpPtNv2w6JRmEN3QpYYDjG4Bwz4J3RMRMtq5z6T1F55hX1hFP7Fca
vN+q4GiJ6m7LMhwiwh7nHU71lmLhUrYHAIrygN/eQobCnV8HiSxBm0eFtnJDXWUd7KdkdJ02E67a
clV625Vwzw+0OKH20XBqO4tO8Yy0TuJnZQGfA/tSxdfp7hxNWlXFHvkaRGTfj9y6tv9WVZrgcNba

XR4c3gjE/GuhGDCqt32ogTKu37cHMBxCRXCgMWEAyz4tBDVT8/UZzDbyFJOe63aroZdoohI4XkEj
50fYT6+AoEl0UoctswbPzq1PdIzXb+u8ki4FZK/2sTwCKJxifplzj9eFcv0mcEVyYozVPAPzAo1a
ksK1/KWSCdHB2Odo5dhLlyiG/AmVcdA7NlQEPg6fSkJcbZV5kNnmkI9bgQv0iVFO9y0s1AlzfFcI
rFCLS/A1UsL6+59H1ifSubehmD4ms8At83/NjyAjEJCs7UvIGkSFe54ifSnIdB03KZaz6cnFIwPy
7ThPU4kCAwEAAaOCAdkwggHVMBIGA1UdEwEB/wQIMAYBAf8CAQAwDgYDVR0PAQH/BAQDAgEGMB0G
A1UdDgQWBBSlPx4kTGz4i9IbcphGUMrohlW52DBkBgNVHSMEXTBbgBQa7f5BOZC0JFm+AfJS1UX2
WjncEaE4pDYwNDELMAkGA1UEBhMCRlIxEjAQBgNVBAoMCURoaW15b3RpczERMA8GA1UEAwwIQ2Vy
dGlnbmGCCQD+3OMBD8ll/zBJBgNVHSAEQjBAMD4GCiqBegGBMQEAAQIwMDAuBggrBgEFBQcCARYi
aHR0cHM6Ly93d3cuY2VydGlnbmEuZnIvYXV0b3JpdGVzLzB8BggrBgEFBQcBAQRwMG4wNAYIKwYB
BQUHMAKGKGh0dHA6Ly9hdXRvcml0ZS5jZXJ0aWduYS5mci9jZXJ0aWduYS5kZXIwNgYIKwYBBQUH
MAKGKmh0dHA6Ly9hdXRvcml0ZS5kaGlteW90aXMuY29tL2NlcnRpZ25hLmRlcjBhBgNVHR8EWjBY
MCmgJ6AlhiNodHRwOi8vY3JsLmNlcnRpZ25hLmZyL2NlcnRpZ25hLmNybDAroCmgJ4YlaHR0cDov
L2NybC5kaGlteW90aXMuY29tL2NlcnRpZ25hLmNybDANBgkqhkiG9w0BAQsFAAOCAQEAq05OtV0W
mCyLpzxxcw98xPV8OiY56TQch4KEGotY1Dfw7H0nM7lap/6kAZkUwfI4WJt4piRedJHgasQOj+aJ
bpxCYX7Hv7vCnGDKZFC6c/vY3B/stbQRGTl//7+iKB2fgB/FoQOohrZqO77C0tqp1KuTfCSq/XAy
ZNtXoVn+YDaILMUHp2vslSHh131XPGjkloeXTMLf/+RcVVimMyAUjwdfcIUQEGU4Z5suQNWiwCU8
9l1UY7qaWC9As/GqWo3vqQG9ALG+HBFBr1HSPnUjW88J6CYUVxOcTDfAj3eJtvUF/3dFjPl6jM4r
AJNeg+LqU6kQ+z/50yhrdgJ/A8cZiQ==

-----END CERTIFICATE-----

Signature algorithm:	*SHA256withRSA*
Issuer CN:	*Certigna*
Issuer O:	*Dhimyotis*
Issuer C:	*FR*
Subject CN:	*Certigna Entity CA*
Subject 2.5.4.97:	*NTRFR-48146308100036*
Subject OU:	*0002 48146308100036*
Subject O:	*DHIMYOTIS*
Subject C:	*FR*
Valid from:	*Wed Nov 25 11:24:07 CET 2015*
Valid to:	*Sat Nov 22 11:24:07 CET 2025*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:D2:54:EB:03:06:1A:38:9A:6F:6D:E4:8F:76:3F:25:E0:
35:54:08:FD:AD:77:96:69:27:A6:01:11:39:23:D0:31:32:6A:2A:E6:CE:1F:90:76:8A:89:BA:C1:34:6C:FB:BB:0D:E8:AF:19:82:DA:21:F6:4F:E7:77:D5:8B:E3:8C:F3:F4
:DF:89:02:BA:D4:1E:77:92:0C:08:D6:D2:F5:9C:48:5D:2D:DE:C6:F0:6E:D2:AC:AB:34:1C:64:A8:7E:4E:8A:31:6A:A7:E2:DD:A4:56:49:2F:A2:DB:87:E5:1C:F1:5B:F4:
EB:63:21:7D:91:4A:C1:BE:A7:00:A9:48:A0:A4:FB:4D:BF:6C:3A:25:19:84:37:74:29:61:80:E3:1B:80:70:CF:82:77:44:C4:4C:B6:AE:73:E9:3D:45:E7:98:57:D6:11:4F
:EC:57:1A:BC:DF:AA:E0:68:89:EA:6E:CB:32:1C:22:C2:1E:E7:1D:4E:F5:96:62:E1:52:B6:07:00:8A:F2:80:DF:DE:42:86:C2:9D:5F:07:89:2C:41:9B:47:85:B6:72:43:5
D:65:1D:EC:A7:64:74:9D:36:13:AE:DA:72:55:7A:DB:95:70:CF:0F:B4:38:A1:F6:D1:70:6A:3B:8B:4E:F1:8C:B4:4E:E2:67:65:01:9F:03:FB:52:C5:D7:E9:EE:1C:4D:5A:
55:C5:1E:F9:1A:44:64:DF:8F:DC:BA:B6:FF:56:55:9A:E0:70:D6:DA:5D:1E:1C:DE:08:C4:FC:6B:A1:18:30:AA:B7:7D:A8:81:32:AE:DF:B7:07:30:1C:42:45:70:A0:31:6
1:00:CB:3E:2D:04:35:53:F3:F5:19:CC:36:F2:14:93:9E:EB:76:AB:A1:97:68:A2:12:38:5E:41:23:E7:47:D8:4F:AF:80:A0:49:74:52:87:2D:B3:06:CF:CE:AD:4F:74:8C:D
7:6F:EB:BC:92:2E:05:64:AF:F6:B1:3C:02:28:9C:62:7E:99:73:8F:D7:85:72:FD:26:70:45:72:62:8C:D5:3C:03:F3:02:8D:5A:92:C2:B5:FC:A5:92:09:D1:C1:D8:E7:68:E
5:D8:4B:97:28:86:FC:09:95:71:D0:3B:36:54:04:3E:0E:9F:4A:42:5C:6D:95:79:90:D9:E6:90:8F:5B:81:0B:F4:89:51:4E:F7:2D:2C:D4:09:73:7C:57:08:AC:50:8B:4B:F
0:35:52:C2:FA:FB:9F:47:D6:27:D2:B9:B7:A1:98:3E:26:B3:C0:2D:F3:7F:CD:8F:20:23:10:90:AC:ED:4B:C8:1A:44:85:7B:9E:22:7D:29:C8:74:1D:37:29:96:B3:E9:C9:
C5:23:03:F2:ED:38:4F:53:89:02:03:01:00:01

Basic Constraints	*IsCA: true - Path length: 0*

Subject Key Identifier

A5:3F:1E:24:4C:6C:F8:8B:D2:1B:72:98:46:50:CA:E8:86:55:B9:D8

Authority Key Identifier

1A:ED:FE:41:39:90:B4:24:59:BE:01:F2:52:D5:45:F6:5A:39:DC:11

Certificate Policies

Policy OID: 1.2.250.1.177.1.0.1.2

CPS pointer: https://www.certigna.fr/autorites/

Authority Info Access

http://autorite.certigna.fr/certigna.der

http://autorite.dhimyotis.com/certigna.der

CRL Distribution Points

http://crl.certigna.fr/certigna.crl

http://crl.dhimyotis.com/certigna.crl

Key Usage:

keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

EB:BF:4D:C6:00:C1:7D:A0:43:81:DE:FD:CF:C1:19:C3:F3:4E:FB:4A:04:D0:86:09:10:B8:13:C7:79:2D:75:85

X509SubjectName

Subject CN:

Certigna Entity CA

Subject 2.5.4.97:

NTRFR-48146308100036

Subject OU:

0002 48146308100036

Subject O:

DHIMYOTIS

Subject C:

FR

X509SKI

X509 SK I

pT8eJExs+IvSG3KYRlDK6IZVudg=

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time

2017-04-30T22:00:00Z

TSP Service Definition URI

URI *[en]* *http://politique.certigna.fr/en/PCcertignaentityca.pdf*

URI *[fr]* *http://politique.certigna.fr/PCcertignaentityca.pdf*

8.9.1 - Extension (critical): Qualifiers [QCWithQSCD]

Qualifier type description	*[en]*	*undefined.*
	[fr]	*undefined.*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithQSCD*

Criteria list assert=all

Key Usage	*[digitalSignature]*	*true*

Policy Identifier nodes:

Identifier *1.2.250.1.177.2.6.1.6.1*

8.9.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

9 - TSP: Ministère de la Justice

TSP Name

Name	*[en]*	*Ministère de la Justice*
Name	*[fr]*	*Ministère de la Justice*

TSP Trade Name

Name	*[en]*	*VATFR-19130005093*
Name	*[fr]*	*VATFR-19130005093*

PostalAddress

Street Address	*[fr]*	*Ministère de la Justice - Secrétariat Général - Direction de Projet dématérialisation, 13, place Vendôme*
Locality	*[fr]*	*Paris Cedex 01*
Postal Code	*[fr]*	*75042*
Country Name	*[fr]*	*FR*

PostalAddress

Street Address *[en]* *Ministère de la Justice - Secrétariat Général - Direction de Projet dématérialisation, 13, place Vendôme*

Locality *[en]* *PARIS CEDEX 01*

Postal Code *[en]* *75042*

Country Name *[en]* *FR*

ElectronicAddress

URI *mailto:ministere@justice.gouv.fr*

URI *http://www.justice.gouv.fr/multilinguisme-12198/english-12200/*

URI *mailto:ministere@justice.gouv.fr*

URI *http://www.justice.gouv.fr/*

TSP Information URI

URI *[en]* *http://www.justice.gouv.fr/igc/ants/en/*

URI *[fr]* *http://www.justice.gouv.fr/igc/ants/*

9.1 - Service (granted): MJL Signature RGS ***

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *MJL Signature RGS ****

Name *[fr]* *MJL Signature RGS ****

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *149200323474317685325070199854501011418359 3*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIFFDCCAvygAwIBAgISESCaerEC4lwbVo8nP27mLEGpMA0GCSqGSIb3DQEBCwUAMGUxCzAJBgNV
BAYTAkZSMRAwDgYDVQQKEwdKdXN0aWNlMRcwFQYDVQQLEw4wMDAyIDExMDAxMDAxNDErMCkGA1UE
AwwiQXV0b3JpdMOpIGRlIGNlcnRpZmljYXRpb24gSnVzdGljZTAeFw0xMDA5MzAwMDAwMDBaFw0x
NjA5MzAwMDAwMDBaMGcxCzAJBgNVBAYTAkZSMRAwDgYDVQQKEwdKdXN0aWNlMRcwFQYDVQQLEw4w
MDAyIDExMDAxMDAxNDEtMCsGA1UEAwwkQXV0b3JpdMOpIGRlIGNlcnRpZmljYXRpb24gcGVyc29u
bmVzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAm7FyelV3dVCEQhGv2ygkxraBlkZg
h/s5X03DmEY7GhhJ7rHoQq2bUZth/s082z6/ndt1MiwuZxzvJ6vt95JETN/MFZH4zKGTQ0kh9zWw
RNuD9SWztTdiQlkojOzR8uYah1EJ7l/V2dnWhWboWqqjitSmR35O74CZRDjkYUnPBkHoGfWuN1Rs
HRP2oa3e415wsrEKgHaP5cxq6J5eWwYs3CK48GahOyniu+VjhinKiMeO99A8GnnOrumGjxNon5/H
XiRe+FdXhgu/WMpGgnzgjUPFsMSj6pZ93Ks2+Z3B/XAkE57d64EJ5RdxQOekG7Mr+oX1q6MsH2Iy
BXZbOfpJIwIDAQABo4G7MIG4MA4GA1UdDwEB/wQEAwIBBjARBgNVHSAECjAIMAYGBFUdIAAwEgYD
VR0TAQH/BAgwBgEB/wIBADA/BgNVHR8EODA2MDSgMqAwhi5odHRwOi8vd3d3Lmp1c3RpY2UuZ291
di5mci9pZ2MvYW50cy9tal9hcmwuY3JsMB0GA1UdDgQWBBRVazbHU29KMXBGbQKsLvSbFraxEDAf
BgNVHSMEGDAWgBR86ZsVtM1DuRGl5puKpW01CLLh3TANBgkqhkiG9w0BAQsFAAOCAgEAuI7yqFRb
fKc2DH0Bt/vpNsedCt66W8AZ6junhYq66kUC4ky7U6vjj0xV3q2gAwBgLri8evtDt1i7OxprfVJt
NxZ5LC+mxbvBKt3Oj4bKPivuZHnBCnXrr3wbemfEVke6dBUU9gU0sPIG9rfcxkFzms0KQkmkJrXB
bpsTE4mVQQ4X9NUZeoWDtzqsN8TR63nJo+PcjwtTcCncqgHxOCJu2JGTEh+WWpLB35LxL/MtmV4w
q9nFaT3W7A4QawQfFuYM8iQSGp5Qaig2sCMrFbhFSWfIF68PUtqFW7VQPhHrRPwP5CpQsCzAdfB9
bU8EcGLyPEx4CO5ZHHJmhC9S+dGTggM/aR/3IWVj/VaAGTQ0m1A7KrtAPB9EU+L7CDbNOEZBYsD1
89tK6XgsSz5Itmq+E6oXUuEgLW+MrZB2NVkI2UfaseCG2C/upvu8JGy0xt+5WhjyoU1nDSiOCMXC
MO7FTnWtzz5rM+m/P9X/lOJmkxncUj7Lo4ak/1iRJPYJK9L6+4cLnJueSNy0lW03RgiWroCavAVo
Qh36RpBB0i1JH9ERlaD6UNmQRl+MT4e6nz1XM63eux+GFq5ctOc6EkP0JdFpdR4hWFL1m6E2WnoT
A6LlZ9t0Wxp9wjXwJ344SniqWVjV/F1FK7eXGbhu37qGQeBvZfJSWNtmR6HIF965Fxk=

-----END CERTIFICATE-----

Signature algorithm:	*SHA256withRSA*
Issuer CN:	*Autorité de certification Justice*
Issuer OU:	*0002 110010014*
Issuer O:	*Justice*
Issuer C:	*FR*
Subject CN:	*Autorité de certification personnes*
Subject OU:	*0002 110010014*
Subject O:	*Justice*
Subject C:	*FR*
Valid from:	*Thu Sep 30 02:00:00 CEST 2010*
Valid to:	*Fri Sep 30 02:00:00 CEST 2016*
Public Key:	

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:9B:B1:72:7A:55:77:75:50:84:42:11:AF:DB:28:24:C6:
B6:81:96:46:60:87:FB:39:5F:4D:C3:98:46:3B:1A:18:49:EE:B1:E8:42:AD:9B:51:9B:61:FE:CD:3C:DB:3E:BF:9D:DB:75:32:2C:2E:67:1C:EF:27:AB:ED:F7:92:44:4C:DF
:CC:15:91:F8:CC:A1:93:43:49:21:F7:35:B0:44:DB:83:F5:25:B3:B5:37:62:42:59:28:8C:EC:D1:F2:E6:1A:87:51:09:EE:5F:D5:D9:D9:D6:85:66:E8:5A:AA:A3:8A:D4:A
6:47:7E:4E:EF:80:99:44:38:E4:61:49:CF:06:41:E8:19:F5:AE:37:54:6C:1D:13:F6:A1:AD:DE:E3:5E:70:B2:B1:0A:80:76:8F:E5:CC:6A:E8:9E:5E:5B:06:2C:DC:22:B8:F
0:66:A1:3B:29:E2:BB:E5:63:86:29:CA:88:C7:8E:F7:D0:3C:1A:79:CE:AE:E9:86:8F:13:68:9F:9F:C7:5E:24:5E:F8:57:57:86:0B:BF:58:CA:46:82:7C:E0:8D:43:C5:B0:C
4:A3:EA:96:7D:DC:AB:36:F9:9D:C1:FD:70:24:13:9E:DD:EB:8
1:09:E5:17:71:40:E7:A4:1B:B3:2B:FA:85:F5:AB:A3:2C:1F:62:32:05:76:5B:39:FA:49:23:02:03:01:00:01

Certificate Policies	*Policy OID: 2.5.29.32.0*

Basic Constraints *IsCA: true - Path length: 0*

CRL Distribution Points *http://www.justice.gouv.fr/igc/ants/mj_arl.crl*

Subject Key Identifier *55:6B:36:C7:53:6F:4A:31:70:46:6D:02:AC:2E:F4:9B:16:B6:B1:10*

Authority Key Identifier *7C:E9:9B:15:B4:CD:43:B9:11:A5:E6:9B:8A:A5:6D:35:08:B2:E1:DD*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *7E:A0:86:B5:4E:03:E8:49:8D:CD:FD:C7:A9:41:34:D5:10:5A:F9:7E:22:BF:54:87:9F:EB:2E:EB:22:1F:B8:DC*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS101456/QCPPublic*

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Signature-3-Stars*

TSP Service Definition URI

URI *[en]* *http://www.justice.gouv.fr/igc/ants/en/MJL-CP-Person-CA_EN.pdf*

URI *[fr]* *http://www.justice.gouv.fr/igc/ants/MJ-PC-AC-Personnes.pdf*

9.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

9.1.2 - History instance n.1 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *MJL Signature RGS ****

Name *[fr]* *MJL Signature RGS ****

Service digital identities

X509SubjectName

Subject CN: *Autorité de certification personnes*

Subject OU: *0002 110010014*

Subject O: *Justice*

Subject C: *FR*

X509SKI

X509 SK I *VWs2x1NvSjFwRm0CrC70mxa2sRA=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2012-12-04T23:00:00Z*

9.2 - Service (granted): Autorité de certification personnes 3

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Autorité de certification personnes 3*

Name *[fr]* *Autorité de certification personnes 3*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1491991415056078467603751525407765416719609*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIFJzCCAw+gAwIBAgISESCRlk1x3MhZW/NP/J8IITT5MA0GCSqGSIb3DQEBCwUAMGUxCzAJBgNV
BAYTAkZSMRAwDgYDVQQKEwdKdXN0aWNlMRcwFQYDVQQLEw4wMDAyIDExMDAxMDAxNDErMCkGA1UE
AwwiQXV0b3JpdMOpIGRlIGNlcnRpZmljYXRpb24gSnVzdGljZTAeFw0xNjA2MDkwMDAwMDBaFw0y
MjA2MDkwMDAwMDBaMHoxCzAJBgNVBAYTAkZSMSEwHwYDVQQKDBhNaW5pc3TDqHJlIGRlIGxhIEp1
c3RpY2UxFzAVBgNVBAsMDjAwMDIgMTEwMDEwMDE0MS8wLQYDVQQDDCZBdXRvcml0w6kgZGUgY2Vy

dGlmaWNhdGlvbiBwZXJzb25uZXMgMzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMck
z0jkM5GfU2PVbWK0tK1S+6Lb2oY2TNlWTi2ZbdZsitgPhLDYnS10HC83fHfgsesu7MxbCDnSgql4
R/fBG+baHB/cmpE7K+qbN4+15edJGIV9Ho2AOJRUG2D/q1AS0pvjRQGyNDeUczJGOX2RjIMZ7PjM
FSWG7Ucm04WqEPdb2G/3xulo1j0vn9K22SUupkA52iNGChsvqg5nGYpoVR24YhziSDV0x0H3pGSJ
Nke15lA3KwvvV4XlJGToU5xLM49H/ia9BgyCXrDXzuRhQu//bb49Wsheq+nS4HyutOC5fGKljNCy
TVyrA/uVHjB5ABBC99rrKAQRprcUi7h+xLUCAwEAAaOBuzCBuDAOBgNVHQ8BAf8EBAMCAQYwEQYD
VR0gBAowCDAGBgRVHSAAMBIGA1UdEwEB/wQIMAYBAf8CAQAwPwYDVR0fBDgwNjA0oDKgMIYuaHR0
cDovL3d3dy5qdXN0aWNlLmdvdXYuZnIvaWdjL2FudHMvbWpfYXJsLmNybDAdBgNVHQ4EFgQUm+hX
3PC2Ibunkzud9qeCMWrgaFowHwYDVR0jBBgwFoAUfOmbFbTNQ7kRpeabiqVtNQiy4d0wDQYJKoZI
hvcNAQELBQADggIBAB/LS+rAqdXpTXyDWlWLROmywQ5gyuWm4CwzxWTe6+LyHPGLOiJ4Ke1gmSmy
c07PV0kj4oqkp7S4KZjBLySOn0pQR+YL7LzctHEW5xSi5wJKO8Vvm9o46qrD14T1bvrC6MbonimZ
KGiz6akYUPTjhRwpEu6Eu+HVDrwpuDwAPiZBIxAWlncrfJUlqUFMYesAhjo6o0w2FHB8dA4G+CuR
u8L+sTlBJ7OdBlfkGzMz4zyyUvQbxfhn3dpwx5SZewAB3MD91XH9A4+qNo9UkrxP6Pxeu1jlqqPF
6/VuvpT01IMu51esDo/oO8KNGh8WVWpwUlMHhd5+IV+TkQ6WAbj6VpiXEtdSQ6vq8Th7CKeMKye7
lN8joZZ4zn1B+hmJWRFD/XC2yCwfh6Oo8cQ84i5JnDMV1Nci5plBiOiP/eYG2jJ6y/OWxk5asXLD
1+M6WI/n5Wbm8TUO0jFJU8ppfM+nahT9ucWFR4SXn88D/JnVdWQysW+0qmsBu+uNoIdlxIEyNLcu
Ruv2EwPS4n0iFo/jl10Y6UiIpVW6GHsE8v849t6xIf0aJZT1uVzg/8TTbcQ14WNe83eRmeS0tRCw
di/t04W6eFixUkijGJqwaYhDGFd+Z+gm8r2gBaxX49xioLSs7yUU5l1UQY3MUR9dxHX/ItJyesYn TuCNeGPS2SsRvHKQ

-----END CERTIFICATE-----

Signature algorithm:	*SHA256withRSA*
Issuer CN:	*Autorité de certification Justice*
Issuer OU:	*0002 110010014*
Issuer O:	*Justice*
Issuer C:	*FR*
Subject CN:	*Autorité de certification personnes 3*
Subject OU:	*0002 110010014*
Subject O:	*Ministère de la Justice*
Subject C:	*FR*
Valid from:	*Thu Jun 09 02:00:00 CEST 2016*
Valid to:	*Thu Jun 09 02:00:00 CEST 2022*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C7:24:CF:48:E4:33:91:9F:53:63:D5:6D:62:B4:B4:AD:
52:FB:A2:DB:DA:86:36:4C:D9:56:4E:2D:99:6D:D6:6C:8A:D8:0F:84:B0:D8:9D:2D:74:1C:2F:37:7C:77:E0:B1:EB:2E:EC:CC:5B:08:39:D2:82:A9:78:47:F7:C1:1B:E6:
DA:1C:1F:DC:9A:91:3B:2B:EA:9B:37:8F:B5:E5:E7:49:18:85:7D:1E:8D:80:38:94:54:1B:60:FF:AB:50:12:D2:9B:E3:45:01:B2:34:37:94:73:32:46:39:7D:91:8C:83:19
:EC:F8:CC:15:25:86:ED:47:26:D3:85:AA:10:F7:5B:D8:6F:F7:C6:E9:68:D6:3D:2F:9F:D2:B6:D9:25:2E:A6:40:39:DA:23:46:0A:1B:2F:AA:0E:67:19:8A:68:55:1D:B8:6
2:1C:E2:48:35:74:C7:41:F7:A4:64:89:36:47:B5:E6:50:37:2B:0B:EF:57:85:E5:24:64:E8:53:9C:4B:33:8F:47:FE:26:BD:06:0C:82:5E:B0:D7:CE:E4:61:42:EF:FF:6D:BE
:3D:5A:C8:5E:AB:E9:D2:E0:7C:AE:B4:E0:B9:7C:62:A5:8C:D0:
B2:4D:5C:AB:03:FB:95:1E:30:79:00:10:42:F7:DA:EB:28:04:11:A6:B7:14:8B:B8:7E:C4:B5:02:03:01:00:01

Certificate Policies	*Policy OID: 2.5.29.32.0*
Basic Constraints	*IsCA: true - Path length: 0*

CRL Distribution Points *http://www.justice.gouv.fr/igc/ants/mj_arl.crl*

Subject Key Identifier *9B:E8:57:DC:F0:B6:21:BB:A7:93:3B:9D:F6:A7:82:31:6A:E0:68:5A*

Authority Key Identifier *7C:E9:9B:15:B4:CD:43:B9:11:A5:E6:9B:8A:A5:6D:35:08:B2:E1:DD*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *C8:24:AB:73:19:07:4F:6E:5A:49:94:D9:DE:9E:AF:4A:93:EC:A4:93:E9:6E:DF:0B:C2:D6:F1:FF:04:4B:BF:CD*

X509SubjectName

Subject CN: *Autorité de certification personnes 3*

Subject OU: *0002 110010014*

Subject O: *Ministère de la Justice*

Subject C: *FR*

X509SKI

X509 SK I *m+hX3PC2Ibunkzud9qeCMWrgaFo=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2017-10-31T23:00:00Z*

TSP Service Definition URI

URI *[en]* *http://www.justice.gouv.fr/igc/ants/en/MJL-CP-Person-CA_EN.pdf*

URI *[fr]* *http://www.justice.gouv.fr/igc/ants/MJ-PC-AC-Personnes.pdf*

9.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

9.2.2 - Extension (critical): Qualifiers [QCWithQSCD, QCForESig]

Qualifier type description *[en]* *undefined.*

[fr] *undefined.*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithQSCD*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForESig*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Policy Identifier nodes:

Identifier *1.2.250.1.120.3.1.1.2*

9.3 - Service (granted): Autorité de certification personnes 2

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Autorité de certification personnes 2*

Name *[fr]* *Autorité de certification personnes 2*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *149199901714582166470653110738814246177458 7*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIFJzCCAw+gAwIBAgISESCXTmloNGU3pr060zxeMer7MA0GCSqGSIb3DQEBCwUAMGUxCzAJBgNV
BAYTAkZSMRAwDgYDVQQKEwdKdXN0aWNlMRcwFQYDVQQLEw4wMDAyIDExMDAxMDAxNDErMCkGA1UE
AwwiQXV0b3JpdMOpIGRlIGNlcnRpZmljYXRpb24gSnVzdGljZTAeFw0xMzA3MjQwMDAwMDBaFw0x
OTA3MjQwMDAwMDBaMHoxCzAJBgNVBAYTAkZSMSEwHwYDVQQKDBhNaW5pc3TDqHJlIGRlIGxhIEp1
c3RpY2UxFzAVBgNVBAsMDjAwMDIgMTEwMDEwMDE0MS8wLQYDVQQDDCZBdXRvcml0w6kgZGUgY2Vy
dGlmaWNhdGlvbiBwZXJzb25uZXMgMjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALlz
jBFW64eNgmcG9MblL3hIYs92hOAMfWJqxAIKjW9uJsnStv0MbitJWGe8181FHjau25oVco0OrVN3
u+r8W4K/DKAttriRRe+2lt8Bk9Dnh6AnksdUzz07dGMLeqaCq0C4C2JCuRRRBHYcyWrf5T1fJ3rH
5bHltSjuOT+42j87pvDxTkUH++F/hOX/X89HyYX95joG9XOuDZ3v7wUWIEpTvdF7UWX7hD9+PoUg
kfQheeUI6jHVmelypFro9jS2w58JU9v8QMTsMNCXwtKmR1TqAPpqcJjCj7A79qwAXrbCV+udDXCm
FmXX4hodlvYGM3QVQXPApRTMdsgFpktVD5sCAwEAAaOBuzCBuDAOBgNVHQ8BAf8EBAMCAQYwEQYD
VR0gBAowCDAGBgRVHSAAMBIGA1UdEwEB/wQIMAYBAf8CAQAwPwYDVR0fBDgwNjA0oDKgMIYuaHR0
cDovL3d3dy5qdXN0aWNlLmdvdXYuZnIvaWdjL2FudHMvbWpfYXJsLmNybDAdBgNVHQ4EFgQU7KEd
G+efFtDldaNXcVFLGt1jozAwHwYDVR0jBBgwFoAUfOmbFbTNQ7kRpeabiqVtNQiy4d0wDQYJKoZI
hvcNAQELBQADggIBAHJrX058Xm5JoH+clNcvps+sAdQEbfw+2iBf8jCrP/n3t5MZOS9PkzXtpJ+I
xGSf3d5EyOKKoAXCsig1eNx1M7PMFP/yNg5rX1VL9BjyCZsBYfUgHkYQD9rPjlfuSeFehgpOGUlK

ksQb6fsBB3kPzrSBg56DuJnN0bsKb647d2Fo7DhAcC4r7B57W3YwZcJPoEphaoaDaYcbUR0srahB
oKPN1Dy6glTMNgWyUJMbwsOg20J0uEg3oMG+kLXmpINQmOIWAP61sHfxmAsp9hRBlSSD2Ichpv5B
v7sKqY/AOPQmgL0AVIOTsFcfGpsWgD1kYO6BFGgXNEt5ppxg7uGN9aUxa4LkEKeTTn4Sn/DtZ/5o
qSPHWQOrJlCh6c5rI+Yf3hZC+wMrjN3squxmOCzvOfFIyKW1uoWBDrYcJPRPROV4wQdJkN3pmZuA
JpBZDOhrfUOcT1G3PgtzhVX5E5WBucRzxzxXwoB9MOLT0Zsib0QImvW3u+SrnBg5MbToAWbZiMZB
O/mxGHvx5grzHEB/y7ipx6uZZm4vgvg22kuhh1yVdDl+zh98MCj8zlTg72HmP+C4X0gcVQFO14qR
k5zhl5Z6gyP9a13QPKNdky88LeHPmPMSMBwIZ4yVGoNFSRVO81S/bEvuS2HO8RDDpOGhT8d4KZ+d s4ZogXpwvKpoxAeB

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Autorité de certification Justice*

Issuer OU: *0002 110010014*

Issuer O: *Justice*

Issuer C: *FR*

Subject CN: *Autorité de certification personnes 2*

Subject OU: *0002 110010014*

Subject O: *Ministère de la Justice*

Subject C: *FR*

Valid from: *Wed Jul 24 02:00:00 CEST 2013*

Valid to: *Wed Jul 24 02:00:00 CEST 2019*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:B9:73:8C:11:56:EB:87:8D:82:67:06:F4:C6:E5:2F:78:48:62:CF:76:84:E0:0C:7D:62:6A:C4:02:0A:8D:6F:6E:26:C9:D2:B6:FD:0C:6E:2B:49:58:67:BC:D7:CD:45:1E:36:AE:DB:9A:15:72:8D:0E:AD:53:77:BB:EA:FC:5B:82:BF:0C:A0:2D:B6:B8:91:45:EF:B6:96:DF:01:93:D0:E7:87:A0:27:92:C7:54:CF:3D:3B:74:63:0B:7A:A6:82:AB:40:B8:0B:62:42:B9:14:51:04:76:1C:C9:6A:DF:E5:3D:5F:27:7A:C7:E5:B1:E5:B5:28:EE:39:3F:B8:DA:3F:3B:A6:F0:F1:4E:45:07:FB:E1:7F:84:E5:FF:5F:CF:47:C9:85:FD:E6:3A:06:F5:73:AE:0D:9D:EF:EF:05:16:20:4A:53:BD:D1:7B:51:65:FB:84:3F:7E:3E:85:20:91:F4:21:79:E5:08:EA:31:D5:99:E9:72:A4:5A:E8:F6:34:B6:C3:9F:09:53:DB:FC:40:C4:EC:30:D0:97:C2:D2:A6:47:54:EA:00:FA:6A:70:98:C2:8F:B0:3B:F6:AC:00:5E:B6:C2:57:EB:9D:0D:70:A6:16:65:D7:E2:1A:1D:96:F6:06:33:74:15:41:73:C0:A5:14:CC:76:C8:05:A6:4B:55:0F:9B:02:03:01:00:01

Certificate Policies *Policy OID: 2.5.29.32.0*

Basic Constraints *IsCA: true - Path length: 0*

CRL Distribution Points *http://www.justice.gouv.fr/igc/ants/mj_arl.crl*

Subject Key Identifier *EC:A1:1D:1B:E7:9F:16:D0:E5:75:A3:57:71:51:4B:1A:DD:63:A3:30*

Authority Key Identifier *7C:E9:9B:15:B4:CD:43:B9:11:A5:E6:9B:8A:A5:6D:35:08:B2:E1:DD*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint:

9D:EE:F3:5D:94:96:69:57:59:33:47:BE:80:F8:A4:46:44:30:45:E3:FF:63:7C:8F:F9:55:4A:E 7:85:D A:22:0E

X509SubjectName

Subject CN: *Autorité de certification personnes 2*

Subject OU: *0002 110010014*

Subject O: *Ministère de la Justice*

Subject C: *FR*

X509 SK I *7KEdG+efFtDldaNXcVFLGt1jozA=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2017-10-31T23:00:00Z*

TSP Service Definition URI

URI *[en]* *http://www.justice.gouv.fr/igc/ants/en/MJL-CP-Person-CA_EN.pdf*

URI *[fr]* *http://www.justice.gouv.fr/igc/ants/MJ-PC-AC-Personnes.pdf*

9.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

9.3.2 - Extension (critical): Qualifiers [QCWithQSCD, QCForESig]

Qualifier type description *[en]* *undefined.*

[fr] *undefined.*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithQSCD*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForESig*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Policy Identifier nodes:

Identifier *PolicySet 1.2.250.1.120.3.1.1.2*

10 - TSP: Docusign France

TSP Name

Name	*[en]*	*Docusign France*
Name	*[fr]*	*Docusign France*

TSP Trade Name

Name	*[en]*	*VATFR-71812611150*
Name	*[fr]*	*VATFR-71812611150*

PostalAddress

Street Address	*[en]*	*9-15, rue Maurice Mallet*
Locality	*[en]*	*Issy-les-Moulineaux*
Postal Code	*[en]*	*92130*
Country Name	*[en]*	*FR*

ElectronicAddress

URI	*https://www.docusign.fr*
URI	*https://www.docusign.fr*
URI	*mailto:emmanuel.montacutelli@docusign.com*
URI	*mailto:emmanuel.montacutelli@docusign.com*

TSP Information URI

URI	*[en]*	*https://www.docusign.fr/societe/politiques-de-certifications*
URI	*[fr]*	*https://www.docusign.fr/societe/politiques-de-certifications*

10.1 - Service (granted): KEYNECTIS ICS QUALIFIED CA

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified*

by the relevant registration services.

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *KEYNECTIS ICS QUALIFIED CA*

Name *[fr]* *KEYNECTIS ICS QUALIFIED CA*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *149244276810028579447422292902077069402110 6*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIE+DCCA+CgAwIBAgISESHlJbyiTgrE7Syf6ZYBJT/yMA0GCSqGSIb3DQEBCwUAMEoxCzAJBgNV
BAYTAkZSMRIwEAYDVQQKEwlLRVlORUNUSVMxDDAKBgNVBAsTA0lDUzEZMBcGA1UEAxMQS0VZTkVD
VElTIElDUyBDQTAeFw0wOTA2MDkwMDAwMDBaFw0xOTA1MjYwMDAwMDBaMG0xCzAJBgNVBAYTAkZS
MRIwEAYDVQQKEwlLRVlORUNUSVMxDDAKBgNVBAsTA0lDUzEXMBUGA1UECxMOMDAwMiA0NzgyMTcz
MTgxIzAhBgNVBAMTGktFWU5FQ1RJUyBJQ1MgUVVBTElGSUVEIENBMIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEAy7MtFwphuEaTLOP3sXefrz0DXak4g2t3/+SKApGZdQzUR7+yaU8lDdFa
l1haDMxuXbg2PkKi6L1KZL2amVb/kNTVefwenQWNhchPB0NXKomXRayKGlnzVsFQ/E79m4ARaOW3
thl/AnDoRbr31J/z7cWzr5sxNXU9dKYPvYr1jfmP/qDxdajvgaqHQ1m/Zd3IoTwohN33kValiuXR
KM0Se0twxGh+gZTfousD3XPi2VzwJl5bh/0p+nDJl8ZOfmyD5GJxB98mvTB0OeftpVbpRR0J6AGM
LgPkdyXDgDA3BiaOIyD+LPhebXbu+oSECdGzSG95agqhnMlvjcfIhmvokQIDAQABo4IBszCCAa8w
QAYIKwYBBQUHAQEENDAyMDAGCCsGAQUFBzABhiRodHRwOi8va3ZhbGlkLmtleW5lY3Rpcy5jb20v
S1NpZ25DQS8wEgYDVR0TAQH/BAgwBgEB/wIBADCBrgYDVR0gBIGmMIGjMIGgBgwrBgEEAYGtWgIJ
AgEwgY8wKAYIKwYBBQUHAgEWHGh0dHA6Ly93d3cua2V5bmVjdGlzLmNvbS9QQy8wYwYIKwYBBQUH
AgIwVxpVVGhpcyBjZXJ0aWZpY2F0ZSBoYXMgYmVlbiBpc3N1ZWQgaW4gYWNjb3JkYW5jZSB3aXRo
IHRoZSBLRVlORUNUSVMgSUNTIENyZWRlbnRpYWxzIENQUzBWBgNVHR8ETzBNMEugSaBHhkVodHRw
Oi8vdHJ1c3RjZW50ZXItY3JsLmNlcnRpZmljYXQyLmNvbS9LZXluZWN0aXMvS0VZTkVDVElTX0lD
U19DQS5jcmwwDgYDVR0PAQH/BAQDAgEGMB0GA1UdDgQWBBRUl0XB6gDFRajN24L4fcv1kEGgeDAf
BgNVHSMEGDAWgBR/SP/U0wv9XhI73wqvoXG9BvQ+eTANBgkqhkiG9w0BAQsFAAOCAQEAbJSEmoye
qJOzuy5bF/RATB17PoekndTnBZJ8r3wZSzXm6SuAP8xNx2RQkvBl92Z2gUy5EffSBLVWI7mDWktf
Ysrna9hXn/kOO3Qy4mIb6HwxnitNQARYuyCPjc76Si54JY0RsPNwDTDige14mVAp+MYQiNFaakPB
DEeHbxoYPk1YYyva3i7wPBoROmY0UWLtU5nJT7WMLv/vme3KF/J/Njr9iylJMyF5KUTDPyrWjV+A
KyE8OkjaF5hItfSF9KLdLPZzNUMZTqIX30h+HDaM7yApvSP+UNXblQXAjOCw2+PjKWYXghivBGcx
3bkmUKZW1af9HdPpIddC5rXBzcqZJA==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *KEYNECTIS ICS CA*

Issuer OU: *ICS*

Issuer O: *KEYNECTIS*

Issuer C: *FR*

Subject CN: *KEYNECTIS ICS QUALIFIED CA*

Subject OU: *0002 478217318*

Subject OU: *ICS*

Subject O: *KEYNECTIS*

Subject C: *FR*

Valid from: *Tue Jun 09 02:00:00 CEST 2009*

Valid to: *Sun May 26 02:00:00 CEST 2019*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:CB:B3:2D:17:0A:61:B8:46:93:2C:E3:F7:B1:77:9F:AF:3D:03:5D:A9:38:83:6B:77:FF:E4:8A:02:91:99:75:0C:D4:47:BF:B2:69:4F:25:0D:D1:5A:23:58:5A:0C:CC:6E:5D:B8:36:3E:42:A2:E8:BD:4A:64:BD:9A:99:56:FF:90:D4:D5:79:FC:1E:9D:05:8D:85:C8:4F:07:43:57:2A:89:97:45:AC:8A:1A:59:F3:56:C1:50:FC:4E:FD:9B:80:11:68:E5:B7:B6:19:7F:02:70:E8:45:BA:F7:D4:9F:F3:ED:C5:B3:AF:9B:31:35:75:3D:74:A6:0F:BD:8A:F5:8D:F9:8F:FE:A0:F1:75:A8:EF:81:AA:87:43:59:BF:65:DD:C8:A1:3C:28:84:DD:F7:91:56:A5:8A:E5:D1:28:CD:12:7B:4B:70:C4:68:7E:81:94:DF:A2:EB:03:DD:73:E2:D9:5C:F0:26:5E:5B:87:FD:29:FA:70:C9:97:C6:4E:7E:6C:83:E4:62:71:07:DF:26:BD:30:74:39:E7:ED:A5:56:E9:45:1D:09:E8:01:8C:2E:03:E4:77:25:C3:80:30:37:06:26:8E:23:20:FE:2C:F8:5E:6D:76:EE:FA:84:84:09:D1:B3:48:6F:79:6A:0A:A1:9C:C9:6F:8D:C7:C8:86:6B:E8:91:02:03:01:00:01

Authority Info Access *http://kvalid.keynectis.com/KSignCA/*

Basic Constraints *IsCA: true - Path length: 0*

Certificate Policies *Policy OID: 1.3.6.1.4.1.22234.2.9.2.1*

CPS pointer: http://www.keynectis.com/PC/

CPS text: [This certificate has been issued in accordance with the KEYNECTIS ICS Credentials CPS]

CRL Distribution Points *http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_ICS_CA.crl*

Subject Key Identifier *54:97:45:C1:EA:00:C5:45:A8:CD:DB:82:F8:7D:CB:F5:90:41:A0:78*

Authority Key Identifier *7F:48:FF:D4:D3:0B:FD:5E:12:3B:DF:0A:AF:A1:71:BD:06:F4:3E:79*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *B6:10:EC:E7:23:32:B9:AB:D2:9D:3E:53:36:A5:07:B3:BA:95:04:C9:6C:73:87:48:03:84:C7:5C:1A:31:54:19*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

Scheme Service Definition URI

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Signature-3-Stars*

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS101456/QCPPublic*

TSP Service Definition URI

URI *[en]* *http://www.opentrust.com/PDF/EN/PC/CPS_KEYNECTIS_ICS_CA_04-01-2011_GB-V1.1.pdf*

URI *[fr]* *http://www.opentrust.com/PDF/FR/PC/DS_PC_AC_K.Sign_ICS_Qualified_Pro_v1s.pdf*

10.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

10.1.2 - History instance n.1 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *KEYNECTIS ICS QUALIFIED CA*

Name *[fr]* *KEYNECTIS ICS QUALIFIED CA*

Service digital identities

X509SubjectName

Subject CN: *KEYNECTIS ICS QUALIFIED CA*

Subject OU: *0002 478217318*

Subject OU: *ICS*

Subject O: *KEYNECTIS*

Subject C: *FR*

X509SKI

X509 SK I *VJdFweoAxUWozduC+H3L9ZBBoHg=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2009-06-08T22:00:00Z*

10.2 - Service (withdrawn): KEYNECTIS QUALIFIED CDS

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *KEYNECTIS QUALIFIED CDS*

Name *[fr]* *KEYNECTIS QUALIFIED CDS*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *149228125571429736435253417666223076180150 5*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIE9DCCA9ygAwIBAgISESFro5UyD6AY07DGzZTAYQchMA0GCSqGSIb3DQEBBQUAMFoxCzAJBgNV
BAYTAkZSMRIwEAYDVQQKEwlLRVlORUNUSVMxHDAaBgNVBAsTE0tFWU5FQ1RJUyBmb3IgQWRvYmUx
GTAXBgNVBAMTEEtFWU5FQ1RJUyBDRFMgQ0EwHhcNMDkwNTI2MDAwMDAwWhcNMTgwNTI2MDAwMDAw
WjB6MQswCQYDVQQGEwJGUjESMBAGA1UEChMJS0VZTkVDVElTMRwwGgYDVQQLExNLRVlORUNUSVMg
Zm9yIEFkb2JlMRcwFQYDVQQLEw4wMDAyIDQ3ODIxNzMxODEgMB4GA1UEAxMXS0VZTkVDVElTIFFV
QUxJRklFRCBDRFMwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDvWgnm4wjkBBgj8Jb6
mQWbzyY+lz27oeUHMSobqVS3fUMW0G2yAr9Dc5nhGHdlAoT7ycD9TzP90Xe9awGH7c+f1j3gkB9q
xNCREd5Kg8UFprF0zaTn/ZZY704Ykn6QtruJlTYtlBenQuhlacnqn7U9nPUepF1RQvpIPc6kFkCm
NvM0Vl9pAdQ9Ps9ANF9fLuAmBkSLFGeqP9SCCsAaRH7PkAwoqofGln0aLra+sDta6BVvh0YD8/iS
ZasqAEaFK67uRK4Xc55Z69el/tNsAUhln0Ydnh5ja9NYCiDtlkljJehvscBzjCu7Y19HlT1pwHml
y3dL9DIx37VNCYH2rAvDAgMBAAGjggGSMIIBjjASBgNVHRMBAf8ECDAGAQH/AgEAMIG5BgNVHSAE
gbEwga4wgasGDSsGAQQBga1aAggCAQEwgZkwKAYIKwYBBQUHAgEWHGh0dHA6Ly93d3cua2V5bmVj
dGlzLmNvbS9QQy8wbQYIKwYBBQUHAgIwYRpfVGhpcyBjZXJ0aWZpY2F0ZSBoYXMgYmVlbiBpc3N1
ZWQgaW4gYWNjb3JkYW5jZSB3aXRoIHRoZSBBZG9iZSBDcmVkZW50aWFscyBDUFMgYW5kIEtFWU5F
Q1RJUyBDUFMwVgYDVR0fBE8wTTBLoEmgR4ZFaHR0cDovL3RydXN0Y2VudGVyLWNybC5jZXJ0aWZp
Y2F0Mi5jb20vS2V5bmVjdGlzL0tFWU5FQ1RJU19DRFNfQ0EuY3JsMA4GA1UdDwEB/wQEAwIBBjAU
BgNVHSUEDTALBgkqhkiG9y8BAQUwHQYDVR0OBBYEFGjcZpZUqDMXfMIlfyQ/+rE3pQHnMB8GA1Ud
IwQYMBaAFJ8ieNdxG94zsH/JIHqpqOBOYuP7MA0GCSqGSIb3DQEBBQUAA4IBAQDdTkFkit3MDnY5
DSi07NuraqVuC5K2wecSqKXXsZ6vfw0bdIngeQwX0GxkdJxrs3axBjSke4R8b2w6KEbshEAGYCc9
ak7PMvAJpW7z3fDXtO37YFTKr/BZBF48x5O/TIF6hSuts/hzsde6H+RKCSV0gVdfjQXGGscgZM/u
5whB+3//3Tfcm7MZoLmnpAQetc+1+JJCGGpPSQr1+JsHfXu/PRqT1cNmMZlk4tNim1Vecj5yhgm1
WgHJ1Ks8+2Vfb1oGM5FcHJQ2OPfiFLoV5DLTThNHY/ikNP2Jv7VW4IDZjL/jhgLBgT+NMWMuljoU
ZxyVdMk49KDOxDTjwOvrwNyH

-----END CERTIFICATE-----

Signature algorithm: *SHA1withRSA*

Issuer CN: *KEYNECTIS CDS CA*

Issuer OU: *KEYNECTIS for Adobe*

Issuer O: *KEYNECTIS*

Issuer C: *FR*

Subject CN: *KEYNECTIS QUALIFIED CDS*

Subject OU: *0002 478217318*

Subject OU: *KEYNECTIS for Adobe*

Subject O: *KEYNECTIS*

Subject C: *FR*

Valid from: *Tue May 26 02:00:00 CEST 2009*

Valid to: *Sat May 26 02:00:00 CEST 2018*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:EF:5A:09:E6:E3:08:E4:04:18:23:F0:96:FA:99:05:9B:CF:26:3E:97:3D:BB:A1:E5:07:31:2A:1B:A9:54:B7:7D:43:16:D0:6D:B2:02:BF:43:73:99:E1:18:77:65:02:84:FB:C9:C0:FD:4F:33:FD:D1:77:BD:6B:01:87:ED:CF:9F:D6:3D:E0:90:1F:6A:C4:D0:91:11:DE:4A:83:C5:05:A6:B1:74:CD:A4:E7:FD:96:58:EF:4E:18:92:7E:90:B6:BB:89:95:36:2D:94:17:A7:42:E8:65:69:C9:EA:9F:B5:3D:9C:F5:1E:A4:5D:51:42:FA:48:3D:CE:A4:16:40:A6:36:F3:34:56:5F:69:01:D4:3D:3E:CF:40:34:5F:5F:2E:E0:26:06:44:8B:14:67:AA:3F:D4:82:0A:C0:1A:44:7E:CF:90:0C:28:AA:87:C6:96:7D:1A:2E:B6:BE:B0:3B:5A:E8:15:6F:87:46:03:F3:F8:92:65:AB:2A:00:46:85:2B:AE:EE:44:AE:17:73:9E:59:EB:D7:A5:FE:D3:6C:01:48:65:9F:46:1D:9E:1E:63:6B:D3:58:0A:20:ED:96:49:63:25:E8:6F:B1:C0:73:8C:2
B:BB:63:5F:47:95:3D:69:C0:79:A5:CB:77:4B:F4:32:31:DF:B5:4D:09:81:F6:AC:0B:C3:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

Certificate Policies *Policy OID: 1.3.6.1.4.1.22234.2.8.2.1.1*

CPS pointer: http://www.keynectis.com/PC/

CPS text: [This certificate has been issued in accordance with the Adobe Credentials CPS and KEYNECTIS CPS]

CRL Distribution Points *http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_CDS_CA.crl*

Extended Key Usage *Unknown ExtendedKeyUsage OID: 1.2.840.113583.1.1.5*

Subject Key Identifier *68:DC:66:96:54:A8:33:17:7C:C2:25:7F:24:3F:FA:B1:37:A5:01:E7*

Authority Key Identifier *9F:22:78:D7:71:1B:DE:33:B0:7F:C9:20:7A:A9:A8:E0:4E:62:E3:FB*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *9D:B3:A8:A9:BB:7F:7D:C3:3C:AE:09:E9:6B:13:B9:02:62:5C:4A:C6:3E:19:86:E6:52:B9:6B:79:42:0E:D1:29*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS101456/QCPPublic*

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Signature-3-Stars*

TSP Service Definition URI

URI *[en]* *http://www.opentrust.com/PDF/EN/PC/DS_PC_AC_K.Sign_CDS_Qualified_Pro_v1.0_GB.pdf*

URI *[fr]* *http://www.opentrust.com/PDF/FR/PC/DSQ_PC_AC_K.Sign_CDS_Qualified_Pro_s_v_0_6.pdf*

10.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

10.2.2 - History instance n.1 - Status: accreditationrevoked

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *KEYNECTIS QUALIFIED CDS*

Name *[fr]* *KEYNECTIS QUALIFIED CDS*

Service digital identities

X509SubjectName

Subject CN: *KEYNECTIS QUALIFIED CDS*

Subject OU: *0002 478217318*

Subject OU: *KEYNECTIS for Adobe*

Subject O: *KEYNECTIS*

Subject C: *FR*

X509SKI

X509 SK I *aNxmllSoMxd8wiV/JD/6sTelAec=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accreditationrevoked*

Status Starting Time *2013-12-12T23:00:00Z*

10.2.3 - History instance n.2 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *KEYNECTIS QUALIFIED CDS*

Name *[fr]* *KEYNECTIS QUALIFIED CDS*

Service digital identities

X509SubjectName

Subject CN: *KEYNECTIS QUALIFIED CDS*

Subject OU: *0002 478217318*

Subject OU: *KEYNECTIS for Adobe*

Subject O: *KEYNECTIS*

Subject C: *FR*

X509SKI

X509 SK I *aNxmllSoMxd8wiV/JD/6sTelAec=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2009-05-25T22:00:00Z*

10.3 - Service (granted): Cloud Signing Personal Signature CA

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Cloud Signing Personal Signature CA*

Name *[fr]* *Cloud Signing Personal Signature CA*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1491977055892871777764697781119576148530444*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIEnTCCA4WgAwIBAgISESCGyNQKGGXAOA5j0SjVM9UMMA0GCSqGSIb3DQEBCwUAMFoxCzAJBgNV
BAYTAkZSMRIwEAYDVQQKEwlLRVlORUNUSVMxHDAaBgNVBAsTE0tFWU5FQ1RJUyBmb3IgQWRvYmUx
GTAXBgNVBAMTEEtFWU5FQ1RJUyBDRFMgQ0EwHhcNMTMwOTI3MDAwMDAwWhcNMTgxMDExMDcwMDAw
WjBoMQswCQYDVQQGEwJGUjESMBAGA1UECgwJT1BFTlRSVVNUMRcwFQYDVQQLDA4wMDAyIDQ3ODIx
NzMxODEsMCoGA1UEAwwjQ2xvdWQgU2lnbmluZyBQZXJzb25hbCBTaWduYXR1cmUgQ0EwggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC6ENIuJqI+wlda+RhaXJTnNrzk8Q08Jt9KRn4VkXdO
suLfMhURRTKLytqH4QYCM3AATH1KgMYU6ToPtMOWRy8aa//FE1B+RMPUPE1DCA4L42cJzaqzY8KY
HQgGZa38Huw4fAHTotwp4v3mBcGoxNBCSk8ZnnNsKVBqrK8dVt4OeiVnKYSSyscY8c5mwhC5eZZv
h7hm9H2uL+FXPyXxmAnV2OROhHmzI7fBt1fd1JrYWN4K0mGqzvFTX4lHimyD0waxXNLOHwbacPKR
YY3kWXCBEMWHXacZgLlL5oJ0zfMq9X0ojH0rQsivGpwIlK2xX4O1mb4B4F8o9Rl13WDkxoAXAgMB
AAGjggFNMIIBSTAOBgNVHQ8BAf8EBAMCAQYwFAYDVR0lBA0wCwYJKoZIhvcvAQEFMHYGA1UdIARv
MG0wMgYEVR0gADAqMCgGCCsGAQUFBwIBFhxodHRwOi8vd3d3Lm9wZW50cnVzdC5jb20vUEMvMDcG
CSqGSIb3LwECATAqMCgGCCsGAQUFBwIBFhxodHRwOi8vd3d3Lm9wZW50cnVzdC5jb20vUEMvMBIG
A1UdEwEB/wQIMAYBAf8CAQAwVQYDVR0fBE4wTDBKoEigRoZEaHR0cDovL3RydXN0Y2VudGVyLWNy
bC5jZXJ0aWZpY2F0Mi5jb20vSW50ZXJuYWwvS0VZTkVDVElTX0NEU19DQS5jcmwwHQYDVR0OBBYE
FJKm/sCn07vooB24naLnFNoqziHKMB8GA1UdIwQYMBaAFJ8ieNdxG94zsH/JIHqpqOBOYuP7MA0G
CSqGSIb3DQEBCwUAA4IBAQCRCocOsDl1+5Z1JMRAwaPUL+XVzRzumHz1p74ngxJKuraEWSsHPLLp
h9f9DeYjcd/xQHqOm3omVurRckQD4RCXv1ZKHGnoyjSgJ0zd4tc5tqwdVwDpjYNDIxKeKD0IgnCl
7d4ZwTvRHZpxpM78PxCEbcQFyaUOLq+mcKl+QPxsdG/aGClt/3Ux9NAJNo8h+8KZPlmVAeomjQSa
6DT04i8tKoJu1sY8lx8eH6CcSgllO10JF5lxz2rmYHyG3r3QsfwDfqoH9bdxXjsTukiRCZh9Hg+l
QMs8uONisqKtAJHch6GETxrmvv8TQL5B5aG1y+SiYUhMTKlYJBPgMEOhthkM

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *KEYNECTIS CDS CA*

Issuer OU: *KEYNECTIS for Adobe*

Issuer O: *KEYNECTIS*

Issuer C: *FR*

Subject CN: *Cloud Signing Personal Signature CA*

Subject OU: *0002 478217318*

Subject O: *OPENTRUST*

Subject C: *FR*

Valid from: *Fri Sep 27 02:00:00 CEST 2013*

Valid to: *Thu Oct 11 09:00:00 CEST 2018*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:BA:10:D2:2E:26:A2:3E:C2:57:5A:F9:18:5A:5C:94:E7:36:BC:E4:F1:0D:3C:26:DF:4A:46:7E:15:91:77:4E:B2:E2:DF:32:15:11:45:32:8B:CA:DA:87:E1:06:02:33:70:00:4C:7D:4A:80:C6:14:E9:3A:0F:B4:C3:96:47:2F:1A:6B:FF:C5:13:50:7E:44:C3:D4:3C:4D:43:08:0E:0B:E3:67:09:CD:AA:B3:63:C2:98:1D:08:06:65:AD:FC:1E:EC:38:7C:01:D3:A2:DC:29:E2:FD:E6:05:C1:A8:C4:D0:42:4A:4F:19:9E:73:6C:29:50:6A:AC:AF:1D:56:DE:0E:7A:25:67:29:84:92:CA:C7:18:F1:CE:66:C2:10:B9:79:96:6F:87:B8:66:F4:7D:AE:2F:E1:57:3F:25:F1:98:09:D5:D8:E4:4E:84:79:B3:23:B7:C1:B7:57:DD:D4:9A:D8:58:DE:0A:D2:61:AA:CE:F1:53:5F:89:47:8A:6C:83:D3:06:B1:5C:D2:CE:1F:06:DA:70:F2:91:61:8D:E4:59:70:81:10:C5:87:5D:A7:19:80:B9:4B:E6:82:74:CD:F3:2A:F5:7D:28:8C:7D:2B:42:C8:AF:1A:9C:08:94:AD:B1:5F:83:B5:99:BE:01:E0:5F:28:F5:19:75:DD:60:E4:C6:80:17:02:03:01:00:01

Extended Key Usage *Unknown ExtendedKeyUsage OID: 1.2.840.113583.1.1.5*

Certificate Policies *Policy OID: 2.5.29.32.0*

CPS pointer: http://www.opentrust.com/PC/

Policy OID: 1.2.840.113583.1.2.1

CPS pointer: http://www.opentrust.com/PC/

Basic Constraints *IsCA: true - Path length: 0*

CRL Distribution Points *http://trustcenter-crl.certificat2.com/Internal/KEYNECTIS_CDS_CA.crl*

Subject Key Identifier *92:A6:FE:C0:A7:D3:BB:E8:A0:1D:B8:9D:A2:E7:14:DA:2A:CE:21:CA*

Authority Key Identifier *9F:22:78:D7:71:1B:DE:33:B0:7F:C9:20:7A:A9:A8:E0:4E:62:E3:FB*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *07:62:1E:47:F6:11:32:79:E6:C4:B4:E8:0E:BE:CA:09:18:DA:10:30:4E:1D:C2:C5:4F:FC:E8:4E:02:87:D2:51*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

Scheme Service Definition URI

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Signature-3-Stars*

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS101456/QCPPublic*

TSP Service Definition URI

URI *[en]* *https://www.opentrustdtm.com/wp-content/uploads/2015/02/Protect-and-Sign_Personal-Signature_PC-Utilisateur-ETSI-V-1-3.pdf*

URI *[fr]* *https://www.opentrustdtm.com/wp-content/uploads/2015/02/Protect-and-Sign_Personal-Signature_PC-Utilisateur-ETSI-V-1-3.pdf*

10.3.1 - Extension (not critical): Qualifiers [QCWithQSCD]

Qualifier type description *[en]* *undefined.*

[fr] *undefined.*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithQSCD*

Criteria list assert=atLeastOne

Policy Identifier nodes:

Identifier *1.3.6.1.4.1.22234.2.8.3.20*

10.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

10.3.3 - History instance n.1 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Cloud Signing Personal Signature CA*

Name *[fr]* *Cloud Signing Personal Signature CA*

Service digital identities

X509SubjectName

Subject CN: *Cloud Signing Personal Signature CA*

Subject OU: *0002 478217318*

Subject O: *OPENTRUST*

Subject C: *FR*

X509 SK I *kqb+wKfTu+igHbidoucU2irOIco=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2013-11-01T00:00:00Z*

10.3.3.1 - Extension (not critical): Qualifiers [QCWithSSCD]

Qualifier type description *[en]* *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the presence or absence of Secure Signature Creation Device (SSCD) support ARE supported by an SSCD (i.e. that that the private key associated with the public key in the certificate is stored in a Secure Signature Creation Device conformant with the applicable European legislation);*

[fr] *elle est assurée par le prestataire de service de confiance et contrôlée (modèle de contrôle) ou vérifiés (modèle d'accréditation) par l'État membre de référence (respectivement son Organe de surveillance ou organisme d'accréditation) que tous les certificats qualifiés délivrés dans le cadre du service identifié dans «Service digital identity» et en outre identifié par les informations des filtres utilisés pour identifier plus précisément dans le cadre du "Sdi" de service de confiance identifiés, l'ensemble précis de certificats qualifiés pour lesquels cette information supplémentaire est nécessaire en ce qui concerne la présence ou l'absence de dispositif sécurisé de création de signature (SSCD) de soutien sont pris en charge par un SSCD (à savoir que la clé privée associée à la clé publique du certificat est stocké dans un dispositif sécurisé conforme à la législation européenne applicable de création de signature);*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithSSCD*

Criteria list assert=atLeastOne

Policy Identifier nodes:

Identifier *1.3.6.1.4.1.22234.2.8.3.20*

10.4 - Service (granted): Keynectis CDS CA for timestamping

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Keynectis CDS CA for timestamping*

Name *[fr]* *Keynectis CDS CA for timestamping*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *149185865027119531231343207380236328702069 7*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIE3TCCA8WgAwIBAgISESAttLwrtkkB2gcOUnIZrqSZMA0GCSqGSIb3DQEBCwUAMFoxCzAJBgNV
BAYTAkZSMRIwEAYDVQQKEwlLRVlORUNUSVMxHDAaBgNVBAsTE0tFWU5FQ1RJUyBmb3IgQWRvYmUx
GTAXBgNVBAMTEEtFWU5FQ1RJUyBDRFMgQ0EwHhcNMTEwNjE3MDAwMDAwWhcNMTgxMDA5MDAwMDAw
WjB+MQswCQYDVQQGEwJGUjESMBAGA1UEChMJS2V5bmVjdGlzMRcwFQYDVQQLEw4wMDAyIDQ3ODIx

NzMxODEWMBQGA1UECxMNS2V5bmVjdGlzIENEUzEqMCgGA1UEAxMhS2V5bmVjdGlzIENEUyBDQSBm
b3IgdGltZXN0YW1waW5nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAulsGWcqRIKYH
lUKHUpWBcccvg3zZ9WLBoazQNTr4+ZdOOTKYMgrhtxkgQXen54Is4ZJzZLKYxFyVAPrEYmH6+u4N
Tk7BvLq0uxQY1OSDgGMzlhv4cereHOl8TnBXUMBag7fnPRN4yaRp0zAObqpETJT1kIP6nVg8/UOP
YScoWzZg2nWHv5o53qv+Npk5sqv4krV0OQKEYw0srjthML4tx2aGPwmQcF5+VDPM54VViAParZhS
XCYvZtn2XWLNZ0JB+tWPtTjFOatY9wo+siR6+NRW6JIfhA0yl7SnDR97Y94f4rK7zGhOaUZdpWaC
A1EVCBhInR0iF8UU54KsGR1NywIDAQABo4IBdzCCAXMwDgYDVR0PAQH/BAQDAgEGMBEGA1UdIAQK
MAgwBgYEVR0gADASBgNVHRMBAf8ECDAGAQH/AgEAMIH5BgNVHR8EgfEwge4wS6BJoEeGRWh0dHA6
Ly90cnVzdGNlbnRlci1jcmwuY2VydGlmaWNhdDIuY29tL0tleW5lY3Rpcy9LRVlORUNUSVNfQ0RT
X0NBLmNybDCBnqCBm6CBmIaBlWxkYXA6Ly9sZGFwLmtleW5lY3Rpcy5jb20vQ049S0VZTkVDVElT
JTIwQ0RTJTIwQ0EsT1U9S0VZTkVDVElTJTIwZm9yJTIwQWRvYmUsTz1LRVlORUNUSVMsQz1GUj9j
ZXJ0aWZpY2F0ZVJldm9jYXRpb25MaXN0O2JpbmFyeT9iYXNlP29iamVjdGNsYXNzPXBraUNBMB0G
A1UdDgQWBBRfqHFgv1WJWLXj7SCZ4Wc3SKmx4TAfBgNVHSMEGDAWgBSfInjXcRveM7B/ySB6qajg
TmLj+zANBgkqhkiG9w0BAQsFAAOCAQEAQoXVd+Ot9A9+csMuR9KE6yFUxrBgXseP/EMv6Pg810mr
qHYfkcWJLWQIrPrdPy+0kCzA0yoEjfFZvWsPwat6blZkscws4Imsu9+tUUPy9ULJKQbXc0g3XfT7
oqYz+eOqHNjwbOnp3O3Nk1S4T4dTUHDq6hKqktW1+HpCCWRHERosAX8RAepFyw/MBCZZGwDS44KB
AGm3eHDa3XFPFXqnZsF66rFsaUMBVtpaZf1lm2b73t4170LIxwXl9BPv9bjMNASC5tFUu/UoljK8
OobzGsq3CXcgnIz7G2beDKZPCaB5MymUcJjqOkzuVz9EzEJbWB4jLxLm4OT1ik9suEyQ1w==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *KEYNECTIS CDS CA*

Issuer OU: *KEYNECTIS for Adobe*

Issuer O: *KEYNECTIS*

Issuer C: *FR*

Subject CN: *Keynectis CDS CA for timestamping*

Subject OU: *Keynectis CDS*

Subject OU: *0002 478217318*

Subject O: *Keynectis*

Subject C: *FR*

Valid from: *Fri Jun 17 02:00:00 CEST 2011*

Valid to: *Tue Oct 09 02:00:00 CEST 2018*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:BA:5B:06:59:CA:91:20:A6:07:95:42:87:52:95:81:71:
C7:2F:83:7C:D9:F5:62:C1:A1:AC:D0:35:3A:F8:F9:97:4E:39:32:98:32:0A:E1:B7:19:20:41:77:A7:E7:82:2C:E1:92:73:64:B2:98:C4:5C:95:00:FA:C4:62:61:FA:FA:EE:
0D:4E:4E:C1:BC:BA:B4:BB:14:18:D4:E4:83:80:63:33:96:1B:F8:71:EA:DE:1C:E9:7C:4E:70:57:50:C0:5A:83:B7:E7:3D:13:78:C9:A4:69:D3:30:0E:6E:AA:44:4C:94:F5
:90:83:FA:9D:58:3C:FD:43:8F:61:27:28:5B:36:60:DA:75:87:BF:9A:39:DE:AB:FE:36:99:39:B2:AB:F8:92:B5:74:39:02:84:63:0D:2C:AE:3B:61:30:BE:2D:C7:66:86:3
F:09:90:70:5E:7E:54:33:CC:E7:85:55:88:03:DA:AD:98:52:5C:26:2F:66:D9:F6:5D:62:CD:67:42:41:FA:D5:8F:B5:38:C5:39:AB:58:F7:0A:3E:B2:24:7A:F8:D4:56:E8:
92:1F:84:0D:32:97:B4:A7:0D:1F:7B:63:DE:1F:E2:B2:BB:CC:68:4E:6
9:46:5D:A5:66:82:03:51:15:08:18:48:9D:1D:22:17:C5:14:E7:82:AC:19:1D:4D:CB:02:03:01:00:01

Certificate Policies *Policy OID: 2.5.29.32.0*

Basic Constraints *IsCA: true - Path length: 0*

CRL Distribution Points

http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_CDS_CA.crl

ldap://ldap.keynectis.com/CN=KEYNECTIS%20CDS%20CA,OU=KEYNECTIS%20for%20Adobe,O=KEYNECTIS,C=FR?certificateRevocationList;binary?base?objectclass=pkiCA

Subject Key Identifier

5F:A8:71:60:BF:55:89:58:B5:E3:ED:20:99:E1:67:37:48:A9:B1:E1

Authority Key Identifier

9F:22:78:D7:71:1B:DE:33:B0:7F:C9:20:7A:A9:A8:E0:4E:62:E3:FB

Key Usage:

keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

58:F6:94:D2:A2:0D:AA:70:32:7B:FB:28:D9:2D:B7:3E:B1:3B:58:86:5A:61:80:5D:EC:11:7F:0A:C8:29:BA:40

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description

[en] *undefined.*

[fr] *undefined.*

Status Starting Time

2016-06-30T22:00:00Z

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS102042/LCP*

TSP Service Definition URI

URI *[en]* *https://www.opentrust.com/wp-content/uploads/2015/04/Opentrust_DMS_PC-Cachet-serveur-RGS_V-1-4s1.pdf*

URI *[fr]* *https://www.opentrust.com/wp-content/uploads/2015/04/Opentrust_DMS_PC-Cachet-serveur-RGS_V-1-4s1.pdf*

10.4.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

10.4.2 - History instance n.1 - Status: accredited

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service Name

Name *[en]* *Keynectis CDS CA for timestamping*

Name *[fr]* *Keynectis CDS CA for timestamping*

Service digital identities

X509SubjectName

Subject CN: *Keynectis CDS CA for timestamping*

Subject OU: *Keynectis CDS*

Subject OU: *0002 478217318*

Subject O: *Keynectis*

Subject C: *FR*

X509SKI

X509 SK I *X6hxYL9ViVi14+0gmeFnN0ipseE=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2011-06-17T00:00:00Z*

10.5 - Service (granted): KEYNECTIS ICS QUALIFIED CA

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *KEYNECTIS ICS QUALIFIED CA*

Name *[fr]* *KEYNECTIS ICS QUALIFIED CA*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *149210310665703207046190797368092707932743 7*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIF3DCCA8SgAwIBAgISESDlnVKIzc3kKRmj69IyjubNMA0GCSqGSIb3DQEBCwUAMF0xCzAJBgNV
BAYTAkZSMRIwEAYDVQQKDAlPcGVuVHJ1c3QxFzAVBgNVBAsMDjAwMDIgNDc4MjE3MzE4MSEwHwYD
VQQDDBhPcGVuVHJ1c3QgQ0EgZm9yIEFBVEwgRzEwHhcNMTQwNTI3MDAwMDAwWhcNMjUxMjMxMDAw

MDAwWjBtMQswCQYDVQQGEwJGUjESMBAGA1UEChMJS0VZTkVDVElTMQwwCgYDVQQLEwNJQ1MxFzAV
BgNVBAsTDjAwMDIgNDc4MjE3MzE4MSMwIQYDVQQDExpLRVlORUNUSVMgSUNTIFFVQUxJRklFRCBD
QTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMuzLRcKYbhGkyzj97F3n689A12pOINr
d//kigKRmXUM1Ee/smlPJQ3RWiNYWgzMbl24Nj5Coui9SmS9mplW/5DU1Xn8Hp0FjYXITwdDVyqJ
l0WsihpZ81bBUPxO/ZuAEWjlt7YZfwJw6EW699Sf8+3Fs6+bMTV1PXSmD72K9Y35j/6g8XWo74Gq
h0NZv2XdyKE8KITd95FWpYrl0SjNEntLcMRofoGU36LrA91z4tlc8CZeW4f9KfpwyZfGTn5sg+Ri
cQffJr0wdDnn7aVW6UUdCegBjC4D5Hclw4AwNwYmjiMg/iz4Xm127vqEhAnRs0hveWoKoZzJb43H
ylZr6JECAwEAAaOCAYQwggGAMA4GA1UdDwEB/wQEAwIBBjB5BgNVHSAEcjBwMDIGBFUdIAAwKjAo
BggrBgEFBQcCARYcaHR0cDovL3d3dy5vcGVudHJ1c3QuY29tL1BDLzA6BgwrBgEEAYGtWgIOAwEw
KjAoBggrBgEFBQcCARYcaHR0cDovL3d3dy5vcGVudHJ1c3QuY29tL1BDLzASBgNVHRMBAf8ECDAG
AQH/AgEAME4GA1UdHwRHMEUwQ6BBoD+GPWh0dHA6Ly9nZXQtY3JsLmNlcnRpZmljYXQuY29tL3B1
YmxpYy9vcGVudHJ1c3RjYWZvcmFhdGxnMS5jcmwwTwYIKwYBBQUHAQEEQzBBMD8GCCsGAQUFBzAB
hjNodHRwOi8vZ2V0LW9jc3AuY2VydGlmaWNhdC5jb20vb3BlbnRydXN0Y2Fmb3JhYXRsZzEwHQYD
VR0OBBYEFFSXRcHqAMVFqM3bgvh9y/WQQaB4MB8GA1UdIwQYMBaAFHh/blSqzOg4uP0nxueFFcEF
h40WMA0GCSqGSIb3DQEBCwUAA4ICAQBX4Gf9C6syTKQp5E8pWJl2LThxImZA7UYF+V/HqWUAEY4S
61shYKzJ5NXzaNllU8NepjPzSqngWOUo2XSoA+QOo0s7vMIIYluMBcDoO3Y2Ef66N/IzvAy9vJ9T
VLo4+LmfG6ogTBuIoHs2O/TpP9AlcMp40t+9zG/CDpbrr57iLnvMSPIh6PPO66Onj+mgXNILZ9OJ
IYW274orfdLq++95SOftaA0BM+bp7AHq1KLKCKNFLxaKLWt4wQrbjtdCJ3jyxymbTgGjGaqPtULe
+usvRkEjY1FWvNwf+lcVA7wQ+3BzA/zmi8d0Mn3CVd/g2zBAaeT68oKyyFSZyFAwUzLraPBBAr+v
7Gr/q3g+lcuJ/OZn1wN+MIIX9eF1ENCm8ecJTXeV3bA4OFSYS4f3I3NFoyX4/87EilddOiuypCkY
8UbvwrXcWP/elujM1E26eKJRNZl2JqS3KeAGRBnHntN0WG1c0hLaZaHJcH896KAKJIjyt48P0Bi2
OqtBdvCBtW11YJdhfpmCy1XUK8XwuBAwD+25f4tuDZQgL58l0VLJ65lleRvXch5bwUbqvEXbWU/m
7n+O9MR159daoxIxSN67NhZIqLoG5h2do51HuAO+Zn6xCa6yQblOd3mOt+yv/cTL79ld0/Nxs2J4
k1+huH57xlM6DRy0lSASUvyFTjz9Xw==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *OpenTrust CA for AATL G1*

Issuer OU: *0002 478217318*

Issuer O: *OpenTrust*

Issuer C: *FR*

Subject CN: *KEYNECTIS ICS QUALIFIED CA*

Subject OU: *0002 478217318*

Subject OU: *ICS*

Subject O: *KEYNECTIS*

Subject C: *FR*

Valid from: *Tue May 27 02:00:00 CEST 2014*

Valid to: *Wed Dec 31 01:00:00 CET 2025*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:CB:B3:2D:17:0A:61:B8:46:93:2C:E3:F7:B1:77:9F:AF:
3D:03:5D:A9:38:83:6B:77:FF:E4:8A:02:91:99:75:0C:D4:47:BF:B2:69:4F:25:0D:D1:5A:23:58:5A:0C:CC:6E:5D:B8:36:3E:42:A2:E8:BD:4A:64:BD:9A:99:56:FF:90:D
4:D5:79:FC:1E:9D:05:8D:85:C8:4F:07:43:57:2A:89:97:45:AC:8A:1A:59:F3:56:C1:50:FC:4E:FD:9B:80:11:68:E5:B7:B6:19:7F:02:70:E8:45:BA:F7:D4:9F:F3:ED:C5:B
3:AF:9B:31:35:75:3D:74:A6:0F:BD:8A:F5:8D:F9:8F:FE:A0:F1:75:A8:EF:81:AA:87:43:59:BF:65:DD:C8:A1:3C:28:84:DD:F7:91:56:A5:8A:E5:D1:28:CD:12:7B:4B:70
:C4:68:7E:81:94:DF:A2:EB:03:DD:73:E2:D9:5C:F0:26:5E:5B:87:FD:29:FA:70:C9:97:C6:4E:7E:6C:83:E4:62:71:07:DF:26:BD:30:74:39:E7:ED:A5:56:E9:45:1D:09:E
8:01:8C:2E:03:E4:77:25:C3:80:30:37:06:26:8E:23:20:FE:2C:F8:5E:6D:76:EE:FA:84:84:09:D1:B3:48:6F:79:6A:0A:A1:9C:C9:6F:8D:C7:C8:86:6B:E8:91:02:03:01:0

0:01

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: http://www.opentrust.com/PC/

Policy OID: 1.3.6.1.4.1.22234.2.14.3.1

CPS pointer: http://www.opentrust.com/PC/

Basic Constraints

IsCA: true - Path length: 0

CRL Distribution Points

http://get-crl.certificat.com/public/opentrustcaforaatlg1.crl

Authority Info Access

http://get-ocsp.certificat.com/opentrustcaforaatlg1

Subject Key Identifier

54:97:45:C1:EA:00:C5:45:A8:CD:DB:82:F8:7D:CB:F5:90:41:A0:78

Authority Key Identifier

78:7F:6E:54:AA:CC:E8:38:B8:FD:27:C6:E7:85:15:C1:05:87:8D:16

Key Usage:

keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

73:C9:E2:98:E2:AB:83:F6:79:90:C2:6C:EB:76:D6:31:E2:DD:F1:11:2C:FF:D4:99:5E:9A:12:F6:FB:B3:CF:27

X509SubjectName

Subject CN:

KEYNECTIS ICS QUALIFIED CA

Subject OU:

0002 478217318

Subject OU:

ICS

Subject O:

KEYNECTIS

Subject C:

FR

X509 SK I

VJdFweoAxUWozduC+H3L9ZBBoHg=

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time

2018-06-24T22:00:00Z

TSP Service Definition URI

URI *[en]* *https://www.docusign.fr/societe/politiques-de-certifications*

URI *[fr]* *https://www.docusign.fr/societe/politiques-de-certifications*

10.5.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

10.5.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

10.5.3 - Extension (critical): Qualifiers [QCWithQSCD, QCForESig]

Qualifier type description *[en]* *undefined.*

[fr] *undefined.*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithQSCD*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForESig*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Policy Identifier nodes:

Identifier *1.3.6.1.4.1.22234.2.9.3.15*

10.5.4 - Extension (critical): Qualifiers [QCNoQSCD, QCForESeal]

Qualifier type description *[en]* *undefined.*

[fr] *undefined.*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCNoQSCD*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForESeal*

Criteria list assert=all

Key Usage *[digitalSignature]* *true*

10.5.5 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *KEYNECTIS ICS QUALIFIED CA*

Name *[fr]* *KEYNECTIS ICS QUALIFIED CA*

Service digital identities

X509SubjectName

Subject CN: *KEYNECTIS ICS QUALIFIED CA*

Subject OU: *0002 478217318*

Subject OU: *ICS*

Subject O: *KEYNECTIS*

Subject C: *FR*

X509SKI

X509 SK I *VJdFweoAxUWozduC+H3L9ZBBoHg=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2017-10-31T23:00:00Z*

10.5.5.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

10.5.5.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

10.5.5.3 - Extension (critical): Qualifiers [QCWithQSCD, QCForESig]

Qualifier type description *[en]* *undefined.*

[fr] *undefined.*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithQSCD*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForESig*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Policy Identifier nodes:

Identifier *1.3.6.1.4.1.22234.2.9.3.15*

10.5.5.4 - Extension (critical): Qualifiers [QCWithQSCD, QCForESeal]

Qualifier type description *[en]* *undefined.*

[fr] *undefined.*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithQSCD*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForESeal*

Criteria list assert=all

Key Usage *[digitalSignature]* *true*

10.6 - Service (granted): Cloud Signing Personal Signature CA

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Cloud Signing Personal Signature CA*

Name *[fr]* *Cloud Signing Personal Signature CA*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1492126987936093636159504198553683475683235*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIF1zCCA7+gAwIBAgISESD3lLB/f1WZUYjEB4ECqdejMA0GCSqGSIb3DQEBCwUAMF0xCzAJBgNV
BAYTAkZSMRIwEAYDVQQKDAlPcGVuVHJ1c3QxFzAVBgNVBAsMDjAwMDIgNDc4MjE3MzE4MSEwHwYD

VQQDDBhPcGVuVHJ1c3QgQ0EgZm9yIEFBVEwgRzEwHhcNMTQwNTI3MDAwMDAwWhcNMjUxMjMxMDAw
MDAwWjBoMQswCQYDVQQGEwJGUjESMBAGA1UECgwJT1BFTlRSVVNUMRcwFQYDVQQLDA4wMDAyIDQ3
ODIxNzMxODEsMCoGA1UEAwwjQ2xvdWQgU2lnbmluZyBQZXJzb25hbCBTaWduYXR1cmUgQ0EwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC6ENIuJqI+wlda+RhaXJTnNrzk8Q08Jt9KRn4V
kXdOsuLfMhURRTKLytqH4QYCM3AATH1KgMYU6ToPtMOWRy8aa//FE1B+RMPUPE1DCA4L42cJzaqz
Y8KYHQgGZa38Huw4fAHTotwp4v3mBcGoxNBCSk8ZnnNsKVBqrK8dVt4OeiVnKYSSyscY8c5mwhC5
eZZvh7hm9H2uL+FXPyXxmAnV2OROhHmzI7fBt1fd1JrYWN4K0mGqzvFTX4lHimyD0waxXNLOHwba
cPKRYY3kWXCBEMWHXacZgLlL5oJ0zfMq9X0ojH0rQsivGpwIlK2xX4O1mb4B4F8o9Rl13WDkxoAX
AgMBAAGjggGEMIIBgDAOBgNVHQ8BAf8EBAMCAQYweQYDVR0gBHIwcDAyBgRVHSAAMCowKAYIKwYB
BQUHAgEWHGh0dHA6Ly93d3cub3BlbnRydXN0LmNvbS9QQy8wOgYMKwYBBAGBrVoCDgMBMCowKAYI
KwYBBQUHAgEWHGh0dHA6Ly93d3cub3BlbnRydXN0LmNvbS9QQy8wEgYDVR0TAQH/BAgwBgEB/wIB
ADBOBgNVHR8ERzBFMEOgQaA/hj1odHRwOi8vZ2V0LWNybC5jZXJ0aWZpY2F0LmNvbS9wdWJsaWMv
b3BlbnRydXN0Y2Fmb3JhYXRsZzEuY3JsME8GCCsGAQUFBwEBBEMwQTA/BggrBgEFBQcwAYYzaHR0
cDovL2dldC1vY3NwLmNlcnRpZmljYXQuY29tL29wZW50cnVzdGNhZm9yYWF0bGcxMB0GA1UdDgQW
BBSSpv7Ap9O76KAduJ2i5xTaKs4hyjAfBgNVHSMEGDAWgBR4f25UqszoOLj9J8bnhRXBBYeNFjAN
BgkqhkiG9w0BAQsFAAOCAgEAKLA2XmXUqtMAAq5+AxPLEXmM80bMtq9wCwtqjiyKX8jcEkCV+n2D
2WsSk31HBUeKSFXkG3luRwd2h6mIuZO96xWvO3pNjargfjo3a9p756TLvMyvc7lgLlNZEzDNELHu
zfIkbaHEub7KpCzBuFG48Ynxr7RdgA5Gux9UWCx6P+4/KPEdtwGX2YE2DlWKJ2nNRflTIWe5mIxj
P0tGGUuJpn14peBYa4GSuvTt6ZGf82doTMhVBUK+sUuo/HNxhblpy2FmvWalwRdpFxmxMLOm4Cm0
WqZdTEURa+TZELPWD/6gmfRlurWZqIZgLbikYjzOaKEe5CK5T8MNnOQok4Jp/xYeFRXxKOn+SsGS
I0K40uCPeSXn4p9K7haa3FRhlJKk/k1Enl6oIrMKkfOSvG1Ai9q1pB+DSK4MrbKUyp7iAdXtaDOp
wXFICuZ00zlnMjnDrifdwr5tcHCFhyEA23tzrhp4Y7C9oIDa0nwauOJQXQUivyNx9mLW/6qBqR4B
Rfj4JdAaVqCIJ2nZJlwe8J+qS89xAKdLpRLsuzkx8ElYj6vrHJWnnIILKFYqDgIqsqiBa/9wX8Pc
yYawKYsPxCrc6Sqo5Yl4E5BVs20J9VS93VoqKX4y5x0ZEKCuMjmCtRr3oj3BhFxEfLl1xzak5X2h
C6rr/fL0frmfDxgiZhTTuZ8=

-----END CERTIFICATE-----

Signature algorithm:	*SHA256withRSA*
Issuer CN:	*OpenTrust CA for AATL G1*
Issuer OU:	*0002 478217318*
Issuer O:	*OpenTrust*
Issuer C:	*FR*
Subject CN:	*Cloud Signing Personal Signature CA*
Subject OU:	*0002 478217318*
Subject O:	*OPENTRUST*
Subject C:	*FR*
Valid from:	*Tue May 27 02:00:00 CEST 2014*
Valid to:	*Wed Dec 31 01:00:00 CET 2025*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:BA:10:D2:2E:26:A2:3E:C2:57:5A:F9:18:5A:5C:94:E7:
36:BC:E4:F1:0D:3C:26:DF:4A:46:7E:15:91:77:4E:B2:E2:DF:32:15:11:45:32:8B:CA:DA:87:E1:06:02:33:70:00:4C:7D:4A:80:C6:14:E9:3A:0F:B4:C3:96:47:2F:1A:6B
:FF:C5:13:50:7E:44:C3:D4:3C:4D:43:08:0E:0B:E3:67:09:CD:AA:B3:63:C2:98:1D:08:06:65:AD:FC:1E:EC:38:7C:01:D3:A2:DC:29:E2:FD:E6:05:C1:A8:C4:D0:42:4A:
4F:19:9E:73:6C:29:50:6A:AC:AF:1D:56:DE:0E:7A:25:67:29:84:92:CA:C7:18:F1:CE:66:C2:10:B9:79:96:6F:87:B8:66:F4:7D:AE:2F:E1:57:3F:25:F1:98:09:D5:D8:E4:
4E:84:79:B3:23:B7:C1:B7:57:DD:D4:9A:D8:58:DE:0A:D2:61:AA:CE:F1:53:5F:89:47:8A:6C:83:D3:06:B1:5C:D2:CE:1F:06:DA:70:F2:91:61:8D:E4:59:70:81:10:C5:8
7:5D:A7:19:80:B9:4B:E6:82:74:CD:F3:2A:F5:7D:28:8C:7D:2B:42:C8:AF:1A:9C:08:94:AD:B1:5F:83:B5:99:BE:01:E0:5F:28:F5:19:75:DD:60:E4:C6:80:17:02:03:01:
00:01

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: http://www.opentrust.com/PC/

Policy OID: 1.3.6.1.4.1.22234.2.14.3.1

CPS pointer: http://www.opentrust.com/PC/

Basic Constraints

IsCA: true - Path length: 0

CRL Distribution Points

http://get-crl.certificat.com/public/opentrustcaforaatlg1.crl

Authority Info Access

http://get-ocsp.certificat.com/opentrustcaforaatlg1

Subject Key Identifier

92:A6:FE:C0:A7:D3:BB:E8:A0:1D:B8:9D:A2:E7:14:DA:2A:CE:21:CA

Authority Key Identifier

78:7F:6E:54:AA:CC:E8:38:B8:FD:27:C6:E7:85:15:C1:05:87:8D:16

Key Usage:

keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

F4:EF:5C:58:BE:17:8F:33:0F:4A:1E:63:72:2D:76:2F:81:66:8D:B7:E9:80:7D:72:7A:01:4B:0A:B7:B6:FE:0F

X509SubjectName

Subject CN:

Cloud Signing Personal Signature CA

Subject OU:

0002 478217318

Subject O:

OPENTRUST

Subject C:

FR

X509SKI

X509 SK I

kqb+wKfTu+igHbidoucU2irOIco=

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description

[en] *undefined.*

[fr] *undefined.*

Status Starting Time

2018-06-30T22:00:00Z

TSP Service Definition URI

URI *[en]* *https://www.docusign.fr/societe/politiques-de-certifications*

URI *[fr]* *https://www.docusign.fr/societe/politiques-de-certifications*

10.6.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

10.6.2 - Extension (critical): Qualifiers [QCWithQSCD, QCForESig]

Qualifier type description *[en]* *undefined.*

[fr] *undefined.*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithQSCD*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForESig*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Policy Identifier nodes:

Identifier *1.3.6.1.4.1.22234.2.8.3.20*

10.7 - Service (granted): DocuSign Premium Cloud Signing CA - SI1

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *DocuSign Premium Cloud Signing CA - SI1*

Name *[fr]* *DocuSign Premium Cloud Signing CA - SI1*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *149244626920380987148301562117014024809810 6*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIGJDCCBAygAwIBAgISESHnyAZdbeRabtUNdugYTUU6MA0GCSqGSIb3DQEBCwUAMF0xCzAJBgNV
BAYTAkZSMRIwEAYDVQQKDAlPcGVuVHJ1c3QxFzAVBgNVBAsMDjAwMDIgNDc4MjE3MzE4MSEwHwYD

VQQDDBhPcGVuVHJ1c3QgQ0EgZm9yIEFBVEwgRzEwHhcNMTcwMzA4MTEzNTUwWhcNMjUxMjMxMDAw
MDAwWjByMQswCQYDVQQGEwJGUjEYMBYGA1UECgwPRG9jdVNpZ24gRnJhbmNlMRcwFQYDVQQLDA4w
MDAyIDgxMjYxMTE1MDEwMC4GA1UEAwwnRG9jdVNpZ24gUHJlbWl1bSBDbG91ZCBTaWduaW5nIENB
IC0gU0kxMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA41sfk8qaBiZ6bSgFeGPBWpup
187Rx5yWcrN7SVVa6T8KK4g1jS1TdL4bdvNTbE0gIkV4zvjm5T+W/5BY36EilM0wOh7km+xMH0js
T2eWEqkp6OVkMls2zPyvd5CB109aM/mqzE3dlNjoTqNOOwwNgM2kVlIoNnLVKF/SdWXKLWbhokLh
iVVi3FMwXpWOoxt15huiDIdsbY0/y4CPgknoZWRO+Zvo36eNcD7p83cFTpP+aeU14bUWBGR1LmEc
Y6tPmOcDg3OnCDmuXGIU3Vt64byFEYagci/b39jdmY/4MZm1MHvLCLJsV4zB1OgwJsvhfFvjDqTi
W77pi7jpPBwl4QIDAQABo4IBxzCCAcMwDgYDVR0PAQH/BAQDAgEGMBIGA1UdEwEB/wQIMAYBAf8C
AQAwgbsGA1UdIASBszCBsDBSBgRVHSAAMEowSAYIKwYBBQUHAgEWPGh0dHBzOi8vd3d3LmRvY3Vz
aWduLmZyL3NvY2lldGUvcG9saXRpcXVlcy1kZS1jZXJ0aWZpY2F0aW9uczBaBgwrBgEEAYGtWgIO
AwEwSjBIBggrBgEFBQcCARY8aHR0cHM6Ly93d3cuZG9jdXNpZ24uZnIvc29jaWV0ZS9wb2xpdGlx
dWVzLWRlLWNlcnRpZmljYXRpb25zME4GA1UdHwRHMEUwQ6BBoD+GPWh0dHA6Ly9nZXQtY3JsLmNl
cnRpZmljYXQuY29tL3B1YmxpYy9vcGVudHJ1c3RjYWZvcmFhdGxnMS5jcmwwTwYIKwYBBQUHAQEE
QzBBMD8GCCsGAQUFBzABhjNodHRwOi8vZ2V0LW9jc3AuY2VydGlmaWNhdC5jb20vb3BlbnRydXN0
Y2Fmb3JhYXRsZzEwHQYDVR0OBBYEFK8jbJFA96wasc81ItdUylANjxwgMB8GA1UdIwQYMBaAFHh/
blSqzOg4uP0nxueFFcEFh40WMA0GCSqGSIb3DQEBCwUAA4ICAQBPiiaE0p13FH+AYuI5PxfaU/Bh
OtVPbw8I1DM8gtJqyb3C9cw07cTJ0FsGw6CAzpZ/YlAfB3pPBFGaSIeE8AcfrY+A137K80RHhNB8
Oc3AFiDwfxvmX03kkcgyS6m0n5rYX0OrqmHhXumqrpuY1TgKgalSATrgwRuE+ICUN91dP/H+ACuO
2c/EY1YyOPmfjAtsGBunp6mSpcupGyaPurclnAxzimRr65C3ltP0FVaFFAob5eFw5YhoDYWihPsa
pZvOTvomtQ8bOeKae7N2zfwT1g+ntn+v45RMYcWw99QTFB/3h8SZcmGddWar+fcUFqzqwI4+Xa2W
kbt7z3nzd33cT1VGByn9r7NHbmXDW2b23hq4eolkbHvn+CbkUh3taqPdFpJPPQhkzQKLiVA7G6Al
b7vDC6Hcq50UayhH3odUrtpdYs8OajHeoZj14yUhvqH+bDCrO8BvWvuReansfq+3l4RDB0O7fJTm
9AZp5wckcvA8up++y2juZjVD5oK8et6/ZBy/4qF11zzi99lht3gQT9paLC1UAu5J2n18M2TYWJH/
UMnbE3OkMxTuzMnNqkizc+5IcyG2QrAKA8ptD/gRoNzlsOgZNKyIYMN4KKoE4aAZ5nBe3OMekuU9
EhKir9uyZoqP/vZYzv+h7anl4mth2g0a2Hln3h/Lsjandt2Cbg==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *OpenTrust CA for AATL G1*

Issuer OU: *0002 478217318*

Issuer O: *OpenTrust*

Issuer C: *FR*

Subject CN: *DocuSign Premium Cloud Signing CA - SI1*

Subject OU: *0002 812611150*

Subject O: *DocuSign France*

Subject C: *FR*

Valid from: *Wed Mar 08 12:35:50 CET 2017*

Valid to: *Wed Dec 31 01:00:00 CET 2025*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:E3:5B:1F:93:CA:9A:06:26:7A:6D:28:05:78:63:C1:5A:
9B:A9:D7:CE:D1:C7:9C:96:72:B3:7B:49:55:5A:E9:3F:0A:2B:88:35:8D:2D:53:74:BE:1B:76:F3:53:6C:4D:20:22:45:78:CE:F8:E6:E5:3F:96:FF:90:58:DF:A1:22:94:CD
:30:3A:1E:E4:9B:EC:4C:1F:48:EC:4F:67:96:12:A9:29:E8:E5:64:32:5B:36:CC:FC:AF:77:90:81:D7:4F:5A:33:F9:AA:CC:4D:DD:94:D8:E8:4E:A3:4E:3B:0C:0D:80:CD:A
4:56:52:28:36:72:D5:28:5F:D2:75:65:CA:2D:66:E1:A2:42:E1:89:55:62:DC:53:30:5E:95:8E:A3:1B:75:E6:1B:A2:0C:87:6C:6D:8D:3F:CB:80:8F:82:49:E8:65:64:4E:F
9:9B:E8:DF:A7:8D:70:3E:E9:F3:77:05:4E:93:FE:69:E5:35:E1:B5:16:04:64:75:2E:61:1C:63:AB:4F:98:E7:03:83:73:A7:08:39:AE:5C:62:14:DD:5B:7A:E1:BC:85:11:8
6:A0:72:2F:DB:DF:D8:DD:99:8F:F8:31:99:B5:30:7B:CB:08:B2:6

C:57:8C:C1:D4:E8:30:26:CB:E1:7C:5B:E3:0E:A4:E2:5B:BE:E9:8B:B8:E9:3C:1C:25:E1:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

Certificate Policies *Policy OID: 2.5.29.32.0*
CPS pointer: https://www.docusign.fr/societe/politiques-de-certifications
Policy OID: 1.3.6.1.4.1.22234.2.14.3.1
CPS pointer: https://www.docusign.fr/societe/politiques-de-certifications

CRL Distribution Points *http://get-crl.certificat.com/public/opentrustcaforaatlg1.crl*

Authority Info Access *http://get-ocsp.certificat.com/opentrustcaforaatlg1*

Subject Key Identifier *AF:23:6C:91:40:F7:AC:1A:B1:CF:35:22:D7:54:CA:50:0D:8F:1C:20*

Authority Key Identifier *78:7F:6E:54:AA:CC:E8:38:B8:FD:27:C6:E7:85:15:C1:05:87:8D:16*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *40:CF:9A:0C:65:86:7B:00:69:CA:10:4F:0A:AC:D6:3C:B1:77:F8:C0:D1:9F:C4:D3:90:23:21:11:B5:74:DB:4D*

X509SubjectName

Subject CN: *DocuSign Premium Cloud Signing CA - SI1*

Subject OU: *0002 812611150*

Subject O: *DocuSign France*

Subject C: *FR*

X509SKI

X509 SK I *ryNskUD3rBqxzzUi11TKUA2PHCA=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*
[fr] *undefined.*

Status Starting Time *2018-06-30T22:00:00Z*

TSP Service Definition URI

URI *[en]* *https://www.docusign.fr/societe/politiques-de-certifications*

URI *[fr]* *https://www.docusign.fr/societe/politiques-de-certifications*

10.7.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

10.7.2 - Extension (critical): Qualifiers [QCWithQSCD, QCForESig]

Qualifier type description *[en]* *undefined.*

[fr] *undefined.*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithQSCD*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForESig*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Policy Identifier nodes:

Identifier *1.3.6.1.4.1.22234.2.14.3.31*

10.8 - Service (granted): UH Qualifiee PA2 20180309 - 1.3.6.1.4.1.22234.2.6.5.8

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[fr] *Un service de génération horodatage création et la signature temps timbres jetons qualifiés.*

Service Name

Name *[en]* *UH Qualifiee PA2 20180309 - 1.3.6.1.4.1.22234.2.6.5.8*

Name *[fr]* *UH Qualifiee PA2 20180309 - 1.3.6.1.4.1.22234.2.6.5.8*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *157937124218189002194050074075260296874746 6*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIFsDCCBJigAwIBAgISEiFa3Ny6O+l88TyjjQG+Ne3KMA0GCSqGSIb3DQEBCwUAMH4xCzAJBgNV
BAYTAkZSMRIwEAYDVQQKEwlLZXluZWN0aXMxFzAVBgNVBAsTDjAwMDIgNDc4MjE3MzE4MRYwFAYD

VQQLEw1LZXluZWN0aXMgQ0RTMSowKAYDVQQDEyFLZXluZWN0aXMgQ0RTIENBIGZvciB0aW1lc3Rh
bXBpbmcwHhcNMTgwMzEzMTQwMDAzWhcNMjQwMzExMTQwMDAzWjCBgjELMAkGA1UEBhMCRlIxGDAW
BgNVBAoMD0RvY3VTaWduIEZyYW5jZTEcMBoGA1UEYQwTVkFURVUtRll3MTgxMjYxMTE1MDEXMBUG
A1UECwwOMDAwMiA4MTI2MTExNTAxIjAgBgNVBAMMGVVIIFF1YWxpZmllZSBQQTIgMjAxODAzMDkw
ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC8Eu5QimanUwPogBmvuRSQLJp7Rik7z/qC
SkIJOeKKxuZTcsf/C1OzPMr1386Bka0HgQUdTZNtkqoZM8wcqFqNfwKm22ahoktdANkELIfcgkSY
E8rtLGAuymGPN06eXmBAc708M+FRFGI+BCVaK7pK7KovrwRvV48U6h84QRO/OSTQgzAl8SaJG6bK
0Gxznf+wRq0PlrHe2oUVAjDcSMPF2NDh0io9FZK+GMHtdE+HahKuyq0VrVR/oRuOP+Zfq+byQ7+r
StBeWWKrKlwQgY1yuEmxGOZtj1mpQ39EnZSJRll7YOAPK45F6VGLTNcz1T2hRW3rKP1V7eNGFlb4
hUPpAgMBAAGjggIhMIICHTAOBgNVHQ8BAf8EBAMCB4AwKwYDVR0QBCQwIoAPMjAxODAzMTMxNDAw
MDNagQ8yMDE5MDMxMzE0MDAwM1owFgYDVR0lAQH/BAwwCgYIKwYBBQUHAwgwRQYDVR0gBD4wPDA6
BgwrBgEEAYGtWgIIAwUwKjAoBggrBgEFBQcCARYcaHR0cDovL3d3dy5vcGVudHJ1c3QuY29tL1BD
LzAMBgNVHRMBAf8EAjAAMGcGA1UdHwRgMF4wXKBaoFiGVmh0dHA6Ly90cnVzdGNlbnRlci1jcmwu
Y2VydGlmaWNhdDIuY29tL0tleW5lY3Rpcy9LZXluZWN0aXNfQ0RTX0NBX2Zvcl90aW1lc3RhbXBp
bmcuY3JsMIGgBggrBgEFBQcBAQSBkzCBkDBDBggrBgEFBQcwAYY3aHR0cDovL29jc3AtaWQuZHNm
LmRvY3VzaWduLm5ldC9jZHNfY2FfZm9yX3RpbWVzdGFtcGluZzBJBggrBgEFBQcwAoY9aHR0cDov
L2NydC5kc2YuZG9jdXNpZ24ubmV0L2tleW5lY3Rpc2Nkc2NhZm9ydGltZXN0YW1waW5nLnA3YzAl
BggrBgEFBQcBAwQZMBcwFQYIKwYBBQUHCwIwCQYHBACL7EkBAjAdBgNVHQ4EFgQUPeoypvlAJvnN
RCOLYqKYQRBA6uowHwYDVR0jBBgwFoAUX6hxYL9ViVi14+0gmeFnN0ipseEwDQYJKoZIhvcNAQEL
BQADggEBAHq2cOxGfx4aSKDDwB67cjO2v/9ge2+B0NB9LrGI6362br29OrvT8IeD6e7tIoTTdJtu
F3H2legS3Zohoo8TN/5WFflJf2d+MmX3GxhH8/gZ+Cvc/114WkYrv4xMhhKZUhECqPNMY+6kyGai
xJs73iWsVs0w6YA1eWstTdHCjToieTooFlMquRx/ult05DGgAc0R6rGkDQKuEYpG4nvwQlhmPeri
6rdkE7DALL9lHrvDbtDIPK+e0tZu2jumPTHCLYiqWkaDfnyhC22ZyOxZV2OseJVIZyYxw0WJeZn/
krSeed1cc6HWJLMeULpQfuiiMdj8RBzlSO46KqitunTZwVQ=

-----END CERTIFICATE-----

Signature algorithm:	*SHA256withRSA*
Issuer CN:	*Keynectis CDS CA for timestamping*
Issuer OU:	*Keynectis CDS*
Issuer OU:	*0002 478217318*
Issuer O:	*Keynectis*
Issuer C:	*FR*
Subject CN:	*UH Qualifiee PA2 20180309*
Subject OU:	*0002 812611150*
Subject 2.5.4.97:	*VATEU-FR71812611150*
Subject O:	*DocuSign France*
Subject C:	*FR*
Valid from:	*Tue Mar 13 15:00:03 CET 2018*
Valid to:	*Mon Mar 11 15:00:03 CET 2024*
Public Key:	

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:BC:12:EE:50:8A:66:A7:53:03:E8:80:19:AF:B9:14:90:
2C:9A:7B:46:29:3B:CF:FA:82:4A:42:09:39:E2:8A:C6:E6:53:72:C7:FF:0B:53:B3:3C:CA:F5:DF:CE:81:91:AD:07:81:05:1D:4D:93:6D:92:AA:19:33:CC:1C:A8:5A:8D:7

F:02:A6:DB:66:A1:A2:4B:5D:00:D9:04:2C:87:DC:82:44:98:13:CA:ED:2C:60:2E:CA:61:8F:37:4E:9E:5E:60:40:73:BD:3C:33:E1:51:14:62:3E:04:25:5A:2B:BA:4A:EC:AA:2F:AF:04:6F:57:8F:14:EA:1F:38:41:13:BF:39:24:D0:83:30:08:F1:26:89:1B:A6:CA:D0:6C:73:9D:FF:B0:46:AD:0F:96:B1:DE:DA:85:15:02:30:DC:48:C3:C5:D8:D0:E1:D2:2A:3D:15:92:BE:18:C1:ED:74:4F:87:6A:12:AE:CA:AD:15:AD:54:7F:A1:1B:8E:3F:E6:5F:AB:E6:F2:43:BF:AB:4A:D0:5E:59:62:AB:2A:5C:10:81:8D:72:B8:49:B1:18:E6:6D:8F:59:A9:43:7F:44:9D:94:89:46:59:7B:60:E0:0F:2B:8E:45:E9:51:8B:4C:D7:33:D5:3D:A1:45:6D:EB:28:FD:55:ED:E3:46:16:56:F8:85:43:E9:02:03:01:00:01

Extended Key Usage *id_kp_timeStamping*

Certificate Policies *Policy OID: 1.3.6.1.4.1.22234.2.8.3.5*

CPS pointer: http://www.opentrust.com/PC/

Basic Constraints *IsCA: false*

CRL Distribution Points *http://trustcenter-crl.certificat2.com/Keynectis/Keynectis_CDS_CA_for_timestamping.crl*

Authority Info Access *http://ocsp-id.dsf.docusign.net/cds_ca_for_timestamping*

http://crt.dsf.docusign.net/keynectiscdscafortimestamping.p7c

Subject Key Identifier *3D:EA:32:A6:F9:40:26:F9:CD:44:23:8B:62:A2:98:41:10:40:EA:EA*

Authority Key Identifier *5F:A8:71:60:BF:55:89:58:B5:E3:ED:20:99:E1:67:37:48:A9:B1:E1*

Key Usage: *digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint: *48:A3:BB:34:64:3E:8B:EE:C2:0C:3F:DC:BF:92:59:D1:6F:D8:2F:97:96:F4:0E:34:33:77:6F:63:2A:50:04:9F*

X509SubjectName

Subject CN: *UH Qualifiee PA2 20180309*

Subject OU: *0002 812611150*

Subject 2.5.4.97: *VATEU-FR71812611150*

Subject O: *DocuSign France*

Subject C: *FR*

X509SKI

X509 SK I *PeoypvlAJvnNRCOLYqKYQRBA6uo=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2018-06-30T22:00:00Z*

TSP Service Definition URI

URI	*[en]*	*https://www.docusign.fr/societe/politiques-de-certifications*
URI	*[fr]*	*https://www.docusign.fr/societe/politiques-de-certifications*

11 - TSP: Ordre National des Experts-Comptables

TSP Name

Name	*[en]*	*Ordre National des Experts-Comptables*
Name	*[fr]*	*Ordre National des Experts-Comptables*

TSP Trade Name

Name	*[en]*	*VATFR-03775670003*
Name	*[fr]*	*VATFR-03775670003*

PostalAddress

Street Address	*[fr]*	*19 rue Cognacq-jay*
Locality	*[fr]*	*Paris*
Postal Code	*[fr]*	*75007*
Country Name	*[fr]*	*FR*

PostalAddress

Street Address	*[en]*	*19 rue Cognacq-jay*
Locality	*[en]*	*Paris*
Postal Code	*[en]*	*75007*
Country Name	*[en]*	*FR*

ElectronicAddress

URI	*mailto:signexpert@cs.experts-comptables.org*
URI	*mailto:signexpert@cs.experts-comptables.org*
URI	*https://www.signexpert.fr/*
URI	*https://www.signexpert.fr/*

TSP Information URI

URI	*[en]*	*https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*
URI	*[fr]*	*https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

11.1 - Service (granted): Ordre des Experts-Comptables - Signature et Authentification

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[fr]	*Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name	*[en]*	*Ordre des Experts-Comptables - Signature et Authentification*
Name	*[fr]*	*Ordre des Experts-Comptables - Signature et Authentification*

Service digital identities

Certificate fields details

Version:	*3*
Serial Number:	*149194987024906366654684505517651581358458 7*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIG8zCCBNugAwIBAgISESByVRBQwnPjxN9WpZo5Vy7LMA0GCSqGSIb3DQEBDAUAMHQxCzAJBgNV
BAYTAkZSMSUwIwYDVQQKExxPcmRyZSBkZXMgRXhwZXJ0cy1Db21wdGFibGVzMRcwFQYDVQQLEw4w
MDAyIDc3NTY3MDAwMzElMCMGA1UEAxMcT3JkcmUgZGVzIEV4cGVydHMtQ29tcHRhYmxlczAeFw0x
NjAyMTgwMDAwMDBaFw0zMTA1MDkwMDAwMDBaMIGuMQswCQYDVQQGEwJGUjElMCMGA1UECgwcT3Jk
cmUgZGVzIEV4cGVydHMtQ29tcHRhYmxlczEXMBUGA1UECwwOMDAwMiA3NzU2NzAwMDMxGDAWBgNV
BGEMD05UUkZSLTc3NTY3MDAwMzFFMEMGA1UEAww8U2lnbmF0dXJlIGV0IEF1dGhlbnRpZmljYXRp
b24gLSBPcmRyZSBkZXMgRXhwZXJ0cy1Db21wdGFibGVzMIICIjANBgkqhkiG9w0BAQEFAAOCAg8A
MIICCgKCAgEAxdtNc9OEmaEetYs4cHGjQVv3cFGgnuJ632d/BXSuzx4u5Gj7+u5MpMoM1xKO5H8Z
+88Heb9DSXzgBfQrmO6Q0uH64RKJM9L2kvQGxNfQev585nn0DD8QHMRdA4BtXx5KsAdl+XwVytBp
U+TohhltsX7akKrjrq78W2r0ezb0Y0f3CqWH4upQhKDkkVAojwGnk7Es68kqtAx76meQqyCcebv2
Lj+x5kr5ZR/m+hX7AuoLPWDsnlrDT8QrimwuBKZRZapn0h27v4ile17ybbdH1V6aqBYxYC7Mk83O
NJfbx9hpjCb8GgXn1x/CUXPTPjmnMEoEDtRxWjSNNNs+pExWLgbb3vzttkveRchubYAxjsl7OItX
hW7Ls+Acy/teX4Lo96T8U9qwhIc2iJoRmfrMaOimyuAnoU7bpGLYZ1mMReiChRtyH6zqTzZ6NuvF
vZSRi8DckxtOwvi0sZgcudZfxULHGc+MHoUAqJ1RMqBFYLEtfDnlQHOFaPa2MoCnIFuMN2G7CSp8
zFXVhSZLMbWdD04PPofweJSD8EU5ezBvTycA2onl861XYHEBYprPJjA5XUK+E/uNUfkWSD342zzG
hIb6/bup6W0SPqy3+srLCENGVNK9aY98iMFrDSZqZTuFcH5YaEV4/hMfbX3Qx9lNGM2bivudyz+t
A/slT4THKlsCAwEAAaOCAUIwggE+MA4GA1UdDwEB/wQEAwIBBjB1BgNVHSAEbjBsMGoGCiqBegGB
JQEBAQIwXDBaBggrBgEFBQcCARZOaHR0cDovL3NlZWMuZXhwZXJ0cy1jb21wdGFibGVzLmZyL1BD
L1BDUmFjaW5lX09yZHJlX2Rlc19FeHBlcnRzLUNvbXB0YWJsZXMucGRmMBIGA1UdEwEB/wQIMAYB
Af8CAQAwYQYDVR0fBFowWDBWoFSgUoZQaHR0cDovL3NlZWMuZXhwZXJ0cy1jb21wdGFibGVzLmZy
L0NSTC9DUkxSYWNpbmVfT3JkcmVfZGVzX0V4cGVydHMtQ29tcHRhYmxlcy5jcmwwHQYDVR0OBBYE
FHtvQ/HNpzwUKXr7Q64zUx70Inp8MB8GA1UdIwQYMBaAFIEHOeMPekYPuX3pXWJ29SSVHBVWMA0G
CSqGSIb3DQEBDAUAA4ICAQClC1B+tmL0zEP6Z0ervnWZc61Zw89xdRtbkmkxHATtB562o8DTjjpl
COCQSjG7r0S6AHhLfP4UDBoFBFU+czjYmeNF6DvHQXQCAoXT6iJ+tOlnQMh/kA7WR+A3avozZhVo
xBslJWEo1eSF3WiPY2bOVsbqlYHAkVBA1Ajyn2DUEGlPRi50gjKzvxcK69IhZNeUlg/HwAQ6weUo

/Lctia3hm7tYqau12uALmWaGX+S6TuR+bicqAxIp8P1DojzTHooQAAUCkjmsGUHpyr4L0rQf1Nqa
/vTYlL6ETDycS9jAWbEM1czMg+d3sHGGeZ3MoqnsOfM7m4Y5ClldL/YU9hDKMa0pfzBi3T6WXtFB
b9xfJbsb3AeKE+NX6IptzYKLzs87+AIeP6eUpNDUo8jWnLoTnxT9qgBBf0iJicjxPwHRUM+IQeeZ
TWn7S6sqFgIaI8N2VJle9vASGWzOgLaoTwFh/OPjXFDWKNDTUZZmYFy3DftbUzmm+S9b53sU58j3
nbgClWfXoQBA7nWuB6XbAreGO3ZS2Gt2SY54LW1Zf/6iNUbCr0xY9ikQ6LAG5TfENZAUPc8LSbzg
18sA6KIHR4t6vyoCxx62QBx0fb7tIdu3fN1oZlJoiM/zVVOyVoC1Ove3GLlyBK2PV0vsN2ht79Kf sErIzFSBVjATk4wc3f8R5g==

-----END CERTIFICATE-----

Signature algorithm: *SHA384withRSA*

Issuer CN: *Ordre des Experts-Comptables*

Issuer OU: *0002 775670003*

Issuer O: *Ordre des Experts-Comptables*

Issuer C: *FR*

Subject CN: *Signature et Authentification - Ordre des Experts-Comptables*

Subject 2.5.4.97: *NTRFR-775670003*

Subject OU: *0002 775670003*

Subject O: *Ordre des Experts-Comptables*

Subject C: *FR*

Valid from: *Thu Feb 18 01:00:00 CET 2016*

Valid to: *Fri May 09 02:00:00 CEST 2031*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:C5:DB:4D:73:D3:84:99:A1:1E:B5:8B:38:70:71:A3:41:
5B:F7:70:51:A0:9E:E2:7A:DF:67:7F:05:74:AE:CF:1E:2E:E4:68:FB:FA:EE:4C:A4:CA:0C:D7:12:8E:E4:7F:19:FB:CF:07:79:BF:43:49:7C:E0:05:F4:2B:98:EE:90:D2:E1:F
A:E1:12:89:33:D2:F6:92:F4:06:C4:D7:D0:7A:FE:7C:E6:79:F4:0C:3F:10:1C:C4:5D:03:80:6D:5F:1E:4A:B0:07:65:F9:7C:15:CA:D0:69:53:E4:E8:86:19:6D:B1:7E:D
A:90:AA:E3:AE:AE:FC:5B:6A:F4:7B:36:F4:63:47:F7:0A:A5:87:E2:EA:50:84:A0:E4:91:50:28:8F:01:A7:93:B1:2C:EB:C9:2A:B4:0C:7B:EA:67:90:AB:20:9C:7
9:BB:F6:2E:3F:B1:E6:4A:F9:65:1F:E6:FA:15:FB:02:EA:0B:3D:60:EC:9E:5A:C3:4F:C4:2B:8A:6C:2E:04:A6:51:65:AA:67:D2:1D:BB:BF:88:A5:7B:5E:F2:6D:B7:47:D5
:5E:9A:A8:16:31:60:2E:CC:93:CD:CE:34:97:DB:C7:D8:69:8C:26:FC:1A:05:E7:D7:1F:C2:51:73:D3:3E:39:A7:30:4A:04:0E:D4:71:5A:34:8D:34:DB:3E:A4:4C:56:2E:
06:DB:DE:FC:ED:B6:4B:DE:45:C8:6E:6D:80:31:8E:C9:7B:38:8B:57:85:6E:CB:B3:E0:1C:CB:FB:5E:5F:82:E8:F7:A4:FC:53:DA:B0:84:87:36:88:9A:11:99:FA:CC:68:E8
:A6:CA:E0:27:A1:4E:DB:A4:62:D8:67:59:8C:45:E8:82:85:1B:72:1F:AC:EA:4F:36:7A:36:EB:C5:BD:94:91:8B:C0:DC:93:1B:4E:C2:F8:B4:B1:98:1C:B9:D6:5F:C5:42:C
7:19:CF:8C:
1E:85:00:A8:9D:51:32:A0:45:60:B1:2D:7C:39:E5:40:73:85:68:F6:B6:32:80:A7:20:5B:8C:37:61:BB:09:2A:7C:CC:55:D5:85:26:4B:31:B5:9D:0F:4E:0F:3E:87:F0:78:
94:83:F0:45:39:7B:30:6F:4F:27:00:DA:89:E5:F3:AD:57:60:71:01:62:9A:CF:26:30:39:5D:42:BE:13:FB:8D:51:F9:16:48:3D:F8:DB:3C:C6:84:86:FA:FD:BB:A9:E9:6D
:12:3E:AC:B7:FA:CA:CB:08:43:46:54:D2:BD:69:8F:7C:88:C1:6B:0D:26:6A:65:3B:85:70:7E:58:68:45:78:FE:13:1F:6D:7D:D0:C7:D9:4D:18:CD:9B:8A:FB:9D:CB:3F:
AD:03:FB:25:4F:84:C7:2A:5B:02:03:01:00:01

Certificate Policies *Policy OID: 1.2.250.1.165.1.1.1.2*

CPS pointer: http://seec.experts-comptables.fr/PC/PCRacine_Ordre_des_Experts-Comptables.pdf

Basic Constraints *IsCA: true - Path length: 0*

CRL Distribution Points *http://seec.experts-comptables.fr/CRL/CRLRacine_Ordre_des_Experts-Comptables.crl*

Subject Key Identifier *7B:6F:43:F1:CD:A7:3C:14:29:7A:FB:43:AE:33:53:1E:F4:22:7A:7C*

Authority Key Identifier *81:07:39:E3:0F:7A:46:0F:B9:7D:E9:5D:62:76:F5:24:95:1C:15:56*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *B9:EB:70:E6:5E:3C:D2:47:D4:A6:87:EE:C8:9A:E3:6E:CF:E0:39:2C:25:6B:7D:90:46:1B:1D:88:7F :D8:0E:9B*

Certificate fields details

Version: *3*

Serial Number: *1492067806633762915051030670191217863412767*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIG8zCCBNugAwIBAgISESDLDskD1knJuEbf3lra7cwfMA0GCSqGSIb3DQEBDQUAMHQxCzAJBgNV
BAYTAkZSMSUwIwYDVQQKExxPcmRyZSBkZXMgRXhwZXJ0cy1Db21wdGFibGVzMRcwFQYDVQQLEw4w
MDAyIDc3NTY3MDAwMzElMCMGA1UEAxMcT3JkcmUgZGVzIEV4cGVydHMtQ29tcHRhYmxlczAeFw0x
NjAyMTgwMDAwMDBaFw0zMTA1MDkwMDAwMDBaMIGuMQswCQYDVQQGEwJGUjElMCMGA1UECgwcT3Jk
cmUgZGVzIEV4cGVydHMtQ29tcHRhYmxlczEXMBUGA1UECwwOMDAwMiA3NzU2NzAwMDMxGDAWBgNV
BGEMD05UUkZSLTc3NTY3MDAwMzFFMEMGA1UEAww8U2lnbmF0dXJlIGV0IEF1dGhlbnRpZmljYXRp
b24gLSBPcmRyZSBkZXMgRXhwZXJ0cy1Db21wdGFibGVzMIICIjANBgkqhkiG9w0BAQEFAAOCAg8A
MIICCgKCAgEAxdtNc9OEmaEetYs4cHGjQVv3cFGgnuJ632d/BXSuzx4u5Gj7+u5MpMoM1xKO5H8Z
+88Heb9DSXzgBfQrmO6Q0uH64RKJM9L2kvQGxNfQev585nn0DD8QHMRdA4BtXx5KsAdl+XwVytBp
U+TohhltsX7akKrjrq78W2r0ezb0Y0f3CqWH4upQhKDkkVAojwGnk7Es68kqtAx76meQqyCcebv2
Lj+x5kr5ZR/m+hX7AuoLPWDsnlrDT8QrimwuBKZRZapn0h27v4ile17ybbdH1V6aqBYxYC7Mk83O
NJfbx9hpjCb8GgXn1x/CUXPTPjmnMEoEDtRxWjSNNNs+pExWLgbb3vzttkveRchubYAxjsl7OItX
hW7Ls+Acy/teX4Lo96T8U9qwhIc2iJoRmfrMaOimyuAnoU7bpGLYZ1mMReiChRtyH6zqTzZ6NuvF
vZSRi8DckxtOwvi0sZgcudZfxULHGc+MHoUAqJ1RMqBFYLEtfDnlQHOFaPa2MoCnIFuMN2G7CSp8
zFXVhSZLMbWdD04PPofweJSD8EU5ezBvTycA2onl861XYHEBYprPjA5XUK+E/uNUfkWSD342zzG
hIb6/bup6W0SPqy3+srLCENGVNK9aY98iMFrDSZqZTuFcH5YaEV4/hMfbX3Qx9lNGM2bivudyz+t
A/slT4THKlsCAwEAAaOCAUIwggE+MA4GA1UdDwEB/wQEAwIBBjB1BgNVHSAEbjBsMGoGCiqBegGB
JQEBAQIwXDBaBggrBgEFBQcCARZOaHR0cDovL3NlZWMuZXhwZXJ0cy1jb21wdGFibGVzLmZyL1BD
L1BDUmFjaW5lX09yZHJlX2Rlc19FeHBlcnRzLUNvbXB0YWJsZXMucGRmMBIGA1UdEwEB/wQIMAYB
Af8CAQAwYQYDVR0fBFowWDBWoFSgUoZQaHR0cDovL3NlZWMuZXhwZXJ0cy1jb21wdGFibGVzLmZy
L0NSTC9DUkxSYWNpbmVfT3JkcmVfZGVzX0V4cGVydHMtQ29tcHRhYmxlcy5jcmwwHQYDVR0OBBYE
FHtvQ/HNpzwUKXr7Q64zUx70lnp8MB8GA1UdIwQYMBaAFIEHOeMPekYPuX3pXWJ29SSVHBVWMA0G
CSqGSIb3DQEBDQUAA4ICAQB0cdIptoPFHP1Z2d/5zoYcUKOozBlTm38COOZD7vs62Qy6LN/ldZo3
eR1dmLPFF8jGa64pq2i1kMh2sxyyCcv5iFALt8SPorh/JZjID+bnUq5PYEB+J3xYYMlrsSr7HpIO
o3VA//YoxSeZ96rm/TZqICml26sJd4Hk36Ib0XiW4Hj72zHIvH42wR74jOZ6lXOzL7XNXLjEX+Sr
gCNclTZmIrcwooEmQeK7k7UkgLXtPrXxHndWfdWAFQkpfBfEZC9gLv41oK8XyyPiNLByYFW/noZb
wRfaytYiFZu4dNHwlzqHbYdZ6TSKgXI6w6By6ZtLw0zO2OI157q2IOTrVb2UajP0DzzlOqkQWcus
Cql9qXMVJozRnrhV2+NEtfM5+0XxpaO3h1RTQ+c9M+STG1lcF2ivcnP6IOIsYQl9/ZW+jKW7s4KF
s/mDfTTsmn04waHyvSvy0XIKNgKdlEKQWwn0soaMFmFTqDpxNRgNgVgcmhNWBt/I0Cshwrz7VSo0
ysMHpKhYvH4tL5R+RpPuKF/8IKdm4XlXGUIIAL17sKCtb/Y1RDF10Cur9tjTd1Rdn706NL2GwlC1
aQIbpXBmppKvy4woOJl/GWWvXFm/PYEs7JxRxzkaYRGP6fpVh1BvcGSShd3WS/FqlpFZk7YBYVhB
bfl7wfnTf43NUhe+ygkZjg==

-----END CERTIFICATE-----

Signature algorithm: *SHA512withRSA*

Issuer CN: *Ordre des Experts-Comptables*

Issuer OU: *0002 775670003*

Issuer O:	*Ordre des Experts-Comptables*
Issuer C:	*FR*
Subject CN:	*Signature et Authentification - Ordre des Experts-Comptables*
Subject 2.5.4.97:	*NTRFR-775670003*
Subject OU:	*0002 775670003*
Subject O:	*Ordre des Experts-Comptables*
Subject C:	*FR*
Valid from:	*Thu Feb 18 01:00:00 CET 2016*
Valid to:	*Fri May 09 02:00:00 CEST 2031*
Public Key:	

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:C5:DB:4D:73:D3:84:99:A1:1E:B5:8B:38:70:71:A3:41:5B:F7:70:51:A0:9E:E2:7A:DF:67:7F:05:74:AE:CF:1E:2E:E4:68:FB:FA:EE:4C:A4:CA:0C:D7:12:8E:E4:7F:19:FB:CF:07:79:BF:43:49:7C:E0:05:F4:2B:98:EE:90:D2:E1:FA:E1:12:89:33:D2:F6:92:F4:06:C4:D7:D0:7A:FE:7C:E6:79:F4:0C:3F:10:1C:C4:5D:03:80:6D:5F:1E:4A:B0:07:65:F9:7C:15:CA:D0:69:53:E4:E8:86:19:6D:B1:7E:DA:90:AA:E3:AE:AE:FC:5B:6A:F4:7B:36:F4:63:47:F7:0A:A5:87:E2:EA:50:84:A0:E4:91:50:28:8F:01:A7:93:B1:2C:EB:C9:2A:B4:0C:7B:EA:67:90:AB:20:9C:79:BB:F6:2E:3F:B1:E6:4A:F9:65:1F:E6:FA:15:FB:02:EA:0B:3D:60:EC:9E:5A:C3:4F:C4:2B:8A:6C:2E:04:A6:51:65:AA:67:D2:1D:BB:BF:88:A5:7B:5E:F2:6D:B7:47:D5:5E:9A:A8:16:31:60:2E:CC:93:CD:CE:34:97:DB:C7:D8:69:8C:26:FC:1A:05:E7:D7:1F:C2:51:73:D3:3E:39:A7:30:4A:04:0E:D4:71:5A:34:8D:34:DB:3E:A4:4C:56:2E:06:DB:DE:FC:ED:B6:4B:DE:45:C8:6E:6D:80:31:8E:C9:7B:38:8B:57:85:6E:CB:B3:E0:1C:CB:FB:5E:5F:82:E8:F7:A4:FC:53:DA:B0:84:87:36:88:9A:11:99:FA:CC:68:E8:A6:CA:E0:27:A1:4E:DB:A4:62:D8:67:59:8C:45:E8:82:85:1B:72:1F:AC:EA:4F:36:7A:36:EB:C5:BD:94:91:8B:C0:DC:93:1B:4E:C2:F8:B4:B1:98:1C:B9:D6:5F:C5:42:C7:19:CF:8C:
1E:85:00:A8:9D:51:32:A0:45:60:B1:2D:7C:39:E5:40:73:85:68:F6:B6:32:80:A7:20:5B:8C:37:61:BB:09:2A:7C:CC:55:D5:85:26:4B:31:B5:9D:0F:4E:0F:3E:87:F0:78:94:83:F0:45:39:7B:30:6F:4F:27:00:DA:89:E5:F3:AD:57:60:71:01:62:9A:CF:26:30:39:5D:42:BE:13:FB:8D:51:F9:16:48:3D:F8:DB:3C:C6:84:86:FA:FD:BB:A9:E9:6D:12:3E:AC:B7:FA:CA:CB:08:43:46:54:D2:BD:69:8F:7C:88:C1:6B:0D:26:6A:65:3B:85:70:7E:58:68:45:78:FE:13:1F:6D:7D:D0:C7:D9:4D:18:CD:9B:8A:FB:9D:CB:3F:AD:03:FB:25:4F:84:C7:2A:5B:02:03:01:00:01

Certificate Policies	*Policy OID: 1.2.250.1.165.1.1.1.2* *CPS pointer: http://seec.experts-comptables.fr/PC/PCRacine_Ordre_des_Experts-Comptables.pdf*
Basic Constraints	*IsCA: true - Path length: 0*
CRL Distribution Points	*http://seec.experts-comptables.fr/CRL/CRLRacine_Ordre_des_Experts-Comptables.crl*
Subject Key Identifier	*7B:6F:43:F1:CD:A7:3C:14:29:7A:FB:43:AE:33:53:1E:F4:22:7A:7C*
Authority Key Identifier	*81:07:39:E3:0F:7A:46:0F:B9:7D:E9:5D:62:76:F5:24:95:1C:15:56*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*A2:53:0C:5F:85:9F:70:D0:6C:EE:29:4A:54:79:49:D6:C9:81:EB:C0:A4:36:0E:72:75:DD:DC:BC:14:2D:15:D0*

X509SubjectName

Subject CN: *Signature et Authentification - Ordre des Experts-Comptables*

Subject 2.5.4.97: *NTRFR-775670003*

Subject OU: *0002 775670003*

Subject O: *Ordre des Experts-Comptables*

Subject C: *FR*

X509SKI

X509 SK I *e29D8c2nPBQpevtDrjNTHvQienw=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2016-10-30T23:00:00Z*

TSP Service Definition URI

URI *[en]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

URI *[fr]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

11.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.1.2 - Extension (critical): Qualifiers [QCWithQSCD, QCForESig]

Qualifier type description *[en]* *undefined.*

[fr] *undefined.*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithQSCD*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForESig*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Policy Identifier nodes:

Identifier *1.2.250.1.165.1.10.1.1*

Policy Identifier nodes:

Identifier

11.1.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *PC Experts Comptables 1.2.250.1.165.1.10.1.1*

Name *[fr]* *PC Experts Comptables 1.2.250.1.165.1.10.1.1*

Service digital identities

X509SubjectName

Subject CN: *Signature et Authentification - Ordre des Experts-Comptables*

Subject 2.5.4.97: *NTRFR-775670003*

Subject OU: *0002 775670003*

Subject O: *Ordre des Experts-Comptables*

Subject C: *FR*

X509SKI

X509 SK I *e29D8c2nPBQpevtDrjNTHvQienw=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-10-30T23:00:00Z*

11.1.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.1.3.2 - Extension (critical): Qualifiers [QCWithSSCD]

Qualifier type description *[en]* *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued*

under the service identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the presence or absence of Secure Signature Creation Device (SSCD) support ARE supported by an SSCD (i.e. that that the private key associated with the public key in the certificate is stored in a Secure Signature Creation Device conformant with the applicable European legislation);

[fr] *elle est assurée par le prestataire de service de confiance et contrôlée (modèle de contrôle) ou vérifiés (modèle d'accréditation) par l'État membre de référence (respectivement son Organe de surveillance ou organisme d'accréditation) que tous les certificats qualifiés délivrés dans le cadre du service identifié dans «Service digital identity» et en outre identifié par les informations des filtres utilisés pour identifier plus précisément dans le cadre du "Sdi" de service de confiance identifiés, l'ensemble précis de certificats qualifiés pour lesquels cette information supplémentaire est nécessaire en ce qui concerne la présence ou l'absence de dispositif sécurisé de création de signature (SSCD) de soutien sont pris en charge par un SSCD (à savoir que la clé privée associée à la clé publique du certificat est stocké dans un dispositif sécurisé conforme à la législation européenne applicable de création de signature);*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithSSCD*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Policy Identifier nodes:

Identifier *1.2.250.1.165.1.10.1.1*

11.2 - Service (granted): Ordre des Experts-Comptables - Cachet Cabinet

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Ordre des Experts-Comptables - Cachet Cabinet*

Name *[fr]* *Ordre des Experts-Comptables - Cachet Cabinet*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *149202609959008710123563024101438636082476 7*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIG3DCCBMSgAwIBAgISESCrrk0AL5o8tld7ouDew7O/MA0GCSqGSIb3DQEBDQUAMHQxCzAJBgNV
BAYTAkZSMSUwIwYDVQQKExxPcmRyZSBkZXMgRXhwZXJ0cy1Db21wdGFibGVzMRcwFQYDVQQLEw4w
MDAyIDc3NTY3MDAwMzElMCMGA1UEAxMcT3JkcmUgZGVzIEV4cGVydHMtQ29tcHRhYmxlczAeFw0x
NjAyMTgwMDAwMDBaFw0zMTA1MDkwMDAwMDBaMIGXMQswCQYDVQQGEwJGUjElMCMGA1UECgwcT3Jk
cmUgZGVzIEV4cGVydHMtQ29tcHRhYmxlczEXMBUGA1UECwwOMDAwMiA3NzU2NzAwMDMxGDAWBgNV
BGEMD05UUkZSLTc3NTY3MDAwMzEuMCwGA1UEAwwlQ2FjaGV0IC0gT3JkcmUgZGVzIEV4cGVydHMt
Q29tcHRhYmxlczCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBALzpJN8WNI54IZrngc67
0Y+oyQ14pbAUEclx9BwdxN7FFZ37gEwHGFSPOZn+AL+8Skt7yqgbxKaeVnPFUrB08FfrCEZAJvGb
pYjgs/pUG5jilEe9JmO/+PCajNcLn06lMlFwLDs5k4Ay60c9dSasMyc7HFl/nYryqU2slD2jX/+o
WqiYvX/lwCCvfSZvvt3HDNXNcIGhYybBeHPhuNNBo3wF6PlLzqkcvCA808OaH0iwPX5m7h19GwNR
p+2BKhYhtb0/ih90N328PM4g1Y+sG/j5q37oDdDUNEyIOFZ2Z0OCV5oAJV4sWZdPYEJ84yE4mhWx

ubJ1LnHGd3ALHUgdpjnVZ7Bz89EV7rfbd4mcip2Kg89QHHTUW2FH29B1muezI70FHPbC2OWMMo5y
e3SiMIY9Roi9aoePXO0+4j5O+jfmo0/z0sD7Ih66lhJRK5q0BD5YBh9skN28uyRAEjDyjlbuMeHD
6vrXtBE8B1PeEpr1XEP1uarC4Bj+eJQ4nKoGuDXqHIdTTSiruulQjqNZBlJ4uKoNaC/NpHkekOJt
2YUeeuBjmdx9SMSSK+eOPaFfbNdg1Ch8BrI6Lp+ln+VrGwSAa2R0juaZL09PaNOwDUKl8vP+WfqA
ZyaptApI+c5ndhS8X64ueXgd9wkg/K3cr/XzOmV4xDsIijj03Awm0C79AgMBAAGjggFCMIIBPjAO
BgNVHQ8BAf8EBAMCAQYwdQYDVR0gBG4wbDBqBgoqgXoBgSUBAQECMFwwWgYIKwYBBQUHAgEWTmh0
dHA6Ly9zZWVjLmV4cGVydHMtY29tcHRhYmxlcy5mci9QQy1JhY2luZV9PcmRyZV9kZXNfRXhw
ZXJ0cy1Db21wdGFibGVzLnBkZjASBgNVHRMBAf8ECDAGAQH/AgEAMGEGA1UdHwRaMFgwVqBUoFKG
UGh0dHA6Ly9zZWVjLmV4cGVydHMtY29tcHRhYmxlcy5mci9DUkwvQ1JMUmFjaW5lX09yZHJlX2Rl
c19FeHBlcnRzLUNvbXB0YWJsZXMuY3JsMB0GA1UdDgQWBBSBiwjNJ//9aiP+rpli8/2OU46b3TAf
BgNVHSMEGDAWgBSBBznjD3pGD7l96V1idvUklRwVVjANBgkqhkiG9w0BAQ0FAAOCAgEAYgLvVRGM
BqEoVQSX8jvea8TFiu5g6EyJ8T8cgFLg2DMl9vYnbjzc6RifeDdTyaFORG61JNYrdwe1A6/VtswN
8tCMyyLltzKo7iNVPywtqamHE3CSCAY2kuejtB+11Snel5Azd4vI+y5zRBdBqv1Rwek4WHuQfd13
0l4ki6LEcdE56aAFrI8lmBypOcPnD1duMvlW9nioWn2Oww2lbjUCZ7ISfyODZ8Nu6bwWWo4uxlei
l/pbBy91vMsXJn+5+O3hahhzh/pkvznQleO+nMP1iZhMCnPDhWSg1bbfRg9bf3+1d6hRFcVw07px
Sr/lt85L8qIRQ2F9rMNEGwiyRu0KX4LVo1Q6VVElBOFIXWIwXEzX1t3xAGqIy7Ef24ZGBzvOm/I9
Jo10i4xfa0p3XavkSKbuQk1WPSSfuo1HsxHzWCH96uJccGNTkEEf+Xax9E68F5qv8Gzz75UOG9ii
9s2iOOtRdRbF0b7wMq+vFkNtXBbuLHR8hVUQjh9JoNAMo5nGuXyrm1eO4C8b5NhnwKfHLt0WPKNX
UM9rKnWHvuxm8ruKomBytvjtJ+dt7Hkkv2J86OravmDo0z1K+nfDEmbBITS5ISjiBHzaxk35ZQ69
ht4sTLx7c1A5z6k3TkMMUK1pIiIW7FV0jtNnocEDjgs/O4j8X8igogZHQ1J5Wb+Fv5A=

-----END CERTIFICATE-----

Signature algorithm:	*SHA512withRSA*
Issuer CN:	*Ordre des Experts-Comptables*
Issuer OU:	*0002 775670003*
Issuer O:	*Ordre des Experts-Comptables*
Issuer C:	*FR*
Subject CN:	*Cachet - Ordre des Experts-Comptables*
Subject 2.5.4.97:	*NTRFR-775670003*
Subject OU:	*0002 775670003*
Subject O:	*Ordre des Experts-Comptables*
Subject C:	*FR*
Valid from:	*Thu Feb 18 01:00:00 CET 2016*
Valid to:	*Fri May 09 02:00:00 CEST 2031*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:BC:E9:24:DF:16:34:8E:78:21:9A:E7:81:CE:BB:D1:8F:
A8:C9:0D:78:A5:B0:14:11:C9:71:F4:1C:1D:C4:DE:C5:15:9D:FB:80:4C:07:18:54:8F:39:99:FE:00:BF:BC:4A:4B:7B:CA:A8:1B:C4:A6:9E:56:73:C5:52:B0:74:F0:57:EB
:08:46:40:26:F1:9B:A5:88:E0:B3:FA:54:1B:98:E2:94:47:BD:26:63:BF:F8:F0:9A:8C:D7:0B:9F:4E:A5:32:51:70:2C:3B:39:93:80:32:EB:47:3D:75:26:AC:33:27:3B:1C
:59:7F:9D:8A:F2:A9:4D:AC:94:3D:A3:5F:FF:A8:5A:A8:98:BD:7F:E5:C0:20:AF:7D:26:6F:BE:DD:C7:0C:D5:CD:70:81:A1:63:26:C1:78:73:E1:B8:D3:41:A3:7C:05:E8:
F9:4B:CE:A9:1C:BC:20:3C:D3:C3:9A:1F:48:B0:3D:7E:66:EE:1D:7D:1B:03:51:A7:ED:81:2A:16:21:B5:BD:3F:8A:1F:74:37:7D:BC:3C:CE:20:D5:8F:AC:1B:F8:F9:AB:7
E:E8:0D:D0:D4:34:4C:88:38:56:76:67:43:82:57:9A:00:25:5E:2C:59:97:4F:60:42:7C:E3:21:38:9A:15:B1:B9:B2:75:2E:71:C6:77:70:0B:1D:48:1D:A6:39:D5:67:B0:
73:F3:D1:15:EE:B7:DB:77:89:9C:8A:9D:8A:83:CF:50:1C:74:D4:5B:61:47:DB:D0:75:9A:E7:B3:23:BD:05:1C:F6:C2:D8:E5:8C:32:8E:72:7B:74:A2:30:86:3D:46:88:B
D:6A:87:8F:5C:ED:3E:E2:3E:4E:FA:37:E6:A3:4F:F3:D2:C0:FB:22:1E:BA:96:12:51:2B:9A:B4:04:3E:58:06:1F:6C:90:DD:BC:BB:24:40:12:30:F2:8E:56:EE:31:E1:C3:E
A:FA:D7

:B4:11:3C:07:53:DE:12:9A:F5:5C:43:F5:B9:AA:C2:E0:18:FE:78:94:38:9C:AA:06:B8:35:EA:1C:87:53:4D:28:AB:BA:E9:50:8E:A3:59:06:52:78:B8:AA:0D:68:2F:CD:A4:79:1E:90:E2:6D:D9:85:1E:7A:E0:63:99:DC:7D:48:C4:92:2B:E7:8E:3D:A1:5F:6C:D7:60:D4:28:7C:06:B2:3A:2E:9F:A5:9F:E5:6B:1B:04:80:6B:64:74:8E:E6:99:2F:4F:4F:68:D3:B0:0D:42:A5:F2:F3:FE:59:FA:80:67:26:A9:B4:0A:48:F9:CE:67:76:14:BC:5F:AE:2E:79:78:1D:F7:09:20:FC:AD:DC:AF:F5:F3:3A:65:78:C4:3B:08:8A:38:F4:DC:0C:26:D0:2E:FD:02:03:01:00:01

Certificate Policies

Policy OID: 1.2.250.1.165.1.1.1.2

CPS pointer: http://seec.experts-comptables.fr/PC/PCRacine_Ordre_des_Experts-Comptables.pdf

Basic Constraints

IsCA: true - Path length: 0

CRL Distribution Points

http://seec.experts-comptables.fr/CRL/CRLRacine_Ordre_des_Experts-Comptables.crl

Subject Key Identifier

81:8B:08:CD:27:FF:FD:6A:23:FE:AE:99:62:F3:FD:8E:53:8E:9B:DD

Authority Key Identifier

81:07:39:E3:0F:7A:46:0F:B9:7D:E9:5D:62:76:F5:24:95:1C:15:56

Key Usage:

keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

E2:47:97:D7:61:62:19:7F:E1:05:CE:0C:96:45:29:8B:80:D5:E9:5B:BF:FB:F5:00:4D:AE:CF:04:BE:E9:A3:21

X509SubjectName

Subject CN:

Cachet - Ordre des Experts-Comptables

Subject 2.5.4.97:

NTRFR-775670003

Subject OU:

0002 775670003

Subject O:

Ordre des Experts-Comptables

Subject C:

FR

X509SKI

X509 SK I

gYsIzSf//Woj/q6ZYvP9jlOOm90=

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description

[en] *undefined.*

[fr] *undefined.*

Status Starting Time

2017-10-31T23:00:00Z

TSP Service Definition URI

URI *[en]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

URI *[fr]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

11.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

11.2.2 - Extension (critical): Qualifiers [QCWithQSCD]

Qualifier type description *[en]* *undefined.*

[fr] *undefined.*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithQSCD*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Policy Identifier nodes:

Identifier *1.2.250.1.165.1.11.1.1*

11.3 - Service (withdrawn): Ordre des Experts-Comptables - région Alsace RGS***

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Alsace RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Alsace RGS****

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *149201037593995151676142950847832567644184*4

X509 Certificate -----BEGIN CERTIFICATE-----

MIIFtTCCA52gAwIBAgISESCf2gkyHdf5onc5BlNCIgD0MA0GCSqGSIb3DQEBCwUAMHQxCzAJBgNV
BAYTAkZSMSUwIwYDVQQKExxPcmRyZSBkZXMgRXhwZXJ0cy1Db21wdGFibGVzMRcwFQYDVQQLEw4w
MDAyIDc3NTY3MDAwMzElMCMGA1UEAxMcT3JkcmUgZGVzIEV4cGVydHMtQ29tcHRhYmxlczAeFw0x
MTA1MTAwMDAwMDBaFw0xOTEyMzEwMTAwMDBaMHcxCzAJBgNVBAYTAkZSMRcwFQYDVQQKEw5DUk9F

QyBkJ0Fsc2FjZTEXMBUGA1UECxMOMDAwMiA3Nzg4Njc3OTYxNjA0BgNVBAMMLU9yZHJlIGRlcyBF
eHBlcnRzLUNvbXB0YWJsZXMgLSByw6lnaW9uIEFsc2FjZTCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAL7fC/Q7rKeuNMx0B+muJmVCIbqbugSPK+3B3NJtBxfqAimffsWmLg3/IdkW99DB
31bLg5den2/9ArRafUhbWxV7X6JprI/W5nRWzmsXIJ/i9lcNctNjicE44R9+vFeQ8PbqsqoTXuPE
XJZ+TO1DFK1CODo2v4p/32W7sQc/4cWgKC406AkvWYxqLC2QQtk1/oVWyXJudPeUWb4yQGC1q+iw
p5lrAx8lWZdg5dVNz1Kv41hhXI1q4mQLg2sBp13GjxvS2BCGZBpk/BBPQRJnAcs4euikGYUlKUpW
7ASwdjaWyNlLvEDGxPeVbMQVDkFzQc7/d23rvy55SQgOmjLq8LUCAwEAAaOCATwwggE4MA4GA1Ud
DwEB/wQEAwIBBjBvBgNVHSAEaDBmMGQGBFUdIAAwXDBaBggrBgEFBQcCARZOaHR0cDovL3NlZWMu
ZXhwZXJ0cy1jb21wdGFibGVzLmZyL1BDL1BDUmFjaW5lX09yZHJlX2Rlc19FeHBlcnRzLUNvbXB0
YWJsZXMucGRmMBIGA1UdEwEB/wQIMAYBAf8CAQAwYQYDVR0fBFowWDBWoFSgUoZQaHR0cDovL3Nl
ZWMuZXhwZXJ0cy1jb21wdGFibGVzLmZyL0NSTC9DUkxSYWNpbmVfT3JkcmVfZGVzX0V4cGVydHMt
Q29tcHRhYmxlcy5jcmwwHQYDVR0OBBYEFBpyHEjW7kFo5j7aRqHK65uqiJ2hMB8GA1UdIwQYMBaA
FIEHOeMPekYPuX3pXWJ29SSVHBVWMA0GCSqGSIb3DQEBCwUAA4ICAQCuNgmMMN3zifx8VzxOe8tP
7dILwHZ0acBo0UPP/4FALwwKQPFSrZUhTEdYw1oCq81r60easjlvQG0258J7azTfh+CM8MZFD4n6
tDSO0OVIwFKoccIP/X0wY4Lr7kdxDNYsRgWPHyILFyLkGYOAIsUkcz/ZB66zwKj2Kagz2xl0w0sP
uhFb3t91nRcYp0FyRMl7h/qWzEf4ArKzH63hw0zQm+yWjCCQlGmTHndVAP1TrcdDP0Hd3jW0v8lJ
ONq5vn33a4tqHXtqn28W3qdte3iTySvFUrAxY+BYSl+y4e9PcHMpeT0A8cWrZwUqvxgyHoJNU/Bn
FOqU88/dpe18+Age+UUFkIZCoBKKiQ69UQiD+lVCGSHxPHtCfYj/bPHzX2o+WyRUSkRzhhijt/9J
zhyc5BYdIs7yDKYuX65lCYqW60mJoitND0dK9GbiCmbaW8V8b0SYts5d+naKbACgmphIYj1LToIQ
wnCVIV5pX9AEVzHO+YinjMkthLCFcnEbB3KMvWS5J9k4V1YLPIrk5nbolmDDgIZoiyJrcGhVLsG4
uwJ6sRCiL3idYd5mmwY4bv43NJKxr2XcBfkukePgA6xBslqgCsuipSUmfGfwCGwXGAlDKHq7QbzT
nHUkU6e3LJ6Vr0s+TlRXlkhLEFx7vqHbAXdOFCJBtyjQdx7dINiUpQ==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Ordre des Experts-Comptables*

Issuer OU: *0002 775670003*

Issuer O: *Ordre des Experts-Comptables*

Issuer C: *FR*

Subject CN: *Ordre des Experts-Comptables - région Alsace*

Subject OU: *0002 778867796*

Subject O: *CROEC d'Alsace*

Subject C: *FR*

Valid from: *Tue May 10 02:00:00 CEST 2011*

Valid to: *Tue Dec 31 02:00:00 CET 2019*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:BE:DF:0B:F4:3B:AC:A7:AE:34:CC:74:07:E9:AE:26:65:
42:21:BA:9B:BA:04:8F:2B:ED:C1:DC:D2:6D:07:17:EA:02:29:9F:7E:C5:A6:2E:0D:FF:21:D9:16:F7:D0:C1:DF:56:CB:83:97:5E:9F:6F:FD:02:B4:5A:7D:48:5B:5B:15:7
B:5F:A2:69:AC:8F:D6:E6:74:56:CE:6B:17:20:9F:E2:F6:57:0D:72:D3:63:89:C1:38:E1:1F:7E:BC:57:90:F0:F6:EA:B2:AA:13:5E:E3:C4:5C:96:7E:4C:ED:43:14:AD:42:3
8:3A:36:BF:8A:7F:DF:65:BB:B1:07:3F:E1:C5:A0:28:2E:34:E8:09:2F:59:8C:6A:2C:2D:90:42:D9:35:FE:85:56:C9:72:6E:74:F7:94:59:BE:32:40:60:B5:AB:E8:B0:A7:9
9:6B
:03:1F:25:59:97:60:E5:D5:4D:CF:52:AF:E3:58:61:5C:8D:6A:E2:64:0B:83:6B:01:A7:5D:C6:8F:1B:D2:D8:10:86:64:1A:64:FC:10:4F:41:12:67:01:CB:38:7A:E8:A4:1
9:85:25:29:4A:56:EC:04:B0:76:36:96:C8:D9:4B:BC:40:C6:C4:F7:95:6C:C4:15:0E:41:73:41:CE:FF:77:6D:EB:BF:2E:79:49:08:0E:9A:32:EA:F0:B5:02:03:01:00:01

Certificate Policies *Policy OID: 2.5.29.32.0*

CPS pointer: http://seec.experts-comptables.fr/PC/PCRacine_Ordre_des_Experts-Comptables.pdf

Basic Constraints *IsCA: true - Path length: 0*

CRL Distribution Points *http://seec.experts-comptables.fr/CRL/CRLRacine_Ordre_des_Experts-Comptables.crl*

Subject Key Identifier *1A:72:1C:48:D6:EE:41:68:E6:3E:DA:46:A1:CA:EB:9B:AA:88:9D:A1*

Authority Key Identifier *81:07:39:E3:0F:7A:46:0F:B9:7D:E9:5D:62:76:F5:24:95:1C:15:56*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *C1:0F:01:B7:58:45:F6:9E:D2:93:85:4B:7E:7B:B4:BA:E0:40:5E:AA:E5:CA:AB:20:A4:03:CE:A7:C7:3F:7C:30*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2018-01-30T01:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS101456/QCPPublic*

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Signature-3-Stars*

TSP Service Definition URI

URI *[fr]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

URI *[en]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

11.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.3.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Alsace RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Alsace RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - région Alsace*

Subject OU: *0002 778867796*

Subject O: *CROEC d'Alsace*

Subject C: *FR*

X509SKI

X509 SK I *GnIcSNbuQWjmPtpGocrrm6qInaE=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

11.3.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.3.3 - History instance n.2 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Alsace RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Alsace RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - région Alsace*

Subject OU: *0002 778867796*

Subject O: *CROEC d'Alsace*

Subject C: *FR*

X509SKI

X509 SK I *GnIcSNbuQWjmPtpGocrrm6qInaE=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2012-11-25T23:00:00Z*

11.4 - Service (withdrawn): Ordre des Experts-Comptables - région Aquitaine RGS***

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Aquitaine RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Aquitaine RGS****

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *149182604767114722136173110731415534280987 6*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIFuzCCA6OgAwIBAgISESAVLbPiU//Dp3b+4b67wEsUMA0GCSqGSIb3DQEBCwUAMHQxCzAJBgNV
BAYTAkZSMSUwIwYDVQQKExxPcmRyZSBkZXMgRXhwZXJ0cy1Db21wdGFibGVzMRcwFQYDVQQLEw4w
MDAyIDc3NTY3MDAwMzElMCMGA1UEAxMcT3JkcmUgZGVzIEV4cGVydHMtQ29tcHRhYmxlczAeFw0x
MTA1MTAwMDAwMDBaFw0xOTEyMzEwMTAwMDBaMH0xCzAJBgNVBAYTAkZSMRowGAYDVQQKExFDUk9F
QyBkJ0FxdWl0YWluZTEXMBUGA1UECxMOMDAwMiA3ODE4NDY0NjQxOTA3BgNVBAMMME9yZHJlIGRl
cyBFeHBlcnRzLUNvbXB0YWJsZXMgLSByw6lnaW9uIEFxdWl0YWluZTCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBAMH+Qyi9MR9VVB3+/F5gEmxpDed7GTgyDMdfBbWEtF53eqwQAX9WgfNp
+hEzPXtGQJVRjXZNS2y8jktatX/tqJyDNSr54Vzx2cP/JB11Deffiw+GF74fbMigxkh3bCmD1j+l
f8zfLpfl92obp2AFVU21Gi5xcJRaQ0gDx6fGkNS/SAZmAajSQtGNZ2IuM5BZrVhKencArVjLL6Oy
hF3UfNlIjEn5AN7hVTTowhgs+dUdx3pST5+FqpAlZdn8q+MA9QezFjgzuoUqTGs3lAl2CCEGVWKS
duJPE5O7Hce9YipAZLx8GltA7f0rfLK5ekUl/lgaUkLB2mgwfcb4XQ9Pk3kCAwEAAaOCATwwggE4
MA4GA1UdDwEB/wQEAwIBBjBvBgNVHSAEaDBmMGQGBFUdIAAwXDBaBggrBgEFBQcCARZOaHR0cDov
L3NlZWMuZXhwZXJ0cy1jb21wdGFibGVzLmZyL1BDL1BDUmFjaW5lX09yZHJlX2Rlc19FeHBlcnRz
LUNvbXB0YWJsZXMucGRmMBIGA1UdEwEB/wQIMAYBAf8CAQAwYQYDVR0fBFowWDBWoFSgUoZQaHR0
cDovL3NlZWMuZXhwZXJ0cy1jb21wdGFibGVzLmZyL0NSTC9DUkxSYWNpbmVfT3JkcmVfZGVzX0V4
cGVydHMtQ29tcHRhYmxlcy5jcmwwHQYDVR0OBBYEFCwx3Z7ipQOo02pnfqok6lPlz/eOMB8GA1Ud
IwQYMBaAFIEHOeMPekYPuX3pXWJ29SSVHBVWMA0GCSqGSIb3DQEBCwUAA4ICAQCE0N2bYttzjx81
ukka+h1PcjOfu1H45BFotRRrlKLz89bqICU+/w7n9KxAufbPP76OOdffUfSenCJzky1K/DjwHrcG

sdSngXMuWTJHF5kLFniosXl2ysoQZH/OEF5O020RxqDJguv0ELenejqKJXHWraenClXsqeuHHPrh
T0xLtKlaPSvABsDkQ0PyLyiYVZt7AA8htgzx5vLlHVnaKJYgmnyK6xsW8W3+SLTAin80s9ZF8nUx
7G7Q64cA8QoLlZQsNLWUl2WRKhcLxihmN6hSyDMHaze5uPcHLUv9xhlma9TsXsZa79AKQ89mjrXl
8Ls/rwSzvWStwRY1VeBBZ1O2ZaEmuo0Qiy74QJZMO5d3/iEP15wRriT52TvjNUhPUV2Rr+hF7ESX
G1uBAJtgptVDXF1vYbOdrQ/0pMFJ9goy9b/P0g3Vk9xDJ9Ba+x/LbfTfEMFwFQjpO2SHoQYZqn8v
wDR6qCLLCt/D1S6JralMVFQx1D8CnR78anNqUHH483OchZVYMLJglwZr0P99w/XLYK9JtxwBdMco
NPZRnanvA+zSSHeR88O2ZneuYLLQNpQtH8NGmjhZzmcxhThgYVsg6ffdbzj3VBH/d03und+KgiXl
lTsoQcKp011xMmNy+geweTMA6JL+dF0I57iz1waHsZkhiViTv8mrUVMVKOOnbQ==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Ordre des Experts-Comptables*

Issuer OU: *0002 775670003*

Issuer O: *Ordre des Experts-Comptables*

Issuer C: *FR*

Subject CN: *Ordre des Experts-Comptables - région Aquitaine*

Subject OU: *0002 781846464*

Subject O: *CROEC d'Aquitaine*

Subject C: *FR*

Valid from: *Tue May 10 02:00:00 CEST 2011*

Valid to: *Tue Dec 31 02:00:00 CET 2019*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C1:FE:43:28:BD:31:1F:55:54:1D:FE:FC:5E:60:12:6C:6
9:0D:E7:7B:19:38:32:0C:C7:5F:05:B5:84:B4:5E:77:7A:AC:10:01:7F:56:81:F3:69:FA:11:33:3D:7B:46:40:95:51:8D:76:4D:4B:6C:BC:8E:4B:5A:B5:7F:ED:A8:9C:83:
35:2A:F9:E1:5C:F1:D9:C3:FF:24:1D:75:0D:E7:DF:8B:0F:86:17:BE:1F:6C:C8:A0:C6:48:77:6C:29:83:D6:3F:A5:7F:CC:DF:2E:97:E5:F7:6A:1B:A7:60:05:55:4D:B5:1A
:2E:71:70:94:5A:43:48:03:C7:A7:C6:90:D4:BF:48:06:66:01:A8:D2:42:D1:8D:67:62:2E:33:90:59:AD:58:4A:7A:77:00:AD:58:CB:2F:A3:B2:84:5D:D4:7C:D9:48:8C:
49:F9:00:DE:E1:55:34:E8:C2:18:2C:F9:D5:1D:C7:7A:52:4F:9F:85:AA:90:25:65:D9:FC:AB:E3:00:F5:07:B3:16:38:33:BA:85:2A:4C:6B:37:94:09:76:08:21:06:55:62:
92:76:E2:4F:13:93:BB:1D:C7:BD:62:2A:40:64:BC:7C:1A:5B:40:E
D:FD:2B:7C:B2:B9:7A:45:25:FE:58:1A:52:42:C1:DA:68:30:7D:C6:F8:5D:0F:4F:93:79:02:03:01:00:01

Certificate Policies *Policy OID: 2.5.29.32.0*

CPS pointer: http://seec.experts-comptables.fr/PC/PCRacine_Ordre_des_Experts-Comptables.pdf

Basic Constraints *IsCA: true - Path length: 0*

CRL Distribution Points *http://seec.experts-comptables.fr/CRL/CRLRacine_Ordre_des_Experts-Comptables.crl*

Subject Key Identifier *2C:31:DD:9E:E2:A5:03:A8:D3:6A:67:7E:AA:24:EA:53:E5:CF:F7:8E*

Authority Key Identifier *81:07:39:E3:0F:7A:46:0F:B9:7D:E9:5D:62:76:F5:24:95:1C:15:56*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *1A:64:AF:2B:5E:38:7D:EB:07:9F:2F:40:15:E3:82:A9:72:FD:2F:A2:77:23:53:36:8D:5E:32:44:AF:C4:AE:33*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2018-01-30T01:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS101456/QCPPublic*

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Signature-3-Stars*

TSP Service Definition URI

URI *[fr]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

URI *[en]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

11.4.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.4.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Aquitaine RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Aquitaine RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - région Aquitaine*

Subject OU: *0002 781846464*

Subject O: *CROEC d'Aquitaine*

Subject C: *FR*

X509SKI

X509 SK I *LDHdnuKlA6jTamd+qiTqU+XP944=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

11.4.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.4.3 - History instance n.2 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Aquitaine RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Aquitaine RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - région Aquitaine*

Subject OU: *0002 781846464*

Subject O: *CROEC d'Aquitaine*

Subject C: *FR*

X509SKI

X509 SK I *LDHdnuKlA6jTamd+qiTqU+XP944=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2012-11-25T23:00:00Z*

11.5 - Service (withdrawn): Ordre des Experts-Comptables - région Auvergne RGS***

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Auvergne RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Auvergne RGS****

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *149188547785859596281544574165761361665813 8*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIFuTCCA6GgAwIBAgISESBB44pZ0gb6GquAiff+ybbaMA0GCSqGSIb3DQEBCwUAMHQxCzAJBgNV
BAYTAkZSMSUwIwYDVQQKExxPcmRyZSBkZXMgRXhwZXJ0cy1Db21wdGFibGVzMRcwFQYDVQQLEw4w
MDAyIDc3NTY3MDAwMzElMCMGA1UEAxMcT3JkcmUgZGVzIEV4cGVydHMtQ29tcHRhYmxlczAeFw0x
MTA1MTAwMDAwMDBaFw0xOTEyMzEwMTAwMDBaMHsxCzAJBgNVBAYTAkZSMRkwFwYDVQQKExBDUk9F
QyBkJ0F1dmVyZ25lMRcwFQYDVQQLEw4wMDAyIDc3OTE4NjMxMTE4MDYGA1UEAwwvT3JkcmUgZGVz
IEV4cGVydHMtQ29tcHRhYmxlcyAtIHLDqWdpb24gQXV2ZXJnbmUwggEiMA0GCSqGSIb3DQEBAQUA
A4IBDwAwggEKAoIBAQC5qyx7PK+jNcIPFhiKL2Y4PUs3as+PknxfrKgMnqGV4PD5FePnoNkzvKGB
yky00dOoG8lpBj+TyPgQFHgQQUimMXWvTL6QzseSpii4R+9IcCLddx43XPE5TlxmQlAKi+V0aP3F
WJed8eic6VqSj5XXjtvxf9JdyrxVataD3bYjpN4+ra58ZeNCwflO3WRcluYIMqbjzIHMa9WwKZxF
w6EA/0lh4E3wB278XX9Lm+Ki5FZCc0dz89H3oAu1e5hJd4t56Xc8h1eJCDv/PP4T7vkYiOIy8FgJ
cpyCRFkLUOJD7G4BpGfGoLBjT8QA+RJ4eHOKCtZIkgS5sg6EDwYmAs5HAgMBAAGjggE8MIIBODAO
BgNVHQ8BAf8EBAMCAQYwbwYDVR0gBGgwZjBkBgRVHSAAMFwwWgYIKwYBBQUHAgEWTmh0dHA6Ly9z
ZWVjLmV4cGVydHMtY29tcHRhYmxlcy5mci9QQy9QQ1JhY2luZV9PcmRyZV9kZXNfRXhwZXJ0cy1D
b21wdGFibGVzLnBkZjASBgNVHRMBAf8ECDAGAQH/AgEAMGEGA1UdHwRaMFgwVqBUoFKGUGh0dHA6
Ly9zZWVjLmV4cGVydHMtY29tcHRhYmxlcy5mci9DUkwvQ1JMUmFjaW5lX09yZHJlX2Rlc19FeHBl
cnRzLUNvbXB0YWJsZXMuY3JsMB0GA1UdDgQWBBQ+cJ/2VuIq7GbsKD62BLDTqmt/pDAfBgNVHSME
GDAWgBSBBznjD3pGD7l96V1idvUklRwVVjANBgkqhkiG9w0BAQsFAAOCAgEAF7oQiDEtpa/gpAwI
cOukLJz8KVqXAWv6pNlUdCsWZ0qsIpfuVUjwe0spXooF4JSirLDBInfCkKJPabuDTrjMGJ9E+tN8
s407oOlTgO+kGD9r066gh2o4MJML5U5uvy8t6KhVwZwgm69bqDlfm3U8B8yJSW0kE4OnrLSkFeni
6b5pzXYbGmDAiCLzRfI9svpd0zqdIYNRW2q8M5d7zWVd4PWydNDFcWp3qaELp2qL/wH68zU9PGMc
BYMcCogVLqlWvgVup+7VVUogExij1hEtkQWttz58PEz1CgID0v9Yqn9JCKjwA9Bdj1KrhXmfc01Y
ta+kLzIJlXKKnXLrnUY2A187HFxzhX5B8j2q4U07ZAMquJzhoWB7mMyXGM4rQQN7TqNw1pIwKVg6
bwAHfQwMS77Fb8xVgiVDHTI4XVI2CltSpt8RGzGhlxVkbOlU26ajIC/XPV4fX4NYCPslIAbNhRta
IUZng3vTRAuD0cVbejiLF+HxooQfW16w7EV5AzcnRIZTM3uP5/RMohpZDLSDpjAb6thhDW6FLJl6
SBVXaPXNewadGwu8wVBuXTWqWXfByu1bF1yop1Y0Yhk2d6P8amPajALGbFfOk1mtAte+N8JpT+x/
IYGcXT/dKpPsJxN4puQDi+6htUi38vMqqQzo6EhdQkyi4H0kW/JOQa5GCj8=

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Ordre des Experts-Comptables*

Issuer OU: *0002 775670003*

Issuer O: *Ordre des Experts-Comptables*

Issuer C: *FR*

Subject CN: *Ordre des Experts-Comptables - région Auvergne*

Subject OU: *0002 779186311*

Subject O: *CROEC d'Auvergne*

Subject C: *FR*

Valid from: *Tue May 10 02:00:00 CEST 2011*

Valid to: *Tue Dec 31 02:00:00 CET 2019*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:B9:AB:2C:7B:3C:AF:A3:35:C2:0F:16:18:8A:2F:66:38:3D:4B:37:6A:CF:8F:92:7C:5F:AC:A8:0C:9E:A1:95:E0:F0:F9:15:E3:E7:A0:D9:33:BC:A1:81:CA:4C:B4:D1:D3:A8:1B:C9:69:06:3F:93:C8:F8:10:14:78:10:41:48:A6:31:75:AF:4C:BE:90:CE:C7:92:A6:28:B8:47:EF:48:70:22:DD:77:1E:37:5C:F1:39:4E:5C:66:42:50:0A:8B:E5:74:68:FD:C5:58:97:9D:F1:E8:9C:E9:5A:92:8F:95:D7:8E:DB:F1:7F:D2:5D:CA:BC:55:6A:D6:83:DD:B6:23:A4:DE:3E:AD:AE:7C:65:E3:42:C1:F9:4E:DD:64:5C:96:E6:08:32:A6:E3:CC:81:CC:6B:D5:B0:29:9C:45:C3:A1:00:FF:49:61:E0:4D:F0:07:6E:FC:5D:7F:4B:9B:E2:A2:E4:56:42:73:47:73:F3:D1:F7:A0:0B:B5:7B:98:49:77:8B:79:E9:77:3C:87:57:89:08:3B:FF:3C:FE:13:EE:F9:18:88:E2:32:F0:58:09:72:9C:82:44:59:0B:50:E2:43:EC:6E:01:A4:67:C6:A0:B0:63:4F:C4:00:F9:12:78:78:73:8A:0A:D6:48:92:04:B9:B2:0E:84:0F:06:26:02:CE:47:02:03:01:00:01

Certificate Policies *Policy OID: 2.5.29.32.0*

CPS pointer: http://seec.experts-comptables.fr/PC/PCRacine_Ordre_des_Experts-Comptables.pdf

Basic Constraints *IsCA: true - Path length: 0*

CRL Distribution Points *http://seec.experts-comptables.fr/CRL/CRLRacine_Ordre_des_Experts-Comptables.crl*

Subject Key Identifier *3E:70:9F:F6:56:E2:2A:EC:66:EC:28:3E:B6:04:B0:D3:AA:6B:7F:A4*

Authority Key Identifier *81:07:39:E3:0F:7A:46:0F:B9:7D:E9:5D:62:76:F5:24:95:1C:15:56*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *5B:A9:EB:05:97:43:01:8D:E8:0E:E4:2A:97:64:9D:43:C6:44:D3:04:5C:F9:A4:29:BA:C9:67:77:C0:F4:ED:89*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2018-01-30T01:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS101456/QCPPublic*

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Signature-3-Stars*

TSP Service Definition URI

URI *[fr]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

URI *[en]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

11.5.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.5.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Auvergne RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Auvergne RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - région Auvergne*

Subject OU: *0002 779186311*

Subject O: *CROEC d'Auvergne*

Subject C: *FR*

X509SKI

X509 SK I *PnCf9lbiKuxm7Cg+tgSw06prf6Q=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

11.5.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.5.3 - History instance n.2 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Auvergne RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Auvergne RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - région Auvergne*

Subject OU: *0002 779186311*

Subject O: *CROEC d'Auvergne*

Subject C: *FR*

X509SKI

X509 SK I *PnCf9lbiKuxm7Cg+tgSw06prf6Q=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2012-11-25T23:00:00Z*

11.6 - Service (withdrawn): Ordre des Experts-Comptables - région Bourgogne RGS***

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Bourgogne RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Bourgogne RGS****

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *149194417648861094601184369756410137734734*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIF2zCCA8OgAwIBAgISESBuDHxAXLBQO7M6oxs/1VCWMA0GCSqGSIb3DQEBCwUAMHQxCzAJBgNV
BAYTAkZSMSUwIwYDVQQKExxPcmRyZSBkZXMgRXhwZXJ0cy1Db21wdGFibGVzMRcwFQYDVQQLEw4w
MDAyIDc3NTY3MDAwMzElMCMGA1UEAxMcT3JkcmUgZGVzIEV4cGVydHMtQ29tcHRhYmxlczAeFw0x
MTA1MTAwMDAwMDBaFw0xOTEyMzEwMTAwMDBaMIGcMQswCQYDVQQGEwJGUjEqMCgGA1UECgwhQ1JP
RUMgZGUgQm91cmdvZ25lIEZyYW5jaGUtQ29tdMOpMRcwFQYDVQQLEw4wMDAyIDc3ODIxMjk1MTFI
MEYGA1UEAww/T3JkcmUgZGVzIEV4cGVydHMtQ29tcHRhYmxlcyAtIHLDqWdpb24gQm91cmdvZ25l
IEZyYW5jaGUtQ29tdMOpMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEArjl2gNSks+gX
Yo99hJVl+NiZ8NiQOlan0GqN48dxJ5XQU7pxw9fJjmJRj2smz0apsbGOIUBYkGhPRiiWxJ3RLnWe
ynqjQDb0nBzGtpGx6+bgSqt+2yH5iUPcFx6u9vY+Jr8XFwqwqYrHVkjDm7ix17thQcAWepJl/uPa
wJLtlykh4lZs0+VaB/j/T6R/ktkB4cwC9dCyxEsl9i4JW9OO+r7lmqRgLljP76r7B5OXzN3r1DgT
PGlsRUOaHmi7WEj+9d5ZCSxNuYUBzLx1mGKlaP0zHGxu9S5UPfjN7607dmoeG6MQQdO29h2vyAXk
grl5G4p+SFT9+HqvIoGKGy52dQIDAQABo4IBPDCCATgwDgYDVR0PAQH/BAQDAgEGMG8GA1UdIARo
MGYwZAYEVR0gADBcMFoGCCsGAQUFBwIBFk5odHRwOi8vc2VlYy5leHBlcnRzLWNvbXB0YWJsZXMu
ZnIvUEMvUENSYWNpbmVfT3JkcmVfZGVzX0V4cGVydHMtQ29tcHRhYmxlcy5wZGYwEgYDVR0TAQH/
BAgwBgEB/wIBADBhBgNVHR8EWjBYMFagVKBShlBodHRwOi8vc2VlYy5leHBlcnRzLWNvbXB0YWJs
ZXMuZnIvQ1JML0NSTFJhY2luZV9PcmRyZV9kZXNfRXhwZXJ0cy1Db21wdGFibGVzLmNybDAdBgNV
HQ4EFgQUP4FakGFRtfdg5wW4mdZ0+W7nh3EwHwYDVR0jBBgwFoAUgQc54w96Rg+5feldYnb1JJUc
FVYwDQYJKoZIhvcNAQELBQADggIBAFO2m+IQ3oKb/h29JFQnbOCzbFTcuYo3eMIYIuzuyrPlZH5U
L40Yd2NhEZtEQuVzAZwSGZ4qTB8q99BLXqOGKjuQ+wdUBcDqExGnMe0625eUE1XcK7qaUd2Qx2i5
bghNaBZ5xffvlbIKVRBIsNVfmRAISIAP8Egxx4+z7dLVvo18K9wSDpiWHPmsD9XKnnZtS6viCraY
vKMM7PZ9Rqmzegg+SvuExBqCsNtAdVKjEuRpDvJPYnr6MHX0crfJZ7BjAH6ffVcrzjEzifSYG/S/
PSJ8anUZ6aSkLvPoJDkTs76sVAv4LArvTWnVeQswa/hS3t1SZMEDTjK+jBfWM08Eg9SGojQeGWM1
QyzSBHz8POavOhxaVBVJ3vWvnBq86GA/EcrlmNfKHq94MuWCReA+5muBfByucj6jixlQbccvbVPH
SbR0t19Ikkohfo8iYHsF+ganbMQdzeeVi/JacMr9YHuhF7V6tChK1sYBcltRX0TuEP2V9JeecAkL
5Ua4xFO8RlzqIomB7+4+Ov/Fg1PcjA7o/lEzw9/COVXbliVv631mrZtxmDoirLmFi9HSX+pNNhCc
0ug4TrdS7ohObi1tpVaMjQxT3NhrBbKtYwDk8KAA4fs5hD0LGbpj1vEjU0JQ8IUYCfozWBtzAA0q
18x32oh1FNZCqSEXov4x9SDA2oQY

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Ordre des Experts-Comptables*

Issuer OU: *0002 775670003*

Issuer O: *Ordre des Experts-Comptables*

Issuer C: *FR*

Subject CN: *Ordre des Experts-Comptables - région Bourgogne Franche-Comté*

Subject OU: *0002 778212951*

Subject O: *CROEC de Bourgogne Franche-Comté*

Subject C: *FR*

Valid from: *Tue May 10 02:00:00 CEST 2011*

Valid to: *Tue Dec 31 02:00:00 CET 2019*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:AE:39:76:80:D4:A4:B3:E8:17:62:8F:7D:84:95:65:F8:D8:99:F0:D8:90:3A:56:A7:D0:6A:8D:E3:C7:71:27:95:D0:53:BA:71:C3:D7:C9:8E:62:51:8F:6B:26:CF:46:A9:B1:B1:8E:21:40:58:90:68:4F:46:28:96:C4:9D:D1:2E:75:9E:CA:7A:A3:40:36:F4:9C:1C:C6:B6:91:B1:EB:E6:E0:4A:AB:7E:DB:21:F9:89:43:DC:17:1E:AE:F6:F6:3E:26:BF:17:17:0A:B0:A9:8A:C7:56:48:C3:9B:B8:B1:D7:BB:61:41:C0:16:7A:92:65:FE:E3:DA:C0:92:ED:97:29:21:E2:56:6C:D3:E5:5A:07:F8:FF:4F:A4:7F:92:D9:01:E1:CC:02:F5:D0:B2:C4:4B:25:F6:2E:09:5B:D3:8E:FA:BE:E5:9A:A4:60:2E:58:CF:EF:AA:FB:07:93:97:CC:DD:EB:D4:38:13:3C:69:6C:45:43:9A:1E:68:BB:58:48:FE:F5:DE:59:09:2C:4D:B9:85:01:CC:BC:75:98:62:A5:68:FD:33:1C:6C:6E:F5:2E:54:3D:F8:CD:EF:AD:3B:76:6A:1E:1B:A3:10:41:D3:B6:F6:1D:AF:C8:05:E4:82:B2:39:1B:8A:7E:48:54:FD:F8:7A:AF:22:81:8A:1B:2E:76:75:02:03:01:00:01

Certificate Policies *Policy OID: 2.5.29.32.0*

CPS pointer: http://seec.experts-comptables.fr/PC/PCRacine_Ordre_des_Experts-Comptables.pdf

Basic Constraints *IsCA: true - Path length: 0*

CRL Distribution Points *http://seec.experts-comptables.fr/CRL/CRLRacine_Ordre_des_Experts-Comptables.crl*

Subject Key Identifier *3F:81:5A:90:61:51:B5:F7:60:E7:05:B8:99:D6:74:F9:6E:E7:87:71*

Authority Key Identifier *81:07:39:E3:0F:7A:46:0F:B9:7D:E9:5D:62:76:F5:24:95:1C:15:56*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *0A:C0:38:91:43:39:41:56:6E:6A:F1:E2:8E:3A:DE:4C:FB:D8:27:05:38:29:F7:BE:2E:1C:2C:E0:28:12:27:96*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2018-01-30T01:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS101456/QCPPublic*

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Signature-3-Stars*

TSP Service Definition URI

URI *[fr]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

URI *[en]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

11.6.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.6.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Bourgogne RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Bourgogne RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - région Bourgogne Franche-Comté*

Subject OU: *0002 778212951*

Subject O: *CROEC de Bourgogne Franche-Comté*

Subject C: *FR*

X509SKI

X509 SK I *P4FakGFRtfdg5wW4mdZ0+W7nh3E=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

11.6.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.6.3 - History instance n.2 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Bourgogne RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Bourgogne RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - région Bourgogne Franche-Comté*

Subject OU: *0002 778212951*

Subject O: *CROEC de Bourgogne Franche-Comté*

Subject C: *FR*

X509SKI

X509 SK I *P4FakGFRtfdg5wW4mdZ0+W7nh3E=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2012-11-25T23:00:00Z*

11.7 - Service (withdrawn): Ordre des Experts-Comptables - région Bretagne RGS***

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Bretagne RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Bretagne RGS****

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *149185594510914443530801825161179061241931 5*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIFujCCA6KgAwIBAgISESArq71iXU1cfMfvkusZSNLzMA0GCSqGSIb3DQEBCwUAMHQxCzAJBgNV
BAYTAkZSMSUwIwYDVQQKExxPcmRyZSBkZXMgRXhwZXJ0cy1Db21wdGFibGVzMRcwFQYDVQQLEw4w
MDAyIDc3NTY3MDAwMzElMCMGA1UEAxMcT3JkcmUgZGVzIEV4cGVydHMtQ29tcHRhYmxlczAeFw0x
MTA1MTAwMDAwMDBaFw0xOTEyMzEwMTAwMDBaMHwxCzAJBgNVBAYTAkZSMRowGAYDVQQKExFDUk9F
QyBkZSBCcmV0YWduZTEXMBUGA1UECxMOMDAwMiA3Nzc3MzM3MDAxODA2BgNVBAMML09yZHJlIGRl
cyBFeHBlcnRzLUNvbXB0YWJsZXMgLSByw6lnaW9uIEJyZXRhZ25lMIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEAnPz3CilwnOpR1GbhhapxIuH8Vh46/3BbNCPN+jAYDRO5X4XibSl21qZf
oSduoDPUZ8GpzVFRt25N/B4SjHQ69uYoGCChCwpyaOGBlkqRf/5Mf1AGcx5Koy3cMCsa1LQ8cVL8
KbPluSoVQ7I9Ma7WjDDNaHzZ1yikLNkBOp52kXb5mKd9TosvZxLaD/DQ7pOtP0gK/kAi3AfYCeb+
KV6XJaQwfdLbj5kfrkIWaxYsnPoN0F55hJxuk0Si6Zj7/sIOWerrzkXKdHrVPUB1TDvJ+yfgrmSD
eLQPjsMw/dJ3bM4POk+Tl8T2eUWgxapAkXpweZxN36hmaQ3uIB5wsSYa+QIDAQABo4IBPDCCATgw
DgYDVR0PAQH/BAQDAgEGMG8GA1UdIARoMGYwZAYEVR0gADBcMFoGCCsGAQUFBwIBFk5odHRwOi8v
c2VlYy5leHBlcnRzLWNvbXB0YWJsZXMuZnIvUEMvUENSYWNpbmVfT3JkcmVfZGVzX0V4cGVydHMt
Q29tcHRhYmxlcy5wZGYwEgYDVR0TAQH/BAgwBgEB/wIBADBhBgNVHR8EWjBYMFagVKBShlBodHRw
Oi8vc2VlYy5leHBlcnRzLWNvbXB0YWJsZXMuZnIvQ1JML0NSTFJhY2luZV9PcmRyZV9kZXNfRXhw
ZXJ0cy1Db21wdGFibGVzLmNybDAdBgNVHQ4EFgQUS3msQ9Y0ie243CTonTYB7CyIpT4wHwYDVR0j
BBgwFoAUgQc54w96Rg+5feldYnb1JJUcFVYwDQYJKoZIhvcNAQELBQADggIBAGGHdjSSn3ewvOSt
36EcDWieBqrZ5uum/hkzSTodEsnIQoeYnwb4TitvFDNQkH4WybW64Nuce34d5welm1vFcr9BxLrJ
m+X4ikROx7NeUfN1kXO5f4stpGfDcJ/V+liLVUrbzeP54jaFhr9wpglBJtvLdZH6Qdvf1sJ+E4BM
jcGKsI4PVZBx5DiHv9iIrYb8AwIv5sYaarflJOhdh40Zz1p4ioNxOVRuFiX+W3VEB2Zp7enRICuQ
kS0ERZ5BAirXt6OubcuNEv2Dh+OGY6WrGTI4eNWft49cPhdD6MqnUe9qvYfbQRV/CjxLo0LmJOPy
38h5VVnyZfsMYszoigAup5oS6NKkGOdBh7LzONjXoE2qXXrIOH4HiJ1ZL7ZNNSqTpGNgXJOctDDA
3qDZFfbFkMLwjj8TFGjo8A2BesVffZKGkb24VZpRIoiaLKZZVkfo9rHny3YYV1SA9BRQj5Czob3H
E9eU9il2t5QfwMBNRp5K6K4BPMTGDgXn1GOKs9y54Pw3ufLRHBWuRN8l6385D90DNjWJ37XOMKA4
R92ggqBcBiUfGKxfna8IOWhqLg+IyWGL/xZuKdanQp/p0sSfZM+Spy6WD946z7YufNer8KCZrN2k
GNEWj5rgnuFmv6V3mCSkJCy42EQBGxM4ZMDG66XN4zg+gim6BFW+YUc0Iw3d

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Ordre des Experts-Comptables*

Issuer OU: *0002 775670003*

Issuer O: *Ordre des Experts-Comptables*

Issuer C: *FR*

Subject CN: *Ordre des Experts-Comptables - région Bretagne*

Subject OU: *0002 777733700*

Subject O: *CROEC de Bretagne*

Subject C: *FR*

Valid from: *Tue May 10 02:00:00 CEST 2011*

Valid to: *Tue Dec 31 02:00:00 CET 2019*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:9C:FC:F7:0A:29:70:9C:EA:51:D4:66:E1:85:AA:71:22:E1:FC:56:1E:3A:FF:70:5B:34:23:CD:FA:30:18:0D:13:B9:5F:85:E2:6D:29:76:D6:A6:5F:A1:27:6E:A0:33:D4:67:C1:A9:CD:51:51:B7:6E:4D:FC:1E:12:8C:74:3A:F6:E6:28:18:20:A1:0B:0A:72:68:E1:81:96:4A:91:7F:FE:4C:7F:50:06:73:1E:4A:A3:2D:DC:30:2B:1A:D4:B4:3C:71:52:FC:29:B3:E5:B9:2A:15:43:B2:3D:31:AE:D6:8C:30:CD:68:7C:D9:D7:28:A4:2C:D9:01:3A:9E:76:91:76:F9:98:A7:7D:4E:8B:2F:67:12:DA:0F:F0:D0:EE:93:AD:3F:48:0A:FE:40:22:DC:07:D8:09:E6:FE:29:5E:97:25:A4:30:7D:D2:DB:8F:99:1F:AE:42:16:6B:16:2C:9C:FA:0D:D0:5E:79:84:9C:6E:93:44:A2:E9:98:FB:FE:C2:0E:59:EA:EB:CE:45:CA:74:7A:D5:3D:40:75:4C:3B:C9:FB:27:E0:AE:64:83:78:B4:0F:8E:C3:30:FD:D2:77:6C:CE:0F:3A:4F:93:97:C4:F6:79:45:A0:C5:AA:40:91:7A:70:79:9C:4D:DF:A8:66:69:0D:EE:20:1E:70:B1:26:1A:F9:02:03:01:00:01

Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: http://seec.experts-comptables.fr/PC/PCRacine_Ordre_des_Experts-Comptables.pdf*
Basic Constraints	*IsCA: true - Path length: 0*
CRL Distribution Points	*http://seec.experts-comptables.fr/CRL/CRLRacine_Ordre_des_Experts-Comptables.crl*
Subject Key Identifier	*4B:79:AC:43:D6:34:89:ED:B8:DC:24:E8:9D:36:01:EC:2C:88:A5:3E*
Authority Key Identifier	*81:07:39:E3:0F:7A:46:0F:B9:7D:E9:5D:62:76:F5:24:95:1C:15:56*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*F4:9E:99:23:64:AA:8A:43:D2:04:55:A3:37:8A:A6:90:36:4F:10:1C:68:8F:A8:36:6F:89:F6:12:FE:37:82:FA*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description	*[en]*	*undefined.*
	[fr]	*undefined.*

Status Starting Time *2018-01-30T01:00:00Z*

Scheme Service Definition URI

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS101456/QCPPublic*
URI	*[fr]*	*http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Signature-3-Stars*

TSP Service Definition URI

URI	*[fr]*	*https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*
URI	*[en]*	*https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

11.7.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.7.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Bretagne RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Bretagne RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - région Bretagne*

Subject OU: *0002 777733700*

Subject O: *CROEC de Bretagne*

Subject C: *FR*

X509SKI

X509 SK I *S3msQ9Y0ie243CTonTYB7CyIpT4=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

11.7.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.7.3 - History instance n.2 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Bretagne RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Bretagne RGS****

Service digital identities

X509SubjectName

Subject CN:	*Ordre des Experts-Comptables - région Bretagne*
Subject OU:	*0002 777733700*
Subject O:	*CROEC de Bretagne*
Subject C:	*FR*
X509 SK I	*S3msQ9Y0ie243CTonTYB7CyIpT4=*
Service Status	*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*
Status Starting Time	*2012-11-25T23:00:00Z*

11.8 - Service (withdrawn): Ordre des Experts-Comptables - région Champagne RGS***

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[fr]	*Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name	*[en]*	*Ordre des Experts-Comptables - région Champagne RGS****
Name	*[fr]*	*Ordre des Experts-Comptables - région Champagne RGS****

Service digital identities

Certificate fields details

Version:	*3*
Serial Number:	*149180293127106512436240446046984908829738 8*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIFvDCCA6SgAwIBAgISESADyaVdnuXovVNk1rz0v4msMA0GCSqGSIb3DQEBCwUAMHQxCzAJBgNV
BAYTAkZSMSUwIwYDVQQKExxPcmRyZSBkZXMgRXhwZXJ0cy1Db21wdGFibGVzMRcwFQYDVQQLEw4w
MDAyIDc3NTY3MDAwMzElMCMGA1UEAxMcT3JkcmUgZGVzIEV4cGVydHMtQ29tcHRhYmxlczAeFw0x
MTA1MTAwMDAwMDBaFw0xOTEyMzEwMTAwMDBaMH4xCzAJBgNVBAYTAkZSMRswGQYDVQQKExJDUk9F
QyBkZSBDaGFtcGFnbmUxFzAVBgNVBAsTDjAwMDIgNzc1NjExNzE4MTkwNwYDVQQDDDBPcmRyZSBk
ZXMgRXhwZXJ0cy1Db21wdGFibGVzIC0gcsOpZ2lvbiBDaGFtcGFnbmUwggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQDcaDnfH0NOZpWt4b0GHP0haClAyfGrLGt9oqXRS1nOppDwwXyBp/v1
cXj/3PbXR2m44s0gqKo71ZKKCG7OMUQ3E3mAqFq9H80c/mGSXY+/PTC1ZegRsBrWjZCEIDvgfx5N
ndXg+FUkTJ1QXQDLbNg6wudPpIyW6XG+E9DBr4AC/CT03HyhWlNgFOssAhbca3rUZXCkZCcDj0YT

8pkMgiKfIK1Fln+S1JzHASWgz9Ca0OQA1cIlkhiaHk1smlfNcZ4Q6inoOP4DodIQWSwUD+fXLz2R
G4lcv/BUij8NhG7MGAQfmrv6mVkhXq6ILE17C5HTPbaqVaR70qorigBZSoLnAgMBAAGjggE8MIIB
ODAOBgNVHQ8BAf8EBAMCAQYwbwYDVR0gBGgwZjBkBgRVHSAAMFwwWgYIKwYBBQUHAgEWTmh0dHA6
Ly9zZWVjLmV4cGVydHMtY29tcHRhYmxlcy5mci9QQy9QQ1JhY2luZV9PcmRyZV9kZXNfRXhwZXJ0
cy1Db21wdGFibGVzLnBkZjASBgNVHRMBAf8ECDAGAQH/AgEAMGEGA1UdHwRaMFgwVqBUoFKGUGh0
dHA6Ly9zZWVjLmV4cGVydHMtY29tcHRhYmxlcy5mci9DUkwvQ1JMUmFjaW5lX09yZHJlX2Rlc19F
eHBlcnRzLUNvbXB0YWJsZXMuY3JsMB0GA1UdDgQWBBRL4vDVLv4R3PVv8oRHKWB0SSyfaTAfBgNV
HSMEGDAWgBSBBznjD3pGD7l96V1idvUklRwVVjANBgkqhkiG9w0BAQsFAAOCAgEAZ20vsduoUtuc
MGKbrvlmFuRBO1Z1QP/+ikf8SGEvjsIlf8SPjy++vI5mJHhjCeLxyjnbZpCLudV0SduztYO5/Uk3
ZO92bBbCC9VNgWyZ86IldmLDMFTtIS3knquLEli/51J2KC72OOE9ahbJnLHjoC+P0NxCDWzR3gik
X4cBIXrYLnccy1LwuYnl8WNxT0QF12EBRqRXJOfercfSXMTfnkcvML+IpCZHcTbzU6og//Xqo8XC
QvPQxfJNC8lj7XQcbKa0GwQ6DRHH6uhv8PG7TLuZFrz0u1433pJ1Qmh+F6pVY1+4ZLbAPHrtAh/H
xSIxmyUJicf1qwAVZDjr4uxlFmq4IZDDQED+YzqbDLg32Y6i2iF86YPTOHssmVjRJDupuhJvZciU
bsV/n3jv6C7YT1MGzj+LfiGuCVT29fH1XbKs8ABYi3ZcGESI3dsC4FiOJw4AyXSDYMs99vp+jo+L
CC3IYNG4UKOho92J35gV61jWovPB6aTqB/Y+1l8AoRriv/cQZ/dcKJrm/V5zC8IBxaCN7pP3q3Mm
kk6ZX5pIcsbl+FufwQiX3WFH5OSJL50u/5Pl/KrzdYwacAD7P0NEhwi/41G0WuCE3QvLx2UAzQ1Q
i9SZKqqT61fOgtApe0JsWgpMLFzHut7B4utFCNN2xu8RONJ9hNDS6NlvAT5AOTs=

-----END CERTIFICATE-----

Signature algorithm:	*SHA256withRSA*
Issuer CN:	*Ordre des Experts-Comptables*
Issuer OU:	*0002 775670003*
Issuer O:	*Ordre des Experts-Comptables*
Issuer C:	*FR*
Subject CN:	*Ordre des Experts-Comptables - région Champagne*
Subject OU:	*0002 775611718*
Subject O:	*CROEC de Champagne*
Subject C:	*FR*
Valid from:	*Tue May 10 02:00:00 CEST 2011*
Valid to:	*Tue Dec 31 02:00:00 CET 2019*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:DC:68:39:DF:1F:43:4E:66:95:AD:E1:BD:06:1C:FD:21:
68:29:40:C9:F1:AB:2C:6B:7D:A2:A5:D1:4B:59:CE:A6:90:F0:C1:7C:81:A7:FB:F5:71:78:FF:DC:F6:D7:47:69:B8:E2:CD:20:A8:AA:3B:D5:92:8A:08:6E:CE:31:44:37:1
3:79:80:A8:5A:BD:1F:CD:1C:FE:61:92:5D:8F:BF:3D:30:B5:65:E8:11:B0:1A:D6:8D:90:84:20:3B:E0:7F:1E:4D:9D:D5:E0:F8:55:24:4C:9D:50:5D:00:CB:6C:D8:3A:C2
:E7:4F:A4:8C:96:E9:71:BE:13:D0:C1:AF:80:02:FC:24:F4:DC:7C:A1:5A:53:60:14:EB:2C:02:16:DC:6B:7A:D4:65:70:A4:64:27:03:8F:46:13:F2:99:0C:82:22:9F:20:A
D:45:96:7F:92:D4:9C:C7:01:25:A0:CF:D0:9A:D0:E4:00:D5:C9:48:92:18:9A:1E:4D:6C:9A:57:CD:71:9E:10:EA:29:E8:38:FE:03:A1:D2:10:59:2C:14:0F:E7:D7:2F:3D:
91:1B:89:5C:BF:F0:54:8A:3F:0D:84:6E:CC:18:04:1F:9A:BB:FA:99:59:21:5E:AE:88:2C:4D:7B:0B:91:D3:3D:B6:AA:55:A4:7B:D2:AA:2B:8A:00:59:4A:82:E7:02:
03:01:00:01

Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: http://seec.experts-comptables.fr/PC/PCRacine_Ordre_des_Experts-Comptables.pdf*
Basic Constraints	*IsCA: true - Path length: 0*

CRL Distribution Points *http://seec.experts-comptables.fr/CRL/CRLRacine_Ordre_des_Experts-Comptables.crl*

Subject Key Identifier *4B:E2:F0:D5:2E:FE:11:DC:F5:6F:F2:84:47:29:60:74:49:2C:9F:69*

Authority Key Identifier *81:07:39:E3:0F:7A:46:0F:B9:7D:E9:5D:62:76:F5:24:95:1C:15:56*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *50:9B:84:92:DB:27:97:69:37:76:80:AD:7C:78:6F:3D:20:82:D7:B7:6B:32:09:F3:FE:87:2A:18:F4:73:36:77*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2018-01-30T01:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS101456/QCPPublic*

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Signature-3-Stars*

TSP Service Definition URI

URI *[fr]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

URI *[en]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

11.8.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.8.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Champagne RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Champagne RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - région Champagne*

Subject OU: *0002 775611718*

Subject O: *CROEC de Champagne*

Subject C: *FR*

X509SKI

X509 SK I *S+Lw1S7+Edz1b/KERylgdEksn2k=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

11.8.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.8.3 - History instance n.2 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Champagne RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Champagne RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - région Champagne*

Subject OU: *0002 775611718*

Subject O: *CROEC de Champagne*

Subject C: *FR*

X509 SK I *S+Lw1S7+Edz1b/KERylgdEksn2k=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2012-11-25T23:00:00Z*

11.9 - Service (withdrawn): Ordre des Experts-Comptables - région Guadeloupe RGS***

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Guadeloupe RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Guadeloupe RGS****

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *149203479240414948499614636955965481401059 3*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIFvzCCA6egAwIBAgISESCyOHnS6J5ou1ynrExWCUzhMA0GCSqGSIb3DQEBCwUAMHQxCzAJBgNV
BAYTAkZSMSUwIwYDVQQKExxPcmRyZSBkZXMgRXhwZXJ0cy1Db21wdGFibGVzMRcwFQYDVQQLEw4w
MDAyIDc3NTY3MDAwMzElMCMGA1UEAxMcT3JkcmUgZGVzIEV4cGVydHMtQ29tcHRhYmxlczAeFw0x
MTA1MTAwMDAwMDBaFw0xOTEyMzEwMTAwMDBaMIGAMQswCQYDVQQGEwJGUjEcMBoGA1UEChMTQ1JP
RUMgZGUgR3VhZGVsb3VwZTEXMBUGA1UECxMOMDAwMiAzNDgzNjc5ODgxOjA4BgNVBAMMMU9yZHJl
IGRlcyBFeHBlcnRzLUNvbXB0YWJsZXMgLSByw6lnaW9uIEd1YWRlbG91cGUwggEiMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQDABav2/fsNhlOm3/UcEFqaPvlL7vqLfcqyQSQQooOfzmWhe/A3
CexktEvxgolcdOBtgGPmKRrvlG4wJNFBoOJ4EH6WPpkbZHYX2QDlJTxHle3z7SIWVPhq18Xfpe6T
exdpN0b7P0Qmhg6LK3c5erAbNdzwJVlQlBm3M4I2KNs1HD+dDMXNLH42oXaoLztQ0s7QmDINhOgV
4uQ2dz+NEA9gzi9pSw4FbQ7MReuOFRNF/rfNhqJzF2uQ0wYmii8sXyjdAP75wizuUlrIMRGZmsjQ
gsjmbSMhE/8UgSxJqIVDMyiBIVr353Hfv/J+UeOH77yoz2P0fVrVt8++m0tVtjdJAgMBAAGjggE8
MIIBODAOBgNVHQ8BAf8EBAMCAQYwbwYDVR0gBGgwZjBkBgRVHSAAMFwwWgYIKwYBBQUHAgEWTmh0
dHA6Ly9zZWVjLmV4cGVydHMtY29tcHRhYmxlcy5mci9QQy9QQ1JhY2luZV9PcmRyZV9kZXNfRXhw
ZXJ0cy1Db21wdGFibGVzLnBkZjASBgNVHRMBAf8ECDAGAQH/AgEAMGEGA1UdHwRaMFgwVqBUoFKG
UGh0dHA6Ly9zZWVjLmV4cGVydHMtY29tcHRhYmxlcy5mci9DUkwvQ1JMUmFjaW5lX09yZHJlX2Rl
c19FeHBlcnRzLUNvbXB0YWJsZXMuY3JsMB0GA1UdDgQWBBRvYaY6RShdqg7sEXJSQjvueUkd6TAf
BgNVHSMEGDAWgBSBBznjD3pGD7l96V1idvUklRwVVjANBgkqhkiG9w0BAQsFAAOCAgEAamm4xT7p
hvtejgcQR4X6l1Y83o4Yy4cRQj5xI/kkXfiMS41J6MkoAMjqSGcd2yW31aLcdGTcbI55AC6XmW31
B0owNR4k4DD3KdMdnZlH5RuidCh3nomQnkvgI9pLmdq6EWOC6p26TkLnI341kM+5ND3Lr7Rwtliz
34XAFWTMrw98LVO6tqe2f3yRu9wXFhdjuUK5b9lmoa+nuAmQ8A1I84+ECzunzaJW3qZo6hhR5pAu
uZkL/iN7cdyd/Du3FbqmhE30u+oTTfM8yyZAjQXef/wjlar5mUsBiczv/tgmefiXhpXeoIKgfBNf
2FLTQ5i5X2aSTGkQ9t6oNcahBAgN23jCmgRTEsS6vf54kLpoE/8vveGtTRs6lBjnj0CN01p+LaL3
bxdZ/JsYqjyHBAiDIJk5W1C9qlUSiC3FNGx9k60bVXw6wfUi8sLXjppTkwfz+Z7kQJLSSc/6432f
AEm72fUTtj4YLHm8+mxII3JKFgBHInxLabvDyjydp3lp/0T/rxRVRDjvahI+H6FEJmEipHoyNHQL
5CxGtH6FxOGKBXfJQt/2/Xs1qo2RvxM+eQlsrKGD/Vpqmhaw5VIlBmInUPft/nlYGGvSfgqbu4Vu
pe5O5qt3Mg2WWWuMyTiTil5s6v64ypO0mIVRwYsTT01XjD18i+CdqHEyiDdi+Cw5TRA=

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Ordre des Experts-Comptables*

Issuer OU: *0002 775670003*

Issuer O: *Ordre des Experts-Comptables*

Issuer C: *FR*

Subject CN: *Ordre des Experts-Comptables - région Guadeloupe*

Subject OU: *0002 348367988*

Subject O: *CROEC de Guadeloupe*

Subject C: *FR*

Valid from: *Tue May 10 02:00:00 CEST 2011*

Valid to: *Tue Dec 31 02:00:00 CET 2019*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C0:05:AB:F6:FD:FB:0D:86:53:A6:DF:F5:1C:10:5A:9A:
3E:F9:4B:EE:FA:8B:7D:CA:B2:41:24:10:A2:83:9F:CE:65:A1:7B:F0:37:09:EC:64:B4:4B:F1:82:89:5C:74:E0:6D:80:63:E6:29:1A:EF:94:6E:30:24:D1:41:A0:E2:78:10:
7E:96:3E:99:1B:64:76:17:D9:00:E5:25:3C:47:95:ED:F3:ED:22:16:54:F8:6A:D7:C5:DF:A5:EE:93:7B:17:69:37:46:FB:3F:44:26:86:0E:8B:2B:77:39:7A:B0:1B:35:DC:
F0:25:59:50:94:19:B7:33:82:36:28:DB:35:1C:3F:9D:0C:C5:CD:2C:7E:36:A1:76:A8:2F:3B:50:D2:CE:D0:98:32:0D:84:E8:15:E2:E4:36:77:3F:8D:10:0F:60:CE:2F:69:
4B:0E:05:6D:0E:CC:45:EB:8E:15:13:45:FE:B7:CD:86:A2:73:17:6B:90:D3:06:26:8A:2F:2C:5F:28:DD:00:FE:F9:C2:2C:EE:52:5A:C8:31:11:99:9A:C8:D0:82:C8:E6:6D
:23:21:13:FF:14:81:2C:49:A8:85:43:33:28:81:21:5A:F7:E7:71:DF:BF:F2:7E:51:E3:87:EF:BC:A8:CF:63:F4:7D:5A:D5:B7:CF:BE:9B:4B:55:B6:37:49:02:03:01:00:01

Certificate Policies *Policy OID: 2.5.29.32.0*

CPS pointer: http://seec.experts-comptables.fr/PC/PCRacine_Ordre_des_Experts-Comptables.pdf

Basic Constraints *IsCA: true - Path length: 0*

CRL Distribution Points *http://seec.experts-comptables.fr/CRL/CRLRacine_Ordre_des_Experts-Comptables.crl*

Subject Key Identifier *6F:61:A6:3A:45:28:5D:AA:0E:EC:11:72:52:42:3B:EE:79:49:1D:E9*

Authority Key Identifier *81:07:39:E3:0F:7A:46:0F:B9:7D:E9:5D:62:76:F5:24:95:1C:15:56*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *F5:03:2D:F8:B4:53:3E:CE:40:6F:11:33:42:6B:B8:53:DB:09:F2:72:01:60:5E:1F:1F:5B:6C:50:1A:0
1:5C:8D*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2018-01-30T01:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS101456/QCPPublic*

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Signature-3-Stars*

TSP Service Definition URI

URI *[fr]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

URI *[en]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

11.9.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.9.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Guadeloupe RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Guadeloupe RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - région Guadeloupe*

Subject OU: *0002 348367988*

Subject O: *CROEC de Guadeloupe*

Subject C: *FR*

X509SKI

X509 SK I *b2GmOkUoXaoO7BFyUkI77nlJHek=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

11.9.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.9.3 - History instance n.2 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Guadeloupe RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Guadeloupe RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - région Guadeloupe*

Subject OU: *0002 348367988*

Subject O: *CROEC de Guadeloupe*

Subject C: *FR*

X509SKI

X509 SK I *b2GmOkUoXaoO7BFyUkI77nlJHek=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2012-11-25T23:00:00Z*

11.10 - Service (withdrawn): Ordre des Experts-Comptables - région Guyane RGS***

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Guyane RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Guyane RGS****

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1491937259426662061640151222735084665801378*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIFtjCCA56gAwIBAgISESBo2E7EWsbmQRV69SE5gYqiMA0GCSqGSIb3DQEBCwUAMHQxCzAJBgNV
BAYTAkZSMSUwIwYDVQQKExxPcmRyZSBkZXMgRXhwZXJ0cy1Db21wdGFibGVzMRcwFQYDVQQLEw4w
MDAyIDc3NTY3MDAwMzElMCMGA1UEAxMcT3JkcmUgZGVzIEV4cGVydHMtQ29tcHRhYmxlczAeFw0x
MTA1MTAwMDAwMDBaFw0xOTEyMzEwMTAwMDBaMHgxCzAJBgNVBAYTAkZSMRgwFgYDVQQKEw9DRE9F
QyBkZSBHdXlhbmUxFzAVBgNVBAsTDjAwMDIgNTA4NzE0NTY1MTYwNAYDVQQDDC1PcmRyZSBkZXMg
RXhwZXJ0cy1Db21wdGFibGVzIC0gY29taXTDqSBHdXlhbmUwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQC4Frt0GcgOejRXlTFsS+bc8wz4nLr82jqt5eCyKcB0Y7uOXQoDtEiUqUdOO6BL
V/DqjslNbomrFqtN/SCExDFp4B0tB7SrGkPdFPKIj73XNiGu06gPBn52UkKpUZrvYTWE+fG97cyx
zhi6GGcNH5mNMaRahC3iSefigCsYUIgcohJNBQ3QenxcqTpalxd+PrY3h2iK10/A6B0KCliSn50r
wzjkfXvxmckCtxko3dhJkS8wZQ2G4D1Gr26U83yKcJSJlCJJB20UXrycrVK97y+KhyjAmwu0lMFa
mxOwTWSaf6POU/5KxAyMHwf6a6SJkjQ3SwJ7BjNp7uzICfN3j40TAgMBAAGjggE8MIIBODAOBgNV
HQ8BAf8EBAMCAQYwbwYDVR0gBGgwZjBkBgRVHSAAMFwwWgYIKwYBBQUHAgEWTmh0dHA6Ly9zZWVj
LmV4cGVydHMtY29tcHRhYmxlcy5mci9QQy9QQ1JhY2luZV9PcmRyZV9kZXNfRXhwZXJ0cy1Db21w
dGFibGVzLnBkZjASBgNVHRMBAf8ECDAGAQH/AgEAMGEGA1UdHwRaMFgwVqBUoFKGUGh0dHA6Ly9z
ZWVjLmV4cGVydHMtY29tcHRhYmxlcy5mci9DUkwvQ1JMUmFjaW5lX09yZHJlX2Rlc19FeHBlcnRz
LUNvbXB0YWJsZXMuY3JsMB0GA1UdDgQWBBR8ArRCj9pQoQW7loWN/5QeFLgqcjAfBgNVHSMEGDAW
gBSBBznjD3pGD7l96V1idvUklRwVVjANBgkqhkiG9w0BAQsFAAOCAgEAXfVCwB/a7kpyFI1jm/9H
6LLs0KcRoaxt1M2FN3pcPMrX+GeS/IZrDs3QenwO9t+6r/dyU8fnEfwpGk9iIqE29GuZpSghmCMj
/IPTgWpRJoDGXt1TTccN1o7FtMnYFobB4uAQBdJ8S8knH72fqB6kVn0teJhCYS5PvcnLaKuib9oS
K4DYvKyKQNLhN8XqEr6SeNxXHzK+EmH7JcnVwqNc4v1o5YWhoTTMpTv61bZAvz9oIEJ/mykVCFOq
4XcDbYSeBoraAfbHckOrtCA2eHgshoeG9u1twYExb6zZzsGif3trwDTdwUJWGV8kqgB/2g3ZGfHl
NOjQBzdoR79JOsXB8JjbeGkbCc64dovAWwNtLvv6zvzUGocLBqRs6ff9Y9LEddwItpqPXrZbROmd
eyGbNtZ2hB5vipXWfttgs2GbNJFB98+V4Ja+lMqXhcme5rrNAPH9QFOEGrQzkFXmHG7NN4lRDwjw
KZ4TpaPGhzQh93XL0nFgycbNsgXAF2g2JDIvu0FEkb9k2QOi+H3vczeuik7BIxPnYy+h8RTS5bzT
5kQopTqOE88EmFYaq29uWL/JKKsq5fvB/6q1EEF/udoJa2eg+ENX08sFBxkydFv9evY6kCS0lwK5
9N4MAl9iP/839LcHyVzkcSGmwzdA46jbqUxAtRT9uP7yGBmqqnfKrbY=

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Ordre des Experts-Comptables*

Issuer OU: *0002 775670003*

Issuer O: *Ordre des Experts-Comptables*

Issuer C: *FR*

Subject CN: *Ordre des Experts-Comptables - comité Guyane*

Subject OU: *0002 508714565*

Subject O: *CDOEC de Guyane*

Subject C: *FR*

Valid from: *Tue May 10 02:00:00 CEST 2011*

Valid to: *Tue Dec 31 02:00:00 CET 2019*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:B8:16:BB:74:19:C8:0E:7A:34:57:95:31:6C:4B:E6:DC:F3:0C:F8:9C:BA:FC:DA:3A:AD:E5:E0:B2:29:C0:74:63:BB:8E:5D:0A:03:B4:48:94:A9:47:4E:3B:A0:4B:57:F0:EA:8E:C9:4D:6E:89:AB:16:AB:4D:FD:20:84:C4:31:69:E0:1D:2D:07:B4:AB:1A:43:DD:14:F2:88:8F:BD:D7:36:21:AE:D3:A8:0F:06:7E:76:52:42:A9:51:9A:EF:61:35:84:F9:F1:BD:ED:CC:B1:CE:18:BA:18:67:0D:1F:99:8D:31:A4:5A:84:2D:E2:49:E7:E2:80:2B:18:50:88:1C:A2:12:4D:05:0D:D0:7A:7C:5C:A9:3A:5A:97:17:7E:3E:B6:37:87:68:8A:D7:4F:C0:E8:1D:0A:0A:58:92:9F:9D:2B:C3:38:E4:7D:7B:F1:99:C9:02:B7:19:28:DD:D8:49:91:2F:30:65:0D:86:E0:3D:46:AF:6E:94:F3:7C:8A:70:94:89:94:22:49:07:6D:14:5E:BC:9C:AD:52:BD:EF:2F:8A:87:28:C0:9B:0B:B4:94:C1:5A:9B:13:B0:4D:64:9A:7F:A3:CE:53:FE:4A:C4:0C:8C:1F:07:FA:6B:A4:89:92:34:37:4B:02:7B:06:33:69:EE:EC:C8:09:F3:77:8F:8D:13:02:03:01:00:01

Certificate Policies *Policy OID: 2.5.29.32.0*

CPS pointer: http://seec.experts-comptables.fr/PC/PCRacine_Ordre_des_Experts-Comptables.pdf

Basic Constraints *IsCA: true - Path length: 0*

CRL Distribution Points *http://seec.experts-comptables.fr/CRL/CRLRacine_Ordre_des_Experts-Comptables.crl*

Subject Key Identifier *7C:02:B4:42:8F:DA:50:A1:05:BB:96:85:8D:FF:94:1E:14:B8:2A:72*

Authority Key Identifier *81:07:39:E3:0F:7A:46:0F:B9:7D:E9:5D:62:76:F5:24:95:1C:15:56*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *E4:A9:E7:E2:3B:A0:B0:BF:B6:CE:20:AD:CB:E7:2A:0D:12:7E:E4:D5:94:7A:1B:C4:BD:C4:4E:D7:D3:86:4B:25*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2018-01-30T01:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS101456/QCPPublic*

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Signature-3-Stars*

TSP Service Definition URI

URI *[fr]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

URI *[en]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

11.10.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.10.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Guyane RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Guyane RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - comité Guyane*

Subject OU: *0002 508714565*

Subject O: *CDOEC de Guyane*

Subject C: *FR*

X509SKI

X509 SK I *fAK0Qo/aUKEFu5aFjf+UHhS4KnI=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

11.10.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.10.3 - History instance n.2 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Guyane RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Guyane RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - comité Guyane*

Subject OU: *0002 508714565*

Subject O: *CDOEC de Guyane*

Subject C: *FR*

X509SKI

X509 SK I *fAK0Qo/aUKEFu5aFjf+UHhS4KnI=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2012-11-25T23:00:00Z*

11.11 - Service (withdrawn): Ordre des Experts-Comptables - région La Réunion RGS***

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région La Réunion RGS****

Name *[fr]* *Ordre des Experts-Comptables - région La Réunion RGS****

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *149193592864489503926696443436142078804005 7*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIFwTCCA6mgAwIBAgISESBn2AIpASLupZGwhyB0BIF5MA0GCSqGSIb3DQEBCwUAMHQxCzAJBgNV
BAYTAkZSMSUwIwYDVQQKExxPcmRyZSBkZXMgRXhwZXJ0cy1Db21wdGFibGVzMRcwFQYDVQQLEw4w
MDAyIDc3NTY3MDAwMzElMCMGA1UEAxMcT3JkcmUgZGVzIEV4cGVydHMtQ29tcHRhYmxlczAeFw0x
MTA1MTAwMDAwMDBaFw0xOTEyMzEwMTAwMDBaMIGCMQswCQYDVQQGEwJGUjEdMBsGA1UECgwUQ1JP
RUMgZGUgTGEgUsOpdW5pb24xFzAVBgNVBAsTDjAwMDIgMzIyOTUxNDQzMTswOQYDVQQDDDJPcmRy
ZSBkZXMgRXhwZXJ0cy1Db21wdGFibGVzIC0gcsOpZ2lvbiBMYSBSw6l1bmlvbjCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAL/XIBTDRe5Mjp0VgLGOVumFQ0m7/zf7ad/HSgJtivFEzHjA
riQlf0Yh8D56pwCuMlV2+1sC+QQM2YynNBSLmWiXocgN8ekXDkJ6ZFVrvi++Lf3PW/o5yo8tcQCv
trKvgiZsUPtT+AlRhEd/2ih0IiC+3ct5KrAgwpAKShceLMBx8Eu/duYJmGE7OPviHVBP5KlcSBsU
OsV7SapwWazt8SCqj7kH2hUX/JbQrmVi4MafXUqFuiXghd5UXFoDPq7mR+6cxA3R38UiZOZkpNJQ
I+hiUdphJ/yoqOqCgtqWliFLAjQUycp5SKojZqG5FK4YJJjHz6SYINFO4gw/m6cQxd0CAwEAAaOC
ATwwggE4MA4GA1UdDwEB/wQEAwIBBjBvBgNVHSAEaDBmMGQGBFUdIAAwXDBaBggrBgEFBQcCARZO
aHR0cDovL3NlZWMuZXhwZXJ0cy1jb21wdGFibGVzLmZyL1BDL1BDUmFjaW5lX09yZHJlX2Rlc19F
eHBlcnRzLUNvbXB0YWJsZXMucGRmMBIGA1UdEwEB/wQIMAYBAf8CAQAwYQYDVR0fBFowWDBWoFSg
UoZQaHR0cDovL3NlZWMuZXhwZXJ0cy1jb21wdGFibGVzLmZyL0NSTC9DUkxSYWNpbmVfT3JkcmVf
ZGVzX0V4cGVydHMtQ29tcHRhYmxlcy5jcmwwHQYDVR0OBBYEFH3/AwSXdRijvSYDq5ukeaQ6VIqJ
MB8GA1UdIwQYMBaAFIEHOeMPekYPuX3pXWJ29SSVHBVWMA0GCSqGSIb3DQEBCwUAA4ICAQBm0Eno
UYXXWaqgmh31EuUK5UhlkQTBfqUb9CbWH3YZKKMpcOEwwFF0sToKmnAXYoOUI3yLFg9JpD70Sogc
YDPRdLrFQwLLZ6Zbbdd31eo90DNZe1C20SFGk1ycR80KvjcUW8/twv1WkSxRx5jRXqms8dFjEd6o
Hb56x5NCwkK9b2wRBXbzAmixgonYqiKZ8hTcDj1hR7IYB4knS/Zt0nh7C5EJmd0inmv7ltE6e1nu
DToZeHFw3NOqJZhNVsIwyYFQBZH/m3f6tvmKs3T8Aih2ZfjRilC02euq3nGfegNDtIdQwsnhbUVV
li9dcMROG4ecEi845uJAydNwkqya0UHPQGGNiA9nASpeqlRloRPazBk/fB4GjYM9tom+gQVtrPEV
rzU9VLh/p6AINcqI1PopauCfWnr0vUCD2BVtuifwjiNYyn97Vjmk0miBzJeKh1FJYJo0dC727kKG
/idGMFobdGtJ/C2t0L34e/JR+Z+Sk7f9/s+AgSX/RlFRGeK8X+HHfdPn0qlY+bihu4KkZapZbcT5
Rhuno3M8l84WPjA6F65SeBUdPov5OhLKgq5Zp7nm+QFsHQTCmEbVOK1pOKjUhZd962vgKX/KK8mb
gj6SKn1/7t0gQzQ/ryNr8dIBuKeTgA77uDYUEURhR8KLhJqpuMcAFdGiKDBk9KlmuPLmoQ==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Ordre des Experts-Comptables*

Issuer OU: *0002 775670003*

Issuer O: *Ordre des Experts-Comptables*

Issuer C: *FR*

Subject CN: *Ordre des Experts-Comptables - région La Réunion*

Subject OU: *0002 322951443*

Subject O: *CROEC de La Réunion*

Subject C: *FR*

Valid from: *Tue May 10 02:00:00 CEST 2011*

Valid to: *Tue Dec 31 02:00:00 CET 2019*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:BF:D7:20:14:C3:45:EE:4C:8E:9D:15:80:B1:8E:56:E9:85:43:49:BB:FF:37:FB:69:DF:C7:4A:02:6D:8A:F1:44:CC:78:C0:AE:24:25:7F:46:21:F0:3E:7A:A7:00:AE:32:55:76:FB:5B:02:F9:04:0C:D9:8C:A7:34:14:8B:99:68:97:A1:C8:0D:F1:E9:17:0E:42:7A:64:55:6B:BE:2F:BE:2D:FD:CF:5B:FA:39:CA:8F:2D:71:00:AF:B6:B2:AF:82:26:6C:50:FB:53:F8:09:51:84:47:7F:DA:28:74:22:20:BE:DD:CB:79:2A:B0:20:C2:90:0A:4A:17:1E:2C:C0:71:F0:4B:BF:76:E6:09:98:61:3B:38:FB:E2:1D:50:4F:E4:A9:5C:48:1B:14:3A:C5:7B:49:AA:70:59:AC:ED:F1:20:AA:8F:B9:07:DA:15:17:FC:96:D0:AE:65:62:E0:C6:9F:5D:4A:85:BA:25:E0:85:DE:54:5C:5A:03:3E:AE:E6:47:EE:9C:C4:0D:D1:DF:C5:22:64:E6:64:A4:D2:50:23:E8:62:51:DA:61:27:FC:A8:A8:EA:82:82:DA:96:96:21:4B:02:34:14:C9:CA:79:48:AA:23:66:A1:B9:14:AE:18:24:98:C7:CF:A4:98:20:D1:4E:E2:0C:3F:9B:A7:10:C5:DD:02:03:01:00:01

Certificate Policies *Policy OID: 2.5.29.32.0*

CPS pointer: http://seec.experts-comptables.fr/PC/PCRacine_Ordre_des_Experts-Comptables.pdf

Basic Constraints *IsCA: true - Path length: 0*

CRL Distribution Points *http://seec.experts-comptables.fr/CRL/CRLRacine_Ordre_des_Experts-Comptables.crl*

Subject Key Identifier *7D:FF:03:04:97:75:18:A3:BD:26:03:AB:9B:A4:79:A4:3A:54:8A:89*

Authority Key Identifier *81:07:39:E3:0F:7A:46:0F:B9:7D:E9:5D:62:76:F5:24:95:1C:15:56*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *09:C8:19:77:03:45:8B:2D:5F:A9:6A:C5:49:C4:23:4D:FD:54:0E:3B:EC:DD:3E:69:73:D2:75:93:5F:24:7A:B6*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description

[en] *undefined.*

[fr] *undefined.*

Status Starting Time *2018-01-30T01:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS101456/QCPPublic*

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Signature-3-Stars*

TSP Service Definition URI

URI *[fr]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

URI *[en]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

11.11.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.11.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région La Réunion RGS****

Name *[fr]* *Ordre des Experts-Comptables - région La Réunion RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - région La Réunion*

Subject OU: *0002 322951443*

Subject O: *CROEC de La Réunion*

Subject C: *FR*

X509SKI

X509 SK I *ff8DBJd1GKO9JgOrm6R5pDpUiok=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

11.11.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.11.3 - History instance n.2 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région La Réunion RGS****

Name *[fr]* *Ordre des Experts-Comptables - région La Réunion RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - région La Réunion*

Subject OU: *0002 322951443*

Subject O: *CROEC de La Réunion*

Subject C: *FR*

X509SKI

X509 SK I *ff8DBJd1GKO9JgOrm6R5pDpUiok=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2012-11-25T23:00:00Z*

11.12 - Service (withdrawn): Ordre des Experts-Comptables - région LN-PCAL RGS***

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région LN-PCAL RGS****

Name *[fr]* *Ordre des Experts-Comptables - région LN-PCAL RGS****

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *149208110086583732436212136762432146481114 3*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIF2zCCA8OgAwIBAgISESDVDylDAxXKKkwXs3LcOD6HMA0GCSqGSIb3DQEBCwUAMHQxCzAJBgNV
BAYTAkZSMSUwIwYDVQQKExxPcmRyZSBkZXMgRXhwZXJ0cy1Db21wdGFibGVzMRcwFQYDVQQLEw4w
MDAyIDc3NTY3MDAwMzElMCMGA1UEAxMcT3JkcmUgZGVzIEV4cGVydHMtQ29tcHRhYmxlczAeFw0x
MTA1MTAwMDAwMDBaFw0xOTEyMzEwMTAwMDBaMIGcMQswCQYDVQQGEwJGUjEqMCgGA1UEChMhQ1JP
RUMgZGUgTGlsbGUgTm9yZCBQYXMtZGUtQ2FsYWlzMRcwFQYDVQQLEw4wMDAyIDM4MDE4MjIxMjFI
MEYGA1UEAww/T3JkcmUgZGVzIEV4cGVydHMtQ29tcHRhYmxlcyAtIHLDqWdpb24gTGlsbGUgTm9y
ZCBQYXMtZGUtQ2FsYWlzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuwCRPxtGfK5S
4Bu36PPuNSofGsJx31bzFW5J0a8jzM3LBR/88YLTGvDSa3HnUbrEKrUjdAijA9/7LWdIoktPzXxy
8cDtS3UFFit9v0c4b1VeVfn0AC2r1e63edz8bwIVFKRRiQJV04SLSc9aXKrcEBC1PunLU+GjaFe9
1ngpClnHwPj/GiKSVPypOjcEPXi4EGbIiFl5vfq5pbDgAZlzYoBsrZSC6JAGz9hnaDNpimgNk2cC
2RR+rMj0MFqj8c6EUMkuknlOoCe/6/D/rqyBbRhtcIIfOzKCncFqO02rA7osJvhLx/rpZLGzr8sq
Qp6OQ997kcexw2SxlhUy8FuqawIDAQABo4IBPDCCATgwDgYDVR0PAQH/BAQDAgEGMG8GA1UdIARo
MGYwZAYEVR0gADBcMFoGCCsGAQUFBwIBFk5odHRwOi8vc2VlYy5leHBlcnRzLWNvbXB0YWJsZXMu
ZnIvUEMvUENSYWNpbmVfT3JkcmVfZGVzX0V4cGVydHMtQ29tcHRhYmxlcy5wZGYwEgYDVR0TAQH/
BAgwBgEB/wIBADBhBgNVHR8EWjBYMFagVKBShlBodHRwOi8vc2VlYy5leHBlcnRzLWNvbXB0YWJs
ZXMuZnIvQ1JML0NSTFJhY2luZV9PcmRyZV9kZXNfRXhwZXJ0cy1Db21wdGFibGVzLmNybDAdBgNV
HQ4EFgQUEOyBrU5F7Zk4vZcjawXiNl/XK+wwHwYDVR0jBBgwFoAUgQc54w96Rg+5feldYnb1JJUc
FVYwDQYJKoZIhvcNAQELBQADggIBAFSL8mKkKVbm8CQJaVcO+BAJYb0Wj6sL82bFPXpGZFQ6TQVL
AbW8qYFPNWkN+1sV0AOKojxor+nTdy5KfMICzm/lzZQh0qEtiMHu/jVw0TLC4yfS01X5UIjdzeUM
txn7wyLNztxgfgXRIGFnPjjSg9JuZkg3+jQdeV8hKv1Nnt6KjV50ahU/pEz8buSK6EvIUcsZ2334
49RK1jP/4tVdkTmT/dz/MJHDwyYiOa9kRNQGWeyC/2DdfL4+2X2Ps0iZE1YawC8rCyQKRqFtX49m
ztSYTBGwXzxMbhjTlPIfnZTYVqO6D/xWgmaf14ZRSBKmFg7KGsoE7T3mW03dLYXZOXwQepDbSC2y
wYV+7XsmVwZv1gfGTpvtBOZnluAC8YX5G2saNwQP5OFQVnmgt3ek5cVj+RKl4Bd1VC64WA1Pm6mi
/JhE8keTS8ixq4BpeC7HEHS/8UV8Y0ebVs3tvYGgakfm+PMBV2fd5lshlhczWrl/vioDbLJNEITa
xEbybUqflghgi6JFhYcL0TSiDfxVkb+c+SR0a8Wk89fYNOYpD7sgFJ4egoHgdv3tVw4+jxKr9oy5
4KFOPJfGD0+3qEe7ob0uug0lM/CY6uJmmV+JdJrJH6zf2U/sXTuJfgqnPcyysHcsZNTnPPZQV4/l
L7zJ8MtBoytPXuc1iyO2z7XOfNnl

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Ordre des Experts-Comptables*

Issuer OU: *0002 775670003*

Issuer O: *Ordre des Experts-Comptables*

Issuer C: *FR*

Subject CN: *Ordre des Experts-Comptables - région Lille Nord Pas-de-Calais*

Subject OU: *0002 380182212*

Subject O: *CROEC de Lille Nord Pas-de-Calais*

Subject C: *FR*

Valid from: *Tue May 10 02:00:00 CEST 2011*

Valid to: *Tue Dec 31 02:00:00 CET 2019*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:BB:00:91:3F:1B:46:7C:AE:52:E0:1B:B7:E8:F3:EE:35:2A:1F:1A:C2:71:DF:56:F3:15:6E:49:D1:AF:23:CC:CD:CB:05:1F:FC:F1:82:D3:1A:F0:D2:6B:71:E7:51:BA:C4:2A:B5:23:74:08:A3:03:DF:FB:2D:67:48:A2:4B:4F:CD:7C:72:F1:C0:ED:4B:75:05:16:2B:7D:BF:47:38:6F:55:5E:55:F9:F4:00:2D:AB:D5:EE:B7:79:DC:FC:6F:02:15:14:A4:51:89:02:55:D3:84:8B:49:CF:5A:5C:AA:DC:10:10:B5:3E:E9:CB:53:E1:A3:68:57:BD:D6:78:29:0A:59:C7:C0:F8:FF:1A:22:92:54:FC:A9:3A:37:04:3D:78:B8:10:66:C8:88:59:79:BD:FA:B9:A5:B0:E0:01:99:73:62:80:6C:AD:94:82:E8:90:06:CF:D8:67:68:33:69:8A:68:0D:93:67:02:D9:14:7E:AC:C8:F4:30:5A:A3:F1:CE:84:50:C9:2E:92:79:4E:A0:27:BF:EB:F0:FF:AE:AC:81:6D:18:6D:70:82:1F:3B:32:82:9D:C1:6A:3B:4D:AB:03:BA:2C:26:F8:4B:C7:FA:E9:64:B1:B3:AF:CB:2A:42:9E:8E:43:DF:7B:91:C7:B1:C3:64:B1:22:15:32:F0:5B:AA:6B:02:03:01:00:01

Certificate Policies *Policy OID: 2.5.29.32.0*

CPS pointer: http://seec.experts-comptables.fr/PC/PCRacine_Ordre_des_Experts-Comptables.pdf

Basic Constraints *IsCA: true - Path length: 0*

CRL Distribution Points *http://seec.experts-comptables.fr/CRL/CRLRacine_Ordre_des_Experts-Comptables.crl*

Subject Key Identifier *10:EC:81:AD:4E:45:ED:99:38:BD:97:23:6B:05:E2:36:5F:D7:2B:EC*

Authority Key Identifier *81:07:39:E3:0F:7A:46:0F:B9:7D:E9:5D:62:76:F5:24:95:1C:15:56*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *94:A4:98:D6:8E:7A:FE:2A:41:B1:E9:88:A1:C8:96:B1:6C:1B:9D:14:22:10:23:A5:58:60:EC:88:76:CF:98:35*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2018-01-30T01:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS101456/QCPPublic*

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Signature-3-Stars*

TSP Service Definition URI

URI *[fr]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

URI *[en]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

11.12.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.12.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région LN-PCAL RGS****

Name *[fr]* *Ordre des Experts-Comptables - région LN-PCAL RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - région Lille Nord Pas-de-Calais*

Subject OU: *0002 380182212*

Subject O: *CROEC de Lille Nord Pas-de-Calais*

Subject C: *FR*

X509SKI

X509 SK I *EOyBrU5F7Zk4vZcjawXiNl/XK+w=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

11.12.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.12.3 - History instance n.2 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région LN-PCAL RGS****

Name *[fr]* *Ordre des Experts-Comptables - région LN-PCAL RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - région Lille Nord Pas-de-Calais*

Subject OU: *0002 380182212*

Subject O: *CROEC de Lille Nord Pas-de-Calais*

Subject C: *FR*

X509SKI

X509 SK I *EOyBrU5F7Zk4vZcjawXiNl/XK+w=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2012-11-25T23:00:00Z*

11.13 - Service (withdrawn): Ordre des Experts-Comptables - région Limoges RGS***

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Limoges RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Limoges RGS****

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *149203523277685787410550708737660826257218 6*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIFuDCCA6CgAwIBAgISESCyjUnf7DNZMf2cCAMV10iaMA0GCSqGSIb3DQEBCwUAMHQxCzAJBgNV
BAYTAkZSMSUwIwYDVQQKExxPcmRyZSBkZXMgRXhwZXJ0cy1Db21wdGFibGVzMRcwFQYDVQQLEw4w
MDAyIDc3NTY3MDAwMzElMCMGA1UEAxMcT3JkcmUgZGVzIEV4cGVydHMtQ29tcHRhYmxlczAeFw0x
MTA1MTAwMDAwMDBaFw0xOTEyMzEwMTAwMDBaMHoxCzAJBgNVBAYTAkZSMRkwFwYDVQQKExBDUk9F
QyBkZSBMaW1vZ2VzMRcwFQYDVQQLEw4wMDAyIDM4MDE4MzMxOTE3MDUGA1UEAwwuT3JkcmUgZGVz
IEV4cGVydHMtQ29tcHRhYmxlcyAtIHLDqWdpb24gTGltb2dlczCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAN/MalefG70IYdRZZOcjaLQ9xeZsNMxkqcS/6sL1AdI4XOSSswgv7OkSsEBH
b4TZc9B87ikeI6A1nFKIwekjrhCJNPnpKdmr+KtP/efty+zb7sG/ZsJggAImRCXGpSzWkuUqnLWl
qyQH+rx1MrL4MfqWIjwt9uaZoAn7SG0Ijh2XMBV/k2AHHc0jLWDliFhSzKDzfutaVrgS0bQzo6xw
eFy3Ee4zc6hAUHpyA/j8KLvqQX88trtvlA3DQLfhkOHR9WqvQIpd4bLHfodpf09SZLHaQc7pzUvs
hs/y7ga2kJMDpFI3oZ8D09Ro82sACDTWduvQrXuBsXzFedNAruTG8S8CAwEAAaOCATwwggE4MA4G
A1UdDwEB/wQEAwIBBjBvBgNVHSAEaDBmMGQGBFUdIAAwXDBaBggrBgEFBQcCARZOaHR0cDovL3Nl
ZWMuZXhwZXJ0cy1jb21wdGFibGVzLmZyL1BDL1BDUmFjaW5lX09yZHJlX2Rlc19FeHBlcnRzLUNv
bXB0YWJsZXMucGRmMBIGA1UdEwEB/wQIMAYBAf8CAQAwYQYDVR0fBFowWDBWoFSgUoZQaHR0cDov
L3NlZWMuZXhwZXJ0cy1jb21wdGFibGVzLmZyL0NSTC9DUkxSYWNpbmVfT3JkcmVfZGVzX0V4cGVy
dHMtQ29tcHRhYmxlcy5jcmwwHQYDVR0OBBYEFFK/yHZqf5U3wfnfM4Bfljmc2TAaMB8GA1UdIwQY
MBaAFIEHOeMPekYPuX3pXWJ29SSVHBVWMA0GCSqGSIb3DQEBCwUAA4ICAQALOPOAxfGqTHxOaz1l
7Rlm14QFwt0ULn+hfnoPQJLLq5GFwSB8kDy21TL5pWCZs/7x/I+Db4URkBveBnDmtk9Q+FCfCGOu
gLRYjA4DioKz3Z6VV25CF0Oi12O0S/c+Y/f68M8WO2ILBz8tm0pKGazQQ6Oc+aGs8QDiFNOjUde0
VBf5NqCoAJK4hyL8Dlq/G5JAxiSzghE0d0gUVmmtPmInoHIi9SfTcvvq/uSyTSYk7p6QPrDqCHfL
DCpZ3hcdf9tisnZUi8QDeMfSYEs52Os1bLujUqDz1wjBJQyqxg6YjJ4F110NdPMCe33eMEsgfB9t
Yz18j+PtZ4BR8N8CSXzWV0wrsw6Mbi1LuHtLdjhxU4Ck+va2TW39Pu28jDFfzO29IYLJDu0VjxHO
fP4WoSI+3VcT7sslRjzc1HyJplv+XsoGJVwitHqqSq1kaBpkuxjk0hOIQvFc77rkilou+i49gb+3
CbABwWUc5McWCXYa0+yPb9GsLk/X3anLOk+BXzKlcffAnIDR2b7ficT2rAbYNTKGiegfEhnoVFOO
MwZENqlXllctgWQ3OrSxU42lMwEAgSzmDzf8vxOGxTbGqPfPlwLpxU+q7GxH1beXNDLOVH8ZwkNH
UYYcPOsUc/fb8wy+U3vJVhvfwvFCO7SNbVq4zuyN3Rn46k3T/H0FRrX3uQ==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Ordre des Experts-Comptables*

Issuer OU: *0002 775670003*

Issuer O: *Ordre des Experts-Comptables*

Issuer C: *FR*

Subject CN: *Ordre des Experts-Comptables - région Limoges*

Subject OU: *0002 380183319*

Subject O: *CROEC de Limoges*

Subject C: *FR*

Valid from: *Tue May 10 02:00:00 CEST 2011*

Valid to: *Tue Dec 31 02:00:00 CET 2019*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:DF:CC:6A:57:9F:1B:BD:08:61:D4:59:64:E7:23:68:B4:3D:C5:E6:6C:34:CC:64:A9:C4:BF:EA:C2:F5:01:D2:38:5C:E4:92:B3:08:2F:EC:E9:12:B0:40:47:6F:84:D9:73:D0:7C:EE:29:1E:23:A0:35:9C:52:88:C1:E9:23:AE:10:89:34:F9:E9:29:D9:AB:F8:AB:4F:FD:E7:ED:CB:EC:DB:EE:C1:BF:66:C2:60:80:02:26:44:25:C6:A5:2C:D6:92:E5:2A:9C:B5:88:AB:24:07:FA:BC:75:32:B2:F8:31:FA:96:22:3C:2D:F6:E6:99:A0:09:FB:48:6D:08:8E:1D:97:30:15:7F:93:60:07:1D:CD:23:2D:60:E5:88:58:52:CC:A0:F3:7E:EB:5A:56:B8:12:D1:B4:33:A3:AC:70:78:5C:B7:11:EE:33:73:A8:40:50:7A:72:03:F8:FC:28:BB:EA:41:7F:3C:B6:BB:6F:94:0D:C3:40:B7:E1:90:E1:D1:F5:6A:AF:40:8A:5D:E1:B2:C7:7E:87:69:7F:4F:52:64:B1:DA:41:CE:E9:CD:4B:EC:86:CF:F2:EE:06:B6:90:93:03:A4:52:37:A1:9F:03:D3:D4:68:F3:6B:00:08:34:D6:76:EB:D0:AD:7B:81:B1:7C:C5:79:D3:40:AE:E4:C6:F1:2F:02:03:01:00:01

Certificate Policies *Policy OID: 2.5.29.32.0*

CPS pointer: http://seec.experts-comptables.fr/PC/PCRacine_Ordre_des_Experts-Comptables.pdf

Basic Constraints *IsCA: true - Path length: 0*

CRL Distribution Points *http://seec.experts-comptables.fr/CRL/CRLRacine_Ordre_des_Experts-Comptables.crl*

Subject Key Identifier *52:BF:C8:76:6A:7F:95:37:C1:F9:DF:33:80:5F:96:39:9C:D9:30:1A*

Authority Key Identifier *81:07:39:E3:0F:7A:46:0F:B9:7D:E9:5D:62:76:F5:24:95:1C:15:56*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *34:02:CD:40:E3:0C:5C:97:C1:47:8A:43:1E:7F:5E:13:69:D4:CE:21:51:68:B1:50:75:64:03:10:7A:17:37:DC*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2018-01-30T01:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS101456/QCPPublic*

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Signature-3-Stars*

TSP Service Definition URI

URI *[fr]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

URI *[en]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

11.13.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.13.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Limoges RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Limoges RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - région Limoges*

Subject OU: *0002 380183319*

Subject O: *CROEC de Limoges*

Subject C: *FR*

X509SKI

X509 SK I *Ur/Idmp/lTfB+d8zgF+WOZzZMBo=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

11.13.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.13.3 - History instance n.2 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Limoges RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Limoges RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - région Limoges*

Subject OU: *0002 380183319*

Subject O: *CROEC de Limoges*

Subject C: *FR*

X509SKI

X509 SK I *Ur/Idmp/lTfB+d8zgF+WOZzZMBo=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2012-11-25T23:00:00Z*

11.14 - Service (withdrawn): Ordre des Experts-Comptables - région Lorraine RGS***

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Lorraine RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Lorraine RGS****

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1491869724956413714771452489234057257349516*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIFujCCA6KgAwIBAgISESA2CaRPA88dEMKBKM3NSPGMMA0GCSqGSIb3DQEBCwUAMHQxCzAJBgNV
BAYTAkZSMSUwIwYDVQQKExxPcmRyZSBkZXMgRXhwZXJ0cy1Db21wdGFibGVzMRcwFQYDVQQLEw4w
MDAyIDc3NTY3MDAwMzElMCMGA1UEAxMcT3JkcmUgZGVzIEV4cGVydHMtQ29tcHRhYmxlczAeFw0x
MTA1MTAwMDAwMDBaFw0xOTEyMzEwMTAwMDBaMHwxCzAJBgNVBAYTAkZSMRowGAYDVQQKExFDUk9F

QyBkZSBMb3JyYWluZTEXMBUGA1UECxMOMDAwMiAzODAxODgxODUxODA2BgNVBAMML09yZHJlIGRl
cyBFeHBlcnRzLUNvbXB0YWJsZXMgLSByw6lnaW9uIExvcnJhaW5lMIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEAokh2d0MgHZNFPpwdGbT19f/I28VQPtA7cdk/eGUd+xq4EgtekaIb0hPX
ABF6JhPFJIJh94TjonfUnExfwwbWa9d/BN9cRoAV9sRP/nsBAb4FqsZqU5cWuFWtObDKq2rrbxku
GTSfxyDTicN8hDQYCQlpWHvzkp/gNS2gQOdP0pUaghU9fwKY/vToWaq+uYrI5saWRKtrZ+i+JJS0
oDBjy1ApJY5dxqbcWFNllGRt+/MKIqVL0PPmKjDUEMAbLJC3fAGjWeiREQY7qHxOfiaUcP5D0eOK
k+xPM4deV7dWniHOO2mwLuimYoDPcBQJZAYflPM6DwBmnnJnmBGxoApt0QIDAQABo4IBPDCCATgw
DgYDVR0PAQH/BAQDAgEGMG8GA1UdIARoMGYwZAYEVR0gADBcMFoGCCsGAQUFBwIBFk5odHRwOi8v
c2VlYy5leHBlcnRzLWNvbXB0YWJsZXMuZnIvUEMvUENSYWNpbmVfT3JkcmVfZGVzX0V4cGVydHMt
Q29tcHRhYmxlcy5wZGYwEgYDVR0TAQH/BAgwBgEB/wIBADBhBgNVHR8EWjBYMFagVKBShlBodHRw
Oi8vc2VlYy5leHBlcnRzLWNvbXB0YWJsZXMuZnIvQ1JML0NSTFJhY2luZV9PcmRyZV9kZXNfRXhw
ZXJ0cy1Db21wdGFibGVzLmNybDAdBgNVHQ4EFgQUdq8OkpwTCbZlHdNetiQkWQT74kQwHwYDVR0j
BBgwFoAUgQc54w96Rg+5feldYnb1JJUcFVYwDQYJKoZIhvcNAQELBQADggIBAAQdEcivmj8FUr9w
Hd6IscuOxuosx7vDtoUP5afbi5fXU6T3Q2syOtvCMZlY8mP89AnWPPVMdjNJu8hCcU5UREgHtK1k
q6PTRWkPTEKcptCllUYesNdA/Og3JhyKRlOAvsd5UeAMVZb/o81aNX707TsWH6P3SjyUWz+opn5X
Gl1uAlZlYSr5VUSQG2LqJd/jbUZoH9DNnZ6P0fgAjR5c3PPghjw/Dg6/A+joNezLU7yk/zK9BppH
eVWTVOw+MBXZL7u9z7rOnK4rHt6RA1CPk3qNeftmr6nFTXDo0gllJR8E4ZhXqwfLKUUcDUOAFbtU
raqSMu2JtwI6R+adA2Pewe3FsOuuXPvKCztc2kyzGmvez3Z/qdRwip4lZdfneXb1UORQldKOgXpT
43nhCx4LKyndLN3o1oTq1T420WqhubwPiLr1UKEegtvjklbX9bd3RiEq8OSmahx0ybPrLNza9gse
nMaK1UNUX0fpvZnw5JtP3ZW5IHBa9FqIarXkXDxkRmpegPBzSgQlY5Q4otLyJBljOzsHMWjRIsOP
lzYw5XSI7EPvlsVjEk7iolsi51vXEQTbxQFXmKZ9S5ZdzHT2H7uxgZKakjoRokfDKP4I9KnzI5ob
wWz+b1BlWH7Q1/hTYGjfHiWbKohnclSdNKN5a9h7Cbz9DassVxK5qtjJycql

-----END CERTIFICATE-----

Signature algorithm:	*SHA256withRSA*
Issuer CN:	*Ordre des Experts-Comptables*
Issuer OU:	*0002 775670003*
Issuer O:	*Ordre des Experts-Comptables*
Issuer C:	*FR*
Subject CN:	*Ordre des Experts-Comptables - région Lorraine*
Subject OU:	*0002 380188185*
Subject O:	*CROEC de Lorraine*
Subject C:	*FR*
Valid from:	*Tue May 10 02:00:00 CEST 2011*
Valid to:	*Tue Dec 31 02:00:00 CET 2019*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:A2:48:76:77:43:20:1D:93:45:3E:9C:1D:19:B4:F5:F5:FF:C8:DB:C5:50:3E:D0:3B:71:D9:3F:78:65:1D:FB:1A:B8:12:0B:5E:91:A2:1B:D2:13:D7:00:11:7A:26:13:C5:24:82:61:F7:84:E3:A2:77:D4:9C:4C:5F:C3:06:D6:6B:D7:7F:04:DF:5C:46:80:15:F6:C4:4F:FE:7B:01:01:BE:05:AA:C6:6A:53:97:16:B8:55:AD:39:B0:CA:AB:6A:EB:6F:19:2E:19:34:9F:C7:20:D3:89:C3:7C:84:34:18:09:09:69:58:7B:F3:92:9F:E0:35:2D:A0:40:E7:4F:D2:95:1A:82:15:3D:7F:02:98:FE:F4:E8:59:AA:BE:B9:8A:C8:E6:C6:96:44:AB:6B:67:E8:BE:24:94:B4:A0:30:63:CB:50:29:25:8E:5D:C6:A6:DC:58:53:65:94:64:6D:FB:F3:0A:22:A5:4B:D0:F3:E6:2A:30:D4:10:C0:1B:2C:90:B7:7C:01:A3:59:E8:91:11:06:3B:A8:7C:4E:7E:26:94:70:FE:43:D1:E3:8A:93:EC:4F:33:87:5E:57:B7:56:9E:21:CE:3B:69:B0:2E:E8:A6:62:80:CF:70:14:09:64:06:1F:94:F3:3A:0F:00:66:9E:72:67:98:11:B1:A0:0A:6D:D1:02:03:01:00:01

Certificate Policies	*Policy OID: 2.5.29.32.0*

CPS pointer: http://seec.experts-comptables.fr/PC/PCRacine_Ordre_des_Experts-Comptables.pdf

Basic Constraints *IsCA: true - Path length: 0*

CRL Distribution Points *http://seec.experts-comptables.fr/CRL/CRLRacine_Ordre_des_Experts-Comptables.crl*

Subject Key Identifier *76:AF:0E:92:9C:13:09:B6:48:1D:D3:5E:B6:24:24:59:04:FB:E2:44*

Authority Key Identifier *81:07:39:E3:0F:7A:46:0F:B9:7D:E9:5D:62:76:F5:24:95:1C:15:56*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *A8:6D:E8:B1:C1:06:85:3D:98:22:B1:42:9E:A3:80:5A:12:4F:8E:5D:D7:75:68:77:C2:36:F1:CF:F1:41:A1:A5*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description

[en] *undefined.*

[fr] *undefined.*

Status Starting Time *2018-01-30T01:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS101456/QCPPublic*

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Signature-3-Stars*

TSP Service Definition URI

URI *[fr]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

URI *[en]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

11.14.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.14.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Lorraine RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Lorraine RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - région Lorraine*

Subject OU: *0002 380188185*

Subject O: *CROEC de Lorraine*

Subject C: *FR*

X509SKI

X509 SK I *dq8OkpwTCbZIHdNetiQkWQT74kQ=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

11.14.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.14.3 - History instance n.2 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Lorraine RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Lorraine RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - région Lorraine*

Subject OU: *0002 380188185*

Subject O: *CROEC de Lorraine*

Subject C: *FR*

X509SKI

X509 SK I *dq8OkpwTCbZIHdNetiQkWQT74kQ=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2012-11-25T23:00:00Z*

11.15 - Service (withdrawn): Ordre des Experts-Comptables - région Marseille PACAC RGS***

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Marseille PACAC RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Marseille PACAC RGS****

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *149194051731923549993744939594661249985347 2*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIFyTCCA7GgAwIBAgISESBrS8FFtUeMxYNfgR6dFrCgMA0GCSqGSIb3DQEBCwUAMHQxCzAJBgNV
BAYTAkZSMSUwIwYDVQQKExxPcmRyZSBkZXMgRXhwZXJ0cy1Db21wdGFibGVzMRcwFQYDVQQLEw4w
MDAyIDc3NTY3MDAwMzElMCMGA1UEAxMcT3JkcmUgZGVzIEV4cGVydHMtQ29tcHRhYmxlczAeFw0x
MTA1MTAwMDAwMDBaFw0xOTEyMzEwMTAwMDBaMIGKMQswCQYDVQQGEwJGUjEhMB8GA1UEChMYQ1JP
RUMgZGUgTWFyc2VpbGxlIFBBQ0FDMRcwFQYDVQQLEw4wMDAyIDc4MjgyNTA0NjE/MD0GA1UEAww2
T3JkcmUgZGVzIEV4cGVydHMtQ29tcHRhYmxlcyAtIHLDqWdpb24gTWFyc2VpbGxlIFBBQ0FDMIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEArgNrIFie25IgiztNC7lS/N7/cAsGuvZkPqNm
OQFiHqdSfPYtuA/wsRqAGVp3CNhnZb1scjH37dn5TqGc+qPlDC4zzmGHU17+Q0Gs6OUx3cPV9Tqe
nX0++HkvMR71u4hKFSPdz54g9lPrF3zNMdxgPedbqtEJEWhSyrw7r/60tJieJL9Db+iKksXPN21a
LsuoNg33E0YmKtYLP+fCdywS2F5DNWmVl1CqP6xyPCwCH/ymiZh0LoiDbCpcRjILPdGLaXra+6Au
nw3imJ0ArLovwuFUaEuKZPsY0wFi642SkIKZbNgJmmGa0fWLnIoYHciVIxbZoGDaztbzm0fTSb8v
XQIDAQABo4IBPDCCATgwDgYDVR0PAQH/BAQDAgEGMG8GA1UdIARoMGYwZAYEVR0gADBcMFoGCCsG
AQUFBwIBFk5odHRwOi8vc2VlYy5leHBlcnRzLWNvbXB0YWJsZXMuZnIvUEMvUENSYWNpbmVfT3Jk
cmVfZGVzX0V4cGVydHMtQ29tcHRhYmxlcy5wZGYwEgYDVR0TAQH/BAgwBgEB/wIBADBhBgNVHR8E
WjBYMFagVKBShlBodHRwOi8vc2VlYy5leHBlcnRzLWNvbXB0YWJsZXMuZnIvQ1JML0NSTFJhY2lu
ZV9PcmRyZV9kZXNfRXhwZXJ0cy1Db21wdGFibGVzLmNybDAdBgNVHQ4EFgQUWT1x57jmg7cF5Aeq
wfMVTkcfhz8wHwYDVR0jBBgwFoAUgQc54w96Rg+5feldYnb1JJUcFVYwDQYJKoZIhvcNAQELBQAD
ggIBAAOWlaydbMS+LWX6QjGwgOREwWWVc/QgUpgOcmV7U4LvweE20c+nzsBwtSf5SA08lE6qNlee
97ZQcntwv0D++zh5990j2jiXE6FxZ2hrbkbTDIoCvLnw/XeivgDzobXbBnoUmyZQgLfAQGOMfV5E
j7FvwTl+9jDFk3ZkJm6TasjvBgzynNxwrFSsTFBzpcBtLmk8ytt51Th89oMHwP/H4qkGKo4AHaZM
DjswHRn0WD1epYABaSoGb+uXP2M5Gi9LgNMfQmrrHt1u3Kv1ML3HXwrDu1gSN5CKj0DN8uICJUtK

VDDTP09uXxLz+T+S/uepWploUws4J97FFNC50oFr1U3QpKch6V1IaYOLx9gjJdJZh1gL4wtQNlfS
jJ3RpgTLKScFupusWkIoo0EruuhxaMZk6dNZf6uX1T0t8HKvXlgZpHdAO1+XN5uktELe75TxPg5O
W5IGPyFJkGIy/NyNYWVPxkBHU5mhdFpE6MLal21/cI3dkHcuUaJHaHoT+k63B6H3RsN6JePcGU7K
pX3s8wV7rLwufe5iQIJZcDpX3ROTATba70voikYmg7g8FMp0sAV90QSv4uwly+qu4f/hU+v7p9dO
VRW747w5Zz5BZqnyxZPOQCrUpTp9zSLlGtg4A+xalq6tz85WDc9WnHiKSoYzmBwFROUJlvckdhiD
hvxZ

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Ordre des Experts-Comptables*

Issuer OU: *0002 775670003*

Issuer O: *Ordre des Experts-Comptables*

Issuer C: *FR*

Subject CN: *Ordre des Experts-Comptables - région Marseille PACAC*

Subject OU: *0002 782825046*

Subject O: *CROEC de Marseille PACAC*

Subject C: *FR*

Valid from: *Tue May 10 02:00:00 CEST 2011*

Valid to: *Tue Dec 31 02:00:00 CET 2019*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:AE:03:6B:20:58:9E:DB:92:20:8B:3B:4D:0B:B9:52:FC:
DE:FF:70:0B:06:BA:F6:64:3E:A3:66:39:01:62:1E:A7:52:7C:F6:2D:B8:0F:F0:B1:1A:80:19:5A:77:08:D8:67:65:BD:6C:72:31:F7:ED:D9:F9:4E:A1:9C:FA:A3:E5:0C:2E
:33:CE:61:87:53:5E:FE:43:41:AC:E8:E5:31:DD:C3:D5:F5:3A:9E:9D:7D:3E:F8:79:2F:31:1E:F5:BB:88:4A:15:23:DD:CF:9E:20:F6:53:EB:17:7C:CD:31:DC:60:3D:E7:5
B:AA:D1:09:11:68:52:CA:BC:3B:AF:FE:B4:B4:98:9E:24:BF:43:6F:E8:8A:92:C5:CF:37:6D:5A:2E:CB:A8:36:0D:F7:13:46:26:2A:D6:0B:3F:E7:C2:77:2C:12:D8:5E:43:
35:69:95:97:50:AA:3F:AC:72:3C:2C:02:1F:FC:A6:89:98:74:2E:88:83:6C:2A:5C:46:32:0B:3D:D1:8B:69:7A:DA:FB:A0:2E:9F:0D:E2:98:9D:00:AC:BA:2F:C2:E1:54:6
8:4B:8A:64:FB:18:D3:01:62:EB:8D:92:90:82:99:6C:D8:09:9A:61:9A:D1:F5:8B:9C:8A:18:1D:C8:95:23:16:D9:A0:60:DA:CE:D6:F3:9B:47:D3:49:BF:2F:5D:02:03:01
:00:01

Certificate Policies *Policy OID: 2.5.29.32.0*

CPS pointer: http://seec.experts-comptables.fr/PC/PCRacine_Ordre_des_Experts-Comptables.pdf

Basic Constraints *IsCA: true - Path length: 0*

CRL Distribution Points *http://seec.experts-comptables.fr/CRL/CRLRacine_Ordre_des_Experts-Comptables.crl*

Subject Key Identifier *59:3D:71:E7:B8:E6:83:B7:05:E4:07:AA:C1:F3:15:4E:47:1F:87:3F*

Authority Key Identifier *81:07:39:E3:0F:7A:46:0F:B9:7D:E9:5D:62:76:F5:24:95:1C:15:56*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *7C:28:82:C1:B4:3C:A8:91:08:E4:34:E7:7F:9B:8C:D8:C8:A3:C1:6B:CF:A8:C5:E5:41:C7:87:A1:AD:D4:37:77*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2018-01-30T01:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS101456/QCPPublic*

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Signature-3-Stars*

TSP Service Definition URI

URI *[fr]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

URI *[en]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

11.15.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.15.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Marseille PACAC RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Marseille PACAC RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - région Marseille PACAC*

Subject OU: *0002 782825046*

Subject O: *CROEC de Marseille PACAC*

Subject C: *FR*

X509SKI

X509 SK I *WT1x57jmg7cF5AeqwfMVTkcfhz8=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

11.15.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.15.3 - History instance n.2 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Marseille PACAC RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Marseille PACAC RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - région Marseille PACAC*

Subject OU: *0002 782825046*

Subject O: *CROEC de Marseille PACAC*

Subject C: *FR*

X509SKI

X509 SK I *WT1x57jmg7cF5AeqwfMVTkcfhz8=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2012-11-25T23:00:00Z*

11.16 - Service (withdrawn): Ordre des Experts-Comptables - région Martinique RGS***

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Martinique RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Martinique RGS****

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *149213055515296814513009576558928774538118O*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIFvzCCA6egAwIBAgISESD6Q7Xea9ttEXWVeVZARGM8MA0GCSqGSIb3DQEBCwUAMHQxCzAJBgNV
BAYTAkZSMSUwIwYDVQQKExxPcmRyZSBkZXMgRXhwZXJ0cy1Db21wdGFibGVzMRcwFQYDVQQLEw4w
MDAyIDc3NTY3MDAwMzElMCMGA1UEAxMcT3JkcmUgZGVzIEV4cGVydHMtQ29tcHRhYmxlczAeFw0x
MTA1MTAwMDAwMDBaFw0xOTEyMzEwMTAwMDBaMIGAMQswCQYDVQQGEwJGUjEcMBoGA1UEChMTQ1JP
RUMgZGUgTWFydGluaXF1ZTEXMBUGA1UECxMOMDAwMiAzODIwNTI1MzgxOjA4BgNVBAMMMU9yZHJl
IGRlcyBFeHBlcnRzLUNvbXB0YWJsZXMgLSByw6lnaW9uIE1hcnRpbmlxdWUwggEiMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQDVeuwCFyMe1jfRT+eMPJwvdwvnsteAk4mMovcTD6ikbn3e3zFI
OrCK3Jge3vbfg0pQPgd1yWfqMSYFl8mefU8al1hVKswTJxCrUgFBAX4MU9+ghujwLgqbloo0SCN0
ciYmmJKjW/DIGvPiW3F9apG5rm7PS54v90jD7m7kuFvs2qOt67MeudjJxDJYS2xn4inuSANdR2z2
Z0X8IhzAupH+vDQphiyvzwQL6kg6sha6sToE5DH9y6ps+oEJEzPB5mH/yRmPF6o21S5Drk1xTtGl
gOeNUaqW0BR+8r+Ys5qOA47UpEB/Bxb7Ep/dV7eefvnLP3LAg55dZ/5iDnD7y/5nAgMBAAGjggE8
MIIBODAOBgNVHQ8BAf8EBAMCAQYwbwYDVR0gBGgwZjBkBgRVHSAAMFwwWgYIKwYBBQUHAgEWTmh0
dHA6Ly9zZWVjLmV4cGVydHMtY29tcHRhYmxlcy5mci9QQy9QQ1JhY2luZV9PcmRyZV9kZXNfRXhw
ZXJ0cy1Db21wdGFibGVzLnBkZjASBgNVHRMBAf8ECDAGAQH/AgEAMGEGA1UdHwRaMFgwVqBUoFKG
UGh0dHA6Ly9zZWVjLmV4cGVydHMtY29tcHRhYmxlcy5mci9DUkwvQ1JMUmFjaW5lX09yZHJlX2Rl
c19FeHBlcnRzLUNvbXB0YWJsZXMuY3JsMB0GA1UdDgQWBBRZixx3WIl8arYe9YDyjGNU6JkcMzAf
BgNVHSMEGDAWgBSBBznjD3pGD7l96V1idvUklRwVVjANBgkqhkiG9w0BAQsFAAOCAgEAkBC+4cfL
rc45sA+CvMN1n8XplMCo5ztjwXWbm1ilzqaRCHeJNzv537qdHUe/yOVpw1Zjiw9GRj/YACrCTh9n
zWlDpceNsqntqCJu038XF10PEpVVj412cJc44FhiVX+XyH4pELuxkvkQQbLl23rFWi4XPvQFyXtW
kB2F1TkKesDEwIm/yoFQABcbyslHn89LzWDh3WiQoLPvvSKSYZmGm9Gg6MNepLep0JcHIZRSNY05
l9B5rRrWjKBr2zbxhWUbsIpkxP8+cL43zx73U90sGkywqJWwTPc6OCPDpMfQCeCJJxUrsQjLo6JC
hEpKWaWRD/9FDZooiekbCRj+2k72R0qsFURzqHgCx4jiuu3wwuBkA0z8TKGagQ5gh2vOcImNtUpT
f/Z+YRR/o2I+vIysv+JRy4HXhWguv9jTYZtDvzMpaV3jbhwuAUEgpbg60h7xLrV5ehg1H5KYUa8a
ijaLh4aOMBeMyxyT0ioIxUbMGeNsjVVXsGcj8yNobOuDDwbb0CV+lCk+hQ+TjSzRADlEcEHmsb1c
GC9+d03jxweEznSLRi0eZc5UyOTP94P5a3l6oD4Sz6RdnSK8ak7BwZSXKvE16+BP6zCy4dHYdq42
aXachPec/vZQO5p71QJNWza0UfkzLYGlXzqGNIhbVHzBGKjWu3y0BP9pVK5nGCmgSUA=

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Ordre des Experts-Comptables*

Issuer OU: *0002 775670003*

Issuer O: *Ordre des Experts-Comptables*

Issuer C: *FR*

Subject CN: *Ordre des Experts-Comptables - région Martinique*

Subject OU: *0002 382052538*

Subject O: *CROEC de Martinique*

Subject C: *FR*

Valid from: *Tue May 10 02:00:00 CEST 2011*

Valid to: *Tue Dec 31 02:00:00 CET 2019*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:D5:7A:EC:02:17:23:1E:D6:37:D1:4F:E7:8C:3C:9C:2F:77:0B:E7:B2:D7:80:93:89:8C:A2:F7:13:0F:A8:A4:6E:7D:DE:DF:31:48:3A:B0:8A:DC:98:1E:DE:F6:DF:83:4A:50:3E:07:75:C9:67:EA:31:26:05:97:C9:9E:7D:4F:1A:97:58:55:2A:CC:13:27:10:AB:52:01:41:01:7E:0C:53:DF:A0:86:E8:F0:2E:0A:9B:22:8A:34:48:23:74:72:26:26:98:92:A3:5B:F0:C8:1A:F3:E2:5B:71:7D:6A:91:B9:AE:6E:CF:4B:9E:2F:F7:48:C3:EE:6E:E4:B8:5B:EC:DA:A3:AD:EB:B3:1E:B9:D8:C9:C4:32:58:4B:6C:67:E2:29:EE:48:03:5D:47:6C:F6:67:45:FC:22:1C:C0:BA:91:FE:BC:34:29:86:2C:AF:CF:04:0B:EA:48:3A:B2:16:BA:B1:3A:04:E4:31:FD:CB:AA:6C:FA:81:09:13:33:C1:E6:61:FF:C9:19:8F:17:AA:36:D5:2E:43:AE:4D:71:4E:D1:A5:80:E7:8D:51:AA:96:D0:14:7E:F2:BF:98:B3:9A:8E:03:8E:D4:A4:40:7F:07:16:FB:12:9F:DD:57:B7:9E:7E:F9:CB:3F:72:C0:83:9E:5D:67:FE:62:0E:70:FB:CB:FE:67:02:03:01:00:01

Certificate Policies *Policy OID: 2.5.29.32.0*

CPS pointer: http://seec.experts-comptables.fr/PC/PCRacine_Ordre_des_Experts-Comptables.pdf

Basic Constraints *IsCA: true - Path length: 0*

CRL Distribution Points *http://seec.experts-comptables.fr/CRL/CRLRacine_Ordre_des_Experts-Comptables.crl*

Subject Key Identifier *59:8B:1C:77:58:89:7C:6A:B6:1E:F5:80:F2:8C:63:54:E8:99:1C:33*

Authority Key Identifier *81:07:39:E3:0F:7A:46:0F:B9:7D:E9:5D:62:76:F5:24:95:1C:15:56*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *2C:3A:D3:4A:16:9D:26:23:59:89:23:3D:27:99:94:0C:D4:D7:19:01:4A:08:4F:7A:0A:37:B2:65:0A:E6:F4:32*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2018-01-30T01:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS101456/QCPPublic*

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Signature-3-Stars*

TSP Service Definition URI

URI *[fr]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

URI *[en]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

11.16.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.16.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Martinique RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Martinique RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - région Martinique*

Subject OU: *0002 382052538*

Subject O: *CROEC de Martinique*

Subject C: *FR*

X509SKI

X509 SK I *WYscd1iJfGq2HvWA8oxjVOiZHDM=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

11.16.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.16.3 - History instance n.2 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Martinique RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Martinique RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - région Martinique*

Subject OU: *0002 382052538*

Subject O: *CROEC de Martinique*

Subject C: *FR*

X509SKI

X509 SK I *WYscd1iJfGq2HvWA8oxjVOiZHDM=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2012-11-25T23:00:00Z*

11.17 - Service (withdrawn): Ordre des Experts-Comptables - région Montpellier RGS***

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Montpellier RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Montpellier RGS****

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *149181618397996366926667050728495721654895 2*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIFwTCCA6mgAwIBAgISESANwgZcolM+ZjUanle5wqhYMA0GCSqGSIb3DQEBCwUAMHQxCzAJBgNV
BAYTAkZSMSUwIwYDVQQKExxPcmRyZSBkZXMgRXhwZXJ0cy1Db21wdGFibGVzMRcwFQYDVQQLEw4w
MDAyIDc3NTY3MDAwMzElMCMGA1UEAxMcT3JkcmUgZGVzIEV4cGVydHMtQ29tcHRhYmxlczAeFw0x
MTA1MTAwMDAwMDBaFw0xOTEyMzEwMTAwMDBaMIGCMQswCQYDVQQGEwJGUjEdMBsGA1UEChMUQ1JP
RUMgZGUgTW9udHBlbGxpZXIxFzAVBgNVBAsTDjAwMDIgNzc2MDM4MDc3MTswOQYDVQQDDDJPcmRy
ZSBkZXMgRXhwZXJ0cy1Db21wdGFibGVzIC0gcsOpZ2lvbiBNb250cGVsbGllcjCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAM6nI36IYfWpHsO9wv7bNm+87IQFcVyx8bB1Fg9N34rMNkum
OnxbKFZa+tCsM1yAZtZXhKJbdzEeQTASGndibAW5Uc3kj+xiRfcpR/xNgQn2TRLeuXPj9n1QsV3O
FKNxukTmsLoJB2/EEzgYbR/gLYqsECpe5wQ3AJmTUFOgt/U7iTZlVuU0sbh6r3dBthnkN8UnuIlj
S6nrlPxhNY/iGQzzl8hEwv8JBVVcHmepNx2qnj/9PGLJmveJfUqR1EgROZU8SIWMO7b/xBW2nhWS
PzBOfJZDVgIGEQlvSCbJuEHn+i7KUV4G71kBoqWCjnCbbXpD+mYfU/El3QyXMy8DfnECAwEAAaOC
ATwwggE4MA4GA1UdDwEB/wQEAwIBBjBvBgNVHSAEaDBmMGQGBFUdIAAwXDBaBggrBgEFBQcCARZO
aHR0cDovL3NlZWMuZXhwZXJ0cy1jb21wdGFibGVzLmZyL1BDL1BDUmFjaW5lX09yZHJlX2Rlc19F
eHBlcnRzLUNvbXB0YWJsZXMucGRmMBIGA1UdEwEB/wQIMAYBAf8CAQAwYQYDVR0fBFowWDBWoFSg
UoZQaHR0cDovL3NlZWMuZXhwZXJ0cy1jb21wdGFibGVzLmZyL0NSTC9DUkxSYWNpbmVfT3JkcmVf
ZGVzX0V4cGVydHMtQ29tcHRhYmxlcy5jcmwwHQYDVR0OBBYEFGBNsWYig1olVKnoex0IRRxvBX+R
MB8GA1UdIwQYMBaAFIEHOeMPekYPuX3pXWJ29SSVHBVWMA0GCSqGSIb3DQEBCwUAA4ICAQBISo1H
WoJe75kpkePbYf7yTqtSIfr8ekzD+sU4hdTdIuBFRlneVz05/lr1ENByCCfoYmpN7uJpOX2nNRax
Uzbl288XAzv8efi/Kcp4eU3xZeVRuEG3f1fyY+5SJmokEiE9ZdPflXILoGX8SXA7HFoATQGFZe+F
Tj/7o/19Fjx0U1oKzAuTPjfgTYX2Zucxd2yKeGInhTVhQuA8keMOpECDCSr9qgRsQLsi4z8xUk5+
ujA4MN68ByUZDw8HahGh5TcSaJQroHBPF9dAEPVb/BJdCg7dciJD4hp9ajEQDx5e3ucc/+sPaZ0Z
2wvdz9QVu/9957kSD573/9x0T/rlW9LuAE8affFq2aDmJwEAgrgsXHdCjDwILtjA4WO4tMwCzJ6o
0UIMlV3BccHibwOUnwbcifSTq9FYNsIYhtE0MbdJY4GPu30oeobRzsz20zRiLGq/OnwxiDbxPMcE
23qmWwNT71ulFPTKHbTkayxEc2nDwyJTRWZhzNZSZSkN9Kc8EjAbz4xE6W4zfopJ9hrC5m6k9YTZ
3Tgo3VHMTwlTP5SalPJNzfhG+hLV2Bu0iQfV2O4VumPfRkNkjmVfbcjCVI6sE6K83X1tIwYeoU4g
PTqNRaorhBCczN1+JdO4+2v+H5CCjiG+q4IaYYS0RPVl56Co2bO2FB5BdpmiFokyVqq9aQ==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Ordre des Experts-Comptables*

Issuer OU: *0002 775670003*

Issuer O: *Ordre des Experts-Comptables*

Issuer C: *FR*

Subject CN: *Ordre des Experts-Comptables - région Montpellier*

Subject OU: *0002 776038077*

Subject O: *CROEC de Montpellier*

Subject C: *FR*

Valid from: *Tue May 10 02:00:00 CEST 2011*

Valid to: *Tue Dec 31 02:00:00 CET 2019*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:CE:A7:23:7E:88:61:F5:A9:1E:C3:BD:C2:FE:DB:36:6F:BC:EC:84:05:71:5C:B1:F1:B0:75:16:0F:4D:DF:8A:CC:36:4B:A6:3A:7C:5B:28:56:5A:FA:D0:AC:33:5C:80:66:D6:57:84:A2:5B:77:31:1E:41:30:12:1A:77:62:6C:05:B9:51:CD:E4:8F:EC:62:45:F7:29:47:FC:4D:81:09:F6:4D:12:DE:B9:73:E3:F6:7D:50:B1:5D:CE:14:A3:71:BA:44:E6:B0:BA:09:07:6F:C4:13:38:18:6D:1F:E0:2D:8A:AC:10:2A:5E:E7:04:37:00:99:93:50:53:A0:B7:F5:3B:89:36:65:56:E5:34:B1:B8:7A:AF:77:41:B6:19:E4:37:C5:27:B8:89:63:4B:A9:EB:94:FC:61:35:8F:E2:19:0C:F3:97:C8:44:C2:FF:09:05:55:5C:1E:67:A9:37:1D:AA:9E:3F:FD:3C:62:C9:9A:F7:89:7D:4A:91:D4:48:11:39:95:3C:48:85:8C:3B:B6:FF:C4:15:B6:9E:15:92:3F:30:4E:7C:96:43:56:02:06:11:09:6F:48:26:C9:B8:41:E7:FA:2E:CA:51:5E:06:EF:59:01:A2:A5:82:8E:70:9B:6D:7A:43:FA:66:1F:53:F1:25:DD:0C:97:33:2F:03:7E:71:02:03:01:00:01

Certificate Policies *Policy OID: 2.5.29.32.0*

CPS pointer: http://seec.experts-comptables.fr/PC/PCRacine_Ordre_des_Experts-Comptables.pdf

Basic Constraints *IsCA: true - Path length: 0*

CRL Distribution Points *http://seec.experts-comptables.fr/CRL/CRLRacine_Ordre_des_Experts-Comptables.crl*

Subject Key Identifier *60:4D:B1:66:22:83:5A:25:54:A9:E8:7B:1D:08:45:1C:6F:05:7F:91*

Authority Key Identifier *81:07:39:E3:0F:7A:46:0F:B9:7D:E9:5D:62:76:F5:24:95:1C:15:56*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *C6:C6:FD:7A:C3:49:A0:6E:CF:7D:19:EF:01:3D:20:12:9C:A5:09:5E:EB:FD:BD:CC:8D:C2:9B:9B:3B:26:00:E8*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2018-01-30T01:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS101456/QCPPublic*

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Signature-3-Stars*

TSP Service Definition URI

URI *[fr]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

URI *[en]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

11.17.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.17.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Montpellier RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Montpellier RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - région Montpellier*

Subject OU: *0002 776038077*

Subject O: *CROEC de Montpellier*

Subject C: *FR*

X509SKI

X509 SK I *YE2xZiKDWiVUqeh7HQhFHG8Ff5E=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

11.17.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.17.3 - History instance n.2 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Montpellier RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Montpellier RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - région Montpellier*

Subject OU: *0002 776038077*

Subject O: *CROEC de Montpellier*

Subject C: *FR*

X509SKI

X509 SK I *YE2xZiKDWiVUqeh7HQhFHG8Ff5E=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2012-11-25T23:00:00Z*

11.18 - Service (withdrawn): Ordre des Experts-Comptables - région Orléans RGS***

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Orléans RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Orléans RGS****

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *149195932617851929706575616016738349073543 1*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIFuTCCA6GgAwIBAgISESB5cjWh4XqPVG+wcGF4ga1HMA0GCSqGSIb3DQEBCwUAMHQxCzAJBgNV
BAYTAkZSMSUwIwYDVQQKExxPcmRyZSBkZXMgRXhwZXJ0cy1Db21wdGFibGVzMRcwFQYDVQQLEw4w
MDAyIDc3NTY3MDAwMzElMCMGA1UEAxMcT3JkcmUgZGVzIEV4cGVydHMtQ29tcHRhYmxlczAeFw0x
MTA1MTAwMDAwMDBaFw0xOTEyMzEwMTAwMDBaMHsxCzAJBgNVBAYTAkZSMRkwFwYDVQQKDBBDUk9F
QyBkJ09ybMOpYW5zMRcwFQYDVQQLEw4wMDAyIDc3NTUwMTM2NDE4MDYGA1UEAwwvT3JkcmUgZGVz

lEV4cGVydHMtQ29tcHRhYmxlcyAtIHLDqWdpb24gT3Jsw6lhbnMwggEiMA0GCSqGSIb3DQEBAQUA
A4IBDwAwggEKAoIBAQC4VyUjYpN84e6nSj+ISgEj/JYUeKZcwPjc5MX3qAmijjzjwizdr5gTxiAb
fj0/Binf3smzhk7IsQFaxX/B8j8RSIAnF4D8KLC1zG3/t33yllFqH9WMuOyzOjxp78yw/RPh5fDb
7YMAoh6WLHYnqhHqgcY645JeSR/RXpbPwVug6OiMWPyh9fiM6j0iqlHJFquOWdWLG2gc90cBdynY
2fpx6eNyAQCn6fl3yCfijtsShfNRAwrTJ/EvUBH+cr7dUEoXMyVrX6O+9A7/NE8kQdodIUpOc1HR
5WNyV3u97nCdqDzZzn8t4p+dIjNvbTVzTkqkRgJhpubP/xY2NHCCXlyZAgMBAAGjggE8MIIBODAO
BgNVHQ8BAf8EBAMCAQYwbwYDVR0gBGgwZjBkBgRVHSAAMFwwWgYIKwYBBQUHAgEWTmh0dHA6Ly9z
ZWVjLmV4cGVydHMtY29tcHRhYmxlcy5mci9QQy1JhY2luZV9PcmRyZV9kZXNfRXhwZXJ0cy1D
b21wdGFibGVzLnBkZjASBgNVHRMBAf8ECDAGAQH/AgEAMGEGA1UdHwRaMFgwVqBUoFKGUGh0dHA6
Ly9zZWVjLmV4cGVydHMtY29tcHRhYmxlcy5mci9DUkwvQ1JMUmFjaW5lX09yZHJlX2Rlc19FeHBl
cnRzLUNvbXB0YWJsZXMuY3JsMB0GA1UdDgQWBBRmN+k1ZuYonbI1BEHXiDx3rPSBMzAfBgNVHSME
GDAWgBSBBznjD3pGD7l96V1idvUklRwVVjANBgkqhkiG9w0BAQsFAAOCAgEAH0bPwvlsp7JFh6L4
5LulTXky4TLy0GHC2TML6rfSOaJr+7hgsCdKA0GZERjybgVaYebqpBMt46dZ9P1i/r6hZVULfMSv
AdLTImrpgUBTDAIiZ+e2s3Gfbv+gb5AzDzUxolUUz9TCaa/MqdfdWJOuf2yqVIW66nwkj5pOu3Ov
ReoVR+dBDH+n35sVPjJRmu0mWglTtQ5hCKlV5QxqHMMDBtQmIXrxbGhd9YQaQFNCq536BprULRFu
0HbBra3xzZABF7pyujhKKqRQDlNUwmvbMjuzLIQ28UQbNLTa4LbuE808ER3OTqBggWFnXp0rXz6X
C40d9KJ/EzHHNMGCy9fwktqLAGFsKGBzQutCVbFjznoIlid0f1C1LrgCiE94xWAiGXbceQXGdbQA
2S43R+8Vkcpkc/cVie+h3fEuMbGsnEJDPxSxx/mRwZD/ZlANjSa2KB6u2V2D3rfmJNZ77VrOpILF
oJIyV9UFgHJftIi4SBFWhfaSTkYGCGes05qVaVSLwk4tqEAvnHjSTaF+ItLhRkEA5ZdVwL40NrJr
a/dzUYxzgbuQfLoplrAHBmPnBO7Wefuri+skTXz0UGw6/sHp048XcffehlGzllnEZHGYiqn1a9qN
yElYzKSqNxs4ul63C9xJL5WTmYhH+LUNPqz7L2kQAqMGPy/F72YfuELOk+Y=

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Ordre des Experts-Comptables*

Issuer OU: *0002 775670003*

Issuer O: *Ordre des Experts-Comptables*

Issuer C: *FR*

Subject CN: *Ordre des Experts-Comptables - région Orléans*

Subject OU: *0002 775501364*

Subject O: *CROEC d'Orléans*

Subject C: *FR*

Valid from: *Tue May 10 02:00:00 CEST 2011*

Valid to: *Tue Dec 31 02:00:00 CET 2019*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:B8:57:25:23:62:93:7C:E1:EE:A7:4A:3F:88:4A:01:23:F
C:96:14:78:A6:5C:C0:F8:DC:E4:C5:F7:A8:09:A2:8E:3C:E3:C2:2C:DD:AF:98:13:C6:20:1B:7E:3D:3F:06:29:DF:DE:C9:B3:86:4E:C8:B1:01:5A:C5:7F:C1:F2:3F:11:48:
80:27:17:80:FC:28:B0:B5:CC:6D:FF:B7:7D:F2:96:51:6A:1F:D5:8C:B8:EC:B3:3A:3C:69:EF:CC:B0:FD:13:E1:E5:F0:DB:ED:83:00:A2:1E:96:2C:76:27:AA:11:EA:81:C6
:3A:E3:92:5E:49:1F:D1:5E:96:CF:C1:5B:A0:E8:E8:8C:58:FC:A1:F5:F8:8C:EA:3D:22:AA:51:C9:16:AB:8E:59:D5:8B:1B:68:1C:F7:47:01:77:29:D8:D9:FA:71:E9:E3:7
2:01:00:A7:E9:F9:77:C8:27:E2:8E:DB:12:85:F3:51:03:0A:D3:27:F1:2F:50:11:FE:72:BE:DD:50:4A:17:33:25:6B:5F:A3:BE:F4:0E:FF:34:4F:24:41:DA:1D:21:4A:4E:7
3:51:D1:E5:63:72:57:7B:BD:EE:70:9D:A8:3C:D9:CE:7F:2D:E2:9F:9D:22:33:6F:6D:35:73:4E:4A:A4:46:02:61:A6:E6:CF:FF:16:36:34:70:82:5E:5C:99:02:03:01:00:0
1

Certificate Policies *Policy OID: 2.5.29.32.0*

CPS pointer: http://seec.experts-comptables.fr/PC/PCRacine_Ordre_des_Experts-Comptables.pdf

Basic Constraints *IsCA: true - Path length: 0*

CRL Distribution Points *http://seec.experts-comptables.fr/CRL/CRLRacine_Ordre_des_Experts-Comptables.crl*

Subject Key Identifier *66:37:E9:35:66:E6:28:9D:B2:35:04:41:D7:88:3C:77:AC:F4:81:33*

Authority Key Identifier *81:07:39:E3:0F:7A:46:0F:B9:7D:E9:5D:62:76:F5:24:95:1C:15:56*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *8D:6D:55:F2:B8:68:95:AE:BD:25:84:E8:A8:C1:13:FA:84:02:65:E8:50:9A:B3:F5:B4:89:8E:EE:B0:95:A6:D9*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2018-01-30T01:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS101456/QCPPublic*

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Signature-3-Stars*

TSP Service Definition URI

URI *[fr]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

URI *[en]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

11.18.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.18.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Orléans RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Orléans RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - région Orléans*

Subject OU: *0002 775501364*

Subject O: *CROEC d'Orléans*

Subject C: *FR*

X509SKI

X509 SK I *ZjfpNWbmKJ2yNQRB14g8d6z0gTM=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

11.18.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.18.3 - History instance n.2 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Orléans RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Orléans RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - région Orléans*

Subject OU: *0002 775501364*

Subject O: *CROEC d'Orléans*

Subject C: *FR*

X509SKI

X509 SK I *ZjfpNWbmKJ2yNQRB14g8d6z0gTM=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2012-11-25T23:00:00Z*

11.19 - Service (withdrawn): Ordre des Experts-Comptables - région Paris RGS***

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Paris RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Paris RGS****

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *149198836186490014995497479821635176221378 3*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIF0TCCA7mgAwIBAgISESCPSkd/WsYOVbhZqdHIaeuXMA0GCSqGSIb3DQEBCwUAMHQxCzAJBgNV
BAYTAkZSMSUwIwYDVQQKExxPcmRyZSBkZXMgRXhwZXJ0cy1Db21wdGFibGVzMRcwFQYDVQQLEw4w
MDAyIDc3NTY3MDAwMzElMCMGA1UEAxMcT3JkcmUgZGVzIEV4cGVydHMtQ29tcHRhYmxlczAeFw0x
MTA1MTAwMDAwMDBaFw0xOTEyMzEwMTAwMDBaMIGSMQswCQYDVQQGEwJGUjElMCMGA1UEChMcQ1JP
RUMgZGUgUGFyaXMgSWxlLWRlLUZyYW5jZTEXMBUGA1UECxMOMDAwMiA3ODQ4NTQ0MDgxQzBBBgNV
BAMMOk9yZHJlIGRlcyBFeHBlcnRzLUNvbXB0YWJsZXMgLSByw6lnaW9uIFBhcmlzIElsZS1kZS1G
cmFuY2UwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCy5FHJSjzN8JgipCB8yUMfSLlv
/18ztiYIWF23rTb2kIiiF6PxtQ5CLplBoNaROFAxCv9IrxpwSApP7EjLbR2HX1zqomZ6A8WeZl4q
ClOtWlH4Xc95/56L4h40oVyM0wdq3mx9Ik/uyETQQjSTIRFY4dECW2Py2NWrZJeSfvADjEB28zuK
kCMWIpYaMiWFRUiMZglrEqx87a0bo6dKG2jOKmN32+tO6h9C8Jd5OxEGOlo4cvWF239fxYjYSbNb
Fpcby92+vdwJ/yrtlV+poToDPe40sS6lp+VOAsDzPKynLWQKX4w/knmq/v7yrRcAgJfjlo0cW/tK
R2P615SzV6rFAgMBAAGjggE8MIIBODAOBgNVHQ8BAf8EBAMCAQYwbwYDVR0gBGgwZjBkBgRVHSAA
MFwwWgYIKwYBBQUHAgEWTmh0dHA6Ly9zZWVjLmV4cGVydHMtY29tcHRhYmxlcy5mci9QQy9QQ1Jh
Y2luZV9PcmRyZV9kZXNfRXhwZXJ0cy1Db21wdGFibGVzLnBkZjASBgNVHRMBAf8ECDAGAQH/AgEA
MGEGA1UdHwRaMFgwVqBUoFKGUGh0dHA6Ly9zZWVjLmV4cGVydHMtY29tcHRhYmxlcy5mci9DUkwv
Q1JMUmFjaW5lX09yZHJlX2Rlc19FeHBlcnRzLUNvbXB0YWJsZXMuY3JsMB0GA1UdDgQWBBSHSdzp
2Hys7GQG+gF1cw0rHOe77DAfBgNVHSMEGDAWgBSBBznjD3pGD7l96V1idvUklRwVVjANBgkqhkiG
9w0BAQsFAAOCAgEACv9IAVALuerl7JfjGPLf1NZl+z3wi5UdHm2RRKci7cpqeGiRP9MZ7XZy17pz
kR+aWhG20Z73LATJkKXzEOd2MJhGsumpqVvNAGd1g2x8bNeEuFnTf9xfeZJznOThC6kHIr4lFo4f
sNzeqlSZxtU/UN8208hNQeMHgTh3SsWLFK1Bhtq0DS/if1UVknRUooqpQcGli317VqoFKR3KJLiA
uql6k9qOgmgtY+gg3uupWCsL/dKOG8qeh/WkIyQpdryyhAxUmega4zdA89GvsHKZAT+G7iyXRCXQ
IOUf+lDY6r/YRViqSFjN5iwhuRt2Lm+UiMPR8r7iKKAyhEAycacGouDZnoG4OOf/5QUKskQ1vwGQ

6RoYEVZRqkBNe/P7gLf2LtES4e6WQ27U4QYkPclIyiedhlrICl8kxztG/Jm41+l+Kn7e66pV9IGD
P2oGEcz2CEDyg4vHl/lqwum9I8LeenJ+zVQM8gCXv89Nw19k6LkfCLl0WOk21w239c8VV1baQ20F
EiHEtIbxEXCTA6XUX4Z1P3mssnPBT6O+f7zEuOJif2kUmbfjmXKL8J+9YtbRvKYILsiAeFf4GRat
OpRNMX8lfGB0+Z40pCYO/6fepIL92fuGHdkGClV/8nuGeuHwcbcIpb2q+QZ+Hzpnthz16kxFxCiE
mhlJXPT2eMGIHM8=

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Ordre des Experts-Comptables*

Issuer OU: *0002 775670003*

Issuer O: *Ordre des Experts-Comptables*

Issuer C: *FR*

Subject CN: *Ordre des Experts-Comptables - région Paris Ile-de-France*

Subject OU: *0002 784854408*

Subject O: *CROEC de Paris Ile-de-France*

Subject C: *FR*

Valid from: *Tue May 10 02:00:00 CEST 2011*

Valid to: *Tue Dec 31 02:00:00 CET 2019*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:B2:E4:51:C9:4A:3C:CD:F0:98:22:A4:20:7C:C9:43:1F:48:B9:6F:FF:5F:33:B6:26:08:58:5D:B7:AD:36:F6:90:88:A2:17:A3:F1:B5:0E:42:2E:99:41:A0:D6:91:38:50:31:0A:FF:48:AF:1A:70:48:0A:4F:EC:48:CB:6D:1D:87:5F:5C:EA:A2:66:7A:03:C5:9E:66:5E:2A:08:83:AD:5A:51:F8:5D:CF:79:FF:9E:8B:E2:1E:34:A1:5C:8C:D3:07:6A:DE:6C:7D:22:4F:EE:C8:44:D0:42:34:93:21:11:58:E1:D1:02:5B:63:F2:D8:D5:AB:64:97:92:7E:F0:03:8C:40:76:F3:3B:8A:90:23:16:22:96:1A:32:25:85:45:48:8C:66:09:6B:12:AC:7C:ED:AD:1B:A3:A7:4A:1B:68:CE:2A:63:77:DB:EB:4E:EA:1F:42:F0:97:79:3B:11:06:3A:5A:38:72:F5:85:DB:7F:5F:C5:88:D8:49:B3:5B:16:97:1B:CB:DD:BE:BD:DC:09:FF:2A:ED:95:5F:A9:A1:3A:03:3D:EE:34:B1:2E:A5:A7:E5:4E:02:C0:F3:3C:AC:A7:2D:64:0A:5F:8C:3F:92:79:AA:FE:FE:F2:AD:17:00:80:97:E3:96:8D:1C:5B:FB:4A:47:63:FA:D7:94:B3:57:AA:C5:02:03:01:00:01

Certificate Policies *Policy OID: 2.5.29.32.0*

CPS pointer: http://seec.experts-comptables.fr/PC/PCRacine_Ordre_des_Experts-Comptables.pdf

Basic Constraints *IsCA: true - Path length: 0*

CRL Distribution Points *http://seec.experts-comptables.fr/CRL/CRLRacine_Ordre_des_Experts-Comptables.crl*

Subject Key Identifier *87:49:DC:E9:D8:7C:AC:EC:64:06:FA:01:75:73:0D:2B:1C:E7:BB:EC*

Authority Key Identifier *81:07:39:E3:0F:7A:46:0F:B9:7D:E9:5D:62:76:F5:24:95:1C:15:56*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *F6:E5:88:91:F2:D2:06:55:42:BD:BE:F7:EC:A2:F8:F8:3F:BE:4E:CF:6E:46:78:08:F7:BC:D7:CA:AE:91:30:3F*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2018-01-30T01:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS101456/QCPPublic*

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Signature-3-Stars*

TSP Service Definition URI

URI *[fr]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

URI *[en]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

11.19.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.19.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Paris RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Paris RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - région Paris Ile-de-France*

Subject OU: *0002 784854408*

Subject O: *CROEC de Paris Ile-de-France*

Subject C: *FR*

X509SKI

X509 SK I *h0nc6dh8rOxkBvoBdXMNKxznu+w=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

11.19.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.19.3 - History instance n.2 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Paris RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Paris RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - région Paris Ile-de-France*

Subject OU: *0002 784854408*

Subject O: *CROEC de Paris Ile-de-France*

Subject C: *FR*

X509SKI

X509 SK I *h0nc6dh8rOxkBvoBdXMNKxznu+w=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2012-11-25T23:00:00Z*

11.20 - Service (withdrawn): Ordre des Experts-Comptables - région Pays de Loire RGS***

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Pays de Loire RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Pays de Loire RGS****

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *149192845227011358595176876062893050961522O*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIFxTCCA62gAwIBAgISESBiOBxsjvxe26WQ5x56STB0MA0GCSqGSIb3DQEBCwUAMHQxCzAJBgNV
BAYTAkZSMSUwIwYDVQQKExxPcmRyZSBkZXMgRXhwZXJ0cy1Db21wdGFibGVzMRcwFQYDVQQLEw4w
MDAyIDc3NTY3MDAwMzElMCMGA1UEAxMcT3JkcmUgZGVzIEV4cGVydHMtQ29tcHRhYmxlczAeFw0x
MTA1MTAwMDAwMDBaFw0xOTEyMzEwMTAwMDBaMIGGMQswCQYDVQQGEwJGUjEfMB0GA1UEChMWQ1JP
RUMgZGUgUGF5cyBkZSBMb2lyZTEXMBUGA1UECxMOMDAwMiAzMzI2MDM2MDQxPTA7BgNVBAMMNE9y
ZHJlIGRlcyBFeHBlcnRzLUNvbXB0YWJsZXMgLSByw6lnaW9uIFBheXMgZGUgTG9pcmUwggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDVZES4Q604dMMIUiP4Zs8zs9Zskb5X7aRFI54+Wei8
PlOzQZYoX7V2sszOyyQnmGU5begNZVefeC+oURfSV9HoGxDzjN1hhLRrygCPHVL3SxHUNQGzfzrT
wFarjvoVZQHr8z+MPXWYChvrkox+ks9vgIfhemJPKk5Jp4MccCYChJ6y6kgEzyet4DUaQ8qsMVlJ
voQTwM/KQw7VZOgF1DfNeCQuUmUomUglMblMJf2JyOtLKu7vxXAtYqQrsL/8krHYIbnYoh61qNO7
XQzlhwbevbGjsWgvHODnnQwrvq6EdaI7JqGqwizQocmK1dTXpapMkuFjYLhv/C399HPAfh5xAgMB
AAGjggE8MIIBODAOBgNVHQ8BAf8EBAMCAQYwbwYDVR0gBGgwZjBkBgRVHSAAMFwwWgYIKwYBBQUH
AgEWTmh0dHA6Ly9zZWVjLmV4cGVydHMtY29tcHRhYmxlcy5mci9QQy9QQ1JhY2luZV9PcmRyZV9k
ZXNfRXhwZXJ0cy1Db21wdGFibGVzLnBkZjASBgNVHRMBAf8ECDAGAQH/AgEAMGEGA1UdHwRaMFgw
VqBUoFKGUGh0dHA6Ly9zZWVjLmV4cGVydHMtY29tcHRhYmxlcy5mci9DUkwvQ1JMUmFjaW5lX09y
ZHJlX2Rlc19FeHBlcnRzLUNvbXB0YWJsZXMuY3JsMB0GA1UdDgQWBBSHAZ3QViH4tHnWG6049g7p
wu/LUjAfBgNVHSMEGDAWgBSBBznjD3pGD7l96V1idvUklRwVVjANBgkqhkiG9w0BAQsFAAOCAgEA
CMLTlP0/HScutals8cETNVgnZ7cuC949BVX8rJsvKvDEgIYVxk5L5NpY+fW9CvsXi5k4AlouImVj
5QoVVDSB5kextFlg91CxDqjICyN5cJACS3Z3smGgP6iCYBLy/hIKWuAIsHOttgkFE5YcKF/3BaKD
klyODepDEnwbH/B8u29MsgAv1YteI0l/UPwaHI2pCTH+SxDjAwsIa69bqYIY+a4MnOT9XNYmd8Wy
H/Sb1yrKakKB86z5JTPdx8iO88cI497tnq10NbYk9tWzCPapmHAdDvSTfghZfs824RvD/hCn6sUV
bgcXpGOg517u0LZSe6ji3/iPatk0/viV9aDtZQltZiSqaYdw+m+RQDahPyy+C7CirFXHcRAMay0Y
A2ZLz4D8bdR0Gg/HboVnUxnCGfTOAimu+qsDCGkenU2qcynHHWQ1sqV3N9zhvwzp7z2sLyScuA0U
SfeonO2qq4kWMMVCgLEtMGIOD3hiNoaMFWxtS3jETXLBZUb6yaAfxmbnJ3qQB4SqaMOSQUadpmay
khVGcVEP40czOEvNvW03cN6B68Q0xoX36RcHhDNDDIroWAwNWvnswr30vyujsKauhFkF4r0kQ3Mx
81M2vdCib5UI76P2P9x4Yj4asTuz7uqxQpPLkJMx5mitJvT65cNd/Mnp2NJaiLFvLkRcYVHFO3o=

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Ordre des Experts-Comptables*

Issuer OU: *0002 775670003*

Issuer O: *Ordre des Experts-Comptables*

Issuer C: *FR*

Subject CN: *Ordre des Experts-Comptables - région Pays de Loire*

Subject OU: *0002 332603604*

Subject O: *CROEC de Pays de Loire*

Subject C: *FR*

Valid from: *Tue May 10 02:00:00 CEST 2011*

Valid to: *Tue Dec 31 02:00:00 CET 2019*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:D5:64:44:B8:43:AD:38:74:C3:08:52:23:F8:66:CF:33:B3:D6:6C:91:BE:57:ED:A4:45:23:9E:3E:59:E8:BC:3E:53:B3:41:96:28:5F:B5:76:B2:CC:CE:CB:24:27:98:65:39:6D:E8:0D:65:57:9F:78:2F:A8:51:17:D2:57:D1:E8:1B:10:F3:8C:DD:61:84:B4:6B:CA:00:8F:1D:52:F7:4B:11:D4:35:01:B3:7F:3A:D3:C0:56:AB:8E:FA:15:65:01:EB:F3:3F:8C:3D:75:98:0A:1B:EB:92:8C:7E:92:CF:6F:80:87:E1:7A:62:4F:2A:4E:49:A7:83:1C:70:26:02:84:9E:B2:EA:48:04:CF:27:AD:E0:35:1A:43:CA:AC:31:59:49:BE:84:13:C0:CF:CA:43:0E:D5:64:E8:05:D4:37:CD:78:24:2E:52:65:28:99:48:25:31:B9:4C:25:FD:89:C8:EB:4B:2A:EE:EF:C5:70:2D:62:A4:2B:B0:BF:FC:92:B1:D8:21:B9:D8:A2:1E:B5:A8:D3:BB:5D:0C:E5:87:06:DE:BD:B1:A3:B1:68:2F:1C:E0:E7:9D:0C:2B:BE:AE:84:75:A2:3B:26:A1:AA:C2:2C:D0:A1:C9:8A:D5:D4:D7:A5:AA:4C:92:E1:63:60:B8:6F:FC:2D:FD:F4:73:C0:7E:1E:71:02:03:01:00:01

Certificate Policies *Policy OID: 2.5.29.32.0*

CPS pointer: http://seec.experts-comptables.fr/PC/PCRacine_Ordre_des_Experts-Comptables.pdf

Basic Constraints *IsCA: true - Path length: 0*

CRL Distribution Points *http://seec.experts-comptables.fr/CRL/CRLRacine_Ordre_des_Experts-Comptables.crl*

Subject Key Identifier *87:01:9D:D0:56:21:F8:B4:79:D6:1B:AD:38:F6:0E:E9:C2:EF:CB:52*

Authority Key Identifier *81:07:39:E3:0F:7A:46:0F:B9:7D:E9:5D:62:76:F5:24:95:1C:15:56*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *0C:B9:E8:6C:85:DD:45:1D:72:73:E2:80:9E:CE:5B:9E:42:A7:2A:74:C9:CE:CE:B0:A9:E2:E3:91:54:97:D0:00*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2018-01-30T01:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS101456/QCPPublic*

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Signature-3-Stars*

TSP Service Definition URI

URI *[fr]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

URI *[en]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

11.20.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.20.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Pays de Loire RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Pays de Loire RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - région Pays de Loire*

Subject OU: *0002 332603604*

Subject O: *CROEC de Pays de Loire*

Subject C: *FR*

X509SKI

X509 SK I *hwGd0FYh+LR51hutOPYO6cLvy1I=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

11.20.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.20.3 - History instance n.2 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Pays de Loire RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Pays de Loire RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - région Pays de Loire*

Subject OU: *0002 332603604*

Subject O: *CROEC de Pays de Loire*

Subject C: *FR*

X509SKI

X509 SK I *hwGd0FYh+LR51hutOPYO6cLvy1I=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2012-11-25T23:00:00Z*

11.21 - Service (withdrawn): Ordre des Experts-Comptables - région Picardie RGS***

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Picardie RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Picardie RGS****

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *149206651785829213532327730916647693950861 4*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIFzTCCA7WgAwIBAgISESDKFpN6fCbladBEC4bchDuGMA0GCSqGSIb3DQEBCwUAMHQxCzAJBgNV
BAYTAkZSMSUwIwYDVQQKExxPcmRyZSBkZXMgRXhwZXJ0cy1Db21wdGFibGVzMRcwFQYDVQQLEw4w
MDAyIDc3NTY3MDAwMzElMCMGA1UEAxMcT3JkcmUgZGVzIEV4cGVydHMtQ29tcHRhYmxlczAeFw0x
MTA1MTAwMDAwMDBaFw0xOTEyMzEwMTAwMDBaMIGOMQswCQYDVQQGEwJGUjEjMCEGA1UEChMaQ1JP
RUMgZGUgUGljYXJkaWUtQXJkZW5uZXMxFzAVBgNVBAsTDjAwMDIgNzgwNjAxODAzMUEwPwYDVQQD
DDhPcmRyZSBkZXMgRXhwZXJ0cy1Db21wdGFibGVzIC0gcsOpZ2lvbiBQaWNhcmRpZS1BcmRlbm5l
czCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALaPHV/rC0+0tQ7Lq4LPPN4MVQYOjHzO
Io5TDPgkBJoPriiKoiX0QeVvsJWXGDprIuN9yrjlSJ1KkHPtLBkIbWtH3XcYbRy1kpTXhvMgx9j9
hjtKJhX836eZvRMqSVbop3b2W7GyA5/blnWpbopinPAhPgl38Kezu0+AZBn5X3OX0Q57snyKXDRP
/lQfd8NDES0Jav1iI+GDFT5/c4o8NIUh9zSgftIp0g+gmHJuvVCHtpIgyA2y8H7Rq3uvp9rvMDsT
TiMKGGsY/2eUi/2kdCS2G8rrGszmNOAVOUXv9CkCYMiH+N1UfBwPw49uXzO+dIvKX/54cncYGlwr
WxX/hFsCAwEAAaOCATwwggE4MA4GA1UdDwEB/wQEAwIBBjBvBgNVHSAEaDBmMGQGBFUdIAAwXDBa
BggrBgEFBQcCARZOaHR0cDovL3NlZWMuZXhwZXJ0cy1jb21wdGFibGVzLmZyL1BDL1BDUmFjaW5l
X09yZHJlX2Rlc19FeHBlcnRzLUNvbXB0YWJsZXMucGRmMBIGA1UdEwEB/wQIMAYBAf8CAQAwYQYD
VR0fBFowWDBWoFSgUoZQaHR0cDovL3NlZWMuZXhwZXJ0cy1jb21wdGFibGVzLmZyL0NSTC9DUkxS
YWNpbmVfT3JkcmVfZGVzX0V4cGVydHMtQ29tcHRhYmxlcy5jcmwwHQYDVR0OBBYEFHQ0lVbCn0aY
v8gTdDcJca8wljobMB8GA1UdIwQYMBaAFIEHOeMPekYPuX3pXWJ29SSVHBVWMA0GCSqGSIb3DQEB
CwUAA4ICAQAW3EB5spUECFA40sEE2bme8y2Fa0bUixNNhMMHPgPDZylNGa5k78fDvDtPml9DK2GU
bFyMctQq9zxK90f5aQWPWh7WqGxNr8ETi7GOZ9rU1vmAvA1H1ZZCGhKL2HqYTKJa80YYHEZ75JPA
M0zAoLSR4Y7v6oY/Af/nsWCm6ud3QkoieWDoKcGWjtjynTiWSuWR1oWJB1aWzdkRzx+iHpfLus5G
0VXE7x5tQdjAO0WMBQdvEUZ2nsQsUDd1gDHd71wM3oK0q5wfaj9symutQ2Cs4+T+xjludO7xsdYn
Pt7IFhvxLOXYmc7Od17ddWPkJdmCCTcVayL/jHtNCMyWZp2PMj9tHiEAIUaQt5fZxWMqk2d10ptY
qzxkRs+5fee8EyMD9kNYkwLrpl9ws7ZUtk7MuLsXMaENhx9mmHE4al+8LrfZpZWEn9g0RyqJJbcz
Pw8mICQ9zudlMAOt7qmZoM79p9Dw7U9yLgHME+kIItCvCYZ/qWPmJNZJvpC9x+W6guFdhQNlcmU+
gWHr/EYFYdOQG6xIlJLS4bMY3zEUJr63HWSNSfNC8fvIw+zmcR9azBuiKGwH7jmDYbLonV94ERAB
AoO63GdCIs/F2vS58QaII54dSz3oKxEOGN6EBlpGD8NZDIOQifgZ46SxLdMyCvkEO82aiI9RUIJM
MobuT2sscg==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Ordre des Experts-Comptables*

Issuer OU: *0002 775670003*

Issuer O: *Ordre des Experts-Comptables*

Issuer C: *FR*

Subject CN: *Ordre des Experts-Comptables - région Picardie-Ardennes*

Subject OU: *0002 780601803*

Subject O: *CROEC de Picardie-Ardennes*

Subject C: *FR*

Valid from: *Tue May 10 02:00:00 CEST 2011*

Valid to: *Tue Dec 31 02:00:00 CET 2019*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:B6:8F:1D:5F:EB:0B:4F:B4:B5:0E:CB:AB:82:CF:3C:DE:0C:55:06:0E:8C:7C:CE:22:8E:53:0C:F8:24:04:9A:0F:AE:28:8A:A2:25:F4:41:E5:6F:B0:95:97:18:3A:6B:22:E3:7D:CA:B8:C8:48:9D:4A:90:73:ED:2C:19:08:6D:6B:47:DD:77:18:6D:1C:B5:92:94:D7:86:F3:20:C7:D8:FD:86:3B:4A:26:15:FC:DF:A7:99:BD:13:2A:49:56:E8:A7:76:F6:5B:B1:B2:03:9F:DB:96:75:A9:6E:8A:62:9C:F0:21:3E:09:77:F0:A7:B3:BB:4F:80:64:19:F9:5F:73:97:D1:0E:7B:B2:7C:8A:5C:34:4F:FE:54:1F:77:C3:43:11:2D:09:6A:FD:62:23:E1:83:15:3E:7F:73:8A:3C:34:85:21:F7:34:A0:7E:D2:29:D2:0F:A0:98:72:6E:BD:50:87:B6:92:20:C8:0D:B2:F0:7E:D1:AB:7B:AF:A7:DA:EF:30:3B:13:4E:23:0A:18:6B:18:FF:67:94:8B:FD:A4:74:24:B6:1B:CA:EB:1A:CC:E6:34:E0:15:39:45:EF:F4:29:02:60:C8:87:F8:DD:54:7C:1C:0F:C3:8F:6E:5F:33:BE:74:8B:CA:5F:FE:78:72:77:18:1A:5C:2B:5B:15:FF:84:5B:02:03:01:00:01

Certificate Policies *Policy OID: 2.5.29.32.0*

CPS pointer: http://seec.experts-comptables.fr/PC/PCRacine_Ordre_des_Experts-Comptables.pdf

Basic Constraints *IsCA: true - Path length: 0*

CRL Distribution Points *http://seec.experts-comptables.fr/CRL/CRLRacine_Ordre_des_Experts-Comptables.crl*

Subject Key Identifier *74:34:95:56:C2:9F:46:98:BF:C8:13:74:37:09:71:AF:30:22:3A:1B*

Authority Key Identifier *81:07:39:E3:0F:7A:46:0F:B9:7D:E9:5D:62:76:F5:24:95:1C:15:56*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *8A:10:0E:E3:5C:E8:06:B3:B4:5E:42:FB:AC:3D:22:67:95:AC:CB:00:5C:EC:67:0C:D6:C4:99:C8:A6:92:EC:A6*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description

[en] *undefined.*

[fr] *undefined.*

Status Starting Time *2018-01-30T01:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS101456/QCPPublic*

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Signature-3-Stars*

TSP Service Definition URI

URI *[fr]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

URI *[en]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

11.21.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.21.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Picardie RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Picardie RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - région Picardie-Ardennes*

Subject OU: *0002 780601803*

Subject O: *CROEC de Picardie-Ardennes*

Subject C: *FR*

X509SKI

X509 SK I *dDSVVsKfRpi/yBN0NwlxrzAiOhs=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

11.21.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.21.3 - History instance n.2 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Picardie RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Picardie RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - région Picardie-Ardennes*

Subject OU: *0002 780601803*

Subject O: *CROEC de Picardie-Ardennes*

Subject C: *FR*

X509SKI

X509 SK I *dDSVVsKfRpi/yBN0NwlxrzAiOhs=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2012-11-25T23:00:00Z*

11.22 - Service (withdrawn): Ordre des Experts-Comptables - région Poitou Charentes RGS***

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Poitou Charentes RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Poitou Charentes RGS****

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *149186080622245035835939878244051389393426 7*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIF2zCCA8OgAwIBAgISESAvU/TGQDB23pMqnIheXaS7MA0GCSqGSIb3DQEBCwUAMHQxCzAJBgNV
BAYTAkZSMSUwIwYDVQQKExxPcmRyZSBkZXMgRXhwZXJ0cy1Db21wdGFibGVzMRcwFQYDVQQLEw4w
MDAyIDc3NTY3MDAwMzElMCMGA1UEAxMcT3JkcmUgZGVzIEV4cGVydHMtQ29tcHRhYmxlczAeFw0x
MTA1MTAwMDAwMDBaFw0xOTEyMzEwMTAwMDBaMIGcMQswCQYDVQQGEwJGUjEqMCgGA1UECgwhQ1JP

RUMgZGUgUG9pdG91LUNoYXJlbnRlcy1WZW5kw6llMRcwFQYDVQQLEw4wMDAyIDMxMTE0NjM4NTFI
MEYGA1UEAww/T3JkcmUgZGVzIEV4cGVydHMtQ29tcHRhYmxlcyAtIHLDqWdpb24gUG9pdG91LUNo
YXJlbnRlcy1WZW5kw6llMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAy7KlUgsaYji4
JjVBr9m4PKymgwIOtgDVnuOIYCKWiZEo2I8SZ0IPCLMmBXlYH7vzUXGYz739LsngO6k+A1K0H6ez
mbJ2caIe5f0WmtgcalFV1K8eozq/fMESP0+RojKcOC0vsm9nOhJiPmM7S9263AeQSxoWSKBnrXFy
U360zZpdE1zADHoiu69lzW/p0caaz2WJPIBIdbyu+f7jZVF1aeVmuywMSo8zzJFXpYfL/Tx7pjVG
zqPhf9a+o57A2wnAh4SYky1nZ9w5Zi2MtwgV9pocq7Lz+8xu5Apbn48a4nhDw0omg1S21vbHW6yI
e/By1U6pTb62y/hyWcltW3iuNQIDAQABo4IBPDCCATgwDgYDVR0PAQH/BAQDAgEGMG8GA1UdIARo
MGYwZAYEVR0gADBcMFoGCCsGAQUFBwIBFk5odHRwOi8vc2VlYy5leHBlcnRzLWNvbXB0YWJsZXMu
ZnIvUEMvUENSYWNpbmVfT3JkcmVfZGVzX0V4cGVydHMtQ29tcHRhYmxlcy5wZGYwEgYDVR0TAQH/
BAgwBgEB/wIBADBhBgNVHR8EWjBYMFagVKBShlBodHRwOi8vc2VlYy5leHBlcnRzLWNvbXB0YWJs
ZXMuZnIvQ1JML0NSTFJhY2luZV9PcmRyZV9kZXNfRXhwZXJ0cy1Db21wdGFibGVzLmNybDAdBgNV
HQ4EFgQUoIrz9g/S8BoV8SqF2dpFBByL0S0wHwYDVR0jBBgwFoAUgQc54w96Rg+5feldYnb1JJUc
FVYwDQYJKoZIhvcNAQELBQADggIBABqNIq/UBfl8M/yAHuPNeYmASPwWeQO9p/qHa0suwc2Lbg88
xU9pguX2VGJ91AaICf6JwH/QGst9cn7qTz5x16Pms0PfyKiRJ+l9/M6H4IZCUpyoLv2MHp3PsR8g
XaQ23ou8UPVP6aln7m3zeOqeBW3W15oZjTFCG2e+qy5S7NPGBASUKVpF8pMtv+xDKNvjyRxaIAHr
+6y/S0tNyHDYvTWputA4p/wpI14rQS5ecbLKMa7duj1B6Ge/lDzyugqbiNY9KOcd1VTwJImGkcoR
5nR3/dxhLH17DvCC2aoQKM31lXp9UYVdrFE+/J66rLQpmTyWYHBJh6iti+kQX/yd2OO1xjdEvRYj
Nro0zW16miBjdKd1AOGSAxzZO4do9a5/M/ZegMBK53JGOrEJZMBnx+gZwfl6ubDZ3QQa4V1AlnLd
CUQTnIRobfXYs09kDNlRAtVMWGq4J6uZB+i7cgtuv8AuRma4fPtF5/JMOog5KF8j93Hlx46/rZtF
sCMyFUSWq6PXOF9sA77tmOkXejIvaGquuLpmibvZ7Zi2Hzdb0hw3ag3Ecq6A4oO0VXcnlc6dUnTm
SBzu4nrvWJFp9xo0e++9l23Hd+tTqZGgzm353bYQG/fpmFfDH5IuMWTJ3rGdp8S3OsCYyqHKcant
PT2nkbTDDo9hNgUyAHf3G/w8/Cri

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Ordre des Experts-Comptables*

Issuer OU: *0002 775670003*

Issuer O: *Ordre des Experts-Comptables*

Issuer C: *FR*

Subject CN: *Ordre des Experts-Comptables - région Poitou-Charentes-Vendée*

Subject OU: *0002 311146385*

Subject O: *CROEC de Poitou-Charentes-Vendée*

Subject C: *FR*

Valid from: *Tue May 10 02:00:00 CEST 2011*

Valid to: *Tue Dec 31 02:00:00 CET 2019*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:CB:B2:A5:52:0B:1A:62:38:B8:26:35:41:AF:D9:B8:3C:AC:A6:83:02:0E:B6:00:D5:9E:E3:88:60:22:96:89:91:28:D8:8F:12:67:42:0F:08:B3:26:05:79:58:1F:BB:F3:51:71:98:CF:BD:FD:2E:C9:E0:3B:A9:3E:03:52:B4:1F:A7:B3:99:B2:76:71:A2:1E:E5:FD:16:9A:D8:1C:6A:51:55:D4:AF:1E:A3:3A:BF:7C:C1:12:3F:4F:91:A2:32:9C:38:2D:2F:B2:6F:67:3A:12:62:3E:63:3B:4B:DD:BA:DC:07:90:4B:1A:16:48:A0:67:AD:71:72:53:7E:B4:CD:9A:5D:13:5C:C0:0C:7A:22:BB:AF:65:CD:6F:E9:D1:C6:9A:CF:65:89:3C:80:48:75:BC:AE:F9:FE:E3:65:51:75:69:E5:66:BB:2C:0C:4A:8F:33:CC:91:57:A5:87:CB:FD:3C:7B:A6:35:46:CE:A3:E1:7F:D6:BE:A3:9E:C0:DB:09:C0:87:84:98:93:2D:67:67:DC:39:66:2D:8C:B7:08:15:F6:9A:1C:AB:B2:F3:FB:CC:6E:E4:0A:5B:9F:8F:1A:E2:78:43:C3:4A:26:83:54:B6:D6:F6:C7:5B:AC:88:7B:F0:72:D5:4E:A9:4D:BE:B6:CB:F8:72:59:C9:6D:5B:78:AE:35:02:03:01:00:01

Certificate Policies *Policy OID: 2.5.29.32.0*

CPS pointer: http://seec.experts-comptables.fr/PC/PCRacine_Ordre_des_Experts-Comptables.pdf

Basic Constraints *IsCA: true - Path length: 0*

CRL Distribution Points *http://seec.experts-comptables.fr/CRL/CRLRacine_Ordre_des_Experts-Comptables.crl*

Subject Key Identifier *A0:8A:F3:F6:0F:D2:F0:1A:15:F1:2A:85:D9:DA:45:04:1C:8B:D1:2D*

Authority Key Identifier *81:07:39:E3:0F:7A:46:0F:B9:7D:E9:5D:62:76:F5:24:95:1C:15:56*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *32:AF:ED:67:BB:3B:8E:3B:E5:B0:EB:9A:A3:EC:3D:27:D7:A7:09:60:AF:2D:76:D5:76:AC:0D:30:6D:56:B6:14*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2018-01-30T01:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS101456/QCPPublic*

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Signature-3-Stars*

TSP Service Definition URI

URI *[fr]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

URI *[en]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

11.22.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.22.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Poitou Charantes RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Poitou Charantes RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - région Poitou-Charentes-Vendée*

Subject OU: *0002 311146385*

Subject O: *CROEC de Poitou-Charentes-Vendée*

Subject C: *FR*

X509SKI

X509 SK I *oIrz9g/S8BoV8SqF2dpFBByL0S0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

11.22.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.22.3 - History instance n.2 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Poitou Charantes RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Poitou Charantes RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - région Poitou-Charentes-Vendée*

Subject OU: *0002 311146385*

Subject O: *CROEC de Poitou-Charentes-Vendée*

Subject C: *FR*

X509SKI

X509 SK I *oIrz9g/S8BoV8SqF2dpFBByL0S0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2012-11-25T23:00:00Z*

11.23 - Service (withdrawn): Ordre des Experts-Comptables - région Rhône Alpes RGS***

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Rhône Alpes RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Rhône Alpes RGS****

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1491828966718464732086515860691870593166305*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIFwzCCA6ugAwIBAgISESAXX+QHRsmO0H9aLm0bsavhMA0GCSqGSIb3DQEBCwUAMHQxCzAJBgNV
BAYTAkZSMSUwIwYDVQQKExxPcmRyZSBkZXMgRXhwZXJ0cy1Db21wdGFibGVzMRcwFQYDVQQLEw4w
MDAyIDc3NTY3MDAwMzElMCMGA1UEAxMcT3JkcmUgZGVzIEV4cGVydHMtQ29tcHRhYmxlczAeFw0x
MTA1MTAwMDAwMDBaFw0xOTEyMzEwMTAwMDBaMIGEMQswCQYDVQQGEwJGUjEeMBwGA1UECgwVQ1JP
RUMgZGUgUmjDtG5lLUFscGVzMRcwFQYDVQQLEw4wMDAyIDc3OTg5Mzg5MDE8MDoGA1UEAwwzT3Jk
cmUgZGVzIEV4cGVydHMtQ29tcHRhYmxlcyAtIHLDqWdpb24gUmjDtG5lLUFscGVzMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA7KsC9A+TO1Gancp7vvjFCLlp0RfHtnpugJDjqvvahziM
QNcu78vVwbKqGKijB8zNFy0l0N0b9De4E0DofOtRo2fXP4lDKEurZj8pYEVwtebAEsPhBDoOP+iM
VsjDw+XgpIcBUE/xKMIlfpe9R9FldeoWVAqXlJ7cqdAzzKemxHp2g61lGr92QJV9hz/hXgdh4FrM
oZ2QZGwGSRvU33JowAiwCvnqAX8e76g3f88xA094xnwZ+UR7ZRLu4eI6qUZmDIU1V7zIHnrtV4S/
wlAFkUbuEIIuSbIB4GEoIuC1tQ1elS19Z58Z5AwTY82mxtYDzCTFtIcaeloPoEBm4405PwIDAQAB
o4IBPDCCATgwDgYDVR0PAQH/BAQDAgEGMG8GA1UdIARoMGYwZAYEVR0gADBcMFoGCCsGAQUFBwIB
Fk5odHRwOi8vc2VlYy5leHBlcnRzLWNvbXB0YWJsZXMuZnIvUEMvUENSYWNpbmVfT3JkcmVfZGVz
X0V4cGVydHMtQ29tcHRhYmxlcy5wZGYwEgYDVR0TAQH/BAgwBgEB/wIBADBhBgNVHR8EWjBYMFag
VKBShlBodHRwOi8vc2VlYy5leHBlcnRzLWNvbXB0YWJsZXMuZnIvQ1JML0NSTFJhY2luZV9PcmRy
ZV9kZXNfRXhwZXJ0cy1Db21wdGFibGVzLmNybDAdBgNVHQ4EFgQUoVhP5yAg5JbOqpmu8aNZYxvN
L/cwHwYDVR0jBBgwFoAUgQc54w96Rg+5feldYnb1JJUcFVYwDQYJKoZIhvcNAQELBQADggIBAGcc
Xe/1gNbw32i6gyTP1HqZmGWJWLQPofHvmObv69UjhVmbKYPBoaDplkB0NydnPx9l+1UrFOr1qguN
iwYZ1FN5szQob9ZN6Xcwy1hYgaMSnjdrNtyt9TVH15M77ml6wo7jXptU3sAd6NeHF8p5oLnUJV5D
eTJ+aNN/7hzKI+lAYawijCN1HZXoeHjwuUqFSH5634WWy24zBclxt9WP4nCGp30sNs/APaqFnJ6L
4DSuiLNwDuXGHDVyszbCFy7kBksQ6x0qN8Ba9q2WhfLpQrpbKxYsXJyY9H3xpEBjRjRSDM0Qr7ae
xexa3g/Zt5Em4qGGe2EJN8xEiuMXk7dEn6oBwP1VIqSRc5LM2ZnYYIDJy3npg7jHekM+8OqOpYFq

JZwcmvsJ0s3c2FDCGpkzA8gDKWQzV2YWFmUwdkAoi/amL9bansaZhtStPVD35NoIwR4rntOILQWT
43S/SHT7BlIhDH3HwQPny0b9+jneCmxygUglQY2EqkvnODccowVaXunnsDyyBEp3Dw1vNcVArac0
8xWPCSSoGjha+nIDxDMvvDaOv7YC2M5BnRCeTxMn4oaTZ0t+fWDG83s78hcyD9BIlPk3wu+T46Id
6lbC6MEnnVcApqno4LOlo/Gv+LQ97jFZLGrvnRlXiMHcqg2QmcWUkuOIR1d0GCcJAHmXeHCM

-----END CERTIFICATE-----

Signature algorithm:	*SHA256withRSA*
Issuer CN:	*Ordre des Experts-Comptables*
Issuer OU:	*0002 775670003*
Issuer O:	*Ordre des Experts-Comptables*
Issuer C:	*FR*
Subject CN:	*Ordre des Experts-Comptables - région Rhône-Alpes*
Subject OU:	*0002 779893890*
Subject O:	*CROEC de Rhône-Alpes*
Subject C:	*FR*
Valid from:	*Tue May 10 02:00:00 CEST 2011*
Valid to:	*Tue Dec 31 02:00:00 CET 2019*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:EC:AB:02:F4:0F:93:3B:51:9A:9D:CA:7B:BE:F8:C5:08:
B9:69:D1:17:C7:B6:7A:6E:80:90:E3:AA:FB:DA:87:38:8C:40:D7:2E:EF:CB:D5:C1:B2:AA:18:A8:A3:07:CC:CD:17:2D:25:D0:DD:1B:F4:37:B8:13:40:E8:7C:EB:51:A3:
67:D7:3F:89:43:28:4B:AB:66:3F:29:60:45:70:B5:E6:C0:12:C3:E1:04:3A:0E:3F:E8:8C:56:C8:C3:C3:E5:E0:A4:87:01:50:4F:F1:28:C2:25:7E:97:BD:47:D1:65:75:EA:
16:54:0A:97:94:9E:DC:A9:D0:33:CC:A7:A6:C4:7A:76:83:AD:65:1A:BF:76:40:95:7D:87:3F:E1:5E:07:61:E0:5A:CC:A1:9D:90:64:6C:06:49:1B:D4:DF:72:68:C0:08:B
0:0A:F9:EA:01:7F:1E:EF:A8:37:7F:CF:31:03:4F:78:C6:7C:19:F9:44:7B:65:12:EE:E1:E2:3A:A9:46:66:0C:85:35:57:BC:C8:1E:7A:ED:57:84:BF:C2:50:05:91:46:EE:10
:82:2E:49:B2:01:E0:61:28:22:E0:B5:B5:0D:5E:95:2D:7D:67:9F:19:E4:0C:13:63:CD:A6:C6:D6:03:CC:24:C5:B4:87:1A:7A:5A:0F:A0:40:66:E3:8D:39:3F:02:03:01:0
0:01

Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: http://seec.experts-comptables.fr/PC/PCRacine_Ordre_des_Experts-Comptables.pdf*
Basic Constraints	*IsCA: true - Path length: 0*
CRL Distribution Points	*http://seec.experts-comptables.fr/CRL/CRLRacine_Ordre_des_Experts-Comptables.crl*
Subject Key Identifier	*A1:58:4F:E7:20:20:E4:96:CE:AA:99:AE:F1:A3:59:63:1B:CD:2F:F7*
Authority Key Identifier	*81:07:39:E3:0F:7A:46:0F:B9:7D:E9:5D:62:76:F5:24:95:1C:15:56*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*

Thumbprint: *EB:63:10:58:F8:E9:4D:7D:27:E2:08:FA:DC:0E:A7:63:F3:D5:B2:9C:1E:FE:B0:11:6C:A5:05:DF:64:D4:FA:94*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2018-01-30T01:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS101456/QCPPublic*

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Signature-3-Stars*

TSP Service Definition URI

URI *[fr]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

URI *[en]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

11.23.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.23.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Rhône Alpes RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Rhône Alpes RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - région Rhône-Alpes*

Subject OU: *0002 779893890*

Subject O: *CROEC de Rhône-Alpes*

Subject C: *FR*

X509SKI

X509 SK I *oVhP5yAg5JbOqpmu8aNZYxvNL/c=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

11.23.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.23.3 - History instance n.2 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Rhône Alpes RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Rhône Alpes RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - région Rhône-Alpes*

Subject OU: *0002 779893890*

Subject O: *CROEC de Rhône-Alpes*

Subject C: *FR*

X509SKI

X509 SK I *oVhP5yAg5JbOqpmu8aNZYxvNL/c=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2012-11-25T23:00:00Z*

11.24 - Service (withdrawn): Ordre des Experts-Comptables - région Rouen Normandie RGS***

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Rouen Normandie RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Rouen Normandie RGS****

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *149203623077734731989018954395504054990266O*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIFyTCCA7GgAwIBAgISESCzTX8ZCO9VgpPFHqcZ1plEMA0GCSqGSIb3DQEBCwUAMHQxCzAJBgNV
BAYTAkZSMSUwIwYDVQQKExxPcmRyZSBkZXMgRXhwZXJ0cy1Db21wdGFibGVzMRcwFQYDVQQLEw4w
MDAyIDc3NTY3MDAwMzElMCMGA1UEAxMcT3JkcmUgZGVzIEV4cGVydHMtQ29tcHRhYmxlczAeFw0x
MTA1MTAwMDAwMDBaFw0xOTEyMzEwMTAwMDBaMIGKMQswCQYDVQQGEwJGUjEhMB8GA1UEChMYQ1JP
RUMgZGUgUm91ZW4gTm9ybWFuZGllMRcwFQYDVQQLEw4wMDAyIDc4MTEyMTg1MDE/MD0GA1UEAww2
T3JkcmUgZGVzIEV4cGVydHMtQ29tcHRhYmxlcyAtIHLDqWdpb24gUm91ZW4gTm9ybWFuZGllMIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsiH5QH8JPueXFdSfpRT0m58udSo/cV/rYOkV
Ojb3wAHdVp2apUU7vb9fP3e4O8WFDQR7QKitgItmW2/HUMnC0YrxTmNCWdDiP5wGB4mS4smIM2SB
RjMOg94xjx/IZhOSeHtYGgWkkSv0tvbYFDWZKu5CqM7gqS3uEDo/fYU33kLhbIDj7pQor2VLKMVk
3dvCEuGtYWMdrNCNy6bPZ1Qa90fmeqX7fqVUG3D276iYnI0KFPdZx7J289NTRu60f8oUQjsgEM+1
pjtzcN2PV/ciN/qV42QAxU3rs3M+hZe4dkj/c7NC5A3HkIChgALFIQ4qfIGO3FNfUelm7TZNga/Q
LQIDAQABo4IBPDCCATgwDgYDVR0PAQH/BAQDAgEGMG8GA1UdIARoMGYwZAYEVR0gADBcMFoGCCsG
AQUFBwIBFk5odHRwOi8vc2VlYy5leHBlcnRzLWNvbXB0YWJsZXMuZnIvUEMvUENSYWNpbmVfT3Jk
cmVfZGVzX0V4cGVydHMtQ29tcHRhYmxlcy5wZGYwEgYDVR0TAQH/BAgwBgEB/wIBADBhBgNVHR8E
WjBYMFagVKBShlBodHRwOi8vc2VlYy5leHBlcnRzLWNvbXB0YWJsZXMuZnIvQ1JML0NSTFJhY2lu
ZV9PcmRyZV9kZXNfRXhwZXJ0cy1Db21wdGFibGVzLmNybDAdBgNVHQ4EFgQUpwIZkZ3takLL82LR
JVjEXzQ+XI8wHwYDVR0jBBgwFoAUgQc54w96Rg+5feldYnb1JJUcFVYwDQYJKoZIhvcNAQELBQAD
ggIBAL070sH+xNmDBhn6I4q7Z7+vnyTuTegdd/hVtnML0zAaj78E/yMzhAxZVYmXLfNqX2QfQoWx
Olyx8nq8P+smawroqPygQhuTru7wnbOBu484Ars4gYZoJRDD5Y+SCxKgJSM9txhbQ3uq6jDWxgGy
K7EfHZvoYp9DxoZmW/jMbWR1Ce5BE4Njtj7cjgWY+OVwjPCmrM9rEVFtz2Wa9jcAo6+SltyKw9KQ
MQpzqR1I7/4qXQ8EaI388xPEbpHZHd/cWQwcB4HlAvXA807zhe81Y1d12TIbQbUPu/lelV96VSGj
9pEgPYuuYwiP6xpt54pGLL10gPXB521mh6RJQ7dKzejg0G9wIT2/2keseQJu1vb/SrZGtsaVtbx8
/sJNu6NfVIzXfEndqdaTCn+j3FAwDRwuAGgB1Emdl6vA+3l9LAnhs9xTNZSksL4KnCuBpqkLRo8x
8f5yry1XznUsmR101c4JfezBrZJCY/RDurEWogRXnVGlUpH0f1JXepq0yfYNhkcKYUI4VRqBInYP
7+MdCLX+nurRVPtmu0052sEXXKyRstATXPqEwhANYWbT1pW6iCV/0YqpdFUMcdJFlhwXYwuUY5gQ
lpdW0oBNwZ0K+GBTpbE4SKdL/RePOspbq9xR5dSwMg3Z/PVi7Se1hCALLAl5yVcmzNNMW14JYoyX Fj8h

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Ordre des Experts-Comptables*

Issuer OU: *0002 775670003*

Issuer O: *Ordre des Experts-Comptables*

Issuer C: *FR*

Subject CN: *Ordre des Experts-Comptables - région Rouen Normandie*

Subject OU: *0002 781121850*

Subject O: *CROEC de Rouen Normandie*

Subject C: *FR*

Valid from: *Tue May 10 02:00:00 CEST 2011*

Valid to: *Tue Dec 31 02:00:00 CET 2019*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:B2:21:F9:40:7F:09:3E:E7:97:15:D4:9F:A5:14:F4:9B:9F:2E:75:2A:3F:71:5F:EB:60:E9:15:3A:36:F7:C0:01:DD:56:9D:9A:A5:45:3B:BD:BF:5F:3F:77:B8:3B:C5:85:0D:04:7B:40:A8:AD:80:8B:66:5B:6F:C7:50:C9:C2:D1:8A:F1:4E:63:42:59:D0:E2:3F:9C:06:07:89:92:E2:C9:88:33:64:81:46:33:0E:83:DE:31:8F:1F:C8:66:13:92:78:7B:58:1A:05:A4:91:2B:F4:B6:F6:D8:14:35:99:2A:EE:42:A8:CE:E0:A9:2D:EE:10:3A:3F:7D:85:37:DE:42:E1:6C:80:E3:EE:94:28:AF:65:4B:28:C5:64:DD:DB:C2:12:E1:AD:61:63:1D:AC:D0:8D:CB:A6:CF:67:54:1A:F7:47:E6:7A:A5:FB:7E:A5:54:1B:70:F6:EF:A8:98:9C:8D:0A:14:F7:59:C7:B2:76:F3:D3:53:46:EE:B4:7F:CA:14:42:3B:20:10:CF:B5:A6:3B:73:70:DD:8F:57:F7:22:37:FA:95:E3:64:00:C5:4D:EB:B3:73:3E:85:97:B8:76:48:FF:73:B3:42:E4:0D:C7:90:80:A1:80:02:C5:21:0E:2A:7C:81:8E:DC:53:5F:51:E9:66:ED:36:4D:81:AF:D0:2D:02:03:01:00:01

Certificate Policies *Policy OID: 2.5.29.32.0*

CPS pointer: http://seec.experts-comptables.fr/PC/PCRacine_Ordre_des_Experts-Comptables.pdf

Basic Constraints *IsCA: true - Path length: 0*

CRL Distribution Points *http://seec.experts-comptables.fr/CRL/CRLRacine_Ordre_des_Experts-Comptables.crl*

Subject Key Identifier *A7:02:19:91:9D:ED:6A:42:CB:F3:62:D1:25:58:C4:5F:34:3E:5C:8F*

Authority Key Identifier *81:07:39:E3:0F:7A:46:0F:B9:7D:E9:5D:62:76:F5:24:95:1C:15:56*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *41:29:E0:44:FC:3B:C1:5C:1C:6C:1E:80:B8:32:4C:93:7D:C4:92:79:CD:91:BF:5D:22:23:03:3C:81:AF:07:C0*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2018-01-30T01:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS101456/QCPPublic*

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Signature-3-Stars*

TSP Service Definition URI

URI *[fr]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

URI *[en]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

11.24.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.24.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Rouen Normandie RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Rouen Normandie RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - région Rouen Normandie*

Subject OU: *0002 781121850*

Subject O: *CROEC de Rouen Normandie*

Subject C: *FR*

X509SKI

X509 SK I *pwIZkZ3takLL82LRJVjEXzQ+XI8=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

11.24.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.24.3 - History instance n.2 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Rouen Normandie RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Rouen Normandie RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - région Rouen Normandie*

Subject OU: *0002 781121850*

Subject O: *CROEC de Rouen Normandie*

Subject C: *FR*

X509 SK I *pwIZkZ3takLL82LRJVjEXzQ+XI8=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2012-11-25T23:00:00Z*

11.25 - Service (withdrawn): Ordre des Experts-Comptables - région Toulouse RGS***

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Toulouse RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Toulouse RGS****

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *149210011598823525841394251119367404845042 4*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIF2zCCA8OgAwIBAgISESDjXVctshOs1wduXmx9La94MA0GCSqGSIb3DQEBCwUAMHQxCzAJBgNV
BAYTAkZSMSUwIwYDVQQKExxPcmRyZSBkZXMgRXhwZXJ0cy1Db21wdGFibGVzMRcwFQYDVQQLEw4w
MDAyIDc3NTY3MDAwMzElMCMGA1UEAxMcT3JkcmUgZGVzIEV4cGVydHMtQ29tcHRhYmxlczAeFw0x
MTA1MTAwMDAwMDBaFw0xOTEyMzEwMTAwMDBaMIGcMQswCQYDVQQGEwJGUjEqMCgGA1UECgwhQ1JP
RUMgZGUgVG91bG91c2UgTWlkaS1QeXLDqW7DqWVzMRcwFQYDVQQLEw4wMDAyIDc3Njk0OTU5NjFI
MEYGA1UEAww/T3JkcmUgZGVzIEV4cGVydHMtQ29tcHRhYmxlcyAtIHLDqWdpb24gVG91bG91c2Ug
TWlkaS1QeXLDqW7DqWVzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsyZ1AIdIi7f4
6AJ5onLRmAbiIEUYHpBnJqFta5Q5QMsyoAMkhrxvp1LwaU4tzs6690sFsPChJ2lsGZg+piUXI4hM
RYK1D3GdIuUVPIINdKztvpT5P5L17bRFSlRL3Px/6ehf85qaEsOcr+H7E4ySQUGIFWp0rdy3Y640
H9ZOYEIO2cDAYj+/raKDjnU8oZDInTf8GtklbuH5usIEUOrD/5u1wSGD/ybEAFeVz9iziAeuUN88
fVgGZRCHUKHDea7t1KMqc2AaPshnsm0Y9kxdY3mXnSHoWzQpL1vJKxkz14W7V24bEgfnGumUYGb/
5fHjeZY8RC6094WPca0bzdInkwIDAQABo4IBPDCCATgwDgYDVR0PAQH/BAQDAgEGMG8GA1UdIARo
MGYwZAYEVR0gADBcMFoGCCsGAQUFBwIBFk5odHRwOi8vc2VlYy5leHBlcnRzLWNvbXB0YWJsZXMu
ZnIvUEMvUENSYWNpbmVfT3JkcmVfZGVzX0V4cGVydHMtQ29tcHRhYmxlcy5wZGYwEgYDVR0TAQH/
BAgwBgEB/wIBADBhBgNVHR8EWjBYMFagVKBShlBodHRwOi8vc2VlYy5leHBlcnRzLWNvbXB0YWJs
ZXMuZnIvQ1JML0NSTFJhY2luZV9PcmRyZV9kZXNfRXhwZXJ0cy1Db21wdGFibGVzLmNybDAd BgNV
HQ4EFgQUsLrOjErkGdZ3glBki8lvfgFJ3XkwHwYDVR0jBBgwFoAUgQc54w96Rg+5feldYnb1JJUc
FVYwDQYJKoZIhvcNAQELBQADggIBAIOYJEsvc0De5YgKr4mbHoNw4p6Mk7b66DgK7kpv/w7nuDu7
XLvgwp6E82XopqtF5ccyPqHGaGzlOrw6W16yoSngv58dK988htfawdJrwsKlp8ZdmxF6NgOOPyAu
voalPWIPz7ckXI2h9tVdpiUeXLuLe7s9IWRbrjtPDXfy30tQuwMlX1zJUx0hsz4v3AiKfyS5716n
5wx+lP6+aIt+y2/7Blj4U5FQQ2V4Yt2t+9hgoHLPvM2J6WauuAle7yC4vZDW5Ual3/qclBAYg1Oa
RhDbsy1EKBFdYG/WZiHPdmIUFA9JWrHVqecG0Cg6h9IUJ5dATIGR0YVNTYseDtaD2HDeyyUgeZm8
O9OcINKHQZNNv2VDj/jpjT4QO077L6o1WQiFfNdK3C+WkgghF7ScP3+Ma01B/Q+3XJe6DwH+P2oo
tPU3trtdwZCgmH/RWxlyiDETоN8heZ4zwe82Pq+w81q614hCnkNhzCgRp5pqPpl8x2FMDVRJAieK
XxQhGu90R5+p0C2j0UMs2FvXwYF6El5CuP6n/KF6auzoBs3PqJD+yQ4ENVGsqAg+dfBaLBxAmdg+
k53rSenF8LIu3VwyGK4RPb0IluzKHB2haNoA7sUL8GcCRupK0OMFGEagiK2tMmGh2/pNRNtIA0b1
x3PyQeBXvAYox0jJpRW9mjk5Tuzj

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Ordre des Experts-Comptables*

Issuer OU: *0002 775670003*

Issuer O: *Ordre des Experts-Comptables*

Issuer C: *FR*

Subject CN: *Ordre des Experts-Comptables - région Toulouse Midi-Pyrénées*

Subject OU: *0002 776949596*

Subject O: *CROEC de Toulouse Midi-Pyrénées*

Subject C: *FR*

Valid from: *Tue May 10 02:00:00 CEST 2011*

Valid to: *Tue Dec 31 02:00:00 CET 2019*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:B3:26:75:00:87:48:8B:B7:F8:E8:02:79:A2:72:D1:98:
06:E2:20:45:18:1E:90:67:26:A1:6D:6B:94:39:40:CB:32:A0:03:24:86:BC:6F:A7:52:F0:69:4E:2D:CE:CE:BA:F7:4B:05:B0:F0:A1:27:69:6C:19:98:3E:A6:25:17:23:88:
4C:45:82:B5:0F:71:9D:22:E5:15:3C:82:0D:74:AC:ED:BE:94:F9:3F:92:F5:ED:B4:45:4A:54:4B:DC:FC:7F:E9:E8:5F:F3:9A:9A:12:C3:9C:AF:E1:FB:13:8C:92:41:41:88:
15:6A:74:AD:DC:B7:63:AE:34:1F:D6:4E:60:42:0E:D9:C0:C0:62:3F:BF:AD:A2:83:8E:75:3C:A1:90:C8:9D:37:FC:1A:D9:25:6E:E1:F9:BA:C2:04:50:EA:C3:FF:9B:B5:C
1:21:83:FF:26:C4:00:57:95:CF:D8:B3:88:07:AE:50:DF:3C:7D:58:06:65:10:87:50:A1:C3:79:AE:ED:D4:A3:2A:73:60:1A:3E:C8:67:B2:6D:18:F6:4C:5D:63:79:97:9D:
21:E8:5B:34:29:2F:5B:C9:2B:19:33:D7:85:BB:57:6E:1B:12:07:E7:
1A:E9:94:60:66:FF:E5:F1:E3:79:96:3C:44:2E:B4:F7:85:8F:71:AD:1B:CD:D2:27:93:02:03:01:00:01

Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: http://seec.experts-comptables.fr/PC/PCRacine_Ordre_des_Experts-Comptables.pdf*
Basic Constraints	*IsCA: true - Path length: 0*
CRL Distribution Points	*http://seec.experts-comptables.fr/CRL/CRLRacine_Ordre_des_Experts-Comptables.crl*
Subject Key Identifier	*B0:BA:CE:8C:4A:E4:19:D6:77:82:50:64:8B:C9:6F:7E:01:49:DD:79*
Authority Key Identifier	*81:07:39:E3:0F:7A:46:0F:B9:7D:E9:5D:62:76:F5:24:95:1C:15:56*
Key Usage:	*keyCertSign - cRLSign*
Thumbprint algorithm:	*SHA-256*
Thumbprint:	*56:3D:8B:2E:4A:71:51:FC:DD:D9:1C:02:F8:FC:95:64:06:B1:55:F8:F4:78:36:DD:4A:B1:2D:E2:32:AE:2A:36*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description	*[en]*	*undefined.*
	[fr]	*undefined.*

Status Starting Time *2018-01-30T01:00:00Z*

Scheme Service Definition URI

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS101456/QCPPublic*
URI	*[fr]*	*http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Signature-3-Stars*

TSP Service Definition URI

URI	*[fr]*	*https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*
URI	*[en]*	*https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

11.25.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI	*[en]*	*http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.25.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Toulouse RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Toulouse RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - région Toulouse Midi-Pyrénées*

Subject OU: *0002 776949596*

Subject O: *CROEC de Toulouse Midi-Pyrénées*

Subject C: *FR*

X509SKI

X509 SK I *sLrOjErkGdZ3glBki8lvfgFJ3Xk=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

11.25.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.25.3 - History instance n.2 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Toulouse RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Toulouse RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - région Toulouse Midi-Pyrénées*

Subject OU: *0002 776949596*

Subject O: *CROEC de Toulouse Midi-Pyrénées*

Subject C: *FR*

X509SKI

X509 SK I *sLrOjErkGdZ3glBki8lvfgFJ3Xk=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2012-11-25T23:00:00Z*

11.26 - Service (withdrawn): Ordre des Experts-Comptables - région Corse RGS***

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Corse RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Corse RGS****

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *149201124585852440000384710517585625086129 7*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIFtDCCA5ygAwIBAgISESCggZN+KZzKj0MDWe2ug7bxMA0GCSqGSIb3DQEBCwUAMHQxCzAJBgNV
BAYTAkZSMSUwIwYDVQQKExxPcmRyZSBkZXMgRXhwZXJ0cy1Db21wdGFibGVzMRcwFQYDVQQLEw4w
MDAyIDc3NTY3MDAwMzElMCMGA1UEAxMcT3JkcmUgZGVzIEV4cGVydHMtQ29tcHRhYmxlczAeFw0x
MjA5MjUwMDAwMDBaFw0xOTEyMzEwMDAwMDBaMHYxCzAJBgNVBAYTAkZSMRcwFQYDVQQKEw5DUk9F
QyBkZSBDb3JzZTEXMBUGA1UECxMOMDAwMiA3NTI0MDYwODIxNTAzBgNVBAMMLE9yZHJlIGRlcyBF
eHBlcnRzLUNvbXB0YWJsZXMgLSByw6lnaW9uIENvcnNlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEAxfbRMEkEgUW3BW9oZIeFminpMuyPi/UiUon0HQuIOZ2iQYbBq1R84W//6uCY2VeM
6rcIs2PuMe9OrfqEw2IoqLcUY9L4/6Qil9ycZMY2uzSI11U77oop9Nfdp19AC3DQ2Lytk7XblrQg
dQzSqAlSgPmW+8asf7Aj4w4jwohb0+Mc51cf5WBrkjq1GpDGxoYjh0pNdvRAYvUKWIacxp7dOwBT
AeE8FwpDP+x3NuS/0E71HsgwVmaU378qwlOHn97kbk8PIAJ/GNz5ddc3bfy2BcM3lQX4VhfUGNys
YCIhXWVN9sSfzFwjBnu2A3MR7++IDeFSHFtWoFrCvB+ZXDFxlQIDAQABo4IBPDCCATgwDgYDVR0P

AQH/BAQDAgEGMG8GA1UdIARoMGYwZAYEVR0gADBcMFoGCCsGAQUFBwIBFk5odHRwOi8vc2VlYy5l
eHBlcnRzLWNvbXB0YWJsZXMuZnIvUEMvUENSYWNpbmVfT3JkcmVfZGVzX0V4cGVydHMtQ29tcHRh
Ymxlcy5wZGYwEgYDVR0TAQH/BAgwBgEB/wIBADBhBgNVHR8EWjBYMFagVKBShlBodHRwOi8vc2Vl
Yy5leHBlcnRzLWNvbXB0YWJsZXMuZnIvQ1JML0NSTFJhY2luZV9PcmRyZV9kZXNfRXhwZXJ0cy1D
b21wdGFibGVzLmNybDAdBgNVHQ4EFgQUu7YA5gRue8pevDW6st+f4sohk/EwHwYDVR0jBBgwFoAU
gQc54w96Rg+5feldYnb1JJUcFVYwDQYJKoZIhvcNAQELBQADggIBAB57g5dLtPTtm9ogiY5YXQ3O
I3S5yu6X0fnYaP17vEMSCGy7S4XlbGWwvrSrHlgUk33hkYZcGJwZ2NnqxmlPvTswMpWUX6nM5W0o
gMvp449oQ/LDHaJjGrWavtBg7xAA/6hPGukjQAUTpoNY76shvHdV4Ipn59ejbBPNLFU8FD/Xhfyj
k5aLlguzdUUANEA4+k7jJU3pHt4jC8vshVsLzimhfVJtfAkOM9wTOHfcMxu8noF1roFgVviAzsaL
4tHYr6ZlKGejYw9G+JS64QvW1Ng6akd/FKe4zLFzSVzTrJMj7bbkR55Dv5RN/e4NwpAZx8J3FLp1
mMTIrs8ymvIUwhDFAo7kHqbhyzjEj8fgrQHOxfFjp+6QsWcaxP604ydMzzBro/NR89mTR1jmoS+m
armzGkw8cfl4C2Orf8cDNru/Fr/U6sE7AuQWgx79t/FgpVhEqqFvenf2DYnguFkE0b91vtO76mTD
5wOfqUfpG+QuR07Ljlw0fi2ca9OKnVXvCkYghhOxaMOCk4ixpCCPw66h+6UhhzqNEo59SMUijCs/
eujmdZtkw6udWJxkVlFGlYtmg1PAoNnp1TxHyDIaMGtH0kyMtugzYzQno3DlLZr22Dn7x0nNjLWu
ZO1T28oN2W9MDW376dxOQNwXpgTSGQ4orJvKkF+cYpRfMESFEkyu

-----END CERTIFICATE-----

Signature algorithm:	*SHA256withRSA*
Issuer CN:	*Ordre des Experts-Comptables*
Issuer OU:	*0002 775670003*
Issuer O:	*Ordre des Experts-Comptables*
Issuer C:	*FR*
Subject CN:	*Ordre des Experts-Comptables - région Corse*
Subject OU:	*0002 752406082*
Subject O:	*CROEC de Corse*
Subject C:	*FR*
Valid from:	*Tue Sep 25 02:00:00 CEST 2012*
Valid to:	*Tue Dec 31 01:00:00 CET 2019*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C5:F6:D1:30:49:04:81:45:B7:05:6F:68:64:87:85:9A:
29:E9:32:EC:8F:8B:F5:22:52:89:F4:1D:0B:88:39:9D:A2:41:86:C1:AB:54:7C:E1:6F:FF:EA:E0:98:D9:57:8C:EA:B7:08:B3:63:EE:31:EF:4E:AD:FA:84:C3:62:28:A8:B7:
14:63:D2:F8:FF:A4:22:97:DC:9C:64:C6:36:BB:34:88:D7:55:3B:EE:8A:29:F4:D7:DD:A7:5F:40:0B:70:D0:D8:BC:AD:93:B5:DB:96:B4:20:75:0C:D2:A8:09:52:80:F9:9
6:FB:C6:AC:7F:B0:23:E3:0E:23:C2:88:5B:D3:E3:1C:E7:57:1F:E5:60:6B:92:3A:B5:1A:90:C6:C6:86:23:87:4A:4D:76:F4:40:62:F5:0A:58:86:9C:C6:9E:DD:3B:00:53:0
1:E1:3C:17:0A:43:3F:EC:77:36:E4:BF:D0:4E:F5:1E:C8:30:56:66:94:DF:BF:2A:C2:53:87:9F:DE:E4:6E:4F:0F:20:02:7F:18:DC:F9:75:D7:37:6D:FC:B6:05:C3:37:95:0
5:F8:56:17:D4:18:DC:AC:60:22:21:5D:65:4D:F6:C4:9F:CC:5C:23:06:7B:B6:03:73:11:EF:EF:88:0D:E1:52:1C:5B:56:A0:5A:C2:BC:1F:99:5C:31:71:95:02:03:01:00:0
1

Certificate Policies	*Policy OID: 2.5.29.32.0* *CPS pointer: http://seec.experts-comptables.fr/PC/PCRacine_Ordre_des_Experts-Comptables.pdf*
Basic Constraints	*IsCA: true - Path length: 0*
CRL Distribution Points	*http://seec.experts-comptables.fr/CRL/CRLRacine_Ordre_des_Experts-Comptables.crl*

Subject Key Identifier *BB:B6:00:E6:04:6E:7B:CA:5E:BC:35:BA:B2:DF:9F:E2:CA:21:93:F1*

Authority Key Identifier *81:07:39:E3:0F:7A:46:0F:B9:7D:E9:5D:62:76:F5:24:95:1C:15:56*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *2F:AB:C4:84:45:F9:D4:E3:4C:59:80:78:78:7A:53:F4:33:F6:7C:A3:D3:74:72:78:81:5B:F4:92:B7:DF:65:37*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2018-01-30T01:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS101456/QCPPublic*

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Signature-3-Stars*

TSP Service Definition URI

URI *[fr]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

URI *[en]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

11.26.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.26.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Corse RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Corse RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - région Corse*

Subject OU: *0002 752406082*

Subject O: *CROEC de Corse*

Subject C: *FR*

X509SKI

X509 SK I *u7YA5gRue8pevDW6st+f4sohk/E=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

11.26.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.26.3 - History instance n.2 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Corse RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Corse RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - région Corse*

Subject OU: *0002 752406082*

Subject O: *CROEC de Corse*

Subject C: *FR*

X509SKI

X509 SK I *u7YA5gRue8pevDW6st+f4sohk/E=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2012-11-25T23:00:00Z*

11.27 - Service (withdrawn): Ordre des Experts-Comptables - région Marseille PACA RGS***

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Marseille PACA RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Marseille PACA RGS****

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1492026870504902272429072316601074821044125*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIFxzCCA6+gAwIBAgISESCsQsYJIQm/wnqIB/uudxedMA0GCSqGSIb3DQEBCwUAMHQxCzAJBgNV
BAYTAkZSMSUwIwYDVQQKExxPcmRyZSBkZXMgRXhwZXJ0cy1Db21wdGFibGVzMRcwFQYDVQQLEw4w
MDAyIDc3NTY3MDAwMzElMCMGA1UEAxMcT3JkcmUgZGVzIEV4cGVydHMtQ29tcHRhYmxlczAeFw0x
MjA5MjUwMDAwMDBaFw0xOTEyMzEwMDAwMDBaMIGIMQswCQYDVQQGEwJGUjEgMB4GA1UEChMXQ1JP
RUMgZGUgTWFyc2VpbGxlIFBBQ0ExFzAVBgNVBAsTDjAwMDIgNzgyODI1MDQ2MT4wPAYDVQQDDDVP
cmRyZSBkZXMgRXhwZXJ0cy1Db21wdGFibGVzIC0gcsOpZ2lvbiBNYXJzZWlsbGUgUEFDQTCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAN5Q8PK+8eTUMCxOWzmEJUPAvpsjiIAmDsOxuk4o
1vAx/aLwP2eLBygm+nailSllKeXVM68syLFgaRJLeJkw0PqHFQeF1vA8Kxy+Vq+boXWmt9sQfTNa
Dr6/7rdJZ6nH5QiVZyrv2iQpeISKBtLqr+tFPG8ry9sh7l5VWa4ksasRjIh8/IwkkzeH5sJqzV1a
1YjowzGRZxjmztPT75UtAOFGWz6W+0UOzBYwkFMe1XYHDGl5dQbbrGYhEPL/k2ahLV7FLcrz0Mag
pl2YEyBLVCAytscYhEnm/XMg6rHXY4FNQ/M83R5TxT67WqirkUDunc2yhIUJ5e1qktm6lWPD1p8C
AwEAAaOCATwwggE4MA4GA1UdDwEB/wQEAwIBBjBvBgNVHSAEaDBmMGQGBFUdIAAwXDBaBggrBgEF
BQcCARZOaHR0cDovL3NlZWMuZXhwZXJ0cy1jb21wdGFibGVzLmZyL1BDL1BDUmFjaW5lX09yZHJl
X2Rlc19FeHBlcnRzLUNvbXB0YWJsZXMucGRmMBIGA1UdEwEB/wQIMAYBAf8CAQAwYQYDVR0fBFow
WDBWoFSgUoZQaHR0cDovL3NlZWMuZXhwZXJ0cy1jb21wdGFibGVzLmZyL0NSTC9DUkxSYWNpbmVf
T3JkcmVfZGVzX0V4cGVydHMtQ29tcHRhYmxlcy5jcmwwHQYDVR0OBBYEFIyz8syddJquVRPeBdZb
5F0NeoeBMB8GA1UdIwQYMBaAFIEHOeMPekYPuX3pXWJ29SSVHBVWMA0GCSqGSIb3DQEBCwUAA4IC
AQAWOKz+QE4cEyp86857nWcFFFM8y9/ZvT4TichPf1ETALPqopCovUffSVLhoUqRoZvlEfEvfIfL
h/EijGWgkY5P6edZ58a18DjfLfxM4wuETSSM3lq2c8nVE/clm2ohLE8CvWxzs21xk6+rfoBBPRYp
nEjS50r9Y6weWPAoI1ZGi/jAKmYRywR1YzhQPJux5Q1SL2dYtCDhKI9AjknkvXEP24rk/sNmFYpA
CY32en3cqrkOWVWJKiZwr2DvZeDLFEfLqsNHe5xfOCTc4N7Eyr/bLo870ikJYEzDHDY81RWoivgF
XeeWM9Dflzi16JUc4kxImAHzDw+mYIeNYASQYeFHZOT7aE3PEuqeR3FwQFRzrhJiGmt+bI8yblhN
c4Fc5Hf9KTz0SByZxai9aA5n7L8VoaI52d4jhABeYcTzPmrsCV59rr2rWL12sz4mz0/WWl+30BQE
MRZKzHX/MgNV2Xk+nwLXSXk77ouRuI2l0ATgee3D5YLdQqFSwdk06NxvsSPTlG3edqdHAlQZzexu
ZmcJaFd8i9sZrwKchKDxcUFHkO9zYIssROPYtHXzZ31VLVbBjvbqbK7gCKtxuWAsiOp4gMg68sJA
6yRRvZAto+y9QaA6bxqpx3vjbZaQK3m44d2WbwPTbg1ZKJwGO1dzV4Zyd8zhXqN3axEWfXJ12B4+ 1g==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Ordre des Experts-Comptables*

Issuer OU: *0002 775670003*

Issuer O: *Ordre des Experts-Comptables*

Issuer C: *FR*

Subject CN: *Ordre des Experts-Comptables - région Marseille PACA*

Subject OU: *0002 782825046*

Subject O: *CROEC de Marseille PACA*

Subject C: *FR*

Valid from: *Tue Sep 25 02:00:00 CEST 2012*

Valid to: *Tue Dec 31 01:00:00 CET 2019*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:DE:50:F0:F2:BE:F1:E4:D4:30:2C:4E:5B:39:84:25:43:C0:BE:9B:23:88:80:26:0E:C3:B1:BA:4E:28:D6:F0:31:FD:A2:F0:3F:67:8B:07:28:26:FA:76:A2:95:22:25:29:E5:D5:33:AF:2C:C8:B1:60:69:12:4B:78:99:30:D0:FA:87:15:07:85:D6:F0:3C:2B:1C:BE:56:AF:9B:A1:75:A6:B7:DB:10:7D:33:5A:0E:BE:BF:EE:B7:49:67:A9:C7:E5:08:95:67:2A:EF:DA:24:29:78:84:8A:06:D2:EA:AF:EB:45:3C:6F:2B:CB:DB:21:EE:5E:55:59:AE:24:B1:AB:11:8C:88:7C:FC:8C:24:93:37:87:E6:C2:6A:CD:5D:5A:D5:88:E8:C3:31:91:67:18:E6:CE:D3:D3:EF:95:2D:00:E1:46:5B:3E:96:FB:45:0E:CC:16:30:90:53:1E:D5:76:07:0C:69:79:75:06:DB:AC:66:21:10:F2:FF:93:66:A1:2D:5E:C5:2D:CA:F3:D0:C6:A0:A6:5D:98:13:20:4B:54:20:32:B6:C7:18:84:49:E6:FD:73:20:EA:B1:D7:63:81:4D:43:F3:3C:DD:1E:53:
C5:3E:BB:5A:A8:AB:91:40:EE:9D:CD:B2:84:85:09:E5:ED:6A:92:D9:BA:95:63:C3:D6:9F:02:03:01:00:01

Certificate Policies *Policy OID: 2.5.29.32.0*

CPS pointer: http://seec.experts-comptables.fr/PC/PCRacine_Ordre_des_Experts-Comptables.pdf

Basic Constraints *IsCA: true - Path length: 0*

CRL Distribution Points *http://seec.experts-comptables.fr/CRL/CRLRacine_Ordre_des_Experts-Comptables.crl*

Subject Key Identifier *8C:B3:F2:CC:9D:74:9A:AE:55:13:DE:05:D6:5B:E4:5D:0D:7A:87:81*

Authority Key Identifier *81:07:39:E3:0F:7A:46:0F:B9:7D:E9:5D:62:76:F5:24:95:1C:15:56*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *2B:5E:8F:38:B7:CE:D3:2B:7B:F8:D9:45:D0:E2:18:9C:33:FC:D2:FD:2C:BA:B0:DB:DD:A7:BE:12:34:05:4A:2E*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description

[en] *undefined.*

[fr] *undefined.*

Status Starting Time *2018-01-30T01:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS101456/QCPPublic*

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Signature-3-Stars*

TSP Service Definition URI

URI *[fr]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

URI *[en]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

11.27.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.27.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Marseille PACA RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Marseille PACA RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - région Marseille PACA*

Subject OU: *0002 782825046*

Subject O: *CROEC de Marseille PACA*

Subject C: *FR*

X509SKI

X509 SK I *jLPyzJ10mq5VE94F1lvkXQ16h4E=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

11.27.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.27.3 - History instance n.2 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Marseille PACA RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Marseille PACA RGS****

Service digital identities

X509SubjectName

Subject CN: *Ordre des Experts-Comptables - région Marseille PACA*

Subject OU: *0002 782825046*

Subject O: *CROEC de Marseille PACA*

Subject C: *FR*

X509SKI

X509 SK I *jLPyzJ10mq5VE94F1lvkXQ16h4E=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2012-11-25T23:00:00Z*

11.28 - Service (withdrawn): Ordre des Experts-Comptables - Elu EC RGS***

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Ordre des Experts-Comptables - Elu EC RGS****

Name *[fr]* *Ordre des Experts-Comptables - Elu EC RGS****

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *149199015669375646408752192581686624670139O*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIF1TCCA72gAwIBAgISESCQo/Nkal/UizdIno9ilzFOMA0GCSqGSIb3DQEBCwUAMHQxCzAJBgNV
BAYTAkZSMSUwIwYDVQQKExxPcmRyZSBkZXMgRXhwZXJ0cy1Db21wdGFibGVzMRcwFQYDVQQLEw4w
MDAyIDc3NTY3MDAwMzElMCMGA1UEAxMcT3JkcmUgZGVzIEV4cGVydHMtQ29tcHRhYmxlczAeFw0x
MTA1MDkwMDAwMDBaFw0xOTEyMzEwMTAwMDBaMIGWMQswCQYDVQQGEwJGUjE9MDsGA1UECgw0Q29u
c2VpbCBTdXDDqXJpZXVyIGRlIGwnT3JkcmUgZGVzIEV4cGVydHMtQ29tcHRhYmxlczEXMBUGA1UE
CxMOMDAwMiA3NzU2NzAwMDMxLzAtBgNVBAMTJkVsdXMgZGUgbCdPcmRyZSBkZXMgRXhwZXJ0cy1D
b21wdGFibGVzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0N5kF7oLzq6cpBXJndqv
SysSU1ZaQn/xb+5/nGGDkBDZU9bIP/nDNfhTNVn3ae0mCu0fVdYyE1rm167bJSUupd1bXu1vI780
eKPbtZH4cHftKH/OYUE/cr1rN2OWrRbSk1xdOMKF9UbpuLxSg2UUeVCy+ys8t2d+e8GSLgHpSZ38
hPKbLnkhQXrFoq4U/MKx9vqSoqo5wzvaoqDFqCBBus5bEwX2VWq1hrceAMVKcPYkEMp9BrCvywSh
8drMLnjart4d5J/a5UbXSjyFIACSrm2pEDeipHuLqdIBhsAX6jKb3ILk8O3W8uzVAQfJHmdACngG
8grxOYFlziSdLzcnmwIDAQABo4IBPDCCATgwDgYDVR0PAQH/BAQDAgEGMG8GA1UdIARoMGYwZAYE
VR0gADBcMFoGCCsGAQUFBwIBFk5odHRwOi8vc2VlYy5leHBlcnRzLWNvbXB0YWJsZXMuZnIvUEMv
UENSYWNpbmVfT3JkcmVfZGVzX0V4cGVydHMtQ29tcHRhYmxlcy5wZGYwEgYDVR0TAQH/BAgwBgEB
/wIBADBhBgNVHR8EWjBYMFagVKBShlBodHRwOi8vc2VlYy5leHBlcnRzLWNvbXB0YWJsZXMuZnIv
Q1JML0NSTFJhY2luZV9PcmRyZV9kZXNfRXhwZXJ0cy1Db21wdGFibGVzLmNybDAdBgNVHQ4EFgQU
1aY9ysmjwwSg3I0BsjUxrWZYC/wwHwYDVR0jBBgwFoAUgQc54w96Rg+5feldYnb1JJUcFVYwDQYJ
KoZIhvcNAQELBQADggIBAE0GZ/rsrxlfSi9IgbclaswqIPkJMne4ytXJJLycCk0RcTZqHzsnMF3/
ljajxQn3rMEm9Jemad2LItq7CFb74KfyHYwdRIXfeXfIEZFcJ/QCnz5OMJPhRVlKg3I7r9os2fgW
vylcRsPUVe7Dl0cfNyzBBTpSSlBBvDA/TX+TS+Yz+MozSYqfle84a1p+JaHo6EwKf2kIaMMFBNaW
skrWiZlV06iuksoZ0187HuruzJ54ZgP1I0TWKQ8JeWQ2SyXapWjl2biUE0LrxUVozhxTdBCPyMai
cfryYPOuzFS5ObilcA6BzwAJ3+yOUMxOduQrHcIkmxXoj2iNgl5CT8tBxczMrRvoo2+yexkP1TY3
H0ngiTitVeD+oZc/ElmS3JYZGj+QigAzMLaZSqXYzxgmSsL4m/KuRCJm7nQ+1co9bEnY6q3PWtvx
wrczjmakBGQZDIA3nZQARu3l0Gdm8wlDq1AkvqEpa666KpMpiQjkjSuzaxqzGBR3oqVHfmG6U/G+
Zol81yVx9vBEWguQPyYzUTFTltakwlfxbDqwEPkJg39xM4UGm3QJlO0MTQ7aTA8raVnc9e8EK6rs
KDEysDW7llPka4bNh14jGxDaMxq1UMmbUlfQJryJNjXEES+tXsP05gLZQNH9hdTbFY2CDbH5rN5z A/FXMkCbOz33eD97ltbO

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Ordre des Experts-Comptables*

Issuer OU: *0002 775670003*

Issuer O: *Ordre des Experts-Comptables*

Issuer C: *FR*

Subject CN: *Elus de l'Ordre des Experts-Comptables*

Subject OU: *0002 775670003*

Subject O: *Conseil Supérieur de l'Ordre des Experts-Comptables*

Subject C: *FR*

Valid from: *Mon May 09 02:00:00 CEST 2011*

Valid to: *Tue Dec 31 02:00:00 CET 2019*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:D0:DE:64:17:BA:0B:CE:AE:9C:A4:15:C9:9D:DA:AF:4B:2B:12:53:56:5A:42:7F:F1:6F:EE:7F:9C:61:83:90:10:D9:53:D6:C8:3F:F9:C3:35:F8:53:35:59:F7:69:ED:26:0A:ED:1F:55:D6:32:13:5A:E6:D7:AE:DB:25:25:2E:A5:DD:5B:5E:ED:6F:23:BF:34:78:A3:DB:B5:91:F8:70:77:ED:28:7F:CE:61:41:3F:72:BD:6B:37:63:96:AD:16:D2:93:5C:5D:38:C2:85:F5:46:E9:B8:BC:52:83:65:14:79:50:B2:FB:2B:3C:B7:67:7E:7B:C1:92:2E:01:E9:49:9D:FC:84:F2:9B:2E:79:21:41:7A:C5:A2:AE:14:FC:C2:B1:F6:FA:92:A2:AA:39:C3:3B:DA:A2:A0:C5:A8:20:41:BA:CE:5B:13:05:F6:55:6A:B5:86:B7:1E:00:C5:4A:70:F6:24:10:CA:7D:06:B0:AF:CB:04:A1:F1:DA:CC:2E:78:DA:AE:DE:1D:E4:9F:DA:E5:46:D7:4A:3C:85:20:00:92:AE:6D:A9:10:37:A2:A4:7B:8B:A9:D2:01:86:C0:17:EA:32:9B:DC:82:E4:F0:ED:D6:F2:EC:D5:01:07:C9:1E:67:40:0A:78:06:F2:0A:F1:39:81:65:CE:24:9D:2F:37:27:9B:02:03:01:00:01

Certificate Policies *Policy OID: 2.5.29.32.0*

CPS pointer: http://seec.experts-comptables.fr/PC/PCRacine_Ordre_des_Experts-Comptables.pdf

Basic Constraints *IsCA: true - Path length: 0*

CRL Distribution Points *http://seec.experts-comptables.fr/CRL/CRLRacine_Ordre_des_Experts-Comptables.crl*

Subject Key Identifier *D5:A6:3D:CA:C9:A3:C3:04:A0:DC:8D:01:B2:35:31:AD:66:58:0B:FC*

Authority Key Identifier *81:07:39:E3:0F:7A:46:0F:B9:7D:E9:5D:62:76:F5:24:95:1C:15:56*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *55:DC:09:2A:E5:F5:37:4D:09:40:B3:DE:EB:30:5A:12:6D:6E:B3:60:A9:30:90:CA:67:98:B0:2A:49:09:8B:6E*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2018-01-30T01:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS101456/QCPPublic*

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Signature-3-Stars*

TSP Service Definition URI

URI *[fr]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

URI *[en]* *https://www.signexpert.fr/cms/index.php/Cadre-legal/La-politique-de-certification*

11.28.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.28.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Elu EC RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Elu EC RGS****

Service digital identities

X509SubjectName

Subject CN: *Elus de l'Ordre des Experts-Comptables*

Subject OU: *0002 775670003*

Subject O: *Conseil Supérieur de l'Ordre des Experts-Comptables*

Subject C: *FR*

X509SKI

X509 SK I *1aY9ysmjwwSg3I0BsjUxrWZYC/w=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

11.28.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

11.28.3 - History instance n.2 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Ordre des Experts-Comptables - région Elu EC RGS****

Name *[fr]* *Ordre des Experts-Comptables - région Elu EC RGS****

Service digital identities

X509SubjectName

Subject CN: *Elus de l'Ordre des Experts-Comptables*

Subject OU: *0002 775670003*

Subject O: *Conseil Supérieur de l'Ordre des Experts-Comptables*

Subject C: *FR*

X509SKI

X509 SK I *1aY9ysmjwwSg3I0BsjUxrWZYC/w=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2012-11-25T23:00:00Z*

12 - TSP: Imprimerie Nationale

TSP Name

Name *[en]* *Imprimerie Nationale*

Name *[fr]* *Imprimerie Nationale*

TSP Trade Name

Name *[en]* *VATFR-08352973622*

Name *[fr]* *VATFR-08352973622*

PostalAddress

Street Address *[en]* *104 avenue du Président Kennedy*

Locality *[en]* *Paris*

Postal Code *[en]* *75016*

Country Name *[en]* *FR*

PostalAddress

Street Address *[fr]* *104 avenue du Président Kennedy*

Locality *[fr]* *Paris*

Postal Code *[fr]* *75016*

Country Name *[fr]* *FR*

ElectronicAddress

URI *http://www.imprimerienationale.fr*

URI *http://www.imprimerienationale.fr*

URI *mailto:michel.brun@imprimerienationale.fr*

URI *mailto:michel.brun@imprimerienationale.fr*

TSP Information URI

URI *[fr]* *http://www.imprimerienationale.fr/GIN/PC*

URI *[en]* *http://www.imprimerienationale.fr/GIN/PC*

12.1 - Service (granted): Pass'IN - Signature RGS***

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Pass'IN - Signature RGS****

Name *[fr]* *Pass'IN - Signature RGS****

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *149190046011473850044523888978483979828500 4*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIFyjCCA7KgAwIBAgISESBNKQScGymddsZjik5VzGLMMA0GCSqGSIb3DQEBCwUAMH8xCzAJBgNV
BAYTAkZSMSQwIgYDVQQKDBtHcm91cGUgSW1wcmltZXJpZSBOYXRpb25hbGUxHDAaBgNVBAsMEzAw
MDIgNDEwNDk0NDk2MDAwNDYxLDAqBgNVBAMMI0FDUiBJbXByaW1lcmllIE5hdGlvbmFsZSBSZW5m
b3Jjw6llMB4XDTEzMDUyODAwMDAwMFoXDTE5MDUyODAwMDAwMFowgYgxCzAJBgNVBAYTAkZSMSQw
IgYDVQQKDBtHcm91cGUgSW1wcmltZXJpZSBOYXRpb25hbGUxHDAaBgNVBAsMEzAwMDIgNDEwNDk0
NDk2MDAwNDYxNTAzBgNVBAMMLEFDIEltcHJpbWVyaWUgTmF0aW9uYWxlIFJlbmZvcmPDqWUgUGVy
c29ubmVsMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwDSM8DY/LrpwaL78sfM50f7r
XAtdsjtiDoKtOdWjbUr5jHkuK55Gs8SVs0Cgbrrmykq30n+IXVbevPgUdxzeE4WgfgCRVOS0IlUo
Iq0Ah7IzL1lu1YjFqrRfOZLGcoEtw477dlgXgthwnTCcsfa79bmsc0Cos5toNzwgPPD6P2vhWo5u
bwUgQBicJdPuLE+52vR1+5yitcfD/TEO2IzaTU+cprf4lcyn5YHVjPLKH2rQ1Z2wLJgTkmtKfmen
zWjl/wFqqt3sn4//E/KBYIABIiT1ZMR8n2IOZWd+jmFfnnRb7h8mBu9FEFcglcAsxSNSyfw2FBZK
vrIhs/jxIYyZgQIDAQABo4IBNDCCATAwEgYDVR0TAQH/BAgwBgEB/wIBADAOBgNVHQ8BAf8EBAMC
AQYwSQYDVR0gBEIwQDA+BgRVHSAAMDYwNAYIKwYBBQUHAgEWKGh0dHA6Ly93d3cuaW1wcmltZXJp
ZW5hdGlvbmFsZS5mci9HSU4vUEMwfwYDVR0fBHgwdjA3oDWgM4YxaHR0cDovL2NybC5pbXByaW1l
cmllbmF0aW9uYWxlLmZyL0dJTi9BQy1SRi1QLmNybDA7oDmgN4Y1aHR0cDovL3d3dy5pbXByaW1l
cmllbmF0aW9uYWxlLmZyL0dJTi9DUkwvQUMtUkYtUC5jcmwwHQYDVR0OBBYEFA8OSr1DJFdEI75u
pFZWXtQt29yuMB8GA1UdIwQYMBaAFAko+6ysn4GGQe776S8APxULOwM0MA0GCSqGSIb3DQEBCwUA
A4ICAQAcEWiI3xaooPXTL/zm3t7h4DAwytq342B1rMFpgzyqaUq/3KqokfT1X6vmd8PwBoZnh90e
g+yat7ps9M7DZh0PD2HWlU1Po+lc9LdcxJSEL7ks/Re91Jj1YMTcbIZU7eGeMPk3Bi/4b8bHZ2aR
j918ZgnYTmqRGK7oVst/8I0pj9DlhBc2WVWqG9+7s9ZoB2sCEQWaiu1ANJ5Ugm8LkgiOfjtOvMKa
GKqOKhg9n3Id4HXIwO7AY7oh+zMQYkrENDJV1SUTFEIZyQxSJOOyxwYeXXfmQtV1/wLAcen/EB8x
TQizPHbGfPIvgyfFeLhoGz93sIz5+HxoFyUV14qOeF+T8HgcC+z6ewXwod+Y6Hsje2UvdFR8lbiy
Rw4gXMays7vtM1i3OoRQ7rRvAKUnSz79rBl5W8MzcSRFEZlLMtVKt0X3vg9OW85OVU8byzN8pfTU
oGEmz0Map2VIndSLhLVOqTkEGaD7e391H/0aZULlfbtRCFo4vuQ0bkcK8JAObptt/V+w+4CjJsnp
oNKp7oR/dTrpNL70bbJuZ3/SkCfWn+kLMsjfH9XpzW3zqJU/jYiOCto8RN/0ah/DXI0EzlENsDxf
RCCQJkPJkgGTCwzTOjjGf1YD/ja0U2T0H7zL8eGEP5pACdfR6KuUWJ4RUyWQCoINXmO4nhQSlOWs 5OgAHw==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *ACR Imprimerie Nationale Renforcée*

Issuer OU: *0002 41049449600046*

Issuer O: *Groupe Imprimerie Nationale*

Issuer C: *FR*

Subject CN: *AC Imprimerie Nationale Renforcée Personnel*

Subject OU: *0002 41049449600046*

Subject O: *Groupe Imprimerie Nationale*

Subject C: *FR*

Valid from: *Tue May 28 02:00:00 CEST 2013*

Valid to: *Tue May 28 02:00:00 CEST 2019*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C0:34:8C:F0:36:3F:2E:BA:70:68:BE:FC:B1:F3:39:D1:F
E:EB:5C:0B:5D:B2:3B:62:0E:82:AD:39:D5:A3:6D:4A:F9:8C:79:2E:2B:9E:46:B3:C4:95:B3:40:A0:6E:BA:E6:CA:4A:B7:D2:7F:88:5D:56:DE:BC:F8:14:77:1C:DE:13:85

:A0:7E:00:91:54:E4:B4:22:55:28:22:AD:00:87:B2:33:2F:59:6E:D5:88:C5:AA:B4:5F:39:92:C6:72:81:2D:C3:8E:FB:76:58:17:82:D8:70:9D:30:9C:B1:F6:BB:F5:B9:AC:73:40:A8:B3:9B:68:37:3C:20:3C:F0:FA:3F:6B:E1:5A:8E:6E:6F:05:20:40:18:9C:25:D3:EE:2C:4F:B9:DA:F4:75:FB:9C:A2:B5:C7:C3:FD:31:0E:D8:8C:DA:4D:4F:9C:A6:
B7:F8:95:CC:A7:E5:81:D5:8C:F2:CA:1F:6A:D0:D5:9D:B0:2C:98:13:92:6B:4A:7E:67:A7:CD:68:E5:FF:01:6A:AA:DD:EC:9F:8F:FF:13:F2:81:60:80:01:22:24:F5:64:C4:7C:9F:62:0E:65:67:7E:8E:61:5F:9E:74:5B:EE:1F:26:0 6:EF:45:10:57:20:95:C0:2C:C5:23:52:C9:FC:36:14:16:4A:BE:B2:21:B3:F8:F1:21:8C:99:81:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

Certificate Policies *Policy OID: 2.5.29.32.0*

CPSpointer: http://www.imprimerienationale.fr/GIN/PC

CRL Distribution Points *http://crl.imprimerienationale.fr/GIN/AC-RF-P.crl*

http://www.imprimerienationale.fr/GIN/CRL/AC-RF-P.crl

Subject Key Identifier *0F:0E:4A:BD:43:24:57:44:23:BE:6E:A4:56:56:5E:D4:2D:DB:DC:AE*

Authority Key Identifier *09:28:FB:AC:AC:9F:81:86:41:EE:FB:E9:2F:00:3F:15:0B:3B:03:34*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *06:23:23:03:31:39:F2:E8:7B:BC:37:3D:6D:CB:CE:18:56:B1:BB:41:5F:06:9B:F5:20:7C:9F:5E:98:BF:A8:10*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

TSP Service Definition URI

URI *[fr]* *http://www.imprimerienationale.fr/GIN/PC*

URI *[en]* *http://www.imprimerienationale.fr/GIN/PC*

12.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

12.1.2 - Extension (critical): Qualifiers [QCWithQSCD, QCForESig]

Qualifier type description *[en]* *undefined.*

[fr] *undefined.*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithQSCD*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForESig*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Policy Identifier nodes:

Identifier *1.2.250.1.295.1.1.5.4.1.102.2*

12.1.3 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Pass'IN*

Name *[fr]* *Pass'IN*

Service digital identities

X509SubjectName

Subject CN: *AC Imprimerie Nationale Renforcée Personnel*

Subject OU: *0002 41049449600046*

Subject O: *Groupe Imprimerie Nationale*

Subject C: *FR*

X509SKI

X509 SK I *Dw5KvUMkV0Qjvm6kVlZe1C3b3K4=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

12.1.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

12.1.4 - History instance n.2 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *Pass'IN*

Name *[fr]* *Pass'IN*

Service digital identities

X509SubjectName

Subject CN: *AC Imprimerie Nationale Renforcée Personnel*

Subject OU: *0002 41049449600046*

Subject O: *Groupe Imprimerie Nationale*

Subject C: *FR*

X509SKI

X509 SK I *Dw5KvUMkV0Qjvm6kVlZe1C3b3K4=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2015-01-18T23:00:00Z*

12.2 - Service (granted): Pass'IN - Signature RGS**

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Pass'IN - Signature RGS***

Name *[fr]* *Pass'IN - Signature RGS***

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *149186646658730658552961521094074966912891 7*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIFxjCCA66gAwIBAgISESAzlhpO9egV3hFsHL2nitrVMA0GCSqGSIb3DQEBCwUAMH0xCzAJBgNV
BAYTAkZSMSQwIgYDVQQKDBtHcm91cGUgSW1wcmltZXJpZSBOYXRpb25hbGUxHDAaBgNVBAsMEzAw
MDIgNDEwNDk0NDk2MDAwNDYxKjAoBgNVBAMMIUFDUiBJbXByaW1lcmllIE5hdGlvbmFsZSBTdGFu
ZGFyZDAeFw0xMzA1MjgwMDAwMDBaFw0xOTA1MjgwMDAwMDBaMIGGMQswCQYDVQQGEwJGUjEkMCIG
A1UECgwbR3JvdXBlIEltcHJpbWVyaWUgTmF0aW9uYWxlMRwwGgYDVQQLDBMwMDAyIDQxMDQ5NDQ5
NjAwMDQ2MTMwMQYDVQQDDCpBQyBJbXByaW1lcmllIE5hdGlvbmFsZSBTdGFuZGFyZCBQZXJzb25u
ZWwwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDEKEH8fAgooXCi4wr7jpsFVNRVpsHg
ZxZQ5PDT5tzPnPqb6Qldv20Jh37mLEgjrwv+emGMpe8f7OVhCCNcVJ5RVkvCn04otVVEpEk1D26x
BRA2Oa2AF/50hgMq9D4ZwIArOOg3WMXW4gVPw/v1e99nmhAM62sDYwco/hPLXaiBh3UnuC5BvHOq
yaEllGw8l9hmWyGqOP6+kpMnm+ezjc9q3sMwKsItGg35jpZNlea2u/nEmiz5Qk4kdB0UnMEVThjm
tFBeojuDYsq6lTlevDxjFPb70O8n1Lwh2px7Ihs2vjxGEKSjRx6CdkQiA7g2VsVwWgQ27kjwH1u/
heRaChx3AgMBAAGjggE0MIIBMDASBgNVHRMBAf8ECDAGAQH/AgEAMA4GA1UdDwEB/wQEAwIBBjBJ
BgNVHSAEQjBAMD4GBFUdIAAwNjA0BggrBgEFBQcCARYoaHR0cDovL3d3dy5pbXByaW1lcmllbmF0
aW9uYWxlLmZyL0dJTi9QQzB/BgNVHR8EeDB2MDegNaAzhjFodHRwOi8vY3JsLmltcHJpbWVyaWVu
YXRpb25hbGUuZnIvR0lOL0FDLVNULVAuY3JsMDugOaA3hjVodHRwOi8vd3d3LmltcHJpbWVyaWVu
YXRpb25hbGUuZnIvR0lOL0NSTC9BQy1TVC1QLmNybDAdBgNVHQ4EFgQU5NVag71IgFOArY60uk9U
RU8yrbQwHwYDVR0jBBgwFoAUGSJk9EVmgc08jhQ4WmYky1VbzccwDQYJKoZIhvcNAQELBQADggIB
AIhwJcHidzpaoRBIUIX8PDDUWgzHhEGsFCAgnucJ6jogxjTS54Bv2t3zQ6FQcWxnxWcHLfTIDaEw
xBj9Zcr3BQNJ97oXFJ4DiEDVozjQ+3fPoYEE3Wz3QmoQvtIMSmUcI27pkjeRvpUFjFzgVfpYtsTZ
Btmm7YjTb4ua7bsluEiZ2kBtwNerJqErGuczuD7N6eMdVDpMfnPtq0RbTtTFXNLC5xev1tX3VDfr
09QptezWq9N3zLPHIcRfU34+Skz6kUJR0sBsCVmwKg0gtL0HVPDjHSLbhCcnTjPqN1tdTkZyKGmc
SwudbA2B9MEEhbbKDjCht1E16p62nvPiuu/5oMWZo7d/ervy5PMb9Palu79aA0Z5dnNbwvJjWTrI
ze7kGTvyybC6vfkNDCUvIoWrq2RCYNGNdx0EZwZMQM+Y3mv/OlbzLtRPQhiwV1YMBjyO79Vr8SxC
YPDePn3HV4hopZPhQTj/m3TVxNv2ygNZ6Ekjse3Uiu0QP7xsY2mWQFJQU4geIshJgIYoyET7iIJl
J0UUAIFeEFYFMPeq4JzbQOmxWjVqIeRkOE/GGImNMBosHAuhlA9Qcj2EED+qKG4mqq7FIwpvKVR7
NF1gTgCZUvA5j4J1lmim7rVlwf5jjYztunh4jq6LHZSrMgA1GwZHyCVVd8FCLCGpk6xpc1ncbU0s

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *ACR Imprimerie Nationale Standard*

Issuer OU: *0002 41049449600046*

Issuer O: *Groupe Imprimerie Nationale*

Issuer C: *FR*

Subject CN: *AC Imprimerie Nationale Standard Personnel*

Subject OU: *0002 41049449600046*

Subject O: *Groupe Imprimerie Nationale*

Subject C: *FR*

Valid from: *Tue May 28 02:00:00 CEST 2013*

Valid to: *Tue May 28 02:00:00 CEST 2019*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C4:28:41:FC:7C:08:28:A1:70:A2:E3:0A:FB:8E:9B:05:
54:D4:55:A6:C1:E0:67:16:50:E4:F0:D3:E6:DC:CF:9C:FA:9B:E9:09:5D:BF:6D:09:87:7E:E6:2C:48:23:AF:0B:FE:7A:61:8C:A5:EF:1F:EC:E5:61:08:23:5C:54:9E:51:56:

4B:C2:9F:4E:28:B5:55:44:A4:49:35:0F:6E:B1:05:10:36:39:AD:80:17:FE:74:86:03:2A:F4:3E:19:C0:80:2B:38:E8:37:58:C5:D6:E2:05:4F:C3:FB:F5:7B:DF:67:9A:10:0C:EB:6B:03:63:07:28:FE:13:CB:5D:A8:81:87:75:27:B8:2E:41:BC:73:AA:C9:A1:25:94:6C:3C:97:D8:66:5B:21:AA:38:FE:BE:92:93:27:9B:E7:B3:8D:CF:6A:DE:C3:30:2A:C2:2D:1A:0D:F9:8E:96:4D:95:E6:B6:BB:F9:C4:9A:2C:F9:42:4E:24:74:1D:14:9C:C1:15:4E:18:E6:B4:50:5E:A2:3B:83:62:CA:BA:95:39:5E:BC:3C:63:14:F6:FB:D0:EF:27:D4:BC:21:DA:9C:7B:22:1B:36:BE:3C:46:10:A4:A3:47:1E:82:76:44:22:03:B8:36:56:C5:70:5A:04:36:EE:48:F0:1F:5B:BF:85:E4:5A:0A:1C:77:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

Certificate Policies *Policy OID: 2.5.29.32.0*

CPSpointer: http://www.imprimerienationale.fr/GIN/PC

CRL Distribution Points *http://crl.imprimerienationale.fr/GIN/AC-ST-P.crl*

http://www.imprimerienationale.fr/GIN/CRL/AC-ST-P.crl

Subject Key Identifier *E4:D5:5A:83:BD:48:80:53:80:AD:8E:B4:BA:4F:54:45:4F:32:AD:B4*

Authority Key Identifier *19:22:64:F4:45:66:81:CD:3C:8E:14:38:5A:66:24:CB:55:5B:CD:C7*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *72:13:AA:35:4A:C3:4C:36:51:92:07:55:7C:9E:53:D7:DD:05:DE:95:5D:F9:0D:6A:2E:C2:D9:BE:7B:AE:E4:EF*

X509SubjectName

Subject CN: *AC Imprimerie Nationale Standard Personnel*

Subject OU: *0002 41049449600046*

Subject O: *Groupe Imprimerie Nationale*

Subject C: *FR*

X509SKI

X509 SK I *5NVag71IgFOArY60uk9URU8yrbQ=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2017-10-31T23:00:00Z*

TSP Service Definition URI

URI *[en]* *http://www.imprimerienationale.fr/GIN/PC*

URI *[fr]* *http://www.imprimerienationale.fr/GIN/PC*

12.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

12.2.2 - Extension (critical): Qualifiers [QCWithQSCD, QCForESig]

Qualifier type description *[en]* *undefined.*

[fr] *undefined.*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithQSCD*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForESig*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Policy Identifier nodes:

Identifier *1.2.250.1.295.1.1.4.3.1.102.2*

12.3 - Service (granted): Pass'IN - Signature eIDAS Elevé

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Pass'IN - Signature eIDAS Elevé*

Name *[fr]* *Pass'IN - Signature eIDAS Elevé*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *149207792582040060146370017270345380418510 5*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIG5DCCBMygAwIBAgISESDSq6tviOWltuRs5UwhS0YRMA0GCSqGSIb3DQEBDAUAMIGPMQswCQYD
VQQGEwJGUjEkMCIGA1UECgwbR3JvdXBlIEltcHJpbWVyaWUgTmF0aW9uYWxlMRcwFQYDVQQLDA4w
MDAyIDQxMDQ5NDQ5NjEYMBYGA1UEYQwPTlRSRlItNDEwNDk0NDk2MScwJQYDVQQDDB5BQyBJbXBy

aW1lcmllIE5hdGlvbmFsZSBSYWNpbmUwHhcNMTYwNDI4MDAwMDAwWhcNMjYwNDI4MDAwMDAwWjCB
mTELMAkGA1UEBhMCRlIxJDAiBgNVBAoMG0dyb3VwZSBJbXByaW1lcmllIE5hdGlvbmFsZTEXMBUG
A1UECwwOMDAwMiA0MTA0OTQ0OTYxGDAWBgNVBGEMD05UUkZSLTQxMDQ5NDQ5NjExMC8GA1UEAwwo
QUMgSW1wcmltZXJpZSBOYXRpb25hbGUgRWxldsOpIFBlcnNvbm5lbDCCAiIwDQYJKoZIhvcNAQEB
BQADggIPADCCAgoCggIBAO83N6fPT2DZoo7/ACsDf/P6MzqMISne8Pau8j8RnKnZzQSXpc/SIH8e
4SoEQn9doEmRBTauPcYa2pZmN0tEplHWYy34mJdYd1pVoBFK/aCuE003sOT1hrrCkl+JKg5SuQct
CnHf/mHuajkkE4O10kwKMYO0VNbNeQcgns8vDbWfOKjMgvkJqzEsRiXvy5x4RCGQa7hM6B02om5z
0/xpq5QmuiEyn65EbfMKuXeLhM7M3W2sygNw8BF/jJBbZeNg0cF3OlGtoo64pA3C8OZ6gYabw0yJ
hRKHdUmAAKnipdCTdH/XFdZn8g8mpbUdyB5K5xAgLqWbHC03fVd5VFqMbpUkLKcmbdgkLrxZFi3D
dV6Ubykaur9Tn8AVsyIF4s80xvUNSONc+6VsSohl722ou7n4TwMxTqKRyzj3qtQ7KepWfFJmY0om
xlcyesHIs8DZvZ53yUQwMWWTVIXF3Lc2P/Ir7KVWbpkxUQgi3IcpvaLFNQ0nymCso2FF6Ky5eY6C
LArbY1c2yml1CRM2g3V2E3FS7vAmcgYHsCyhjDDtcBr786Nv3KbBdB/QhwB2qEmEzcpNo/WgeUtz
OHQHK42sAH7S3+SWnlUS0cWIH7BpAV/HS9ruSkFygCrAcDliyA2WJEY+4gxvodPMVFGIL/m327BK
4z68lMnOCEgiR1DJrSObAgMBAAGjggEsMIIBKDAOBgNVHQ8BAf8EBAMCAQYwSQYDVR0gBEIwQDA+
BgRVHSAAMDYwNAYIKwYBBQUHAgEWKGh0dHA6Ly93d3cuaW1wcmltZXJpZW5hdGlvbmFsZS5mci9H
SU4vUEMwEgYDVR0TAQH/BAgwBgEB/wIBADB3BgNVHR8EcDBuMDegNaAzhjFodHRwOi8vd3d3Lmlt
cHJpbWVyaWVuYXRpb25hbGUuZnIvR0lOL0NSTC9BQ1luY3JsMDOgMaAvhi1odHRwOi8vY3JsLmlt
cHJpbWVyaWVuYXRpb25hbGUuZnIvR0lOL0FDUi5jcmwwHQYDVR0OBBYEFMmqtpc1mbXdR82fVL5/
3igpzjoVMB8GA1UdIwQYMBaAFM0PZw6rbyEEqHc6VrtEUH/o+JTpMA0GCSqGSIb3DQEBDAUAA4IC
AQCxPN8XIvp7dNRClF3I7whYDY691Yz8H0KMX+GpvN4ZOS03UyyDbkUwIWHSYbvktuqcsLI4BisT
0wl0Ld+mkp87N6VYKxZaLmksEC6SxL6iaffESKeVVe77Wi/NG+JdgRxGRC/8xe+mMhsY2IRG/I/+
VgIll7WO2TRyabNa8wtbvZyqIkP/PzwpvAfUKuK/+A/Gp8TGmjlg8/KD2NYWz06kZuir28ifIuui
ZI+iTI9Keu7hXmhzAyBjw66fNyj7rw8klft4kMbJwfril7ALEtjpCJeQLCt1POBq787NQrMtXLfR
QljhGEUr/5yAfKUtjeYF4D0fjLIQRI0IRzZx7ppzqDOVQbgWU8hl9t/K3iQLR4OrLSA/VQuz8HEE
wnfDVtf8DBKeb0kuCVFlYfxF3Nl6LI+xd2IbydLJY4WixX8J4oJNGJx51ky2O8BGKSdYx1hcxHf1
pBecbnxGq7zYdDbgrd+6aPRACr4pr8pM7svpI18Z26aBNZP0GEBqMiCKx8PqCtpHPUckOponsCXg
83m6/jucKpgC97rBTD/OS7RMkpAl3izgNX6HK/p2O4fAeCEL9cQzKSiQ1wlGt1I7AkDbGbW9snI9
AcEDmcGnRW+BdOegAKVY80i9vdEVTKw3DxGzRkQYa3vJkgHqpK7qA+x30sgFQS3DrreaOwKkM5j8 mw==

-----END CERTIFICATE-----

Signature algorithm: *SHA384withRSA*

Issuer CN: *AC Imprimerie Nationale Racine*

Issuer 2.5.4.97: *NTRFR-410494496*

Issuer OU: *0002 410494496*

Issuer O: *Groupe Imprimerie Nationale*

Issuer C: *FR*

Subject CN: *AC Imprimerie Nationale Elevé Personnel*

Subject 2.5.4.97: *NTRFR-410494496*

Subject OU: *0002 410494496*

Subject O: *Groupe Imprimerie Nationale*

Subject C: *FR*

Valid from: *Thu Apr 28 02:00:00 CEST 2016*

Valid to: *Tue Apr 28 02:00:00 CEST 2026*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:EF:37:37:A7:CF:4F:60:D9:A2:8E:FF:00:2B:03:7F:F3:FA:33:3A:8C:21:29:DE:F0:F6:AE:F2:3F:11:9C:A9:D9:CD:04:97:A5:CF:D2:20:7F:1E:E1:2A:04:42:7F:5D:A0:49:91:05:36:AE:3D:C6:1A:DA:96:66:37:4B:44:A6:51:D6:63:2D:F8:98:97:58:77:5A:55:A0:11:4A:FD:A0:AE:13:4D:37:B0:E4:F5:86:BA:C2:92:5F:89:2A:0E:52:B9:07:2D:0A:71:DF:FE:61:EE:6A:39:24:13:83:B5:D2:4C:0A:31:83:B4:54:D6:CD:79:07:20:9E:CF:2F:0D:B5:9F:38:A8:CC:82:F9:09:AB:31:2C:46:25:EF:CB:9C:78:44:21:90:6B:B8:4C:E8:1D:36:A2:6E:73:D3:FC:69:AB:94:26:BA:21:32:9F:AE:44:6D:F3:0A:B9:77:8B:84:CE:CC:DD:6D:AC:CA:03:70:F0:11:7F:8C:90:5B:65:E3:60:D1:C1:77:3A:51:AD:A2:8E:B8:A4:0D:C2:F0:E6:7A:81:86:9B:C3:4C:89:85:12:87:75:49:80:00:A9:E2:A5:D0:93:74:7F:D7:15:D6:67:F2:0F:26:A5:B5:1D:C8:1E:4A:E7:10:20:2E:A5:9B:1C:2D:37:7D:57:79:54:5A:8C:6E:95:24:2C:A7:26:6D:D8:24:2E:BC:59:16:2D:C3:75:5E:94:6F:29:1A:BA:BF:53:9F:C0:15:B3:22:05:E2:CF:34:C6:F5:0D:48:E3:5C:FB:A5:6C:4A:88:65:EF:6D:A8:BB:B9:F8:4F:03:31:4E:A2:91:CB:38:F7:AA:D4:3B:29:EA:56:7C:52:66:63:4A:26:C6:57:32:7A:C1:C8:B3:C0:D9:BD:9E:77:C9:44:30:31:65:93:54:85:C5:DC:B7:36:3F:F2:2B:EC:A5:56:6E:99:31:51:08:22:DC:87:29:BD:A2:C5:35:0D:27:CA:60:AC:A3:61:45:E8:AC:B9:79:8E:82:2C:0A:DB:63:57:36:CA:62:35:09:13:36:83:75:76:13:71:52:EE:F0:26:72:06:07:B0:2C:A1:8C:30:ED:70:1A:FB:F3:A3:6F:DC:A6:C1:74:1F:D0:87:00:76:A8:49:84:CD:CA:4D:A3:F5:A0:79:4B:73:38:74:07:2B:8D:AC:00:7E:D2:DF:E4:96:9E:55:12:D1:C5:88:1F:B0:69:01:5F:C7:4B:DA:EE:4A:41:72:80:2A:C0:70:39:62:C8:0D:96:24:46:3E:E2:0C:6F:A1:D3:CC:54:51:88:2F:F9:B7:DB:B0:4A:E3:3E:BC:94:C9:CE:08:48:22:47:50:C9:AD:23:9B:02:03:01:00:01

Certificate Policies

Policy OID: 2.5.29.32.0

CPSpointer: http://www.imprimerienationale.fr/GIN/PC

Basic Constraints

IsCA: true - Path length: 0

CRL Distribution Points

http://www.imprimerienationale.fr/GIN/CRL/ACR.crl

http://crl.imprimerienationale.fr/GIN/ACR.crl

Subject Key Identifier

C9:AA:B6:97:35:99:B5:DD:47:CD:9F:54:BE:7F:DE:28:29:CE:3A:15

Authority Key Identifier

CD:0F:67:0E:AB:6F:21:04:A8:77:3A:56:BB:44:50:7F:E8:F8:94:E9

Key Usage:

keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

FD:1C:1F:E5:3E:9A:CD:8E:F0:CB:C3:A4:DC:1F:89:BD:F6:1C:1D:DF:B5:99:48:3A:07:E9:51:2B:12:6E:B1:CC

X509SubjectName

Subject CN:

AC Imprimerie Nationale Elevé Personnel

Subject 2.5.4.97:

NTRFR-410494496

Subject OU:

0002 410494496

Subject O:

Groupe Imprimerie Nationale

Subject C:

FR

X509 SK I

yaq2lzWZtd1HzZ9Uvn/eKCnOOhU=

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description

[en] *undefined.*

[fr] *undefined.*

Status Starting Time

2017-10-31T23:00:00Z

TSP Service Definition URI

URI *[en]* *http://www.imprimerienationale.fr/GIN/PC*

URI *[fr]* *http://www.imprimerienationale.fr/GIN/PC*

12.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

12.3.2 - Extension (critical): Qualifiers [QCWithQSCD, QCForESig]

Qualifier type description *[en]* *undefined.*

[fr] *undefined.*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithQSCD*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForESig*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Policy Identifier nodes:

Identifier *1.2.250.1.295.1.1.20.7.1.102.1*

12.4 - Service (granted): Pass'IN - Signature eIDAS Substantiel

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *Pass'IN - Signature eIDAS Substantiel*

Name *[fr]* *Pass'IN - Signature eIDAS Substantiel*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *149189272103883433173186539038929825443189l*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIG6TCCBNGgAwIBAgISESBHVoa1VSz2Vr7d9uVdVcaTMA0GCSqGSIb3DQEBDAUAMIGPMQswCQYD
VQQGEwJGUjEkMCIGA1UECgwbR3JvdXBlIEltcHJpbWVyaWUgTmF0aW9uYWxlMRcwFQYDVQQLDA4w
MDAyIDQxMDQ5NDQ5NjEYMBYGA1UEYQwPTlRSRlItNDEwNDk0NDk2MScwJQYDVQQDDB5BQyBJbXBy
aW1lcmllIE5hdGlvbmFsZSBSYWNpbmUwHhcNMTYwNDI4MDAwMDAwWhcNMjYwNDI4MDAwMDAwWjCB
njELMAkGA1UEBhMCRlIxJDAiBgNVBAoMG0dyb3VwZSBJbXByaW1lcmllIE5hdGlvbmFsZTEXMBUG
A1UECwwOMDAwMiA0MTA0OTQ0OTYxGDAWBgNVBGEMD05UUkZSLTQxMDQ5NDQ5NjE2MDQGA1UEAwwt
QUMgSW1wcmltZXJpZSBOYXRpb25hbGUgU3Vic3RhbnRpZWwgUGVyc29ubmVsMIICIjANBgkqhkiG
9w0BAQEFAAOCAg8AMIICCgKCAgEA3mblo/SwKcYJ2ANLU7nPo1sVZxG8t+Wg/hSbpJ2UERzxHwvU
ZbXwgQzEMlDSFXqnyiebUV+Qc2+fGvy5QazgxxVGw5QWz00bdZ1aWTYt/sg/2zqSrKiqx0k48S75
UjAEJn5Hcdt215uJ5QVcNI7qTyrngC+KCuAI9fFqcBsXlJuIr9g42Vd7Yf2Ict8dXE+b16P2wbjr
bh7KAtvnnASPngfLV2aFaJ2eQdonausGlzGN1P5GPCgr7j9B0y+RhyTwPi6ISrdk9F84pXNzcGc2
BDJF4UiSBOwsehy1Yv6YtsXnQZyXth0BEvmJ7aCbqByUkmSRAs3QaSAsLS5LYHHqr8rVZBNDwUtN
UAyRR3nf+jYMFDHK0DWPwkyXyTQl8eUzQh9i4+mkWdY2HMtFmerm+6v4TEQuNoUKIqXBYPSZm+dr
tFLYL4vn+Ka1vTN/aFjFOOKKs+K5PgIBSzdqOBAhg+b/Yht68YAwcnRANZyv3SXRlGuaO5wL5dS8
ywIvFSA6klBYG61Yso/cHeK8yfj7847AoLwDnMjTVWhooAQrNH075GxsVx/TQDrXj4+5dKjLq0b8
HkGuUWZaJYjqdhTq+kgnoMQEUQYpfzoZd47YBJ1c7DkZV+phMoUDEORFqTURRENRehw94PyMhuTm
uSBUb7brMeA98WM+A201Hbkkiw0CAwEAAaOCASwwggEoMA4GA1UdDwEB/wQEAwIBBjBJBgNVHSAE
QjBAMD4GBFUdIAAwNjA0BggrBgEFBQcCARYoaHR0cDovL3d3dy5pbXByaW1lcmllbmF0aW9uYWxl
LmZyL0dJTi9QQzASBgNVHRMBAf8ECDAGAQH/AgEAMHcGA1UdHwRwMG4wN6A1oDOGMWh0dHA6Ly93
d3cuaW1wcmltZXJpZW5hdGlvbmFsZS5mci9HSU4vQ1JML0FDUi5jcmwwM6AxoC+GLWh0dHA6Ly9j
cmwuaW1wcmltZXJpZW5hdGlvbmFsZS5mci9HSU4vQUNSLmNybDAdBgNVHQ4EFgQU1dLlRV9D2gJ0
NTWfvJguzbOn4dAwHwYDVR0jBBgwFoAUzQ9nDqtvIQSodzpWu0RQf+j4lOkwDQYJKoZIhvcNAQEM
BQADggIBAHt4aEvgG20oyD66Rryl63QmTCIVUWYwA+O2HzqkR01R6luSTvbcE10nlt8HCpUsrpT0
1rdUZBXi/HT7EWMgzxotBmm43Lc6JcfouDVFnRPtkIhFW/ZoZngVIOOUryiN/uY3E5WGf2tDf3Wd
jr3n2e1jGWh4AGDp5DR/fKf105oP/dGwPiqfs8/tIeEGsQWALePKyqzWS+w7ii4bvg1jV7kIWALf
VJdi4zLFqyX4VsfptOJNX9rIo8I+9fxMSLfNj8EjU8MrIp2kPxFU4XR0+WqPK8xs9H2xVtB0ZDOA
tGz5qPNDa2jDqAUJhNRJDlcWZtYZPZ1PshuHqh5CFiZ/kn38ZPkxRQLPVOwEoXWR7POgYG3HQxcD
qN8DIkcyQo8/VdOHnT/UiXxkd1fBx8yiFCpSujOj/o0R1TWgQFP7CMF7gsSwumxXrrRcUFxlrMe4
vxjGFvhELFoPY49XFyThNvcEpJbKCcw5L6GjweAqa1uK7zjypu75cLgUnL+gF5YEZ/xbNPJZyBuZ
59Q/WHOM+GAo/RoGH2IuJyOlmInVN+b401EidSkUxgVn371a5cjyWdRBeTRHVcsY/XUvQ1cq+0v1
PFiJ3AOKi6eJK5r7EkPMxdSblek2IoFzsqzighkeGZ97IYK/WXljYP3RqvFQtUsBAXh9aoLwEojs
kXwjnxi2

-----END CERTIFICATE-----

Signature algorithm: *SHA384withRSA*

Issuer CN: *AC Imprimerie Nationale Racine*

Issuer 2.5.4.97: *NTRFR-410494496*

Issuer OU: *0002 410494496*

Issuer O: *Groupe Imprimerie Nationale*

Issuer C: *FR*

Subject CN: *AC Imprimerie Nationale Substantiel Personnel*

Subject 2.5.4.97: *NTRFR-410494496*

Subject OU: *0002 410494496*

Subject O: *Groupe Imprimerie Nationale*

Subject C: *FR*

Valid from: *Thu Apr 28 02:00:00 CEST 2016*

Valid to: *Tue Apr 28 02:00:00 CEST 2026*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:DE:66:E5:A3:F4:B0:29:C6:09:D8:03:4B:53:B9:CF:A3:5B:15:67:11:BC:B7:E5:A0:FE:14:9B:A4:9D:94:11:1C:F1:1F:0B:D4:65:B5:F0:81:0C:C4:32:50:D2:15:7A:A7:CA:27:9B:51:5F:90:73:6F:9F:1A:FC:B9:41:AC:E0:C7:15:46:C3:94:16:CF:4D:1B:75:9D:5A:59:36:2D:FE:C8:3F:DB:3A:92:AC:A8:AA:C7:49:38:F1:2E:F9:52:30:04:26:7E:47:71:DB:76:D7:9B:89:E5:05:5C:34:8E:EA:4F:2A:E7:80:2F:8A:0A:E0:08:F5:F1:6A:70:1B:17:94:9B:88:AF:D8:38:D9:57:7B:61:FD:88:72:DF:1D:5C:4F:9B:D7:A3:F6:C1:B8:EB:6E:1E:CA:02:DB:E7:9C:04:8F:9E:07:CB:57:66:85:68:9D:9E:41:DA:27:6A:EB:06:97:31:8D:D4:FE:46:3C:28:2B:EE:3F:41:D3:2F:91:87:24:F0:3E:2E:88:4A:B7:64:F4:5F:38:A5:73:73:70:67:36:04:32:45:E1:48:92:04:EC:2C:7A:1C:B5:62:FE:98:B6:C5:E7:41:9C:97:B6:1D:01:12:F9:89:ED:A0:9B:A8:1C:94:92:64:91:02:CD:D0:69:20:2C:2D:2E:4B:60:71:EA:AF:CA:D5:64:13:43:C1:4B:4D:50:0C:91:47:79:DF:FA:36:0C:14:31:CA:D0:35:8F:C2:4C:97:C9:34:25:F1:E5:33:42:1F:62:E3:E9:A4:59:D6:36:1C:CB:45:99:EA:E6:FB:AB:F8:4C:44:2E:36:85:0A:22:A5:C1:60:F4:99:9B:E7:6B:B4:52:D8:2F:8B:E7:F8:A6:B5:BD:33:7F:68:58:C5:38:E2:8A:B3:E2:B9:3E:02:01:4B:37:6A:38:10:21:83:E6:FF:62:1B:7A:F1:80:30:72:74:40:35:9C:AF:DD:25:D1:94:6B:9A:3B:9C:0B:E5:D4:BC:CB:02:2F:15:20:3A:92:50:58:1B:AD:58:B2:8F:DC:1D:E2:BC:C9:F8:FB:F3:8E:C0:A0:BC:03:9C:C8:D3:55:68:68:A0:04:2B:34:7D:3B:E4:6C:6C:57:1F:D3:40:3A:D7:8F:8F:B9:74:A8:CB:AB:46:FC:1E:41:AE:51:66:5A:25:88:EA:76:14:EA:FA:48:27:A0:C4:04:51:06:29:7F:3A:19:77:8E:D8:04:9D:5C:EC:39:19:57:EA:61:32:85:03:10:E4:45:A9:35:11:44:43:51:7A:1C:3D:E0:FC:8C:86:E4:E6:B9:20:54:6F:B6:EB:31:E0:3D:F1:63:3E:03:6D:35:1D:B9:24:8B:0D:02:03:01:00:01

Certificate Policies *Policy OID: 2.5.29.32.0*

CPSpointer: http://www.imprimerienationale.fr/GIN/PC

Basic Constraints *IsCA: true - Path length: 0*

CRL Distribution Points *http://www.imprimerienationale.fr/GIN/CRL/ACR.crl*

http://crl.imprimerienationale.fr/GIN/ACR.crl

Subject Key Identifier *D5:D2:E5:45:5F:43:DA:02:74:35:35:9F:BC:98:2E:CD:B3:A7:E1:D0*

Authority Key Identifier *CD:0F:67:0E:AB:6F:21:04:A8:77:3A:56:BB:44:50:7F:E8:F8:94:E9*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *B3:22:10:E4:C5:D7:02:79:09:A4:3A:4A:BB:F5:13:C3:C7:C0:1C:01:35:19:4A:FB:93:55:41:F2:89:B1:A1:15*

X509SubjectName

Subject CN: *AC Imprimerie Nationale Substantiel Personnel*

Subject 2.5.4.97: *NTRFR-410494496*

Subject OU: *0002 410494496*

Subject O: *Groupe Imprimerie Nationale*

Subject C: *FR*

X509 SK I *1dLlRV9D2gJ0NTWfvJguzbOn4dA=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2017-10-31T23:00:00Z*

TSP Service Definition URI

URI *[en]* *http://www.imprimerienationale.fr/GIN/PC*

URI *[fr]* *http://www.imprimerienationale.fr/GIN/PC*

12.4.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

12.4.2 - Extension (critical): Qualifiers [QCWithQSCD, QCForESig]

Qualifier type description *[en]* *undefined.*

[fr] *undefined.*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithQSCD*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForESig*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Policy Identifier nodes:

Identifier *1.2.250.1.295.1.1.8.6.1.102.1*

13 - TSP: Conseil Supérieur du Notariat

TSP Name

Name *[fr]* *Conseil Supérieur du Notariat*

Name *[en]* *The High Council of French Notariat*

TSP Trade Name

Name *[en]* *VATFR-67784350134*

Name *[fr]* *VATFR-67784350134*

PostalAddress

Street Address	*[fr]*	*Membre du bureau du CSN - Chargé des technologies de l'information et de la communication - 60 Boulevard de la Tour-Maubourg*
Locality	*[fr]*	*Paris*
Postal Code	*[fr]*	*75007*
Country Name	*[fr]*	*FR*

PostalAddress

Street Address	*[en]*	*Membre du bureau du CSN;chargé des technologies de l'information et de la communication;60 Boulevard de la Tour Maubourg*
Locality	*[en]*	*Paris*
Postal Code	*[en]*	*75007*
Country Name	*[en]*	*FR*

ElectronicAddress

URI	*mailto:autorite-certification@notaires.fr*
URI	*http://http://www.preuve-electronique.org/contacts.html*

TSP Information URI

URI	*[en]*	*https://www.preuve-electronique.org*
URI	*[fr]*	*https://www.preuve-electronique.org*

13.1 - Service (granted): REAL 2017 - Délivrance de certificats de signature clé REAL

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description	*[en]*	*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*
	[fr]	*Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name	*[fr]*	*REAL 2017 - Délivrance de certificats de signature clé REAL*
Name	*[en]*	*REAL 2017 - Délivrance de certificats de signature clé REAL*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *3*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIEKjCCAxKgAwIBAgIBAzANBgkqhkiG9w0BAQsFADBlMQswCQYDVQQGEwJGUjEmMCQGA1UECgwd
Q09OU0VJTCBTVVBFUklFVVIgRFUgTk9UQVJJQVQxFzAVBgNVBAsMDjAwMDIgNzg0MzUwMTM0MRUw
EwYDVQQLDAxOb3RhaXJlczIwMjAwHhcNMTMxMjEyMDg1ODI1WhcNMTcxMjEyMDg1ODI1WjBhMQsw
CQYDVQQGEwJGUjEmMCQGA1UECgwdQ09OU0VJTCBTVVBFUklFVVIgRFUgTk9UQVJJQVQxFzAVBgNV
BAsMDjAwMDIgNzg0MzUwMTM0MREwDwYDVQQLDAhSRUFMMjAxNzCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAKj+xNdcy6AGdPBY6ygHsyIFloEJcLv1PERHserpf3YOGb1WGzo+nnPl9wtu
tdp1fUiDe4FUkpQ5sxWF7fl6W+L1xxlaKb7o79i6TxzvJWVkPwwSg7lj8xJFw+saoFaiXkTD2Hc/
5TpcY3qYLzxiuPABWXbt1lU1DEawb24WjZZctmnc3Q53dz7PzzVG2reYsL+P06KTW2fDvFr/HV1x
XPO54eqW6k80AVEbZOfQYqludKRx2R6x5Qp2hfnxHV36UpqHvCNtJQZfzhf4W3PW1aybqBQ0MU2g
9GnbxnkNWldz1x/iaq0cTtx+4mEid8P5tHgBdVnPyuJhuo2GrNGLBBcCAwEAAaOB6DCB5TAPBgNV
HRMBAf8EBTADAQH/MB0GA1UdDgQWBBSj4oVJ5os2elDYjEPUazuz/QO/WTAfBgNVHSMEGDAWgBTc
iNpXcr0sc8tXe+LlTd2jzPghZzArBgNVHSAEJDAiMA0GCyqBegFOAQEDAQEFMBEGDyqBeg FOAQED
AQMBAgQDBDAOBgNVHQ8BAf8EBAMCAQYwVQYDVR0fBE4wTDBKoEigRoZEaHR0cDovL3d3dy5wcmV1
dmUtZWxlY3Ryb25pcXVlLm9yZy9MaXN0ZVJldm9jYXRpb25zL25vdGFpcmVzMjAyMC5hcmwwDQYJ
KoZIhvcNAQELBQADggEBAJ7GYvJJccTwPR0vK2SXgHsThoe3AmvRn1qAnh1FbQTeGSXbAWsW4fKJ
fPehIcNyIAtxuszWEATSa+UkE2rFGOW1APs7MnIpFfVpguCwFxJ+KnYTI3q4YXQnW8gk8qBctVmQ
H3eAocYc9NpjkV4Cqqx3Oi2dE6osbALnsUgdgwVz7gczxmqfpaMZ0c2R78uKHseYND48MzC3/2X0
3XMeJ1v8cHHpGelNdq+Ck5Juh7lZhi+EMGXmiM+ho8ZQkbsjWr+pMHGZ1oC1AV4XsoNJt/WmjiAQ
Wsuho743jYSVHsQhGkjtCo7riY7qxipaVA0HD3AU4d4BV1SOvArgFrFazYw=

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer OU: *Notaires2020*

Issuer OU: *0002 784350134*

Issuer O: *CONSEIL SUPERIEUR DU NOTARIAT*

Issuer C: *FR*

Subject OU: *REAL2017*

Subject OU: *0002 784350134*

Subject O: *CONSEIL SUPERIEUR DU NOTARIAT*

Subject C: *FR*

Valid from: *Thu Dec 12 09:58:25 CET 2013*

Valid to: *Tue Dec 12 09:58:25 CET 2017*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:A8:FE:C4:D7:5C:CB:A0:06:74:F0:58:EB:28:07:B3:22:
05:96:81:09:70:BB:F5:3C:44:47:B1:EA:E9:7F:76:0E:19:BD:56:1B:3A:3E:9E:73:E5:F7:0B:6E:B5:DA:75:7D:48:83:7B:81:54:92:94:39:B3:15:85:ED:F9:7A:5B:E2:F5:
C7:19:5A:29:BE:E8:EF:D8:BA:4F:1C:EF:25:65:64:3F:0C:12:83:B2:23:F3:12:45:C3:EB:1A:A0:56:A2:5E:44:C3:D8:77:3F:E5:3A:5C:63:7A:98:2F:3C:62:B8:F0:01:59:
76:ED:D6:55:35:0C:46:B0:6F:6E:16:8D:96:5C:B6:69:DC:DD:0E:77:77:3E:CF:CF:35:46:DA:B7:98:B0:BF:8F:D3:A2:93:5B:67:C3:BC:5A:FF:1D:5D:71:5C:F3:B9:E1:E

A:96:EA:4F:34:01:51:1B:64:E7:D0:62:A9:6E:74:A4:71:D9:1E:B1:E5:0A:76:85:F9:F1:1D:5D:FA:52:9A:87:BC:23:6D:25:06:5F:CE:17:F8:5B:73:D6:D5:AC:9B:A8:14:34:31:4D:A0:F4:69:DB:C6:79:0D:5A:57:73:D7:1F:E2:6A:AD:1
C:4E:DC:7E:E2:61:22:77:C3:F9:B4:78:01:75:59:CF:CA:E2:61:BA:8D:86:AC:D1:8B:04:17:02:03:01:00:01

Basic Constraints *IsCA: true*

Subject Key Identifier *A3:E2:85:49:E6:8B:36:7A:50:D8:8C:43:D4:6B:3B:B3:FD:03:BF:59*

Authority Key Identifier *DC:88:DA:57:72:BD:2C:73:CB:57:7B:E2:E5:4D:DD:A3:CC:F8:21:67*

Certificate Policies *Policy OID: 1.2.250.1.78.1.1.3.1.1.5*

Policy OID: 1.2.250.1.78.1.1.3.1.3.1.2.4.3.4

CRL Distribution Points *http://www.preuve-electronique.org/ListeRevocations/notaires2020.arl*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *D5:CD:4C:04:16:39:41:62:0C:2E:08:D9:CE:A1:F4:70:D5:4E:3E:67:53:15:4B:7F:7A:DD:42:48:BD:DD:A5:74*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS101456/QCPPublic*

TSP Service Definition URI

URI *[en]* *http://www.preuve-electronique.org/PC_AC_REAL_1.2.250.1.78.1.1.3.1.3.1.1.22.pdf*

13.1.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

13.1.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[fr]* *AC REAL 2017 1.2.250.1.78.1.1.3.1.3.1.1.22*

Name *[en]* *AC REAL 2017 1.2.250.1.78.1.1.3.1.3.1.1.22*

Service digital identities

X509SubjectName

Subject OU: *REAL2017*

Subject OU: *0002 784350134*

Subject O: *CONSEIL SUPERIEUR DU NOTARIAT*

Subject C: *FR*

X509SKI

X509 SK I *o+KFSeaLNnpQ2IxD1Gs7s/0Dv1k=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

13.1.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

13.1.3 - History instance n.2 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[fr]* *AC REAL 2017*

Name *[en]* *AC REAL 2017*

Service digital identities

X509SubjectName

Subject OU: *REAL2017*

Subject OU: *0002 784350134*

Subject O: *CONSEIL SUPERIEUR DU NOTARIAT*

Subject C: *FR*

X509 SK I *o+KFSeaLNnpQ2IxD1Gs7s/0Dv1k=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

13.1.3.2 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

13.1.4 - History instance n.3 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[fr]* *AC REAL 2017*

Name *[en]* *AC REAL 2017*

Service digital identities

X509SubjectName

Subject OU: *REAL2017*

Subject OU: *0002 784350134*

Subject O: *CONSEIL SUPERIEUR DU NOTARIAT*

Subject C: *FR*

X509SKI

X509 SK I *o+KFSeaLNnpQ2IxD1Gs7s/0Dv1k=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2011-12-12T00:00:00Z*

13.2 - Service (withdrawn): AC REAL 2016

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[fr]* *AC REAL 2016*

Name *[en]* *AC REAL 2016*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIEjTCCA3WgAwIBAgIBATANBgkqhkiG9w0BAQsFADBlMQswCQYDVQQGEwJGUjEmMCQGA1UECgwd
Q09OU0VJTCBTVVBFUklFVVIgRFUgTk9UQVJJQVQxFzAVBgNVBAsMDjAwMDIgNzg0MzUwMTM0MRUw
EwYDVQQLDAxOb3RhaXJlczIwMjAwHhcNMTIwMjAxMDkyOTIwWhcNMTYwMjAxMDkyOTIwWjBhMQsw
CQYDVQQGEwJGUjEmMCQGA1UECgwdQ09OU0VJTCBTVVBFUklFVVIgRFUgTk9UQVJJQVQxFzAVBgNV
BAsMDjAwMDIgNzg0MzUwMTM0MREwDwYDVQQLDAhSRUFMMjAxNjCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAMjeBn9s7KfL3LCwp8ecC2HtBkT9Mqd3YlkPimyG7Zyr7Cok1g4rh3OQC4Uj
wwW9gZDCUlc3RZR/VIL6p+LybNuGT1JidQEaklLaygWbpKjs+1RZ6ggaKjnyLsF4w7OmHfDEFHo4
T5xFgSm+AxkolDwzNvAZ9n+MeY1XCBUVBg1NC/tC/91cVna7GWc1hX1KXmVuymqVrroNsgrI5jLx
a84+H06dT+ZilsBAXroPjM+yHbDUgv5PGv1rsQNd/8SPGx/CVzwcvl8WbA4zVToQBiqXytTXvtTy
2q8wUw/PxjsignhW7awg0ADVLAPxuF0CfoWvbFTkbELquk1QjSGVENUCAwEAAaOCAUowggFGMA8G
A1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFFC+XBmPIyr5KNulet8xhem4tLhCMB8GA1UdIwQYMBaA
FNyI2ldyvSxzy1d74uVN3aPM+CFnMIGLBgNVHSAEgYMwgYAwawYLKoF6AU4BAQMBAQUwXDBaBggr
BgEFBQcCARZOaHR0cDovL3d3dy5wcmV1dmUtZWxlY3Ryb25pcXVlLm9yZy9QQ19BQ19OT1RBSVJF
U18xLjIuMjUwLjEuNzguMS4xLjMuMS4xLjUucGRmMBEGDyqBegFOAQEDAQMBAgQDBDAOBgNVHQ8B
Af8EBAMCAQYwVQYDVR0fBE4wTDBKoEigRoZEaHR0cDovL3d3dy5wcmV1dmUtZWxlY3Ryb25pcXVl
Lm9yZy9MaXN0ZVJldm9jYXRpb25zL25vdGFpcmVzMjAyMC5hcmwwDQYJKoZIhvcNAQELBQADggEB
AD6ip2ORTtzyGGCj34gccuBxX9RUjyVFoO0MyL9zsXo9Jf2XiOjq9t3GD9sBRMzoFdJo+VL/t7+u
IW059DfjZBVsQdF2ZIFXcyIOTrFCH6MPKy/EABtUUSPtG/Mx8MTZTKdKb3rFQROXmx/+mLw0B3au
g4fkZgD9aHj54jqBqosLmNE9T/CliDH54StCbMQ3n2J+I/ZRdIFmh4PnsTW+KOUrNKyzw0YnaF6n
K5Cl1gQcfojqv4iww3vFbmY8UtOzHLcZKdhs5QuIEqsEkuX4sGuxwS01AphFSwQrkAz9ekiDGpgK
A5UVEmKkzs7lrRI2LOWWYF/UzLPCSlyT9iXktyM=

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer OU: *Notaires2020*

Issuer OU: *0002 784350134*

Issuer O: *CONSEIL SUPERIEUR DU NOTARIAT*

Issuer C: *FR*

Subject OU: *REAL2016*

Subject OU: *0002 784350134*

Subject O: *CONSEIL SUPERIEUR DU NOTARIAT*

Subject C: *FR*

Valid from: *Wed Feb 01 10:29:20 CET 2012*

Valid to: *Mon Feb 01 10:29:20 CET 2016*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C8:DE:06:7F:6C:EC:A7:CB:DC:B0:B0:A7:C7:9C:0B:61:ED:06:44:FD:32:A7:77:62:59:0F:8A:6C:86:ED:9C:AB:EC:2A:24:D6:0E:2B:87:73:90:0B:85:23:C3:05:BD:81:90:C2:52:57:37:45:94:7F:54:82:FA:A7:E2:F2:6C:DB:86:4F:52:62:75:01:1A:92:52:DA:CA:05:9B:A4:A8:EC:FB:54:59:EA:08:1A:2A:39:F2:2E:C1:78:C3:B3:A6:1D:F0:C4:14:7A:38:4F:9C:45:81:29:BE:03:19:28:94:3C:33:36:F0:19:F6:7F:8C:79:8D:57:08:15:15:06:0D:4D:0B:FB:42:FF:DD:5C:56:76:BB:19:67:35:85:7D:4A:5E:65:6E:CA:6A:95:AE:BA:0D:B2:0A:C8:E6:32:F1:6B:CE:3E:1F:4E:9D:4F:E6:62:96:C0:40:5E:BA:0F:8C:CF:B2:1D:B0:D4:82:FE:4F:1A:FD:6B:B1:03:5D:FF:C4:8F:1B:1F:C2:57:3C:1C:BE:5F:16:6C:0E:33:55:3A:10:06:2A:97:CA:D4:D7:BE:D4:F2:DA:AF:30:53:0F:CF:C6:3B:22:82:78:56:ED:A
C:20:D0:00:D5:2C:03:F1:B8:5D:02:7E:85:AF:6C:54:E4:6C:42:EA:BA:4D:50:8D:21:95:10:D5:02:03:01:00:01

Basic Constraints *IsCA: true*

Subject Key Identifier *50:BE:5C:19:8F:23:2A:F9:28:DB:A5:7A:DF:31:85:E9:B8:B4:B8:42*

Authority Key Identifier *DC:88:DA:57:72:BD:2C:73:CB:57:7B:E2:E5:4D:DD:A3:CC:F8:21:67*

Certificate Policies *Policy OID: 1.2.250.1.78.1.1.3.1.1.5*
CPS pointer: http://www.preuve-electronique.org/PC_AC_NOTAIRES_1.2.250.1.78.1.1.3.1.1.5.pdf Policy OID: 1.2.250.1.78.1.1.3.1.3.1.2.4.3.4

CRL Distribution Points *http://www.preuve-electronique.org/ListeRevocations/notaires2020.arl*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *C8:78:1A:8B:5B:BE:24:90:0F:97:D4:14:F8:24:D9:33:73:D8:2E:0F:A6:70:F5:95:2B:2B:AF:E9:C9:C8:99:D6*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*
[fr] *undefined.*

Status Starting Time *2016-09-30T00:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS101456/QCPPublic*

TSP Service Definition URI

URI *[en]* *http://www.preuve-electronique.org/PC_AC_REAL_1.2.250.1.78.1.1.3.1.3.1.1.22.pdf*

13.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

13.2.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[fr]* *AC REAL 2016*

Name *[en]* *AC REAL 2016*

Service digital identities

X509SubjectName

Subject OU: *REAL2016*

Subject OU: *0002 784350134*

Subject O: *CONSEIL SUPERIEUR DU NOTARIAT*

Subject C: *FR*

X509SKI

X509 SK I *UL5cGY8jKvko26V63zGF6bi0uEI=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

13.2.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

13.2.3 - History instance n.2 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[fr]* *AC REAL 2016*

Name *[en]* *AC REAL 2016*

Service digital identities

X509SubjectName

Subject OU: *REAL2016*

Subject OU: *0002 784350134*

Subject O: *CONSEIL SUPERIEUR DU NOTARIAT*

Subject C: *FR*

X509 SK I *UL5cGY8jKvko26V63zGF6bi0uEI=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2011-12-12T00:00:00Z*

13.3 - Service (withdrawn): AC REAL 2014

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[fr]* *AC REAL 2014*

Name *[en]* *AC REAL 2014*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIEjTCCA3WgAwIBAgIBATANBgkqhkiG9w0BAQUFADBlMQswCQYDVQQGEwJGUjEmMCQGA1UECgwd
Q09OU0VJTCBTVVBFUklFVVIgRFUgTk9UQVJJQVQxFzAVBgNVBAsMDjAwMDIgNzg0MzUwMTM0MRUw
EwYDVQQLDAxOb3RhaXJlczIwMTgwHhcNMTAwMzA4MTMzODA2WhcNMTQwMzA4MTMzODA2WjBhMQsw
CQYDVQQGEwJGUjEmMCQGA1UECgwdQ09OU0VJTCBTVVBFUklFVVIgRFUgTk9UQVJJQVQxFzAVBgNV
BAsMDjAwMDIgNzg0MzUwMTM0MREwDwYDVQQLDAhSRUFMMjAxNDCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAM0W+AbQlqh3at844+Mjfw33GVWedKH98lnVTVni/8M1vaU6QWXL3HEwdAm3
LPOKO+7cHyrRFLYdWmae8E6gDTqXxrlrioJW45ANt5uSmB+6/EOUvueSxZJUX4HzP3NyCsOzOYmN
S77qdYuhs629z7j8qmRrCY+rHEyeYuuZV5UQUHZeq+GNUEKhGaVxYpUOT4iQvYwc+XobKS4IWx02
vSUJ9YhRaDlTt+a7ilMbvKb412O3aeJH3pBswdBjsMciclN6i9gXE/MHIWeHZvLY8z0hrgrrtVQD
kzrQzvIh2KmU8u8w2li0qwJdPBLsgRRA87GFJDG/MVMbIqx8cybpTtsCAwEAAaOCAUowggFGMA8G
A1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFLx/fok25jSLCwEdUg/GuVSr5SbzMB8GA1UdIwQYMBaA
FBuCXELZ9iUJwC4N9c45IpROb1hUMIGLBgNVHSAEgYMwgYAwawYLKoF6AU4BAQMBAQMwXDBaBggr
BgEFBQcCARZOaHR0cDovL3d3dy5wcmV1dmUtZWxlY3Ryb25pcXVlLm9yZy9QQ19BQ19QC19OT1RBSVJF
U18xLjIuMjUwLjEuNzguMS4xLjMuMS4xLjMucGRmMBEGDyqBegFOAQEDAQMBAgQDBDAOBgNVHQ8B
Af8EBAMCAQYwVQYDVR0fBE4wTDBKoEigRoZEaHR0cDovL3d3dy5wcmV1dmUtZWxlY3Ryb25pcXVl
Lm9yZy9MaXN0ZVJldm9jYXRpb25zL25vdGFpcmVzMjAxOC5hcmwwDQYJKoZIhvcNAQEFBQADggEB
ABTJaYydyThsCVlwci1aLVnUEV02yMdvLDRc+aGqbZOAA3C6a6yrs3tG45gNWBWTdxX/nzNLVa1t
M+XhVjXjGQwis5VsddvHidQeGTlvRwRkBwxlM2nyRR3yve82QoB6JIREpApeZ53c05BvWenowzpx
wfelzru7qHWkkigDQF1GbMA8dIMg+oK4p6LjN5IulKQRRWpukw4OJi/c6IRV/NujlmDeLRcojRTC
NouYSp9wQ+oPGEeEBqAiRJit9ZcW4eWVpZXphiMjkCTlEfbigRAzEAXBr0POIfdLJ/ymZBlv5jb5
sFpYDD3jbaxQt1o55azb9WczokFHmWuenBSQP6U=

-----END CERTIFICATE-----

Signature algorithm: *SHA1withRSA*

Issuer OU: *Notaires2018*

Issuer OU: *0002 784350134*

Issuer O: *CONSEIL SUPERIEUR DU NOTARIAT*

Issuer C: *FR*

Subject OU: *REAL2014*

Subject OU: *0002 784350134*

Subject O: *CONSEIL SUPERIEUR DU NOTARIAT*

Subject C: *FR*

Valid from: *Mon Mar 08 14:38:06 CET 2010*

Valid to: *Sat Mar 08 14:38:06 CET 2014*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:CD:16:F8:06:D0:96:A8:77:6A:DF:38:E3:E3:23:7F:0D:
F7:19:55:9E:74:A1:FD:F2:59:D5:4D:59:E2:FF:C3:35:BD:A5:3A:41:65:CB:DC:71:30:74:09:B7:2C:F3:8A:3B:EE:DC:1F:2A:D1:14:B6:1D:5A:66:9E:F0:4E:A0:0D:3A:9
7:C6:B9:6B:8A:82:56:E3:90:0D:B7:9B:92:98:1F:BA:FC:43:94:BE:E7:92:C5:92:54:5F:81:F3:3F:73:72:0A:C3:B3:39:89:8D:4B:BE:EA:75:8B:A1:B3:AD:BD:CF:B8:FC:
AA:64:6B:09:8F:AB:1C:4C:9E:62:EB:99:57:95:10:50:76:5E:AB:E1:8D:50:42:A1:19:A5:71:62:95:0E:4F:88:90:BD:8C:1C:F9:7A:1B:29:2E:08:5B:1D:36:BD:25:09:F5
:88:51:68:39:53:B7:E6:BB:8A:53:1B:BC:A6:F8:D7:63:B7:69:E2:47:DE:90:6C:C1:D0:63:B0:C7:22:72:53:7A:8B:D8:17:13:F3:07:21:67:87:66:F2:D8:F3:3D:21:AE:0
A:EB:B5:54:03:93:3A:D0:CE:F2:21:D8:A9:94:F2:EF:30:DA:58:
B4:AB:02:5D:3C:12:EC:81:14:40:F3:B1:85:24:31:BF:31:53:1B:22:AC:7C:73:26:E9:4E:DB:02:03:01:00:01

Basic Constraints *IsCA: true*

Subject Key Identifier *BC:7F:7E:89:36:E6:34:8B:0B:01:1D:52:0F:C6:B9:54:AB:E5:26:F3*

Authority Key Identifier *1B:82:5C:42:D9:F6:25:09:C0:2E:0D:F5:CE:39:22:94:4E:6F:58:54*

Certificate Policies *Policy OID: 1.2.250.1.78.1.1.3.1.1.3*

CPS pointer: http://www.preuve-electronique.org/PC_AC_NOTAIRES_1.2.250.1.78.1.1.3.1.1.3.pdf Policy OID: 1.2.250.1.78.1.1.3.1.3.1.2.4.3.4

CRL Distribution Points *http://www.preuve-electronique.org/ListeRevocations/notaires2018.arl*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *7F:6A:E9:5D:BC:05:30:F3:C7:BB:5E:66:EB:D3:5A:3A:23:EF:F0:EB:B0:F4:CD:81:40:82:EA:F6:C9:0A:67:93*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS101456/QCPPublic*

TSP Service Definition URI

URI *[en]* *http://www.preuve-electronique.org/PC_AC_REAL_1.2.250.1.78.1.1.3.1.3.1.1.17.pdf*

13.3.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

13.3.2 - History instance n.1 - Status: accreditationceased

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[fr]* *AC REAL 2014*

Name *[en]* *AC REAL 2014*

Service digital identities

X509SubjectName

Subject OU: *REAL2014*

Subject OU: *0002 784350134*

Subject O: *CONSEIL SUPERIEUR DU NOTARIAT*

Subject C: *FR*

X509SKI

X509 SK I *vH9+iTbmNIsLAR1SD8a5VKvlJvM=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accreditationceased*

Status Starting Time *2014-03-08T00:00:00Z*

13.3.3 - History instance n.2 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[fr]* *AC REAL 2014*

Name *[en]* *AC REAL 2014*

Service digital identities

X509SubjectName

Subject OU: *REAL2014*

Subject OU: *0002 784350134*

Subject O: *CONSEIL SUPERIEUR DU NOTARIAT*

Subject C: *FR*

X509SKI

X509 SK I *vH9+iTbmNIsLAR1SD8a5VKvlJvM=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2011-12-12T00:00:00Z*

13.4 - Service (withdrawn): AC REAL

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[fr]* *AC REAL*

Name *[en]* *AC REAL*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *1571110*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIEDjCCAvigAwIBAgIDF/kmMAsGCSqGSIb3DQEBBTBFMQswCQYDVQQGEwJmcjEjMCEGA1UECgwa
UHJvZmVzc2lvbnMgUsOpZ2xlbWVudMOpZXMxETAPBgNVBAsTCE5vdGFpcmVzMB4XDTA4MDMyMTEz
NTQwN1oXDTEyMDMyMTEzNTQwN1owbTELMAkGA1UEBhMCZnIxIzAhBgNVBAoMGlByb2Zlc3Npb25z
IFLDqWdsZW1lbnTDqWVzMREwDwYDVQQLEwhOb3RhaXJlczEXMBUGA1UECwwOQUMgZMOpbMOpZ3XD
qWUxDTALBgNVBAsTBFJFQUwwggEgMAsGCSqGSIb3DQEBAQOCAQ8AMIIBCgKCAQEAwaDDdFZIJHQz
Jhhi2IBzmkEgeBjQszmFt+HZKhqVLnDE2CgvfkvuDfccNxvLz07fjDJli2qfMON7R97GutcPLsJV
ElpW20KWSiLP3ko/gQT48rEj24CyGfPI2BogbIqCzBr1/eAkH4BY3iCIzqYQFffT7UMhz357HLmB
ygoDRchX1QIcUNRXOetgPCr5F2PEFrQMD0UH1uYZUtY22ltL8pOPIzAcvlobNlKKkw2H2L1G+u3J
fl7VDqtY3SOSZPqk7xgt7f9Qa9AVWieqI8Gfjubg6Y0IlaAB+FUc802Zp1o4RZ7PE/0H+IO1ql2b
Iluomw52l6awSWeEPFBXn74tHQIDAQABo4HkMIHhMA4GA1UdDwEB/wQEAwIBBjAPBgNVHRMBAf8E
BTADAQH/MB0GA1UdDgQWBBQoaeULKjI75FVJpKlx7wG1HMu9XTAfBgNVHSMEGDAWgBQQFLycdt0R
eWRmMOkfkyuH0g/RDDArBgNVHSAEJDAiMA0GCyqBegFOAQEDAQEBMBEGDyqBegFOAQEDAQMBAgQD
BDBRBgNVHR8ESjBIMEagRKBChkBodHRwOi8vd3d3LnByZXV2ZS1lbGVjdHJvbmlxdWUub3JnL0xp
c3RlUmV2b2NhdGlvbnMvbm90YWlyZXMuYXJsMAsGCSqGSIb3DQEBBQOCAQEAIlsSgWK31eWHfxt2
x88rCgkhQ0r1k3cKzuoiu/J+Ov+dISA7wNvdj2FHBQF3mPJQKmIjZhhWN7XV6s6q1/MxrAha4RaV
4jIBKm7/pRbkTzNwVWAxrMXoR5RMAP0iSDzNx0cPfiLBJLVp5UdK50A9Z36iX59C9ewAgm8eptVx
nprQV00XwGG8361UV09aRUDSUN18IE1q3ymPkP7a4Ycc9EXLm+6ss+qhoBNVKGiYoanWAvX02Fh2
hutugf00zNbtjAcv60uEsj+2n1v0P1na/cjCYyi+4StlXbcG0LXlk+FDvkMZDnSceZVzlQtyi2Vk G2X/4wzTlcAlIH39Fm9p1w==

-----END CERTIFICATE-----

Signature algorithm: *SHA1withRSA*

Issuer OU: *Notaires*

Issuer O: *Professions Réglementées*

Issuer C: *fr*

Subject OU: *REAL*

Subject OU: *AC déléguée*

Subject OU: *Notaires*

Subject O: *Professions Réglementées*

Subject C: *fr*

Valid from: *Fri Mar 21 14:54:07 CET 2008*

Valid to: *Wed Mar 21 14:54:07 CET 2012*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C1:A0:C3:74:56:48:24:74:33:26:18:62:D8:80:73:9A:41:20:78:18:D0:B3:39:85:B7:E1:D9:2A:1A:95:2E:70:C4:D8:28:2F:7E:4B:EE:0D:F7:1C:37:1B:CB:CF:4E:DF:8C:32:65:8B:6A:9F:30:E3:7B:47:DE:C6:BA:D7:0F:2E:C2:55:12:5A:56:DB:42:96:4A:22:CF:DE:4A:3F:81:04:F8:F2:B1:23:DB:80:B2:19:F3:C8:D8:1A:20:6C:8A:82:CC:1A:F5:FD:E0:24:1F:80:58:DE:20:88:CE:A6:10:15:F7:D3:ED:43:21:CF:7E:7B:1C:B9:81:CA:0A:03:45:C8:57:D5:02:1C:50:D4:57:39:EB:60:3C:2A:F9:17:63:C4:16:B4:0C:0F:45:07:D6:E6:19:52:D6:36:DA:5B:4B:F2:93:8F:23:30:1C:BE:5A:1B:36:52:8A:93:0D:87:D8:BD:46:FA:ED:C9:7E:5E:D5:0E:AB:58:DD:23:92:64:FA:A4:EF:18:2D:ED:FF:50:6B:D0:15:5A:27:AA:23:C1:9F:8E:E6:E0:E9:8D:25:21:A0:01:F8:55:1C:F3:4D:99:A7:5A:38:45:9E:CF:13:F
D:07:F8:83:B5:AA:5D:9B:22:5B:A8:9B:0E:76:97:A6:B0:49:67:84:3C:50:57:9F:BE:2D:1D:02:03:01:00:01

Basic Constraints *IsCA: true*

Subject Key Identifier *28:69:E5:0B:2A:32:3B:E4:55:49:A4:A9:71:EF:01:B5:1C:CB:BD:5D*

Authority Key Identifier *10:14:BC:9C:76:DD:11:79:64:66:30:E9:1F:93:2B:87:D2:0F:D1:0C*

Certificate Policies *Policy OID: 1.2.250.1.78.1.1.3.1.1.1*

Policy OID: 1.2.250.1.78.1.1.3.1.3.1.2.4.3.4

CRL Distribution Points *http://www.preuve-electronique.org/ListeRevocations/notaires.arl*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *2D:80:6C:41:93:BC:C4:85:B9:03:BA:E8:E5:29:5F:CD:C9:C5:1A:4F:21:9C:3C:C6:54:0D:34:81:E4:85:1C:CF*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS101456/QCPPublic*

TSP Service Definition URI

URI *[en]* *http://www.preuve-electronique.org/PC_AC_REAL_1.2.250.1.78.1.1.3.1.3.1.1.10.pdf*

13.4.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

13.4.2 - History instance n.1 - Status: accreditationceased

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[fr]* *AC REAL*

Name *[en]* *AC REAL*

Service digital identities

X509SubjectName

Subject OU: *REAL*

Subject OU: *AC déléguée*

Subject OU: *Notaires*

Subject O: *Professions Réglementées*

Subject C: *fr*

X509SKI

X509 SK I *KGnlCyoyO+RVSaSpce8BtRzLvV0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accreditationceased*

Status Starting Time *2012-03-21T00:00:00Z*

13.4.3 - History instance n.2 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[fr]* *AC REAL*

Name *[en]* *AC REAL*

Service digital identities

X509SubjectName

Subject OU: *REAL*

Subject OU: *AC déléguée*

Subject OU: *Notaires*

Subject O: *Professions Réglementées*

Subject C: *fr*

X509SKI

X509 SK I *KGnlCyoyO+RVSaSpce8BtRzLvV0=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2011-12-12T00:00:00Z*

13.5 - Service (withdrawn): AH NOTAIRES

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[fr] *Un service de génération horodatage création et la signature temps timbres jetons qualifiés.*

Service Name

Name *[fr]* *AH NOTAIRES*

Name *[en]* *AH NOTAIRES*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *5*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIELjCCAxagAwIBAgIBBTANBgkqhkiG9w0BAQsFADBlMQswCQYDVQQGEwJGUjEmMCQGA1UECgwd
Q09OU0VJTCBTVVBFUklFVVIgRFUgTk9UQVJJQVQxFzAVBgNVBAsMDjAwMDIgNzg0MzUwMTM0MRUw
EwYDVQQLDAxOb3RhaXJlczIwMjAwHhcNMTMxMjEyMTAxOTU5WhcNMTcxMjEyMTAxOTU5WjBlMQsw
CQYDVQQGEwJGUjEmMCQGA1UECgwdQ09OU0VJTCBTVVBFUklFVVIgRFUgTk9UQVJJQVQxFzAVBgNV

BAsMDjAwMDIgNzg0MzUwMTM0MRUwEwYDVQQLDAxSRUFMVEVDSDIwMTcwggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQDuoSqC15sZg3WqYeZhOjNAfykjTYO2Fx1q1UFUt2YZ/+3QBoHDJjLp
JVx+hLW85Hlm5kcfoRq/hk5y8PSOjcuER7CQWzjDRyTY8g5okGahv8ZUzQJQCTvdfQw/7mShyBMb
FIAALyC1jEqk6/gcTa6VtOvssn4okM8F3QfOLXtRRdfc4rUxSElWUADV52luXRegXgWn6HY+kidF
+F9KhR4eS2AqdbHRuw9VZBSs8YfL89clla43Ui/5O8iTYedqhMrbem2zSuwpmRXCaDTZOpw7z2Tq
LtyHOkQnpo43VFSWiQ3RmH6r1FKjX+PsLs6V1IfNniMyAHvBKNjSEJUsCQzdAgMBAAGjgegwgeUw
DwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUURMtNmk+tKHzpIy674nzzn2wPFMwHwYDVR0jBBgw
FoAU3IjaV3K9LHPLV3vi5U3do8z4IWcwKwYDVR0gBCQwIjANBgsqgXoBTgEBAwEBBTARBg8qgXoB
TgEBAwEDBAIEAwQwDgYDVR0PAQH/BAQDAgEGMFUGA1UdHwROMEwwSqBIoEaGRGh0dHA6Ly93d3cu
cHJldXZlLWVsZWN0cm9uaXF1ZS5vcmcvTGlzdGVSZXZvY2F0aW9ucy9ub3RhaXJlczIwMjAuYXJs
MA0GCSqGSIb3DQEBCwUAA4IBAQCbXynxEuMRWkf6wdohPjiRUHSizaT75nRnkR1DQPrkTkg0zeJM
bfN/UFs/x/gXvLLH3jVbKn1gGymCcNHDc4U8LOrM8z8rPxWJ83N9jW1H0YHJdfblF9Mpwl3dev8z
Y7c3Mwrt/XYaSWfApQj9xe9qri8yIbVvyrJ3qiKOkg0ROvXYCbsuoMvATvz30SZ/FrTzikR2zJbY
mwqBE8LwKzf/t+jW8QICGoDLc2N4S21XUCbTuwiCjPMLXhfGtkzmUHXSI4FwoD34khhp6p5f+ME5
z/p85M8AW/Fuwg+Tm8zJcwBdZB52GEy7OMiFmavet0EzRqli8KcapouQYUBpZC9U

-----END CERTIFICATE-----

Signature algorithm:	*SHA256withRSA*
Issuer OU:	*Notaires2020*
Issuer OU:	*0002 784350134*
Issuer O:	*CONSEIL SUPERIEUR DU NOTARIAT*
Issuer C:	*FR*
Subject OU:	*REALTECH2017*
Subject OU:	*0002 784350134*
Subject O:	*CONSEIL SUPERIEUR DU NOTARIAT*
Subject C:	*FR*
Valid from:	*Thu Dec 12 11:19:59 CET 2013*
Valid to:	*Tue Dec 12 11:19:59 CET 2017*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:EE:A1:2A:82:D7:9B:19:83:75:AA:61:E6:61:3A:33:40:
7F:29:23:4D:83:B6:17:1D:6A:D5:41:54:B7:66:19:FF:ED:D0:06:81:C3:26:32:E9:25:5C:7E:84:B5:BC:E4:79:66:E6:47:1F:A1:1A:BF:86:4E:72:F0:F4:8E:8D:CB:84:47:
B0:90:5B:38:C3:47:24:D8:F2:0E:68:90:66:A1:BF:C6:54:CD:02:50:09:3B:DD:7D:0C:3F:EE:64:A1:C8:13:1B:14:80:00:2F:20:B5:8C:4A:A4:EB:F8:1C:4D:AE:95:B4:E
B:EC:B2:7E:28:90:CF:05:DD:07:CE:2D:7B:51:45:D7:DC:E2:B5:31:48:49:56:50:00:D5:E7:69:6E:5D:17:A0:5E:05:A7:E8:76:3E:92:27:45:F8:5F:4A:85:1E:1E:4B:60:
2A:75:B1:D1:BB:0F:55:64:14:AC:F1:87:CB:F3:D7:25:95:AE:37:52:2F:F9:3B:C8:93:61:E7:6A:84:CA:DB:7A:6D:B3:4A:EC:29:99:15:C2:68:34:D9:3A:9C:3B:CF:64:E
A:2E:DC:87:3A:44:27:A6:8E:37:54:54:96:89:0D:D1:98:7E:AB:D4:52:A3:5F:E3:EC:2E:CE:95:D4:87:CD:9E:23:32:00:7B:C1:28:D8:D2:10:95:2C:09:0C:DD:02:03:01
:00:01

Basic Constraints	*IsCA: true*
Subject Key Identifier	*51:13:2D:36:69:3E:B4:A1:F3:A4:8C:BA:EF:89:F3:CE:7D:B0:3C:53*
Authority Key Identifier	*DC:88:DA:57:72:BD:2C:73:CB:57:7B:E2:E5:4D:DD:A3:CC:F8:21:67*
Certificate Policies	*Policy OID: 1.2.250.1.78.1.1.3.1.1.5*

Policy OID: 1.2.250.1.78.1.1.3.1.3.4.2.4.3.4

CRL Distribution Points *http://www.preuve-electronique.org/ListeRevocations/notaires2020.arl*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *23:9A:FF:9B:EE:4C:7B:E8:23:EB:2E:EB:08:41:E0:9D:D4:5F:4F:A5:5B:98:E9:74:18:E1:71:40:60:83:76:E7*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

Scheme Service Definition URI

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Time-Stamping*

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS102023/LCP*

TSP Service Definition URI

URI *[en]* *http://www.preuve-electronique.org/ListeRevocations/PH_1.2.250.1.78.1.1.3.1.4.6.1.3.pdf*

13.5.1 - History instance n.1 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service Name

Name *[fr]* *AH NOTAIRES*

Name *[en]* *AH NOTAIRES*

Service digital identities

X509SubjectName

Subject OU: *REALTECH2017*

Subject OU: *0002 784350134*

Subject O: *CONSEIL SUPERIEUR DU NOTARIAT*

Subject C: *FR*

X509SKI

X509 SK I *URMtNmk+tKHzpIy674nzzn2wPFM=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2012-10-09T00:00:00Z*

13.6 - Service (granted): Autorité d'Horodatage du Notariat REALTS2019 1.2.250.1.78.1.1.3.1.4.6.1.6

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description

[en] *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[fr] *Un service de génération horodatage création et la signature temps timbres jetons qualifiés.*

Service Name

Name *[en]* *Autorité d'Horodatage du Notariat REALTS2019 1.2.250.1.78.1.1.3.1.4.6.1.6*

Name *[fr]* *Autorité d'Horodatage du Notariat REALTS2019 1.2.250.1.78.1.1.3.1.4.6.1.6*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *642367946715962639270843523 71*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIEnjCCA4agAwIBAgINAM+PbmDSjy3ElZoDczANBgkqhkiG9w0BAQsFADBlMQswCQYDVQQGEwJG
UjEmMCQGA1UECgwdQ09OU0VJTCBTVVBFUklFVVIgRFUgTk9UQVJJQVQxFzAVBgNVBAsMDjAwMDIg
Nzg0MzUwMTM0MRUwEwYDVQQDDAxOb3RhaXJlczIwMjMwHhcNMTUwNTExMTI1NjMyWhcNMTkwNTEx
MTI1NjMyWjBjMQswCQYDVQQGEwJGUjEmMCQGA1UECgwdQ09OU0VJTCBTVVBFUklFVVIgRFUgTk9U
QVJJQVQxFzAVBgNVBAsMDjAwMDIgNzg0MzUwMTM0MRMwEQYDVQQDDApSRUFMVFMyMDE5MIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvbO5cr2Ku711BiOUz3HPo5+dz/KC4KNZo5v/xGKO
yhkk3iG6aWs5DFq7I75U9jaMccsbplu2tS9D3LwpQPp6By9ZPxfBtxUoMIyhcOk3XUDAjy4hLnNO
elpf2K2iI5FpU3XPXzzN5XBpILxWb8GxYa3cs+HGyc9L9pr/2TH9UtwXC2DPKJrGpDwaeWzmTQrn
24M+geT0UK65MkudchN6XtlsNJBkQ7CKLC7b2H66EiXNdhEVsaroUGIyt+m3GTkPAY4R4tgssrFk
huJucK0vBA/691x1Nopp+Bg+Tv84vQ+5NNwhsNq6ft1BK4xOwlfQeCqX7TWxM1zZWXM3ve3x6QID
AQABo4IBTTCCAUkwEgYDVR0TAQH/BAgwBgEB/wIBADAdBgNVHQ4EFgQUbn2j//NDbiglN3ywvM84
oZA4kFQwHwYDVR0jBBgwFoAUTCIsPyWLT8VKypmBmJ3eVR5WsjgwgYsGA1UdIASBgzCBgDBrBgsq
gXoBTgEBAwEBBTBcMFoGCCsGAQUFBwIBFk5odHRwOi8vd3d3LnByZXV2ZS1lbGVjdHJvbmlxdWUu
b3JnL1BDX0FDX05PVEFJUkVTXzEuMi4yNTAuMS43OC4xLjEuMy4xLjEuNS5wZGYwEQYPKoF6AU4B
AQMBAwUCBAMEMA4GA1UdDwEB/wQEAwIBBjBVBgNVHR8ETjBMMEqgSKBGhkRodHRwOi8vd3d3LnBy
ZXV2ZS1lbGVjdHJvbmlxdWUub3JnL0xpc3RlUmV2b2NhdGlvbnMvbm90YWlyZXMyMDIzLmFybDAN
BgkqhkiG9w0BAQsFAAOCAQEAnFjnppYV5totszgyPth+cCHMhIaHoN3HQeQV2folvJr0zuW+ZSs5
JYCTafaGbUQVXF1gstGUt2ZfbtbEThw8autokBar6OwbAev/UQZ77rZmPEy8qDILbzeNLzl8fa21
fCH9TCVlsyBO+DzGiXEAwiGG71jCcf+zZmrPmRRk+zgYP1zYYDGa+UsBNakNnagA/sHslhKlWuuk
QKhKHqF/ibzgIZ1eFn48XTxIje5fRxv+QWOBJeboeWHnukOEW0kFCjDE3Gq9iYcUk18FYXRXRjs6
gHYpDevRdHLL6CMPYCVchb3UA2OIPQnrhcIkKUSCfEg0IGW68xYYfEbSxl1z+w==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Notaires2023*

Issuer OU: *0002 784350134*

Issuer O: *CONSEIL SUPERIEUR DU NOTARIAT*

Issuer C: *FR*

Subject CN: *REALTS2019*

Subject OU: *0002 784350134*

Subject O: *CONSEIL SUPERIEUR DU NOTARIAT*

Subject C: *FR*

Valid from: *Mon May 11 14:56:32 CEST 2015*

Valid to: *Sat May 11 14:56:32 CEST 2019*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:BD:B3:B9:72:BD:8A:BB:BD:75:06:23:94:CF:71:CF:A3:9F:9D:CF:F2:82:E0:A3:59:A3:9B:FF:C4:62:8E:CA:19:24:DE:21:BA:69:6B:39:0C:5A:BB:23:BE:54:F6:36:8C:71:CB:1B:A6:5B:B6:B5:2F:43:DC:BC:29:40:FA:7A:07:2F:59:3F:17:C1:B7:15:28:30:8C:A1:70:E9:37:5D:40:C0:8F:2E:21:2E:73:4E:7A:5A:5F:D8:AD:A2:23:91:69:53:75:CF:5F:3C:CD:E5:70:69:20:BC:56:6F:C1:B1:61:AD:DC:B3:E1:C6:C9:CF:4B:F6:9A:FF:D9:31:FD:52:DC:17:0B:60:CF:28:9A:C6:A4:3C:1A:79:6C:E6:4D:0A:E7:DB:83:3E:81:E4:F4:50:AE:B9:32:4B:9D:72:13:7A:5E:D9:6C:3
4:90:64:43:B0:8A:2C:2E:DB:D8:7E:BA:12:25:CD:76:11:15:B1:AA:E8:50:62:32:B7:E9:B7:19:39:0F:01:8E:11:E2:D8:2C:B2:B1:64:86:E2:6E:70:AD:2F:04:0F:FA:F7:5C:75:36:8A:69:F8:18:3E:4E:FF:38:BD:0F:B9:34:DC:21:B0:DA:BA:7E:DD:41:2B:8C:4E:C2:57:D0:78:2A:97:ED:35:B1:33:5C:D9:59:73:37:BD:ED:F1:E9:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *6E:7D:A3:FF:F3:43:6E:28:25:37:7C:B0:BC:CF:38:A1:90:38:90:54*

Authority Key Identifier *4C:22:2C:3F:25:8B:4F:C5:4A:CA:99:81:98:9D:DE:55:1E:56:B2:38*

Certificate Policies *Policy OID: 1.2.250.1.78.1.1.3.1.1.5*
CPS pointer: http://www.preuve-electronique.org/PC_AC_NOTAIRES_1.2.250.1.78.1.1.3.1.1.5.pdf Policy OID: 1.2.250.1.78.1.1.3.1.3.5.2.4.3.4

CRL Distribution Points *http://www.preuve-electronique.org/ListeRevocations/notaires2023.arl*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *00:0B:11:A9:50:4C:32:E5:14:F2:B8:1A:80:DF:F0:01:E1:EC:84:0D:CA:FD:BD:17:AE:85:84:CC:FA:15:24:C1*

X509SubjectName

Subject CN: *REALTS2019*

Subject OU: *0002 784350134*

Subject O: *CONSEIL SUPERIEUR DU NOTARIAT*

Subject C: *FR*

X509SKI

X509 SK I *bn2j//NDbiglN3ywvM84oZA4kFQ=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2016-09-18T22:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS102023/LCP*

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Time-Stamping*

TSP Service Definition URI

URI *[en]* *http://www.preuve-electronique.org/PH_1.2.250.1.78.1.1.3.1.4.6.1.6.pdf*

URI *[fr]* *http://www.preuve-electronique.org/PH_1.2.250.1.78.1.1.3.1.4.6.1.6.pdf*

13.7 - Service (granted): REAL 2019 - Délivrance de certificats de signature clé REAL

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *REAL 2019 - Délivrance de certificats de signature clé REAL*

Name *[fr]* *REAL 2019 - Délivrance de certificats de signature clé REAL*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *642367946727894763732805895 31*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIEnDCCA4SgAwIBAgINAM+PbmDjHlIqcrQG2zANBgkqhkiG9w0BAQsFADBlMQswCQYDVQQGEwJG
UjEmMCQGA1UECgwdQ09OU0VJTCBTVVBFUklFVVIgRFUgTk9UQVJJQVQxFzAVBgNVBAsMDjAwMDIg
Nzg0MzUwMTM0MRUwEwYDVQQDDAxOb3RhaXJlczIwMjMwHhcNMTUxMTAzMTQwNTE2WhcNMTkxMTAy
MTQwNTE2WjBhMQswCQYDVQQGEwJGUjEmMCQGA1UECgwdQ09OU0VJTCBTVVBFUklFVVIgRFUgTk9U
QVJJQVQxFzAVBgNVBAsMDjAwMDIgNzg0MzUwMTM0MREwDwYDVQQDDAhSRUFMMjAxOTCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBAMi+BIJYlJz1iZpscuHYbU83EwvPHG3MduC0kKqttN5+
m+kvIaGhZAZ5kibcdGuTUjWtxqelPkw07BX4xmjERP7hgaapiR2np2258BPnh48jrOHNHLj8vb+Y
mooMZPVkHG6VrJ2UMUjHAfKghcXploYiaA4wL4TrPgnnqp2Y99EjcFCOYcagtuR6TyaZ67+GozrV
mGRJTO5t2LSpZftEJ4vYary6VggZ/zCUik0M99nl+hP3ZDnjPBaGEExNQxIf+u66xW+kKolh2JmD
1gTBzS9Nn3B7vtRzR6taNyDlNsptq1raiFmNilBoq1xRLrDyP+4A6Jct0MlzAhyARPdymVUCAwEA
AaOCAU0wggFJMBIGA1UdEwEB/wQIMAYBAf8CAQAwHQYDVR0OBBYEFFL5PwswfN1Y6pS9TmP3tUYo
pxqWMB8GA1UdIwQYMBaAFEwiLD8li0/FSsqZgZid3lUeVrI4MIGLBgNVHSAEgYMwgYAwawYLKoF6
AU4BAQMBAQUwXDBaBggrBgEFBQcCARZOaHR0cDovL3d3dy5wcmV1dmUtZWxlY3Ryb25pcXVlLm9y
Zy9QQ19BQ19OT1RBSVJFU18xLjIuMjUwLjEuNzguMS4xLjMuMS4xLjUucGRmMBEGDyqBegFOAQED
AQMBAgQDBDAOBgNVHQ8BAf8EBAMCAQYwVQYDVR0fBE4wTDBKoEigRoZEaHR0cDovL3d3dy5wcmV1
dmUtZWxlY3Ryb25pcXVlLm9yZy9MaXN0ZVJldm9jYXRpb25zL25vdGFpcmVzMjAyMy5hcmwwDQYJ
KoZIhvcNAQELBQADggEBAE29ixSgVXOCjn+ivYexEdWbiV/gUlvSgSoQvLXRSZJf7YhyyVJBwoxO
MPgbQ00PF9hnRrYhamBfaBrYmoZEylfjRmqIRyZqgYnHdTYQ1ySYy40ngaNjmv1R7jxHlzSgZ//c
HSoi9w6PGSSkEJYtQtwzm3GZc5lCrL483jowtI72p9NG+sysSzNZ3ZJgn00M1nLUok9GEwGArfL8
MPlwtQBF0NMGftZalK9JbRUiAr32M+BhNK6lifLvW4SXpgl+djxN7JbRxQf/MlRYsKFPLr7HI1dQ
/3PljYGZS4cOCV+z+gK6ftWIsi3WXR14Nae990XTqfZY9S/cSnCsrJtOrvU=

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Notaires2023*

Issuer OU: *0002 784350134*

Issuer O: *CONSEIL SUPERIEUR DU NOTARIAT*

Issuer C: *FR*

Subject CN: *REAL2019*

Subject OU: *0002 784350134*

Subject O: *CONSEIL SUPERIEUR DU NOTARIAT*

Subject C: *FR*

Valid from: *Tue Nov 03 15:05:16 CET 2015*

Valid to: *Sat Nov 02 15:05:16 CET 2019*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C8:BE:04:82:58:94:9C:F5:89:9A:6C:72:E1:D8:6D:4F:
37:13:0B:CF:1C:6D:CC:76:E0:B4:90:AA:AD:B4:DE:7E:9B:E9:2F:21:A1:A1:64:06:79:92:26:DC:74:6B:93:52:35:AD:C6:A7:A5:3E:4C:34:EC:15:F8:C6:68:C4:44:FE:E
1:81:A6:A9:89:1D:A7:A7:6D:B9:F0:13:E7:87:8F:23:AC:E1:CD:1C:B8:FC:BD:BF:98:9A:8A:0C:64:F5:64:1C:6E:95:AC:9D:94:31:48:C7:01:F2:A0:85:C5:E9:96:86:22:
68:0E:30:2F:84:EB:3E:09:E7:AA:9D:98:F7:D1:23:70:50:8E:61:C6:A0:B6:E4:7A:4F:26:99:EB:BF:86:A3:3A:D5:98:64:49:4C:EE:6D:D8:B4:A9:65:FB:44:27:8B:D8:6A
:BC:B
A:56:08:19:FF:30:94:8A:4D:0C:F7:D9:E5:FA:13:F7:64:39:E3:3C:16:86:10:4C:4D:43:12:1F:FA:EE:BA:C5:6F:A4:2A:89:61:D8:99:83:D6:04:C1:CD:2F:4D:9F:70:7B:
BE:D4:73:47:AB:5A:37:20:E5:36:CA:6D:AB:5A:DA:88:
59:8D:8A:50:68:AB:5C:51:2E:B0:F2:3F:EE:00:E8:97:2D:D0:C9:73:02:1C:80:44:F7:72:99:55:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *52:F9:3F:0B:30:7C:DD:58:EA:94:BD:4E:63:F7:B5:46:28:A7:1A:96*

Authority Key Identifier *4C:22:2C:3F:25:8B:4F:C5:4A:CA:99:81:98:9D:DE:55:1E:56:B2:38*

Certificate Policies *Policy OID: 1.2.250.1.78.1.1.3.1.1.5*
CPS pointer: http://www.preuve-electronique.org/PC_AC_NOTAIRES_1.2.250.1.78.1.1.3.1.1.5.pdf Policy OID: 1.2.250.1.78.1.1.3.1.3.1.2.4.3.4

CRL Distribution Points *http://www.preuve-electronique.org/ListeRevocations/notaires2023.arl*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *B9:7D:19:43:41:29:89:7D:3A:3C:30:43:B5:9B:02:7F:69:84:60:16:66:27:15:52:99:63:F6:4F:53:D2:5C:E6*

X509SubjectName

Subject CN: *REAL2019*

Subject OU: *0002 784350134*

Subject O: *CONSEIL SUPERIEUR DU NOTARIAT*

Subject C: *FR*

X509SKI

X509 SK I *Uvk/CzB83VjqlL1OY/e1RiinGpY=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*
[fr] *undefined.*

Status Starting Time *2016-09-29T22:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS101456/QCPPublic*

TSP Service Definition URI

URI *[en]* *http://www.preuve-electronique.org/PC_AC_REAL_1.2.250.1.78.1.1.3.1.3.1.1.22.pdf*

URI *[fr]* *http://www.preuve-electronique.org/PC_AC_REAL_1.2.250.1.78.1.1.3.1.3.1.1.22.pdf*

13.7.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

13.7.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *REAL 2019 - Délivrance de certificats de signature clé REAL*

Name *[fr]* *REAL 2019 - Délivrance de certificats de signature clé REAL*

Service digital identities

X509SubjectName

Subject CN: *REAL2019*

Subject OU: *0002 784350134*

Subject O: *CONSEIL SUPERIEUR DU NOTARIAT*

Subject C: *FR*

X509SKI

X509 SK I *Uvk/CzB83VjqlL1OY/e1RiinGpY=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-09-29T22:00:00Z*

13.7.3 - History instance n.2 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *AC REAL 2019 1.2.250.1.78.1.1.3.1.3.1.1.22*

Name *[fr]* *AC REAL 2019 1.2.250.1.78.1.1.3.1.3.1.1.22*

Service digital identities

X509SubjectName

Subject CN: *REAL2019*

Subject OU: *0002 784350134*

Subject O: *CONSEIL SUPERIEUR DU NOTARIAT*

Subject C: *FR*

X509SKI

X509 SK I *Uvk/CzB83VjqlL1OY/e1RiinGpY=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-09-29T22:00:00Z*

13.8 - Service (granted): Autorité d'Horodatage du Notariat REALTS2021 1.2.250.1.78.1.1.3.1.4.6.1.6

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[fr] *Un service de génération horodatage création et la signature temps timbres jetons qualifiés.*

Service Name

Name *[en]* *Autorité d'Horodatage du Notariat REALTS2021 1.2.250.1.78.1.1.3.1.4.6.1.6*

Name *[fr]* *Autorité d'Horodatage du Notariat REALTS2021 1.2.250.1.78.1.1.3.1.4.6.1.6*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *642367946633199366459592056 44*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIEnTCCA4WgAwIBAgINAM+PbmBfs8H0oUNDDDANBgkqhkiG9w0BAQsFADBlMQswCQYDVQQGEwJG
UjEmMCQGA1UECgwdQ09OU0VJTCBTVVBFUklFVVIgRFUgTk9UQVJJQVQxFzAVBgNVBAsMDjAwMDIg
Nzg0MzUwMTM0MRUwEwYDVQQDDAxOb3RhaXJlczIwMjMwHhcNMTcwMjE1MDk0NjIxWhcNMjEwMjE1
MDk0NjIxWjBiMQswCQYDVQQGEwJGUjEmMCQGA1UECgwdQ09OU0VJTCBTVVBFUklFVVIgRFUgTk9U
QVJJQVQxFjAUBgNVBAsMDTAwMiA3ODQzNTAxMzQxEzARBgNVBAMMClJFQUxUUzIwMjEwggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDQ03WYSfZBBEL1tyHcJfqvEhR9c1zcj9uqbBNFYFPh
HbmLSJlO/dbpY7Zy2RxcZxoUts4r2As1osFEMPGPbCD9gh487t/iTuQ9T/Qb0rH/I/iKjR9JDIxP
4kgE4q1xX4hvMvTx4c92bS6JbHcy48gqcGJkWVMdgTjAYoxQ1i8oOo6r+XAkAdowRl+CjXJN/bJF
R+5U0OXiKHLFGtykaal9TvX0S0gRz88LukfHdq4f5arEgAjnKoSytMFeZoSCoarIaKbYXKm9dPqB

OgEuA4QTP/Jrc866XTn7slYMbSKS9mYkTLpxiDKZFGuh1MggeOWzJ9W1I33FJZ5SSuFoe1T7AgMB
AAGjggFNMIIBSTASBgNVHRMBAf8ECDAGAQH/AgEAMB0GA1UdDgQWBBThlCYf7BZmKzKnYMFAReDU
tQSsqTAfBgNVHSMEGDAWgBRMIiw/JYtPxUrKmYGYnd5VHlayODCBiwYDVR0gBIGDMIGAMGsGCyqB
egFOAQEDAQEFMFwwWgYIKwYBBQUHAgEWTmh0dHA6Ly93d3cucHJldXZlLWVsZWN0cm9uaXF1ZS5v
cmcvUENfQUNfTk9UQUlSRVNfMS4yLjI1MC4xLjc4LjEuMS4zLjEuMS41LnBkZjARBg8qgXoBTgEB
AwEDBQIEAwQwDgYDVR0PAQH/BAQDAgEGMFUGA1UdHwROMEwwSqBIoEaGRGh0dHA6Ly93d3cucHJl
dXZlLWVsZWN0cm9uaXF1ZS5vcmcvTGlzdGVSZXZvY2F0aW9ucy9ub3RhaXJlczIwMjMuYXJsMA0G
CSqGSIb3DQEBCwUAA4IBAQAgVxyXjLghJBHjopbbM+deXlZaJweaoLkhMgFDOPRAbOtMb9wkFfUe
i/MID8h7a1VsKoumR6u4KYfHbGFZW9X7QE2fgGIbEnErisL5ogyF1YVVcG31ATGF+cQf5c8KLCAH
+nA7HHsJ97T76qwS42E5eEkWX3cBGYNG1otekx2jEzMOiyZ2y3+b7dxkJJRBX01QghIq6hArh5eX
51LouF+IUqEs97OHwCTppaLNASmf3CmbPjPkWwRnTiqn6s/dE/uQKCEO3AqGSMoozeqHFsNPbLrT
sVDhHwLL0o+CvexeA/pmhymer0FVLsUGMB956zbMbJPKdCQjbmJ1XBxwly7r

-----END CERTIFICATE-----

Signature algorithm:	*SHA256withRSA*
Issuer CN:	*Notaires2023*
Issuer OU:	*0002 784350134*
Issuer O:	*CONSEIL SUPERIEUR DU NOTARIAT*
Issuer C:	*FR*
Subject CN:	*REALTS2021*
Subject OU:	*002 784350134*
Subject O:	*CONSEIL SUPERIEUR DU NOTARIAT*
Subject C:	*FR*
Valid from:	*Wed Feb 15 10:46:21 CET 2017*
Valid to:	*Mon Feb 15 10:46:21 CET 2021*
Public Key:	

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:D0:D3:75:98:49:F6:41:04:42:F5:B7:21:DC:25:FA:AF:12:14:7D:73:5C:DC:8F:DB:AA:6C:13:45:60:53:E1:1D:B9:8B:48:99:4E:FD:D6:E9:63:B6:72:D9:1C:5C:67:1A:14:B6:CE:2B:D8:0B:35:A2:C1:44:30:F1:8F:6C:20:FD:82:1E:3C:EE:DF:E2:4E:E4:3D:4F:F4:1B:D2:B1:FF:23:F8:8A:8D:1F:49:0C:8C:4F:E2:48:04:E2:AD:71:5F:88:6F:32:F4:F1:E1:CF:76:6D:2E:89:6C:77:32:E3:C8:2A:70:62:64:59:53:1D:81:38:C0:62:8C:50:D6:2F:28:3A:8E:AB:F9:70:24:01:DA:30:46:5F:82:8D:72:4D:FD:B2:45:47:EE:54:D0:E5:E2:28:72:C5:1A:DC:A4:69:A9:7D:4E:F5:F4:4B:48:11:CF:CF:0B:BA:47:C7:76:AE:1F:E5:AA:C4:80:08:E7:2A:84:B2:B4:C1:5E:66:84:82:A1:AA:C8:68:A6:D8:5C:A9:BD:74:FA:81:3A:01:2E:03:84:13:3F:F2:6B:73:CE:BA:5D:39:FB:B2:56:0C:6D:22:92:F6:66:24:4C:BA:71:88:32:99:14:6B:A1:D4:C8:20:78:E5:B3:27:D5:B5:23:7D:C5:25:9E:52:4A:E1:68:7B:54:FB:02:03:01:00:01

Basic Constraints	*IsCA: true - Path length: 0*
Subject Key Identifier	*E1:94:26:1F:EC:16:66:2B:32:A7:60:C1:40:45:E0:D4:B5:04:AC:A9*
Authority Key Identifier	*4C:22:2C:3F:25:8B:4F:C5:4A:CA:99:81:98:9D:DE:55:1E:56:B2:38*
Certificate Policies	*Policy OID: 1.2.250.1.78.1.1.3.1.1.5* *CPS pointer: http://www.preuve-electronique.org/PC_AC_NOTAIRES_1.2.250.1.78.1.1.3.1.1.5.pdf Policy OID:*

1.2.250.1.78.1.1.3.1.3.5.2.4.3.4

CRL Distribution Points *http://www.preuve-electronique.org/ListeRevocations/notaires2023.arl*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *DB:4F:C3:64:33:B2:12:13:57:93:5F:CA:19:D6:B1:0D:17:55:AE:48:80:DE:1A:09:98:D3:7C:98:75:0F:D9:F0*

X509SubjectName

Subject CN: *REALTS2021*

Subject OU: *002 784350134*

Subject O: *CONSEIL SUPERIEUR DU NOTARIAT*

Subject C: *FR*

X509SKI

X509 SK I *4ZQmH+wWZisyp2DBQEXg1LUErKk=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2017-02-28T23:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS102023/LCP*

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Time-Stamping*

TSP Service Definition URI

URI *[en]* *http://www.preuve-electronique.org/PH_1.2.250.1.78.1.1.3.1.4.6.1.6.pdf*

URI *[fr]* *http://www.preuve-electronique.org/PH_1.2.250.1.78.1.1.3.1.4.6.1.6.pdf*

13.9 - Service (granted): REAL 2021 - Délivrance de certificats de signature clé REAL

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *REAL 2021 - Délivrance de certificats de signature clé REAL*

Name *[fr]* *REAL 2021 - Délivrance de certificats de signature clé REAL*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *642367946721152063013820594 87*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIEnDCCA4SgAwIBAgINAM+PbmDZwtUbnIOl3zANBgkqhkiG9w0BAQsFADBlMQswCQYDVQQGEwJG
UjEmMCQGA1UECgwdQ09OU0VJTCBTVVBFUklFVVIgRFUgTk9UQVJJQVQxFzAVBgNVBAsMDjAwMDIg
Nzg0MzUwMTM0MRUwEwYDVQQDDAxOb3RhaXJlczIwMjMwHhcNMTcwNzEyMTMzOTE3WhcNMjEwNzEy
MTMzOTE3WjBhMQswCQYDVQQGEwJGUjEmMCQGA1UECgwdQ09OU0VJTCBTVVBFUklFVVIgRFUgTk9U
QVJJQVQxFzAVBgNVBAsMDjAwMDIgNzg0MzUwMTM0MREwDwYDVQQDDAhSRUFMMjAyMTCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBAMYvpQTPbNhG+J5FHJ3hyKHtOB1I+J9viuAFJzuGaBkB
dpqW6zgzGmwggA7S7qmkOKcw22J3g2GXXIQaEsF/iYSXy78PrVCDyJtOHKD3gVv7fLSEQ4wBMZJY
dPXVZC/w1/xxmUZTV3hdcSTNXPaHnEuz+al7uHhRe28ONNRli1pNj9R5DzumD93x2CQRVtvXxF1h
IafbdanDECpnlW20BYtaTTkRYzRYqlo/dfoI5ENNMDuFqcWp+BgSJCYUmHcmKmF8UVjLFaPYPJMu
8M2vITROt4K7s6ZJqoe5H18Tt4aY8FNETqmejkPCvjKvqN3XbXDFqlpi9I+46pxPdhgihIMCAwEA
AaOCAU0wggFJMBIGA1UdEwEB/wQIMAYBAf8CAQAwHQYDVR0OBBYEFPmxXi6NRY534ydvTtMta4uD
JQkQMB8GA1UdIwQYMBaAFEwiLD8li0/FSsqZgZid3lUeVrI4MIGLBgNVHSAEgYMwgYAwawYLKoF6
AU4BAQMBAQUwXDBaBggrBgEFBQcCARZOaHR0cDovL3d3dy5wcmV1dmUtZWxlY3Ryb25pcXVlLm9y
Zy9QQ19BQ19OT1RBSVJFU18xLjIuMjUwLjEuNzguMS4xLjMuMS4xLjUucGRmMBEGDyqBegFOAQED
AQMBAgQDBDAOBgNVHQ8BAf8EBAMCAQYwVQYDVR0fBE4wTDBKoEigRoZEaHR0cDovL3d3dy5wcmV1
dmUtZWxlY3Ryb25pcXVlLm9yZy9MaXN0ZVJldm9jYXRpb25zL25vdGFpcmVzMjAyMy5hcmwwDQYJ
KoZIhvcNAQELBQADggEBAAumvx2FaYU0bsq4syLMFhjngmcNMSXX+epMqKF2VLIaaKDdekLppj+q
ercvzK+LkoyilwiGz8T2vn/R3NgTVgAb+nFmzGOL9R3o2tyHEK11HXApQGkoTdTopOQAAQ1nJOaO
PIcszQztgoA3ucJKqCIXpa6AuMkSdoZikpB9HQtqqRanTvNwABhnf0a+lsyTdcHnDtaai2PNvw2t
9h/9lsD4FbRN38Ft1ddHqXSuE3CS6Ky0MyLbHCySZfaC/IeVGXVy/QiWf7Q8zXSszRx4ZmAsslLt
lcW6xXAvjttVbFE7VDsrb+nnXiFdjxD42BJ8C3FBC1rjOr1qdyar4JS/9RY=

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Notaires2023*

Issuer OU: *0002 784350134*

Issuer O: *CONSEIL SUPERIEUR DU NOTARIAT*

Issuer C: *FR*

Subject CN: *REAL2021*

Subject OU: *0002 784350134*

Subject O: *CONSEIL SUPERIEUR DU NOTARIAT*

Subject C: *FR*

Valid from: *Wed Jul 12 15:39:17 CEST 2017*

Valid to: *Mon Jul 12 15:39:17 CEST 2021*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C6:2F:A5:04:CF:6C:D8:46:F8:9E:45:1C:9D:E1:C8:A1:ED:38:1D:48:F8:9F:6F:8A:E0:05:27:3B:86:68:19:01:76:9A:96:EB:38:33:1A:6C:20:80:0E:D2:EE:A9:A4:38:A7:30:DB:62:77:83:61:97:5C:84:1A:12:C1:7F:89:84:97:CB:BF:0F:AD:50:83:C8:9B:4E:1C:A0:F7:81:5B:FB:7C:B4:84:43:8C:01:31:92:58:74:F5:D5:64:2F:F0:D7:FC:71:99:46:53:57:78:5D:71:24:CD:5C:F6:87:9C:4B:B3:F9:A9:7B:B8:78:51:7B:6F:0E:34:D4:65:8B:5A:4D:8F:D4:79:0F:3B:A6:0F:DD:F1:D8:24:11:56:DB:D7:C4:5D:61:21:A7:DB:75:A9:C3:10:2A:67:95:6D:B4:05:8B:5A:4D:39:11:63:34:58:AA:5A:3F:75:FA:08:E4:43:4D:30:3B:85:A9:C5:A9:F8:18:12:24:26:14:98:77:26:2A:61:7C:51:58:CB:15:A3:D8:3C:93:2E:F0:CD:AF:21:34:4E:B7:82:BB:B3:A6:49:AA:87:B9:1F:5F:13:B7:86:98:F0:53:44:4E:A9:9E:8E:43:C2:BE:32:AF:A8:DD:D7:6D:70:C5:AA:5A:62:F4:8F:B8:EA:9C:4F:76:18:22:84:83:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *F9:B1:5E:2E:8D:45:8E:77:E3:27:6F:4E:D3:2D:6B:8B:83:25:09:10*

Authority Key Identifier *4C:22:2C:3F:25:8B:4F:C5:4A:CA:99:81:98:9D:DE:55:1E:56:B2:38*

Certificate Policies *Policy OID: 1.2.250.1.78.1.1.3.1.1.5*

CPS pointer: http://www.preuve-electronique.org/PC_AC_NOTAIRES_1.2.250.1.78.1.1.3.1.1.5.pdf Policy OID: 1.2.250.1.78.1.1.3.1.3.1.2.4.3.4

CRL Distribution Points *http://www.preuve-electronique.org/ListeRevocations/notaires2023.arl*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *53:45:D0:6E:A4:A6:9E:C4:8E:6C:74:FF:6C:38:14:38:9A:8E:35:84:D9:55:98:9A:B6:45:9A:B3:4F:AB:69:A3*

X509SubjectName

Subject CN: *REAL2021*

Subject OU: *0002 784350134*

Subject O: *CONSEIL SUPERIEUR DU NOTARIAT*

Subject C: *FR*

X509 SK I *+bFeLo1FjnfjJ29O0y1ri4MlCRA=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2017-09-07T22:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS101456/QCPPublic*

TSP Service Definition URI

URI *[en]* *http://www.preuve-electronique.org/PC_AC_REAL_1.2.250.1.78.1.1.3.1.3.1.1.22.pdf*

URI *[fr]* *http://www.preuve-electronique.org/PC_AC_REAL_1.2.250.1.78.1.1.3.1.3.1.1.22.pdf*

13.9.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

13.10 - Service (granted): REALSIGN 2025 - Délivrance de certificats de signature clé REAL

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *REALSIGN 2025 - Délivrance de certificats de signature clé REAL*

Name *[fr]* *REALSIGN 2025 - Délivrance de certificats de signature clé REAL*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *766848291897609720853039923 42*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIHTzCCBTegAwIBAgINAPfINDg1/713+XxgFjANBgkqhkiG9w0BAQ0FADCBijELMAkGA1UEBhMC
RlIxJjAkBgNVBAoMHUNPTlNFSUwgU1VQRVJJRVVSIERVIE5PVEFSSUFUMRcwFQYDVQQLDA4wMDAy
IDc4NDM1MDEzNDEYMBYGA1UEYQwPU0k6RlItNzg0MzUwMTM0MSAwHgYDVQQDDBdOT1RBSVJFUyBE
RSBGUkFOQ0UgMjAzMzAeFw0xNzAxMjQxMTEwMTFaFw0yNTAxMjIxMTEwMTFaMIGAMQswCQYDVQQG
EwJGUjEmMCQGA1UECgwdQ09OU0VJTCBTVVBFUklFVIgRFUgTk9UQVJJQVQxFzAVBgNVBAsMDjAw
MDIgNzg0MzUwMTM0MRgwFgYDVQRhDA9TSTpGUi03ODQzNTAxMzQxFjAUBgNVBAMMDVJFQUxTSUdO
IDIwMjUwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDS9WqUGB7AfiC0kT2l9nUIhndo
UMeDwHvVr0JsRz5MF2NZMsoaOMR/rNerbwDg295DPt7l4PiiZD8IRN598GIk1ReP7eCVY/8XVWJi
K5RTjA6390EMcHebOSQTA/QDZCn7+Oepc7ZdYjdmZR2c9r9SS7BrTFz8oYLUsbKl/qKxinjYQBfY
Du6tnfiQkTEHZNKCBf1QBYmYQ5DJsmxc0D66VO5Y1StYtXiiwB/LhDQDpFWsjV2aWIOfdk2V6IxA
rhxbARrBp/afjBauUA0v59DsswRfYK+YKE44Derp1qZ6thA4c6wlZQKMaXiG+yBN8T1bB0JX4PPN
VTVtZTVYWnAFN+jZ3V2JQa+KH/WidqTI41sYJmMdpstRr6PZdYY8AqYoA+I1Sli8GPQs0tXLLQfe
XnSoPyumFHKzuQHTjV4QmJQeOrHTdxfec2eTweMvQM2oKN6/Vxi3Zon+jeKGeA1Tp+I0LYbSjul5

4QLOVIFHsaiE6xfHQoNEiqnGbmJDBhXfXlpofKxWE+0+fZbK+yx7+Bs+sJjnINmHHC9nTrl4AwT0
QvqGNugh143pUa84ZxDJfhKlgGjwB7inizGP3fszH9WSg2YFRMMFrcJsp5XpPecRJv52pFtqFwOF
Ke/z8yuXAVYNMIS25E4O6CrYz3GpDiZl+TsZl7oHApnoVu0JFQIDAQABo4IBujCCAbYwEgYDVR0T
AQH/BAgwBgEB/wIBADAdBgNVHQ4EFgQU4Ia9N6x9QRg1TX2y0qS2A/aPwHEwHwYDVR0jBBgwFoAU
9qW1KWB+8eoDZZUzMcuFDWXIGvQwgYYGA1UdIAR/MH0wagYJKoF6AU4CAQEBMF0wWwYIKwYBBQUH
AgEWT2h0dHA6Ly93d3cucHJldXZlLWVsZWN0cm9uaXF1ZS5vcmcvUENfTk9UQUlSRVNERUZSQU5D
RV8xLjIuMjUwLjEuNzguMi4xLjEuMS5wZGYwDwYNKoF6AU4CAQMBAgQDBDAOBgNVHQ8BAf8EBAMC
AQYwXQYDVR0fBFYwVDBSoFCgToZMaHR0cDovL3d3dy5wcmV1dmUtZWxlY3Ryb25pcXVlLm9yZy9M
aXN0ZVJldm9jYXRpb25zL25vdGFpcmVzZGVmcmFuY2UyMDMzLmFybDBoBggrBgEFBQcBAQRcMFow
WAYIKwYBBQUHMAKGTGh0dHA6Ly93d3cucHJldXZlLWVsZWN0cm9uaXF1ZS5vcmcvTGlzdGVSZXZv
Y2F0aW9ucy9ub3RhaXJlc2RlZnJhbmNlMjAzMy5jcnQwDQYJKoZIhvcNAQENBQADggIBAC1MPkpn
7oTsKkKU5gqFGUzQYDzaaip5pxiXfaS+zxjk9kmvfeqOL2fEu9SYDeJbwg2+kMFFLuUBjlyuawe+
uQYSkJur0y6S4ZCcfYSFUP7cldPvvKK+3RoVUsm0CgVsBZJIF1FYHtRuWUwT1CO9BPSDINcO0MKv
MZjWLc1MFY28qivK5fkmdC3PcYyNxvDQdYluqBH45Ksgn/O2BytCFl9a6r8C3DHuzebDWDqGzYHg
OmemD4yUpRgMwuAvWekaP4uZBQ1+ac9w7KEUBA2iQYbPqhNkyS0Xyy5kvk+bQlb2YwJar4tjX+PB
QlSNsVH7qtrIG8oxpt+zrrobPVMKli7g5u628BbIgSLDepUECojnsfyEetNtgPhrbDe2jfdyZJB5
C0eXcIzAlakauRi3fXptVy+fA9eKS2TFgevFrVUVvOQo8haNWzSf09cUiw7FqYFS3raLPGiwNvXK
koN6CyiZ5Zk6qbYZ/mC5ZpaZWQU76R94FZjxxYjz+zbf29q9/wdHAjiVqIJ2ybd8cIud9JoebiT5
YvBvJI6KVPC3LkswgjUQEHry5vbhrsIDllxpy0Z7WZFM0hXtbmcdQWdcnFPdVocEWF+p2MzvXIs8
mCGGNej4WCkIIGVQi4xDHLc9eVndjouftKO5WLz1ejWWOcD1JsOFI6dQX0FNb2aKdcZk

-----END CERTIFICATE-----

Signature algorithm:	*SHA512withRSA*
Issuer CN:	*NOTAIRES DE FRANCE 2033*
Issuer 2.5.4.97:	*SI:FR-784350134*
Issuer OU:	*0002 784350134*
Issuer O:	*CONSEIL SUPERIEUR DU NOTARIAT*
Issuer C:	*FR*
Subject CN:	*REALSIGN 2025*
Subject 2.5.4.97:	*SI:FR-784350134*
Subject OU:	*0002 784350134*
Subject O:	*CONSEIL SUPERIEUR DU NOTARIAT*
Subject C:	*FR*
Valid from:	*Tue Jan 24 12:10:11 CET 2017*
Valid to:	*Wed Jan 22 12:10:11 CET 2025*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:D2:F5:6A:94:18:1E:C0:7E:20:B4:91:3D:A5:F6:75:08:
86:77:68:50:C7:83:C0:7B:D5:AF:42:6C:47:3E:4C:17:63:59:32:CA:1A:38:C4:7F:AC:D7:AB:6F:00:E0:DB:DE:43:3E:DE:E5:E0:F8:A2:64:3F:08:44:DE:7D:F0:62:24:D5
:17:8F:ED:E0:95:63:FF:17:55:62:62:2B:94:53:8C:0E:B7:F7:41:0C:70:77:9B:39:24:13:03:F4:03:64:29:FB:F8:E7:A9:73:B6:5D:62:37:66:65:1D:9C:F6:BF:52:4B:B0:
6B:4C:5C:FC:A1:82:D4:B1:B2:A5:FE:A2:B1:8A:78:D8:40:17:D8:0E:EE:AD:9D:F8:90:91:31:07:64:D2:82:05:FD:50:05:89:98:43:90:C9:B2:6C:5C:D0:3E:BA:54:EE:5
8:D5:2B:58:B5:78:A2:C0:1F:CB:84:34:03:A4:55:AC:8D:5D:9A:58:83:9F:76:4D:95:EA:5C:40:AE:1C:5B:01:1A:C1:A7:F6:9F:8C:16:AE:50:0D:2F:E7:D0:EC:B3:04:5F:
60:AF:98:28:4E:38:0D:EA:E9:D6:A6:7A:B6:10:38:73:AC:25:65:02:8C:69:78:86:FB:20:4D:F1:3D:5B:07:42:57:E0:F3:CD:55:35:6D:65:35:58:5A:70:05:37:E8:D9:D
D:5D:89:41:AF:8A:1F:F5:A2:76:A4:C8:E3:5B:18:26:63:1D:A6:CB:51:AF:A3:D9:75:86:3C:02:A6:28:03:E2:35:4A:58:BC:18:F4:2C:D2:D5:CB:2D:07:DE:5E:74:A8:3F
:2B:A6:14:72:B3:B9:01:D3:8D:5E:10:98:94:1E:3A:B1:D3:77:17:DE:73:67:93:C1:E3:2F:40:CD:A8:28:DE:BF:57:18:B7:66:89:FE:8D:E2:86:78:0D:53:A7:E2:34:2D:8

6:D2:8E:E9:79:E1:02:CE:54:81:47:B1:A8:84:EB:17:C7:42:83:44:8A:A9:C6:6E:62:43:06:15:DF:5E:5A:68:7C:AC:56:13:ED:3E:7D:96:CA:FB:2C:7B:F8:1B:3E:B0:98:E7:20:D9:87:1C:2F:67:4E:B9:78:03:04:F4:42:FA:86:36:E8:21:D7:8D:E9:51:AF:38:67:10:C9:7E:12:88:80:68:F0:07:B8:A7:8B:31:8F:DD:FB:33:1F:D5:92:83:66:05:44:C3:05:AD:C2:6C:A7:95:E9:3D:E7:11:26:FE:76:A4:5B:6A:17:03:85:29:EF:F3:F3:2B:97:01:56:0D:30:84:B6:E4:4E:0E:E8:2A:D8:CF:71:A9:0E:26:65:F9:3B:19:97:BA:07:02:99:E8:56:ED:09:15:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *E0:86:BD:37:AC:7D:41:18:35:4D:7D:B2:D2:A4:B6:03:F6:8F:C0:71*

Authority Key Identifier *F6:A5:B5:29:60:7E:F1:EA:03:65:95:33:31:CB:85:0D:65:C8:1A:F4*

Certificate Policies *Policy OID:*

1.2.250.1.78.2.1.1.1 CPS

pointer: http://www.preuve-electronique.org/PC_NOTAIRESDEFRANCE_1.2.250.1.78.2.1.1.1.pdf

Policy OID: 1.2.250.1.78.2.1.3.1.2.4.3.4

CRL Distribution Points *http://www.preuve-electronique.org/ListeRevocations/notairesdefrance2033.arl*

Authority Info Access *http://www.preuve-electronique.org/ListeRevocations/notairesdefrance2033.crt*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *B1:6F:FB:E0:00:C9:23:CB:F5:18:1F:A0:09:B4:E6:47:35:DB:D1:0C:9F:9B:1A:10:98:D5:63:E1:04:4E:8E:26*

X509SubjectName

Subject CN: *REALSIGN 2025*

Subject 2.5.4.97: *SI:FR-784350134*

Subject OU: *0002 784350134*

Subject O: *CONSEIL SUPERIEUR DU NOTARIAT*

Subject C: *FR*

X509SKI

X509 SK I *4Ia9N6x9QRg1TX2y0qS2A/aPwHE=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2017-10-31T23:00:00Z*

TSP Service Definition URI

URI *[en]* *http://www.preuve-electronique.org/PC_REALSIGN_1.2.250.1.78.2.1.3.1.1.1.pdf*

URI *[fr]* *http://www.preuve-electronique.org/PC_REALSIGN_1.2.250.1.78.2.1.3.1.1.1_fr.pdf*

URI *[en]* *http://www.preuve-electronique.org/PC_REALSIGN_1.2.250.1.78.2.1.3.1.1.4.pdf* **URI**

[fr] *http://www.preuve-electronique.org/PC_REALSIGN_1.2.250.1.78.2.1.3.1.1.4_fr.pdf*

13.10.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

13.10.2 - Extension (critical): Qualifiers [QCWithQSCD, QCForESig]

Qualifier type description *[en]* *undefined.*

[fr] *undefined.*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithQSCD*

Qualifier *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForESig*

Criteria list assert=all

Key Usage *[nonRepudiation]* *true*

Policy Identifier nodes:

Identifier *1.2.250.1.78.2.1.3.1.1.1*

Policy Identifier nodes:

Identifier *1.2.250.1.78.2.1.3.1.1.4*

13.11 - Service (granted): AUTORITE D'HORODATAGE DU NOTARIAT

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[fr] *Un service de génération horodatage création et la signature temps timbres jetons qualifiés.*

Service Name

Name *[fr]* *AUTORITE D'HORODATAGE DU NOTARIAT*

Name *[en]* *AUTORITE D'HORODATAGE DU NOTARIAT*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *766848292003137822768903744 51*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIHTzCCBTegAwIBAgINAPfINDjIctptPR0xMzANBgkqhkiG9w0BAQ0FADCBijELMAkGA1UEBhMC
RlIxJjAkBgNVBAoMHUNPTlNFSUwgU1VQRVJJRVVSIERVIE5PVEFSSUFUMRcwFQYDVQQLDA4wMDAy
IDc4NDM1MDEzNDEYMBYGA1UEYQwPU0k6RlItNzg0MzUwMTM0MSAwHgYDVQQDDBdOT1RBSVJFUyBE
RSBGUkFOQ0UgMjAzMzAeFw0xNzEyMTIxMzUzMjZaFw0yNTEyMTAxMzUzMjZaMIGAMQswCQYDVQQG
EwJGUjEmMCQGA1UECgwdQ09OU0VJTCBTVVBFUklFVIgRFUgTk9UQVJJQVQxFzAVBgNVBAsMDjAw
MDIgNzg0MzUwMTM0MRowGAYDVQRhDBFWQVRGUi02Nzc4NDM1MDEzNDEUMBIGA1UEAwwLUkVBTFRT
IDIwMjUwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCs6xXwzFQIDI4rtIfclI8RywzE
EVgSpg9y0pk6/DDnb+8B6xwOP8C1Tfy6sO0QMIuEM6fuBuTRlp4AzPSjofb9M/gU6fJOqEYSgjDL
Am9feS65+DzI/T8tYc3yGpl8aFJb041NXvFYNtPlMWRI7jlbS3TJbtYZUw22t9+kyqgTuVlkjsOn
068yKDErtSZlMhAwBjdXMocDet1iGgoRwg2DYpZz/Yi2NPzfYnf3sBNXNUkHZDD6V0/8uHIw0VAm
PDvJdv07RJFOlNLOIJ7thxuzd8MSHVRO3RcfRBkdBuEjV93N6SZq1ztf74+Drt4KgyxUL/uDUIjf
GVTT5giiz6YH2M8SgwUeYxtovgvnSqXaGn1I+b8Vow/knxSwBTHFqbImyxEc6CIOjkuNnYxY18ZO
jh7JxXchKYN5XHn3bkrnN8qfWAjzPeByD4uqxgkg5s4THE7o0KqSZxjWzAPyocKQd7Nh6OO9h/4D
oR5rmXgr0/00XHrE+w01T0Jfggby3n5BAu2iC5PZb5HpPM/s+1M6h8ZlHj9NwBnSnDFCuuwv3J1H
UEcn5rrocmQHxvSfKceIIZmaPH6koQj7Fpqrlukz6RoxAFaI0KEdp5/kgH6sDZOaXY+x1ggG28J9
DmIaOvJhNRu2tF6qeaFbQ7sLEIxXvtJk2weVvTkg/mK1aii2zQIDAQABo4IBujCCAbYwEgYDVR0T
AQH/BAgwBgEB/wIBADAdBgNVHQ4EFgQU3EpKlVMUh/5Pp2mbDVotIHLXwgAwHwYDVR0jBBgwFoAU
9qW1KWB+8eoDZZUzMcuFDWXIGvQwgYYGA1UdIAR/MH0wagYJKoF6AU4CAQEBMF0wWwYIKwYBBQUH
AgEWT2h0dHA6Ly93d3cucHJldXZlLWVsZWN0cm9uaXF1ZS5vcmcvUENfTk9UQUlSRVNERUZSQU5D
RV8xLjIuMjUwLjEuNzguMi4xLjEuMS5wZGYwDwYNKoF6AU4CAQMFAgQDBDAOBgNVHQ8BAf8EBAMC
AQYwXQYDVR0fBFYwVDBSoFCgToZMaHR0cDovL3d3dy5wcmV1dmUtZWxlY3Ryb25pcXVlLm9yZy9M
aXN0ZVJldm9jYXRpb25zL25vdGFpcmVzZGVmcmFuY2UyMDMzLmFybDBoBggrBgEFBQcBAQRcMFow
WAYIKwYBBQUHMAKGTGh0dHA6Ly93d3cucHJldXZlLWVsZWN0cm9uaXF1ZS5vcmcvTGlzdGVSZXZv
Y2F0aW9ucy9ub3RhaXJlc2RlZnJhbmNlMjAzMy5jcnQwDQYJKoZIhvcNAQENBQADggIBAEcGfiKg
dDSIRMkwvI6HH6Ond/goax2Yt6BkBga2xgE6rS5D2lmAtXtUcJD8uyX7cO8DVXgaoWEd11c08Rhj
JCvhmVBRGtsufr4gGoFo3fVjdRbrPsOTkxIyZzqIRxv6w9eRVM3pGKO3XFvNwPhfwRmyzxWpQ9t+
mZhFUq4RdbDvuwQ28WjJptwy2hnDMS3Slrv1RMzdv76nYr8rKL6OW2k2aufV1jhQJsCx9znQNq73
b3ymMdrbyhm9TkIktTtBiCpZhwuajgPvy9LR5Gr/NhFXFNOUqu05Z+RjJhU0mDkL8yuJ7ZkgT5LL
v8JXwnLzM9LTrjwMiNvc33EkEGbEZv4LVryfKn2N68X1C6ohuNDNkCv8x29ngd3OIofAoS5atW74
lSWlsnLVqHhamQNZ9AQLvWGugDDZZQnkrO6LLnaN+bxXzG4NEQ3yaU+K8cVC6wDOvnpJropTdmbW
mnc34w5pDwnylTIp2KUr7Wxi0mpAIIZyaax14DBKrUgoMSd/0y6kGaE7O7PUV7O58YtS0jIY7mxW
ZmWeUMCsF4vMI1RMZcKL//oYgQFIerfRIAITzkghbA5g+ERAm8teJLHKpw3cO9HvFm8aeiY3WlHt
X3I6jjtOMo0PkhwVPEnB+gqAer4v4kRpFO5heR1GOQ19MeODg2L+sslWQadk47ffP91M

-----END CERTIFICATE-----

Signature algorithm: *SHA512withRSA*

Issuer CN: *NOTAIRES DE FRANCE 2033*

Issuer 2.5.4.97: *SI:FR-784350134*

Issuer OU: *0002 784350134*

Issuer O: *CONSEIL SUPERIEUR DU NOTARIAT*

Issuer C: *FR*

Subject CN: *REALTS 2025*

Subject 2.5.4.97: *VATFR-67784350134*

Subject OU: *0002 784350134*

Subject O: *CONSEIL SUPERIEUR DU NOTARIAT*

Subject C: *FR*

Valid from: *Tue Dec 12 14:53:26 CET 2017*

Valid to: *Wed Dec 10 14:53:26 CET 2025*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:AC:EB:15:F0:CC:54:08:0C:8E:2B:B4:87:DC:94:8F:11:CB:0C:C4:11:58:12:A6:0F:72:D2:99:3A:FC:30:E7:6F:EF:01:EB:1C:0E:3F:C0:B5:4D:FC:BA:B0:ED:10:30:8B:84:33:A7:EE:06:E4:D1:96:9E:00:CC:F4:A3:A1:F6:FD:33:F8:14:E9:F2:4E:A8:46:12:82:30:CB:02:6F:5F:79:2E:B9:F8:3C:C8:FD:3F:2D:61:CD:F2:1A:99:7C:68:52:5B:D3:8D:4D:5E:F1:58:36:D3:E5:31:64:48:EE:39:5B:4B:74:C9:6E:D6:19:53:0D:B6:B7:DF:A4:CA:A8:13:B9:59:64:8E:C3:A7:D3:AF:32:28:31:2B:B5:26:65:32:10:30:06:37:57:32:87:03:7A:DD:62:1A:0A:11:C2:0D:83:62:96:73:FD:88:B6:34:FC:DF:62:77:F7:B0:13:57:35:49:07:64:30:FA:57:4F:FC:B8:72:30:D1:50:26:3C:3B:C9:76:FD:3B:44:91:4E:94:D2:CE:20:9E:ED:87:1B:B3:77:C3:12:1D:54:4E:DD:17:1F:44:19:1D:06:E1:23:57:DD:CD:E9:26:6A:D7:3B:5F:EF:8F:83:AE:DE:0A:83:2C:54:2F:FB:83:50:88:DF:19:54:D3:E6:08:A2:CF:A6:07:D8:CF:12:83:05:1E:63:1B:68:BE:0B:E7:4A:A5:DA:1A:7D:48:F9:BF:15:A3:0F:E4:9F:14:B0:05:31:C5:A9:B2:26:CB:11:1C:E8:22:0E:8E:4B:8D:9D:8C:58:D7:C6:4E:8E:1E:C9:C5:77:21:29:83:79:5C:79:F7:6E:4A:E7:37:CA:9F:58:08:F3:3D:E0:72:0F:8B:AA:C6:09:20:E6:CE:13:1C:4E:E8:D0:AA:92:67:18:D6:CC:03:F2:A1:C2:90:77:B3:61:E8:E3:BD:87:FE:0
3:A1:1E:6B:99:78:2B:D3:FD:34:5C:7A:C4:FB:0D:35:4F:42:5F:82:06:F2:DE:7E:41:02:ED:A2:0B:93:D9:6F:91:E9:3C:CF:EC:FB:53:3A:87:C6:65:1E:3F:4D:C0:19:D2:9C:31:42:BA:EC:2F:DC:9D:47:50:47:27:E6:BA:E8:72:64:07:C6:F4:9F:29:C7:88:21:99:9A:3C:7E:A4:A1:08:FB:16:9A:AB:96:E9:33:E9:1A:31:00:56:88:D0:A1:1D:A7:9F:E4:80:7E:AC:0D:93:9A:5D:8F:B1:D6:08:06:DB:C2:7D:0E:62:1A:3A:F2:61:35:1B:B6:B4:5E:AA:79:A1:5B:43:BB:0B:10:8C:57:BE:D2:64:DB:07:95:BD:39:20:FE:62:B5:6A:28:B6:CD:02:03:01:00:01

Basic Constraints *IsCA: true - Path length: 0*

Subject Key Identifier *DC:4A:4A:95:53:14:87:FE:4F:A7:69:9B:0D:5A:2D:20:72:D7:C2:00*

Authority Key Identifier *F6:A5:B5:29:60:7E:F1:EA:03:65:95:33:31:CB:85:0D:65:C8:1A:F4*

Certificate Policies *Policy OID:*

1.2.250.1.78.2.1.1.1 CPS

pointer: http://www.preuve-electronique.org/PC_NOTAIRESDEFRANCE_1.2.250.1.78.2.1.1.1.pdf

Policy OID: 1.2.250.1.78.2.1.3.5.2.4.3.4

CRL Distribution Points *http://www.preuve-electronique.org/ListeRevocations/notairesdefrance2033.arl*

Authority Info Access *http://www.preuve-electronique.org/ListeRevocations/notairesdefrance2033.crt*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *11:E7:09:86:5A:45:7A:7E:F7:02:58:C4:D8:7D:2E:A9:3A:A7:82:9F:E6:04:1E:13:17:BC:37:3F:1C:65:09:9B*

X509SubjectName

Subject CN: *REALTS 2025*

Subject 2.5.4.97: *VATFR-67784350134*

Subject OU: *0002 784350134*

Subject O: *CONSEIL SUPERIEUR DU NOTARIAT*

Subject C: *FR*

X509SKI

X509 SK I *3EpKlVMUh/5Pp2mbDVotIHLXwgA=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2018-06-01T00:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS102023/LCP*

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Time-Stamping*

TSP Service Definition URI

URI *[en]* *http://www.preuve-electronique.org/PH_1.2.250.1.78.2.1.3.5.4.6.1.1.pdf*

URI *[fr]* *http://www.preuve-electronique.org/PH_1.2.250.1.78.2.1.3.5.4.6.1.1.pdf*

14 - TSP: Le groupe La Poste

TSP Name

Name *[en]* *Le groupe La Poste*

Name *[fr]* *Le groupe La Poste*

TSP Trade Name

Name *[en]* *VATFR-39356000000*

Name *[fr]* *VATFR-39356000000*

PostalAddress

Street Address *[en]* *Direction des Systèmes d'Information Courrier - 111 boulevard Brune*

Locality *[en]* *Paris*

Postal Code *[en]* *75014*

Country Name *[en]* *FR*

ElectronicAddress

URI *mailto:ld-horodatage-mco@laposte.fr*

URI *http://www.laposte.fr*

TSP Information URI

URI *[en]* *http://www.certinomis.fr/nos-solutions/horodatage-et-cachet-electronique-de-la-poste/service-dhorodatage-electronique*

URI *[fr]* *http://www.certinomis.fr/nos-solutions/horodatage-et-cachet-electronique-de-la-poste/service-dhorodatage-electronique*

14.1 - Service (withdrawn): La Poste - Autorité d'horodatage

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[fr] *Un service de génération horodatage création et la signature temps timbres jetons qualifiés.*

Service Name

Name *[en]* *La Poste - Autorité d'horodatage*

Name *[fr]* *La Poste - Autorité d'horodatage*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *21*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIFhTCCA22gAwIBAgIBFTANBgkqhkiG9w0BAQUFADBjMQswCQYDVQQGEwJGUjETMBEGA1UEChMK
Q2VydGlub21pczEXMBUGA1UECxMOMDAwMiA0MzM5OTg5MDMxJjAkBgNVBAMMHUNlcnRpbm9taXMg
LSBBdXRvcml0w6kgUmFjaW5lIMB4XDTA4MTIxMjA5MjIzOVoXDTE4MTIxMjA5MjIzOVowXTELMAkG
A1UEBhMCRlIxEzARBgNVBAoTCkNlcnRpbm9taXMxFzAVBgNVBAsTDjAwMDIgNDMzOTk4OTAzMSAw
HgYDVQQDDBdDZXJ0aW5vbWlzIEFDIDEgw6l0b2lsZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBANilBu6IDJIHhD+O4y7+tNK9iF46oh46/7101EfamwRLvU5c3B95JEuCQ/01cEd4C37Q
+EGZAl9B6RBbHra+twfIU80+a8qoUzeO3m2OzziY5VjFmUzleYvqNS7eT4PnXD6+KPtTeoyoRkYe
ROzVi6AcQJYlBPLO9sKSCZOVd+m6BItyBCcyKyKjz1uzRFrv2zijp0Q7MJML6+2MLVRhTOsP9Tlv
GDiJgU1cdY/26tuRV4d9se4CI1n3xKiku6bI78Q5Q3Rx4M1M1cJM8wV2WSZAhI78XvycZAvz6kSP
RZK6k4yJwSZ15NWp0T5rgZGeXY97HSi0fBq4RvjiwjW3DY0CAwEAAaOCAUgwggFEMA8GA1UdEwEB
/wQFMAMBAf8wDgYDVR0PAQH/BAQDAgEGMB8GA1UdIwQYMBaAFA2MtmHaRLjRFH3Dvn1eSPDOymqw
MB0GA1UdDgQWBBQuCseRNigwVtXOkRqGuThrqIK/CjCBxwYDVR0fBIG/MIG8MDegNaAzhjFodHRw
Oi8vY3JsLmNlcnRpbm9taXMuY29tL0FDX1JhY2luZS9jcmwvY3JsLTEuY3JsMIGAoH6gfIITbGRh
cC5jZXJ0aW5vbWlzLmNvbaRlMGMxCzAJBgNVBAYTAkZSMRMwEQYDVQQKEwpDZXJ0aW5vbWlzMRcw
FQYDVQQLEw4wMDAyIDQzMzk5ODkwMzEmMCQGA1UEAwwdQ2VydGlub21pcyAtIEF1dG9yaXTDqSBS

YWNpbmUwFwYDVR0gBBAwDjAMBgoqgXoBVgICAAEBMA0GCSqGSIb3DQEBBQUAA4ICAQCavK53sMBr
vMUfv3+12ufW7Up89v5B2Yiy2EgroeKpl/TEq5l8zCQrFtDlviWDOSeQLCnDbmfCW920Uj2EEGKM
EybHQ6AW3Ui/DJ84zCuj65I4bSKbVMUeTMMcD5vsQSLgAwxIwjgUUqqbwHDmo0hp+OEs2G5zGouI
01OPh6A0gN245tAL4+mHOFHxtRR+FaKCwse5jiPAO03b+pLMD3dJiTDEpk7dbJuq4Id8vCWhogJ2
EAztrjU/dzY1YCEWMdAFuQxiLGWtrLZtKCAGUISnyEmALfhFweTitLKiKVJXWDJya9oef3b+fEp9
XceAhYLMjxdAteiHg3NsVSmm2escIHWOh8LDrHHJxtf7wfYbiVHGgQvPmy7oY/Mk5KM3pOSaFDKA
5KWoyIxQl9WDhXiKDFKHF0CiOxExAb/AvO0gIbHUOr4KhzvZrh7NOaGVJStfQGxWnUftkXDezJWf
qDdelXBTQjh3o4n2LWiJOQ0RrJG0F+qDsmi8Q5D8NDxOSaO0C5oNSn2leMSxlvbdSDRx1zoo1HLZ
UXgUgg7NFPagI9D6U8WB/ttgvxX/9W2RL6452qMMQfkqTb8GojtYQnGLgqbRbgJVjtkhJvLB7AQT
mVuVh0Tl5eCVlURvBhuJ75dv80BTpULo7rs968z2T4sF2AAQcc6IkuRWDqu0pHWpBg==

-----END CERTIFICATE-----

Signature algorithm: *SHA1withRSA*

Issuer CN: *Certinomis - Autorité Racine*

Issuer OU: *0002 433998903*

Issuer O: *Certinomis*

Issuer C: *FR*

Subject CN: *Certinomis AC 1 étoile*

Subject OU: *0002 433998903*

Subject O: *Certinomis*

Subject C: *FR*

Valid from: *Fri Dec 12 10:22:39 CET 2008*

Valid to: *Wed Dec 12 10:22:39 CET 2018*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:D8:A5:06:EE:88:0C:92:07:84:3F:8E:E3:2E:FE:B4:D2:
BD:88:5E:3A:A2:1E:3A:FF:BD:74:D4:47:DA:9B:04:4B:BD:4E:5C:DC:1F:79:24:4B:82:43:FD:35:70:47:78:0B:7E:D0:F8:41:99:02:5F:41:E9:10:5B:1E:B6:BE:B7:07:C
8:53:CD:3E:6B:CA:A8:53:37:8E:DE:6D:8E:CF:38:98:E5:58:C5:99:4C:E5:79:8B:EA:35:2E:DE:4F:83:E7:5C:3E:BE:28:FB:53:7A:8C:A8:46:46:1E:44:EC:D5:8B:A0:1C:
40:96:25:04:F2:CE:F6:C2:92:09:93:95:77:E9:BA:04:8B:72:04:27:32:2B:22:A3:CF:5B:B3:44:5A:EF:DB:38:A3:A7:44:3B:30:93:0B:EB:ED:8C:2D:54:61:4C:EB:0F:F5:
39:6F:18:38:89:81:4D:5C:75:8F:F6:EA:DB:91:57:87:7D:B1:EE:02:23:59:F7:C4:A8:A4:BB:A6:C8:EF:C4:39:43:74:71:E0:CD:4C:D5:C2:4C:F3:05:76:59:26:40:84:8E:
FC:5E:FC:9C:64:0B:F3:EA:44:8F:45:92:BA:93:8C:89:C1:26:75:
E4:D5:A9:D1:3E:6B:81:91:9E:5D:8F:7B:1D:28:B4:7C:1A:B8:46:F8:E2:C2:35:B7:0D:8D:02:03:01:00:01

Basic Constraints *IsCA: true*

Authority Key Identifier *0D:8C:B6:61:DA:44:B8:D1:14:7D:C3:BE:7D:5E:48:F0:CE:CA:6A:B0*

Subject Key Identifier *2E:0A:C7:91:36:28:30:56:D5:CE:91:1A:86:B9:38:6B:A8:82:BF:0A*

CRL Distribution Points *http://crl.certinomis.com/AC_Racine/crl/crl-1.crl*

2: ldap.certinomis.com

C=FR,O=Certinomis,OU=0002 433998903,CN=Certinomis - Autorité Racine

Certificate Policies *Policy OID: 1.2.250.1.86.2.2.0.1.1*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *14:B4:0B:14:D1:54:4A:C1:19:40:0D:ED:8D:FD:5A:4F:2B:41:60:FC:DC:85:8E:9D:B2:56:54:F0:AB:C2:72:D0*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS102023/LCP*

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Time-Stamping*

TSP Service Definition URI

URI *[fr]* *http://www.certinomis.com/publi/rgs/DT-FL-1310-020-PC-SERV-1.4.pdf*

URI *[fr]* *http://www.cachetdelaposte.com/Documents/Politiquedhorodatage-ServicedhorodatageLaPosteV5.pdf*

14.1.1 - History instance n.1 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service Name

Name *[en]* *La Poste - Autorité d'horodatage*

Name *[fr]* *La Poste - Autorité d'horodatage*

Service digital identities

X509SubjectName

Subject CN: *Certinomis AC 1 étoile*

Subject OU: *0002 433998903*

Subject O: *Certinomis*

Subject C: *FR*

X509SKI

X509 SK I *LgrHkTYoMFbVzpEahrk4a6iCvwo=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2012-06-19T22:00:00Z*

14.2 - Service (granted): La Poste - Autorité d'horodatage - UH1 1.2.250.1.8.1.1.1.1.6

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[fr] *Un service de génération horodatage création et la signature temps timbres jetons qualifiés.*

Service Name

Name *[en]* *La Poste - Autorité d'horodatage - UH1 1.2.250.1.8.1.1.1.1.6*

Name *[fr]* *La Poste - Autorité d'horodatage - UH1 1.2.250.1.8.1.1.1.1.6*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *152238051066055272326907137846144874762549177611*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIGPjCCBCagAwIBAgIUGqqXHoVW5nbSHQn26ldgjmHBrQswDQYJKoZIhvcNAQELBQAwWzELMAkG
A1UEBhMCRlIxEzARBgNVBAoTCkNlcnRpbm9taXMxFzAVBgNVBAsTDjAwMDIgNDMzOTk4OTAzMR4w
HAYDVQQDExVDZXJ0aW5vbWlzIC0gUHJpbWUgQ0EwHhcNMTUwNjA5MTUwODM2WhcNMTkwNzA5MTUw
ODM2WjCBnjELMAkGA1UEBhMCRlIxIDAeBgNVBAoTF0xBIFBPU1RFIC0gRFNJIENPVVJSSUVSMRww
GgYDVQQLExMwMDAyIDM1NjAwMDAwMDY1MzA3MRAwDgYDVQQHEwdTVCBPVUVOMSwwKgYDVQQDDCNM
QV9QT1NURV9VTklURV9IT1JPREFUQUdFXzkyNTM1NV8xMDEPMA0GA1UEBRMGMS00MzM0MIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxsKyXdNpRZ6qaQa/nWM6bqgN8h/GF4LP7zjsojJr
EOrF0UcDKKZgkS1Rd/Mng6cZoR6YBCMeKWoKGMf3tSAdUpIujTRbC3wjheA65TRT0F4aYy2Gol1K
cEe/0bbFAiGlovHsfC6twaar/LCkXAqf3HLq/auzTIQaKwxM1/Yjp0T4l3RL9NR3e+AG9OWshzQD
hqy6rc6mde7qT3BHxhHcSRn8v4KdfszKIwBvjzTq67isKEYgUkSCb3HZRGTtWI+zeP67jDF2Zkhr
4OC0Dshj8w4cf2ki+N9E7QqrMSLzJgGWx1br9Xb5Rlpprs5tpsdzzju1QD2ugi1kowPjGGfCrQID
AQABo4IBtDCCAbAwFgYDVR0lAQH/BAwwCgYIKwYBBQUHAwgwDgYDVR0PAQH/BAQDAgeAMFYGCCsG
AQUFBwEBBEowSDBGBggrBgEFBQcwAYY6aHR0cDovL2lnYy1nMy5jZXJ0aW5vbWlzLmNvbS9JTlNU
QU5DRV9TSEEyL29jc3AvT0NTUF9QUklNRTAfBgNVHSMEGDAWgBRwiYD8E7V0w78+mYxLUoQwnjDt
njAJBgNVHRMEAjAAMBcGA1UdIAQQMA4wDAYKKoF6AVYCAwMYATCBjAYDVR0fBIGEMIGBMEugSaBH
hkVodHRwOi8vY3JsLmlnYy1nMy5jZXJ0aW5vbWlzLmNvbS9JTlNUQU5DRV9TSEEyL2NybC9BQ19Q
UklNRS1jcmwtMS5jcmwwMqAwoC6GLGh0dHA6Ly93d3cuY2VydGlub21pcy5jb20vY3JsL2FjZzMt
UFJJTUUuY3JsMDsGA1UdEQQ0MDKkMDAuMSwwKgYDVQQDDCNMQV9QT1NURV9VTklURV9IT1JPREFU
QUdFXzkyNTM1NV8xMDAdBgNVHQ4EFgQU16DUjOsmG+ZEuiwI+dxJNiUn6dUwDQYJKoZIhvcNAQEL
BQADggIBAAlfY8sbT/FkpDt/nPw/WHTYcBnYYBBuZE876wqGa2QGpC1RZ6Fc+0vY9A3YvXtjITqJ
ww6p4Gc5swo+Z1G5oJQUJWuCYYuh2xZNXj02rJDwBQwIptxfcMyII2r/V4/9walOvcCCOm1GdTXG
15Cp08Er39nn9PNElwgqh0xtTdlUj0gKN/U1hw+xN81FUO3HMSuh73a3DrYrKipwhYGKONYuDdPU
IZ6BY+ceA/Lx86EsWcnApXzH+/XKk0lCphm7SUuC7Iui9StP20syt7/SiqP91nlwoQGmGYB9AwXZ
WXW5G3DN3Ap4f8er9tcvHI0AjpB7u8GL3T01Yc1bT4LvcOzEHOoxlKKymuFb6Y+yVN5aWu7fstis
no/Ta2Qhn5Z4n8LFwzRXKfohSvmWmexV30SmOSifG8huut4eikoThUsophaCouypnK069+1DC829
m2ZTLPeECas8mcLD2hlNCcTASXUSF5mh5LaqzAtFtpsmA1T3G8EktvfdB6kj4ySRNWT39tyN/Kn+

ixbYwjqHoLo51/iVrFFLhJETLvei0TLCPcGOf2CJZbvUwWh3x//18gV2TU7Jw1j6VGUnyeWotoR/
DLTmc0rcVakctUGD5zNIaFy3Oq4arxgvhX3KNBbxs7scGRN5Iuk3xQJi7uOaG46DTQlF2WkvKgZi XwUBZx7W

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Certinomis - Prime CA*

Issuer OU: *0002 433998903*

Issuer O: *Certinomis*

Issuer C: *FR*

Subject SERIAL NUMBER: *1-4334*

Subject CN: *LA_POSTE_UNITE_HORODATAGE_925355_10*

Subject L: *ST OUEN*

Subject OU: *0002 35600000065307*

Subject O: *LA POSTE - DSI COURRIER*

Subject C: *FR*

Valid from: *Tue Jun 09 17:08:36 CEST 2015*

Valid to: *Tue Jul 09 17:08:36 CEST 2019*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C6:C2:B2:5D:D3:69:45:9E:AA:69:06:BF:9D:63:3A:6E:
A8:0D:F2:1F:C6:17:82:CF:EF:38:EC:A2:32:6B:10:EA:C5:D1:47:03:28:A6:60:91:2D:51:77:F3:27:83:A7:19:A1:1E:98:04:23:1E:29:6A:0A:18:C7:F7:B5:20:1D:52:92:
2E:8D:34:5B:0B:7C:23:85:E0:3A:E5:34:53:D0:5E:1A:63:2D:86:A2:5D:4A:70:47:BF:D1:B6:C5:02:21:A5:A2:F1:EC:7C:2E:AD:C1:A6:AB:FC:B0:A4:5C:0A:9F:DC:72:E
A:FD:AB:B3:4C:84:1A:2B:0C:4C:D7:F6:23:A7:44:F8:97:74:4B:F4:D4:77:7B:E0:06:F4:E5:AC:87:34:03:86:AC:BA:AD:CE:A6:75:EE:EA:4F:70:47:C6:11:DC:49:19:FC:
BF:
82:9D:7E:CC:CA:23:00:6F:8F:34:EA:EB:B8:AC:28:46:20:52:44:82:6F:71:D9:44:64:ED:58:8F:B3:78:FE:BB:8C:31:76:66:48:6B:E0:E0:B4:0E:C8:63:F3:0E:1C:7F:69:
22:F8:DF:44:ED:0A:AB:31:22:F3:26:01:96:C7:56:EB:F5:76:F9:46:5A:69:AE:CE:6D:A6:C7:73:CE:3B:B5:40:3D:AE:82:2D:64:A3:03:E3:18:67:C2:AD:02:03:01:00:01

Extended Key Usage *id_kp_timeStamping*

Authority Info Access *http://igc-g3.certinomis.com/INSTANCE_SHA2/ocsp/OCSP_PRIME*

Authority Key Identifier *70:89:80:FC:13:B5:74:C3:BF:3E:99:8C:4B:52:84:30:9E:30:ED:9E*

Basic Constraints *IsCA: false*

Certificate Policies *Policy OID: 1.2.250.1.86.2.3.3.24.1*

CRL Distribution Points *http://crl.igc-g3.certinomis.com/INSTANCE_SHA2/crl/AC_PRIME-crl-1.crl*

http://www.certinomis.com/crl/acg3-PRIME.crl

Subject Alternative Name *CN=LA_POSTE_UNITE_HORODATAGE_925355_10*

Subject Key Identifier *D7:A0:D4:8C:EB:26:1B:E6:44:BA:2C:08:F9:DC:49:36:25:27:E9:D5*

Key Usage: *digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint: *D2:FC:85:06:EC:75:D2:80:7E:31:F3:98:79:C7:B1:24:11:B1:F0:19:E7:94:EC:E6:CF:C5:FE: 8D:EC: 6F:BE:02*

X509SubjectName

Subject SERIAL NUMBER: *1-4334*

Subject CN: *LA_POSTE_UNITE_HORODATAGE_925355_10*

Subject L: *ST OUEN*

Subject OU: *0002 35600000065307*

Subject O: *LA POSTE - DSI COURRIER*

Subject C: *FR*

X509SKI

X509 SK I *16DUjOsmG+ZEuiwI+dxJNiUn6dU=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2017-02-28T23:00:00Z*

TSP Service Definition URI

URI *[en]* *http://cachetdelaposte.com/Documents/Politiquedhorodatage-ServicedhorodatageLaPosteV6.pdf*

URI *[fr]* *http://cachetdelaposte.com/Documents/Politiquedhorodatage-ServicedhorodatageLaPosteV6.pdf*

14.3 - Service (granted): La Poste - Autorité d'horodatage - UH2 1.2.250.1.8.1.1.1.1.6

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[fr] *Un service de génération horodatage création et la signature temps timbres jetons qualifiés.*

Service Name

Name *[en]* *La Poste - Autorité d'horodatage - UH2 1.2.250.1.8.1.1.1.1.6*

Name *[fr]* *La Poste - Autorité d'horodatage - UH2 1.2.250.1.8.1.1.1.1.6*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *983682914577683000705872756986928995491207970790*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIGPzCCBCegAwIBAgIVAKxN3hC3VxwaS4LSxJMghaejC//mMA0GCSqGSIb3DQEBCwUAMFsxCzAJ
BgNVBAYTAkZSMRMwEQYDVQQKEwpDZXJ0aW5vbWlzMRcwFQYDVQQLEw4wMDAyIDQzMzk5ODkwMzEe
MBwGA1UEAxMVQ2VydGlub21pcyAtIFByaW1lIENBMB4XDTE1MDYwOTE1MDg0OFoXDTE5MDcwOTE1
MDg0OFowgZ4xCzAJBgNVBAYTAkZSMSAwHgYDVQQKExdMQSBQT1NURSAtIERTSSBDT1VSUklFUjEc
MBoGA1UECxMTMDAwMiAzNTYwMDAwMDA2NTMwNzEQMA4GA1UEBxMHU1QgT1VFTjEsMCoGA1UEAwwj
TEFfUE9TVEVfVU5JVEVfSE9ST0RBVEFHRV85MjUzNDBfMTExDzANBgNVBAUTBjEtNDMzNTCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALhFXytHiTTaC/QTUEhd7qdVaK3JWT6aWAhYogxF
hp+oj+W0Y40Fo0YSttJoEDkj5F09CZnsFtSereRLMFaKz/cgPkC3zJApQ7iLXSma7xUKImVJXu48
gjkIUl5JbBMvBILyRgIDOxYL5eS7XwqO7Pzth5wLxGvV6e5czxGKSDmrD2ZNWsDSAkU7kYkBOgTS
GQQAnYWPz1gIABqYoqWzjt6NWTHfahTuWSD8n32NVaq9vwVg0ts1tC6YKb2TQbcNyeSe3SvIgD3t
Q2zO12R7NVDFcl+Rdy8GAZg8bf7gIHr5u2TZ2PW3FKvc+8hnjKSouKLBFVyt4SUT56bfVfVc2IUC
AwEAAaOCAbQwggGwMBYGA1UdJQEB/wQMMAoGCCsGAQUFBwMIMA4GA1UdDwEB/wQEAwIHgDBWBggr
BgEFBQcBAQRKMEgwRgYIKwYBBQUHMAGGOmh0dHA6Ly9pZ2MtZzMuY2VydGlub21pcy5jb20vSU5T
VEFOQ0VfU0hBMi9vY3NwL09DU1BfUFJJTUUwHwYDVR0jBBgwFoAUcImA/BO1dMO/PpmMS1KEMJ4w
7Z4wCQYDVR0TBAIwADAXBgNVHSAEEDAOMAwGCiqBegFWAgMDGAEwgYwGA1UdHwSBhDCBgTBLoEmg
R4ZFaHR0cDovL2NybC5pZ2MtZzMuY2VydGlub21pcy5jb20vSU5TVEFOQ0VfU0hBMi9jcmwvQUNf
UFJJTUUtY3JsLTEuY3JsMDKgMKAuhixodHRwOi8vd3d3LmNlcnRpbm9taXMuY29tL2NybC9hY2cz
LVBSSU1FLmNybDA7BgNVHREENDAypDAwLjEsMCoGA1UEAwwjTEFfUE9TVEVfVU5JVEVfSE9ST0RB
VEFHRV85MjUzNDBfMTEwHQYDVR0OBBYEFF5/Kr47LwoS4Am5NeByu1F3AIiYMA0GCSqGSIb3DQEB
CwUAA4ICAQCHuFuS7hHv2ltGzYAzzN8EAYwM6Y677RhLt7F4fovsY8b4unwmLS/3G+GNh70UyuU1
xrrLG1dT7q0ncsBiz7uoSlTi1F3n7GVpXlCneA+rpuZJdtQRLQGCH6201+Npx/+9s2iNhqmg3DSc
EkiuFHmJ4iHmNjib7IiEb8ZCWll0fwCJeWKoPo4+X7Vf8LU2iA/L2UbCVrVvNc10RvRcA6xAZGFd
ejR4PxQgi026Tlx81H0HnJaAQHleIL+na6VBAntu81Ow+qVplXlySj5aPyt4u2BfED0JgY5FTR+O
tGpPcdCeoon9c9dYthLH/m2XpQGypX/s6gogwGblahO/3Zrh/tGwL/6YBV4EQGlEShZKVQCrcqru
WgclxaYOMwtoVTfCkOBvhxTZXo3PE+2QLhgHOpVuPNnL1gqthQBtkH/75aqzXe0fkE5bXc08OwXB
M611OK2YBFiBcUOPI+98baMk9bxxvIlgD6MNUicbiWAdsFlAmpqYZaEHnrWoKVMfUwfMRKEupMXw
TkDbeMWbWnrVKFiVDTucoOa8K5Kir3Z+hGxAxU8h6m+N37KO5jhMVmuZnkFDiN9bYel1pF0tmb8p
Vw8gBRT0BNoWGv0mBTBfv1ZmtUKenyB8+Hokos7HBiiDl7szgY9qSRp7H/2vLFsNNutXThebHE0T
AqbjatS4Bg==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Certinomis - Prime CA*

Issuer OU: *0002 433998903*

Issuer O: *Certinomis*

Issuer C: *FR*

Subject SERIAL NUMBER: *1-4335*

Subject CN: *LA_POSTE_UNITE_HORODATAGE_925340_11*

Subject L: *ST OUEN*

Subject OU: *0002 35600000065307*

Subject O: *LA POSTE - DSI COURRIER*

Subject C: *FR*

Valid from: *Tue Jun 09 17:08:48 CEST 2015*

Valid to: *Tue Jul 09 17:08:48 CEST 2019*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:B8:45:5F:2B:47:89:34:DA:0B:F4:13:50:48:5D:EE:A7:
55:68:AD:C9:59:3E:9A:58:08:58:A2:0C:45:86:9F:A8:8F:E5:B4:63:8D:05:A3:46:12:B6:D2:68:10:39:23:E4:5D:3D:09:99:EC:16:D4:9E:AD:E4:4B:30:56:8A:CF:F7:20
:3E:40:B7:CC:90:29:43:B8:8B:5D:29:9A:EF:15:0A:22:65:49:5E:EE:3C:82:39:08:52:5E:49:6C:13:2F:04:82:F2:46:02:03:3B:16:0B:E5:E4:BB:5F:0A:8E:EC:FC:ED:87:
9C:0B:C4:6B:D5:E9:EE:5C:CF:11:8A:48:39:AB:0F:66:4D:5A:C0:D2:02:45:3B:91:89:01:3A:04:D2:19:04:00:9D:85:8F:CF:58:08:00:1A:98:A2:A5:B3:8E:DE:8D:59:3
1:DF:6A:14:EE:59:20:FC:9F:7D:8D:55:AA:BD:BF:05:60:D2:DB:35:B4:2E:98:29:BD:93:41:B7:0D:C9:E4:9E:DD:2B:C8:80:3D:ED:43:6C:CE:D7:64:7B:35:50:C5:72:5
F:91:77:2F:06:01:98:3C:6D:FE:E0:20:7A:F9:BB:64:D9:D8:F5:B7:1
4:AB:DC:FB:C8:67:8C:A4:A8:B8:A2:C1:15:5C:AD:E1:25:13:E7:A6:DF:55:F5:5C:D8:85:02:03:01:00:01

Extended Key Usage *id_kp_timeStamping*

Authority Info Access *http://igc-g3.certinomis.com/INSTANCE_SHA2/ocsp/OCSP_PRIME*

Authority Key Identifier *70:89:80:FC:13:B5:74:C3:BF:3E:99:8C:4B:52:84:30:9E:30:ED:9E*

Basic Constraints *IsCA: false*

Certificate Policies *Policy OID: 1.2.250.1.86.2.3.3.24.1*

CRL Distribution Points *http://crl.igc-g3.certinomis.com/INSTANCE_SHA2/crl/AC_PRIME-crl-1.crl*

http://www.certinomis.com/crl/acg3-PRIME.crl

Subject Alternative Name *CN=LA_POSTE_UNITE_HORODATAGE_925340_11*

Subject Key Identifier *5E:7F:2A:BE:3B:2F:0A:12:E0:09:B9:35:E0:72:BB:51:77:00:88:98*

Key Usage: *digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint: *D3:5E:3A:5F:C3:DB:0B:A1:54:B0:47:E4:4C:60:63:2A:0C:89:D5:AD:55:CE:22:87:53:5F:67:0E:E9
:02:41:4B*

X509SubjectName

Subject SERIAL NUMBER: *1-4335*

Subject CN: *LA_POSTE_UNITE_HORODATAGE_925340_11*

Subject L: *ST OUEN*

Subject OU: *0002 35600000065307*

Subject O: *LA POSTE - DSI COURRIER*

Subject C: *FR*

X509SKI

X509 SK I *Xn8qvjsvChLgCbk14HK7UXcAiJg=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2017-02-28T23:00:00Z*

TSP Service Definition URI

URI *[en]* *http://cachetdelaposte.com/Documents/Politiquedhorodatage-ServicedhorodatageLaPosteV6.pdf*

URI *[fr]* *http://cachetdelaposte.com/Documents/Politiquedhorodatage-ServicedhorodatageLaPosteV6.pdf*

14.4 - Service (granted): La Poste - Autorité d'horodatage - UH3 1.2.250.1.8.1.1.1.1.6

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[fr] *Un service de génération horodatage création et la signature temps timbres jetons qualifiés.*

Service Name

Name *[en]* *La Poste - Autorité d'horodatage - UH3 1.2.250.1.8.1.1.1.1.6*

Name *[fr]* *La Poste - Autorité d'horodatage - UH3 1.2.250.1.8.1.1.1.1.6*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *139136906404536937207002877849487016662508292980 5*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIGQjCCBCqgAwIBAgIVAPO3JYq8Td0L/HjcyUSzJDcIr/KNMA0GCSqGSIb3DQEBCwUAMFsxCzAJ
BgNVBAYTAkZSMRMwEQYDVQQKEwpDZXJ0aW5vbWlzMRcwFQYDVQQLEw4wMDAyIDQzMzk5ODkwMzEe
MBwGA1UEAxMVQ2VydGlub21pcyAtIFByaW1lIENBMB4XDTE1MDYwOTE1MDgxOFoXDTE5MDcwOTE1
MDgxOFowgaExCzAJBgNVBAYTAkZSMSAwHgYDVQQKExdMQSBQT1NURSAtIERTSSBDT1VSUklFUjEc
MBoGA1UECxMTMDAwMiAzNTYwMDAwMDA2NTMwNzETMBEGA1UEBxMKU0FJTlQgT1VFTjEsMCoGA1UE
AwwjTEFfUE9TVEVfVU5JVEVfSE9ST0RBVEFHRV85MjUzNjlfMTAxDzANBgNVBAUTBjEtNDMzMzCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANxN81NBVfHswkGWRoRPgnfltfs3P+DUZOSY
Gw5WNW6wtckdfOJG6FFIdoPGs0tJ3U769YvFy6r//vxDDJSzULFlWDYsftmvctkxC94q4N7eUnNN
gf2AcLtOXFyMQJ9mQXc73cwy1rNnQCnRnLm1ZktjlHqc0DVP4tf3f4ErXTehHAVGkA1qtSBW08E0
JrPBEwGny43BcYgosrXLuAOuumnH1KmxQ8r5BI2/RoJpNUM22XCCfwzVOBq9TIPUJ1Bc2TXloYIH
h6568ljipbUQ0QYe1s1scdaJFSQzxHFruR7syVjj8eohe93bEnR+ByrvEuzkEWJrDTp5OXCR8RhA
UfUCAwEAAaOCAbQwggGwMBYGA1UdJQEB/wQMMAoGCCsGAQUFBwMIMA4GA1UdDwEB/wQEAwIHgDBW
BggrBgEFBQcBAQRKMEgwRgYIKwYBBQUHMAGGOmh0dHA6Ly9pZ2MtZzMuY2VydGlub21pcy5jb20v
SU5TVEFOQ0VfU0hBMi9vY3NwL09DU1BfUFJJTUUwHwYDVR0jBBgwFoAUcImA/BO1dMO/PpmMS1KE
MJ4w7Z4wCQYDVR0TBAIwADAXBgNVHSAEEDAOMAwGCiqBegFWAgMDGAEwgYwGA1UdHwSBhDCBgTBL
oEmgR4ZFaHR0cDovL2NybC5pZ2MtZzMuY2VydGlub21pcy5jb20vSU5TVEFOQ0VfU0hBMi9jcmwv
QUNfUFJJTUUtY3JsLTEuY3JsMDKgMKAuhixodHRwOi8vd3d3LmNlcnRpbm9taXMuY29tL2NybC9h
Y2czLVBSSU1FLmNybDA7BgNVHREENDAypDAwLjEsMCoGA1UEAwwjTEFfUE9TVEVfVU5JVEVfSE9S
T0RBVEFHRV85MjUzNjlfMTAwHQYDVR0OBBYEFEt+YXCOuPJPJvSwX60Qr1WMJ1mcMA0GCSqGSIb3
DQEBCwUAA4ICAQDBMhNnrWev0HfVVgRuQWs9dP32+9SRNOER1e+F7VdV20a6MQNwSSuShBzRsjdj
adlmEgj9uqzo5aDE5t2O1Ntxu24nsO9tZAvYdKJ5knLK9GCTfPlzTzf2qk7oY+MUMn5H9i9eFZNm
ZI5MSqeRyN31ThENZrCfg5Wxt/Ejuu9+WLn+asHR3QQk9L3tZbu4j4kLTKQfObpZv+CbJ6PN2L0G
qZ0Q86PH0zbU/Glej8MkhL9lqguTFcst9JnN+IxmiNYVMgNa72Z9vq8ZrayRUNXF+PD8D45o6Uha
Cm7UM0GL+ZrQHKiVCFtCT6PfyDI35+DG1JFKtsqZlJYPOfIF9Fbx1y1loq1j8igWUgH/QURBwZAb
WijnQbsQRfmbFvkOh4hceCi3RVr/VYrMyzALTNibDhpD1kUIrejJQja9dMhCmY3I71Tq+NlB/s+U
bzwbcRZlJa5r8KmGOSwNhoj5+ybju1+qgtjQ1G8S6JrbFHu0KgAyQlBLaQu7fhNQaCTxL8xkIVGS
Cwtkt79xfC1/oKKtKRGWg0odrX6wj8e/gtiKjm68NQz1lnmc5WzQl/pujckKlB01CYATYhGY5X5m
4X69seHlkSrALRLD/j4cmjHkfEKMwatzkKE+2+TSM/iba3RP7Q/xOB+z493djwr/AV+oD0J0bDS6 X56UvRUTgTJTwA==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *Certinomis - Prime CA*

Issuer OU: *0002 433998903*

Issuer O: *Certinomis*

Issuer C: *FR*

Subject SERIAL NUMBER: *1-4333*

Subject CN: *LA_POSTE_UNITE_HORODATAGE_925369_10*

Subject L: *SAINT OUEN*

Subject OU: *0002 35600000065307*

Subject O: *LA POSTE - DSI COURRIER*

Subject C: *FR*

Valid from: *Tue Jun 09 17:08:18 CEST 2015*

Valid to: *Tue Jul 09 17:08:18 CEST 2019*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:DC:4D:F3:53:41:55:F1:EC:C2:41:96:46:84:4F:82:77:E5:B5:FB:37:3F:E0:D4:64:E4:98:1B:0E:56:35:6E:B0:B5:C9:1D:7C:E2:46:E8:51:48:76:83:C6:B3:4B:49:DD:4E:FA:F5:8B:C5:CB:AA:FF:FE:FC:43:0C:94:B3:50:B1:65:58:36:2C:7E:D9:AF:72:D9:31:0B:DE:2A:E0:DE:DE:52:73:4D:81:FD:80:70:BB:4E:5C:5C:8C:40:9F:66:41:77:3B:DD:CC:32:D6:B3:67:40:29:D1:9C:B9:B5:66:4B:63:20:7A:9C:D0:35:4F:E2:D7:F7:7F:81:2B:5D:37:A1:1C:05:46:90:0D:6A:B5:20:56:D3:C1:34:26:B3:C1:13:01:A7:CB:8D:C1:71:88:28:B2:B5:CB:B8:03:AE:BA:69:C7:D4:A9:B1:43:CA:F9:04:8D:BF:46:82:69:35:43:36:D9:70:82:7F:0C:D5:38:1A:BD:4C:83:D4:27:50:5C:D9:35:E5:A1:82:07:87:AE:7A:F2:58:E2:A5:B5:10:D1:06:1E:D6:CD:6C:71:D6:89:15:24:33:C4:71:6B:B9:1E:EC:C9:58:E3:F1:EA:21:7B:DD:DB:12:74:7E:07:2A:EF:12:EC:E4:11:62:6B:0D:3A:79:39:70:91:F1:18:40:51:F5:02:03:01:00:01

Extended Key Usage *id_kp_timeStamping*

Authority Info Access *http://igc-g3.certinomis.com/INSTANCE_SHA2/ocsp/OCSP_PRIME*

Authority Key Identifier *70:89:80:FC:13:B5:74:C3:BF:3E:99:8C:4B:52:84:30:9E:30:ED:9E*

Basic Constraints *IsCA: false*

Certificate Policies *Policy OID: 1.2.250.1.86.2.3.3.24.1*

CRL Distribution Points *http://crl.igc-g3.certinomis.com/INSTANCE_SHA2/crl/AC_PRIME-crl-1.crl*

http://www.certinomis.com/crl/acg3-PRIME.crl

Subject Alternative Name *CN=LA_POSTE_UNITE_HORODATAGE_925369_10*

Subject Key Identifier *4B:7E:61:70:8E:B8:F2:4F:26:F4:B0:5F:AD:10:AF:55:8C:27:59:9C*

Key Usage: *digitalSignature*

Thumbprint algorithm: *SHA-256*

Thumbprint: *65:A8:3F:B0:4F:7D:AD:4F:31:8D:E8:3B:5F:43:1F:A8:1F:AD:8A:47:B3:43:00:1D:8A:79:6C:93:48:6C:7F:0D*

X509SubjectName

Subject SERIAL NUMBER: *1-4333*

Subject CN: *LA_POSTE_UNITE_HORODATAGE_925369_10*

Subject L: *SAINT OUEN*

Subject OU: *0002 35600000065307*

Subject O: *LA POSTE - DSI COURRIER*

Subject C: *FR*

X509SKI

X509 SK I *S35hcI648k8m9LBfrRCvVYwnWZw=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description	*[en]*	*undefined.*
	[fr]	*undefined.*

Status Starting Time *2017-02-28T23:00:00Z*

TSP Service Definition URI

URI	*[en]*	*http://cachetdelaposte.com/Documents/Politiquedhorodatage-ServicedhorodatageLaPosteV6.pdf*
URI	*[fr]*	*http://cachetdelaposte.com/Documents/Politiquedhorodatage-ServicedhorodatageLaPosteV6.pdf*

15 - TSP: Almerys

TSP Name

Name	*[en]*	*Almerys*
Name	*[fr]*	*Almerys*

TSP Trade Name

Name	*[en]*	*VATFR-04432701630*
Name	*[fr]*	*VATFR-04432701630*

PostalAddress

Street Address	*[en]*	*Almerys – 46 rue du Ressort*
Locality	*[en]*	*Clermont-Ferrand Cedex 9*
Postal Code	*[en]*	*63967*
Country Name	*[en]*	*FR*

PostalAddress

Street Address	*[fr]*	*Autorité de Gouvernance IGC almerys;Almerys – 46 rue du Ressort*
Locality	*[fr]*	*CLERMONT-FERRAND CEDEX 9*
Postal Code	*[fr]*	*63967*
Country Name	*[fr]*	*FR*

ElectronicAddress

URI *http://pki.almerys.com/*

URI *mailto:gouvernance.igc@almerys.com*

TSP Information URI

URI *[en]* *http://pki.almerys.com/customers.html*

URI *[fr]* *http://pki.almerys.com/customers.html*

15.1 - Service (withdrawn): ALMERYS CUSTOMER SERVICES CA

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[fr] *Un service de génération horodatage création et la signature temps timbres jetons qualifiés.*

Service Name

Name *[en]* *ALMERYS CUSTOMER SERVICES CA*

Name *[fr]* *ALMERYS CUSTOMER SERVICES CA*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *10021*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIGTjCCBDagAwIBAgICJyUwDQYJKoZIhvcNAQELBQAwUjELMAkGA1UEBhMCRlIxE
DAOBgNVBAoTB0FMTUVSWVMxFzAVBgNVBAsTDjAwMDIgNDMyNzAxNjM5MRgwFgYDVQQDEw9BTE1FUllTIFJPT1Qg
Q0EwHhcNMTIwODI5MTAwNDE5WhcNMjIwODI5MTAwNDE5WjB+MQswCQYDVQQGEwJGUjEQMA4GA1UE
ChMHQUxNRVJZUzEXMBUGA1UECxMOMDAwMiA0MzI3MDE2MzkxGjAYBgNVBAsTEUFEVkFOQ0VEIFNF
UlZJQ0VTMSgwJgYDVQQDEx9BTE1FUllTIENVU1RPTUVSIFNFUlZJQ0VTIENBIE5CMIICIjANBgkq
hkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA06O5R4y4jZD5vX1hyWYjWxzrDqnrTdPXqMU2UnDU/tIK
CQ0zguy/PQH8bGIgwIiK1EfL8NB6FgWt792OltTI6ZZsDmgjsBxGNeBJ40xoc7/B0cUebjTOjSP6
K2m4PrPAWIWolRdAaAZVc7jm8tvAXOZ9LIudBokfWByPqFYtaI9lmmDeKf+GdZYLQaSIKoE+YzPD
cDevW1eNOB+MPrTC0tdwU9u6GY3FuS9Jqj42EOrcDNEkPv+OAGySTmp+Hw0SNnicymdMMSwg3BU0
jXEodnqfPfw8PsACS321WnAqBXtPg4et4pqNf+iGE3ThBvrBkKZDNENEFz4JofMrIhkAz6hRu4Jq
xXaTprem2keEhgwrqjfYdp4Y+Ur57+T15vhchjjEK2SRnXCs1PGRBZGVcEB6Ae8lkHj1Jr/asYuv
O+TAbfxpmg7XaDByMFzwqqtyrwFCNxHZ8rg7LO1NlLAu4rzVjq1COxA5rCeMkB/nFW2LLn/Z+CXn
3TvLCiHrWZXGY8Bw442ZvmBV66jA2jYZ8UQQQ3iMDOweMBD6yz0V1By8trcvJspXDQYqacpqjQUa
X3TlqgbjBoyecHE+sa7AjIDrK2l5KJES55m8ZosB0gQL9CdjQV2ckUm/qKpLzv45IzQfqmHMLesz
R4LRQvVUGqeCNjG06uPFYn+PsTDr6gkCAwEAAaOCAQAwgf0wDwYDVR0TAQH/BAUwAwEB/zAdBgNV
HQ4EFgQUCHPdjwG/a4diDGYwoOKzhLAabaMwGQYDVR0gBBIwEDAOBgwqgXoBEAwFKQEFAgEwHwYD
VR0jBBgwFoAUm2BNqvD0JVL6o6Fr6G38i5gb1cUwRAYIKwYBBQUHAQEEODA2MDQGCCsGAQUFBzAC
hihodHRwOi8vcGtpLmFsbWVyeXMuY29tL2FsbWVyeXNyb290Y2EuY2VyMA4GA1UdDwEB/wQEAwIB
BjA5BgNVHR8EMjAwMC6gLKAqhihodHRwOi8vcGtpLmFsbWVyeXMuY29tL2FsbWVyeXNyb290Y2Eu
Y3JsMA0GCSqGSIb3DQEBCwUAA4ICAQDDsxC3IWvIiXpKDvJmeSArVXFLeLCvbaBo1DTuWYomw9Jb
iAzJKWby3VkEBEU0nM3mD3h41DP6HL+ITqGa6CENe9kCr6/TxXTxypV+EtfLemhaUbfWDL+z0z/4
+zUnHhYuWuUw3MTkhbwFocHrhY25RNNU6EbHNd91mOKgaFjJpXAAmUDR3M9n9F8KdRgnz8vBTpYc
8d3Zcym9qXmuaVJ4cbkis/5aQEXHUcTmQz6Qa0lEHsKL72aANq/45ZZumw424jzeGRnnFjmzhJKz
CuczX4UD6rEa5z++v/2d7qiLQ4qPzruGgjOKjHgoylqrFNVENs041piuUD5O1k4nFcZ9yvtZz532
r8ruZLoj7ugcwdpVkv/mfBHV7jMPDlRg8/7rIc080VbY9aJ+RD55c+B0p1db90wRn34SCQ1q6Wud
D1pOdoFJCu9OqWD0R8F3xnzrrywXMxyTCteqFGDx+0Oe17RK3m2whqA+6ylNLNVDBLsigovMQ5io

vSt6HNEhPGdjNYwyJPaA6z+SLwRoWFo6f2fu/h5XMon7c3gYkfTAl0PM6xE9NhlyrdF8oWNz6UZC
Ng7XuVpU9hA8K2/7B5VwPMtL0poSd3AFkQYCzTkbQ+qlJrhoYcvn6EpzOoSPgXezLSx2wX27I7Mp
XtE/2O5bd3VV4IMKefEwfHd8U48R9w==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer CN: *ALMERYS ROOT CA*

Issuer OU: *0002 432701639*

Issuer O: *ALMERYS*

Issuer C: *FR*

Subject CN: *ALMERYS CUSTOMER SERVICES CA NB*

Subject OU: *ADVANCED SERVICES*

Subject OU: *0002 432701639*

Subject O: *ALMERYS*

Subject C: *FR*

Valid from: *Wed Aug 29 12:04:19 CEST 2012*

Valid to: *Mon Aug 29 12:04:19 CEST 2022*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:D3:A3:B9:47:8C:B8:8D:90:F9:BD:7D:61:C9:66:23:5B
:1C:EB:0E:A9:EB:4D:D3:D7:A8:C5:36:52:70:D4:FE:D9:4A:09:0D:33:82:EC:BF:3D:01:FC:6C:62:20:C0:88:8A:D4:47:CB:F0:D0:7A:16:05:AD:EF:DD:8E:96:D4:C8:E9:
96:6C:0E:68:23:B0:1C:46:35:E0:49:E3:4C:68:73:BF:C1:D1:C5:1E:6E:34:CE:8D:23:FA:2B:69:B8:3E:B3:C0:58:85:A8:95:17:40:68:06:55:73:B8:E6:F2:DB:C0:5C:E6:
7D:2C:8B:9D:06:89:1F:58:1C:8F:A8:56:2D:68:8F:65:9A:60:DE:29:FF:86:75:96:0B:41:A4:88:2A:81:3E:63:33:C3:70:37:AF:5B:57:8D:38:1F:8C:3E:B4:C2:D2:D7:70
:53:DB:BA:19:8D:C5:B9:2F:49:AA:3E:36:10:EA:DC:0C:D1:24:3E:FF:8E:00:6C:92:4E:6A:7E:1F:0D:12:36:78:9C:CA:67:4C:31:2C:20:DC:15:34:8D:71:28:76:7A:9F:3
D:FC:3C:3E:C0:02:4B:7D:B5:5A:70:2A:05:7B:4F:83:87:AD:E2:9A:8D:7F:E8:86:13:74:E1:06:FA:C1:90:A6:43:34:43:44:17:3E:09:A1:F3:2B:22:19:00:CF:A8:51:BB:
82:6A:C5:76:93:A6:B7:A6:DA:47:84:86:0C:2B:AA:37:D8:76:9E:18:F9:4A:F9:EF:E4:F5:E6:F8:5C:86:38:C4:2B:64:91:9D:70:AC:D4:F1:91:05:91:95:70:40:7A:01:EF:
25:90:78:F5:26:BF:DA:B1:8B:AF:3B:E4:C0:6D:FC:69:9A:0E:D7:68:30:72:30:5C:F0:AA:AB:72:AF:01:42:37:11:D9:F2:B8:3B:2C:ED:4D:94:B0:2E:E2:BC:D5:8E:AD:4
2:3B:10:39:AC:27:8C:90:1F:E7:15:6D:8B:2E:7F:D9:F8:25:E7:DD:3B:CB:0A:21:EB:59:95:C6:63:C0:70:E3:8D:99:BE:60:55:EB:A8:C0:DA:36:19:F1:44:10:43:78:8C:
0C:EC:1E:30:10:FA:CB:3D:15:D4:1C:BC:B6:B7:2F:26:CA:57:0D:06:2A:69:CA:6A:8D:05:1A:5F:74:E5:AA:06:E3:06:8C:9E:70:71:3E:B1:AE:C0:8C:80:EB:2B:69:79:2
8:91:12:E7:99:BC:66:8B:01:D2:04:0B:F4:27:63:41:5D:9C:91:49:BF:A8:AA:4B:CE:FE:39:23:34:1F:AA:61:CC:2D:EB:33:47:82:D1:42:F5:54:1A:A7:82:36:31:B4:EA:
E3:C5:62:7F:8F:B1:30:EB:EA:09:02:03:01:00:01

Basic Constraints *IsCA: true*

Subject Key Identifier *08:73:DD:8F:01:BF:6B:87:62:0C:66:30:A0:E2:B3:84:B0:1A:6D:A3*

Certificate Policies *Policy OID: 1.2.250.1.16.12.5.41.1.5.2.1*

Authority Key Identifier *9B:60:4D:AA:F0:F4:25:52:FA:A3:A1:6B:E8:6D:FC:8B:98:1B:D5:C5*

Authority Info Access *http://pki.almerys.com/almerysrootca.cer*

CRL Distribution Points *http://pki.almerys.com/almerysrootca.crl*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *4C:DB:E5:C4:BF:27:0C:40:E3:FE:21:4F:BB:CD:C8:D6:0B:1A:23:7B:C8:18:1C:33:D6:B2:FD:47:41:96:47:10*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2016-06-30T22:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS101456/QCP+*

URI *[fr]* *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/FR/Time-Stamping*

TSP Service Definition URI

URI *[fr]* *http://pki.almerys.com/almeryscustomerservicescanb-1.6.pdf*

URI *[en]* *http://pki.almerys.com/almeryscustomerservicescanb-cgu-eng1.5.pdf*

15.1.1 - History instance n.1 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service Name

Name *[en]* *ALMERYS CUSTOMER SERVICES CA*

Name *[fr]* *ALMERYS CUSTOMER SERVICES CA*

Service digital identities

X509SubjectName

Subject CN: *ALMERYS CUSTOMER SERVICES CA NB*

Subject OU: *ADVANCED SERVICES*

Subject OU: *0002 432701639*

Subject O: *ALMERYS*

Subject C: *FR*

X509SKI

X509 SK I *CHPdjwG/a4diDGYwoOKzhLAabaM=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2012-10-01T00:00:00Z*

15.2 - Service (withdrawn): ALMERYS SIGNATURE AND AUTHENTICATION CA

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description

[en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[fr] *Un service de génération de certificat et la signature de la création de certificats qualifiés sur la base de l'identité et d'autres attributs vérifiées par les services d'enregistrement pertinents.*

Service Name

Name *[en]* *ALMERYS SIGNATURE AND AUTHENTICATION CA*

Name *[fr]* *ALMERYS SIGNATURE AND AUTHENTICATION CA*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *10028*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIGWjCCBEKgAwIBAgICJywwDQYJKoZIhvcNAQELBQAwUjELMAkGA1UEBhMCRlIxEDAOBgNVBAoT
B0FMTUVSWVMxFzAVBgNVBAsTDjAwMDIgNDMyNzAxNjM5MRgwFgYDVQQDEw9BTE1FUllTIFJPT1Qg
Q0EwHhcNMTMxMDMwMTQwNTQ2WhcNMjMxMDMwMTQwNTQ2WjCBiTELMAkGA1UEBhMCRlIxEDAOBgNV
BAoTB0FMTUVSWVMxFzAVBgNVBAsTDjAwMDIgNDMyNzAxNjM5MRowGAYDVQQLExFBRFZBTkNFRCBT
RVJWSUNFUzEzMDEGA1UEAxMqQUxNRVJZUyBTSUdOQVRVUkUgQU5EIEFVVEhFTlRJQ0FUSU9OIENB
IE5DMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAu53DzeDL+VaBHDHoJeyxtWhGifT0
jctEVpZL0Rz3Xs2EKnKi6PTJHPw8nGwENUTarMkp6wsdTFksWAxEA0aqF2eaaclg/siaPP159WgO
9wBTXvmIsX8a0jwOw+qwXjKHICVROy8QzMYalQ6sSLrOi1+cad+hh4Ki91a1hiktcFcAyQpvIwp0
baWItiAZtWVagTSa+GUVUE5Fn9lpLRpR28iqTQYM2BmKuFZ+Pi8Xzhu0YgMUUTZF7TYcjIt8BExw
NMbagLWqeZ1OeloDkiqh4+IAT3G6v+B7c4JkDn3MqvS5XV5MLqJzNDRbmA2I5olmKUrgTuV0Fy9g
19mDDu2WQsGF4xRqvjzzAWOxbMgnRQk/uxqz83qGXSuMj8kG2jHGmbQZfIznWYvFEkWHX5Rb1kxl
V67RkyN6f4LarJ4DNWE+qbgDeg8jbI4x44j0OUB9bmmqDHXWyXMBfKQ0JiAAAMByYf9oR+KXpnCn
PMgjT7zMILdp1mybiBlmV0FNnFzcVuRbGnVQK7pufUeQrFBKcwmdVBxqZwLaAwpksEOHPAUgHkNy
jgUmp06o11aIuOGT+ILFOcVYQn8IVAun6LUsL5RMfyjGLIiM2b7fBoBpWpibNy82Jbpdgkh3YrGU
0WBrmFBns2Osg8YiWTA0EihMB5onMy1/12aDoAwY7ypF2dcCAwEAAaOCAQAwgf0wDwYDVR0TAQH/
BAUwAwEB/zAdBgNVHQ4EFgQUcVRnGiMDlzGf6zJ3z0lYVP8QzRUwGQYDVR0gBBIwEDAOBgwqgXoB
EAwFKQEHAwEwHwYDVR0jBBgwFoAUm2BNqvD0JVL6o6Fr6G38i5gb1cUwRAYIKwYBBQUHAQEEODA2
MDQGCCsGAQUFBzAChihodHRwOi8vcGtpLmFsbWVyeXMuY29tL2FsbWVyeXNyb290Y2EuY2VyMA4G
A1UdDwEB/wQEAwIBBjA5BgNVHR8EMjAwMC6gLKAqhihodHRwOi8vcGtpLmFsbWVyeXMuY29tL2Fs
bWVyeXNyb290Y2EuY3JsMA0GCSqGSIb3DQEBCwUAA4ICAQA2owwshK4rZTbkX7iwlApRFi7ukDUG
BWVYv+NwUnA6VtkXU35f3rmS5zivOjTqCLTT8yopbrNvWTDMk6oNLiH7qrfr2q2tuju/7KD04CZo
oxDH1LRf9RUuSnoZMPF9VPLg4WTmSrI82Gjm1OlsffVlNk/PVmWI10TfRP7yMBhkLGKX+cx+AJ2N
HC3HRfNifhriVePv3VSHAHSQDtQ5m7Nn46o56q6g1E0FxKjwLqUOra9I8/FdNqNkIRDLlxNRNWce
nqmZCgbdOqjfb1xZjCzhNx05Iofs6UDD4HfOF0kmUqJRPTOwikhKOIpwEBUIssBpqOKuJ5PkCiZa
ePk/8XXjoQDf7VI7gd6mjUqcXE3HlWecIaHnbNCkLyf7HL38a/bFVM8ertlHReF05Yz7jugsxDfU
r0wm9u1Q14nEbwVLaPVYQNsIeLes6gGMjBtsLPts9OYT1sdV7TJNBnkSRIZNg8hYbCbnLkybQyez

rsHOC6L2iTmGjHeamHp35bW0Ts3fJjpQSb9fT4KX+AD6+AcEzUHFC02KpgVnPn4BdMw21MmDD8zR
Z8kJtX8Eo9m5ikA99M72uYvhSCClQ7r2VLTn9GhfIRLV2vn5FXL2DTWfbov3lNPxnGhGd1JiTFWZ
AvxNUA8zjwczq5ntnQrnl2nY/CopgPsyLOF8jzhevgCYsw==

-----END CERTIFICATE-----

Signature algorithm:	*SHA256withRSA*
Issuer CN:	*ALMERYS ROOT CA*
Issuer OU:	*0002 432701639*
Issuer O:	*ALMERYS*
Issuer C:	*FR*
Subject CN:	*ALMERYS SIGNATURE AND AUTHENTICATION CA NC*
Subject OU:	*ADVANCED SERVICES*
Subject OU:	*0002 432701639*
Subject O:	*ALMERYS*
Subject C:	*FR*
Valid from:	*Wed Oct 30 15:05:46 CET 2013*
Valid to:	*Mon Oct 30 15:05:46 CET 2023*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:BB:9D:C3:CD:E0:CB:F9:56:81:1C:31:E8:25:EC:B1:B5:
68:46:89:F4:F4:8D:CB:44:56:96:4B:D1:1C:F7:5E:CD:84:2A:72:A2:E8:F4:C9:1C:FC:3C:9C:6C:04:35:44:DA:AC:C9:29:EB:0B:1D:4C:59:2C:58:0C:44:03:46:AA:17:6
7:9A:69:C9:60:FE:C8:9A:3C:FD:79:F5:68:0E:F7:00:53:5E:F9:88:B1:7F:1A:D2:3C:0E:C3:EA:B0:5E:32:87:20:25:51:3B:2F:10:CC:C6:1A:95:0E:AC:48:BA:CE:8B:5F:9
C:69:DF:A1:87:82:A2:F7:56:B5:86:29:2D:70:57:00:C9:0A:6F:23:0A:74:6D:A5:88:B6:20:19:B5:65:5A:81:34:9A:F8:65:15:50:4E:45:9F:D9:69:2D:1A:51:DB:C8:AA:
4D:06:0C:D8:19:8A:B8:56:7E:3E:2F:17:CE:1B:B4:62:03:14:51:36:45:ED:36:1C:8C:8B:7C:04:4C:70:34:C6:DA:80:B5:AA:79:9D:4E:7A:5A:03:92:2A:A1:E3:E2:00:4
F:71:BA:BF:E0:7B:73:82:64:0E:7D:CC:AA:F4:B9:5D:5E:4C:2E:A2:73:34:34:5B:98:0D:88:E6:89:66:29:4A:E0:4E:E5:74:17:2F:60:D7:D9:83:0E:ED:96:42:C1:85:E3:1
4:6A:BE:3C:F3:01:63:B1:6C:C8:27:45:09:3F:BB:1A:B3:F3:7A:86:5D:2B:8C:8F:C9:06:DA:31:C6:99:B4:19:7C:8C:E7:59:8B:C5:12:45:87:5F:94:5B:D6:4C:65:57:AE:
D1:93:23:7A:7F:82:DA:AC:9E:03:35:61:3E:A9:B8:03:7A:0F:23:6C:8E:31:E3:88:F4:39:40:7D:6E:69:AA:0C:75:D6:C9:73:01:7C:A4:34:26:20:00:00:C0:72:61:FF:68:
47:E2:97:A6:70:A7:3C:C8:23:4F:BC:CC:20:B7:69:D6:6C:9B:88:19:66:57:41:4D:9C:5C:DC:56:E4:5B:1A:75:50:2B:BA:6E:7D:47:90:AC:50:4A:73:09:9D:54:1C:6A:6
7:02:DA:03:0A:64:B0:43:87:3C:05:20:1E:43:72:8E:05:26:A7:4E:A8:D7:56:88:B8:E1:93:F8:82:C5:39:C5:58:42:7F:08:54:0B:A7:E8:B5:2C:2F:94:4C:7F:28:C6:2C:8
8:8C:D9:BE:DF:06:80:69:5A:98:9B:37:2F:36:25:BA:5D:82:48:77:62:B1:94:D1:60:6B:98:50:67:B3:63:AC:83:C6:22:59:30:34:12:28:4C:07:9A:27:33:2D:7F:D7:66:
83:A0:0C:18:EF:2A:45:D9:D7:02:03:01:00:01

Basic Constraints	*IsCA: true*
Subject Key Identifier	*71:54:67:1A:23:03:97:31:9F:EB:32:77:CF:49:58:54:FF:10:CD:15*
Certificate Policies	*Policy OID: 1.2.250.1.16.12.5.41.1.7.3.1*
Authority Key Identifier	*9B:60:4D:AA:F0:F4:25:52:FA:A3:A1:6B:E8:6D:FC:8B:98:1B:D5:C5*
Authority Info Access	*http://pki.almerys.com/almerysrootca.cer*

CRL Distribution Points *http://pki.almerys.com/almerysrootca.crl*

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *CB:82:23:E9:4A:C5:4A:56:8B:51:4B:3F:98:D2:0D:1D:59:C2:AE:6C:D3:2A:1B:63:84:E7:A9:56:D7:DD:93:EE*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2017-10-03T00:00:00Z*

Scheme Service Definition URI

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS102042/NCP+*

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR/TS101456/QCP+*

TSP Service Definition URI

URI *[fr]* *http://pki.almerys.com/almeryssignatureandauthenticationcanc-1.3.pdf*

URI *[en]* *http://pki.almerys.com/almeryssignatureandauthenticationcanc-cgu-eng-1.3.pdf*

15.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

15.2.2 - History instance n.1 - Status: granted

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *ALMERYS SIGNATURE AND AUTHENTICATION CA*

Name *[fr]* *ALMERYS SIGNATURE AND AUTHENTICATION CA*

Service digital identities

X509SubjectName

Subject CN: *ALMERYS SIGNATURE AND AUTHENTICATION CA NC*

Subject OU: *ADVANCED SERVICES*

Subject OU: *0002 432701639*

Subject O: *ALMERYS*

Subject C: *FR*

X509SKI

X509 SK I *cVRnGiMDlzGf6zJ3z0lYVP8QzRU=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

15.2.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

15.2.3 - History instance n.2 - Status: accredited

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service Name

Name *[en]* *ALMERYS SIGNATURE AND AUTHENTICATION CA*

Name *[fr]* *ALMERYS SIGNATURE AND AUTHENTICATION CA*

Service digital identities

X509SubjectName

Subject CN: *ALMERYS SIGNATURE AND AUTHENTICATION CA NC*

Subject OU: *ADVANCED SERVICES*

Subject OU: *0002 432701639*

Subject O: *ALMERYS*

Subject C: *FR*

X509SKI

X509 SK I *cVRnGiMDlzGf6zJ3z0lYVP8QzRU=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited*

Status Starting Time *2013-12-31T23:00:00Z*

16 - TSP: Yousign

TSP Name

Name *[en]* *Yousign*

Name *[fr]* *Yousign*

TSP Trade Name

Name *[en]* *VATFR-61794513986*

Name *[fr]* *VATFR-61794513986*

PostalAddress

Street Address *[en]* *8 allée Henri Pigis*

Locality *[en]* *Caen*

Postal Code *[en]* *14000*

Country Name *[en]* *FR*

ElectronicAddress

URI *mailto:direction@yousign.fr*

URI *https://yousign.fr*

TSP Information URI

URI *[en]* *https://yousign.fr/fr/public/document*

16.1 - Service (granted): Yousign Timestamp

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description *[en]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[fr] *Un service de génération horodatage création et la signature temps timbres jetons qualifiés.*

Service Name

Name *[en]* *Yousign Timestamp*

Name *[fr]* *Yousign Timestamp*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *3871889179248856277*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIGkjCCBHqgAwIBAgIINbu2scLOjNUwDQYJKoZIhvcNAQELBQAwejEfMB0GA1UEAwwWWU9VU0lH
TiBTQVMgLSBST09UMiBDQTESMBAGA1UECwwJNzk0NTEzOTg2MRQwEgYDVQQKDAtZT1VTSUdOIFNB
UzENMAsGA1UEBwwEQ0FFTjERMA8GA1UECAwIQ0FMVkFET1MxCzAJBgNVBAYTAkZSMB4XDTE1MTAy
MTIyNTkyN1oXDTI1MTAyMTIyNTkyN1owejEfMB0GA1UEAwwWWU9VU0lHTiBTQVMgLSBTSUdOMiBD
QTESMBAGA1UECwwJNzk0NTEzOTg2MRQwEgYDVQQKDAtZT1VTSUdOIFNBUzENMAsGA1UEBwwEQ0FF
TjERMA8GA1UECAwIQ0FMVkFET1MxCzAJBgNVBAYTAkZSMIICIjANBgkqhkiG9w0BAQEFAAOCAg8A
MIICCgKCAgEAwXOohy0+2rgG4elk8VkOGis41FGrk9Bp3VlOBkRDYHngMvWVxbcs+J/AKvO4exzW
sBgXSl4twov22zmf5PJ6VaFnC8ReJxwAoFI8zwUPIMlb2apcpvU46Fmi/ihsQbOH/Vote0sy8nA8
DINTMc+cla1vC7tQzLnSID3SY9Yh2pa1UbgdrDgey8wURNqDfQ91ewUQB3aLptYKkfVQaec8rMgn
tPgxAfw+M3zjxIM3OENjWQQpanO/G7tV6AcmGTEpzL34n5DmzxkDzxkNyLc/4dUQqsJizl7R/EO1
TxA2HukXi7ksdKHQnXMO0HJHlD+j9cMBRAd4BgUFT4pG5HWSNmBBqx5A/JP42qp9zkzLav3GShL9
qZprbYUMbnLJrbpuiqOLzx8YRUAX1E55i6f/qI9C34WsZpeENb9KkGQtT92E1XThaHKNNymT4i4A
LD2hGIr4BX6+EHMCJjEYWdZzr75GX80U5gLUcnooRKOou5FMRUXTmHh6TqQzRgfWywiyGOMK6Z+x
5700BSYJEj21d2XwCXSJtA6UTCOdSagK84OkaA8M+4m11O3gcqZrpkr7K95nPdiqAme22JPOIUZH
uZXA/ssEeWVxJ8zJzXO1JIF+7FwgbN9CCyaEufBP/xrHeOOPACBjrDYui2R1B8UrItNNq0O+lRGf
tQdmrZ/BKHUCAwEAAaOCARowggEWMB0GA1UdDgQWBBTlRX/Am34ff8dep3c2I4cKvMkGLjAPBgNV
HRMBAf8EBTADAQH/MB8GA1UdIwQYMBaAFMduZ/CoExeWEdwgOKd5CmHKbxvHMlGyBgNVHR8Egaow
gacwNaAzoDGGL2h0dHA6Ly9jcmwueW91c2lnbi5mci9jcmwveW91c2lnbnNhc3Jvb3QyY2EuY3Js
MDagNKAyhjBodHRwOi8vY3JsMi55b3VzaWduLmZyL2NybC95b3VzaWduc2Fzcm9vdDJjYS5jcmww
NqA0oDKGMGh0dHA6Ly9jcmwzLnlvdXNpZ24uZnIvY3JsL3lvdXNpZ25zYXNyb290MmNhLmNybDAO
BgNVHQ8BAf8EBAMCAQYwDQYJKoZIhvcNAQELBQADggIBAH1XJUeU5rY9q4+cKUOZC1EySzDkMX1D
HQNGPTYYUe0aweLNayUXjMN+wxvG4fqJQFrlWTTlqsDPVo7j8MF7MWlE0+InhJ893Igulmi8Xwt5
gKeGSaUDS4LBsoyhFfcirfnkRNZCmVO2bM1EfOAWWTNJaUa/KkluJ/W0Yi0ogj7tx9JhVjT4Mtkm
7uuHmsoE89TKGLLWalPS0E4eSvBqc/8ssSbpIleAGG7oT9F0+U0bpWWRfUUQawDj3JSf3SOkCCbr
n1wzkBLMvEvgrBeMDOFN2gI1HSSowABEzxb12mYBzprpIJNZXlLExliUDAna3TxyKAmW6yZMUqJg
tVawTsPXB7VWeqfXOXwScHr2c+PmS/HL51TBVaDH6gjJs2q0wfBoG+zrjvDagU2lGqx38ha/IM8Y
KkgQksacWqAAxkHFghxVKV/+oWsSp19/FNUtDkkry/+pBTT1kjUzE5sEjxwHRCP9m4Hk/llqSIr7
Adv58SZLvEiAMgtpMq7Zzv1jPhqA22KlBHgDQmUrS7Fdz5MOjVTnC1Ex4SGBIdEB/FcRbIlpIIJj
HVROnGKejlXSQNGGqzpTdDYfqqJHZwCEDri6DLhjY8HNr03BsFqmKlyz8Lgy+wMe4eTHOiAB+Yp9
xkyA16DItTejKO8JabGuPEbBSm9uOCA7ljW5FubjF+fn

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer C: *FR*

Issuer ST: *CALVADOS*

Issuer L: *CAEN*

Issuer O: *YOUSIGN SAS*

Issuer OU: *794513986*

Issuer CN: *YOUSIGN SAS - ROOT2 CA*

Subject C: *FR*

Subject ST: *CALVADOS*

Subject L: *CAEN*

Subject O: *YOUSIGN SAS*

Subject OU: *794513986*

Subject CN: *YOUSIGN SAS - SIGN2 CA*

Valid from: *Thu Oct 22 00:59:27 CEST 2015*

Valid to: *Wed Oct 22 00:59:27 CEST 2025*

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:C1:73:A8:87:2D:3E:DA:B8:06:E1:E9:64:F1:59:0E:1A:2B:38:D4:51:AB:93:D0:69:DD:59:4E:06:44:43:60:79:E0:32:F5:95:C5:B7:2C:F8:9F:C0:2A:F3:B8:7B:1C:D6:B0:18:17:48:8E:2D:C2:8B:F6:DB:39:9F:E4:F2:7A:55:A1:67:0B:C4:5E:27:1C:00:A0:52:3C:CF:05:0F:20:C9:5B:D9:AA:5C:A6:F5:38:E8:59:A2:FE:28:6C:41:B3:87:FD:5A:2D:7B:4B:32:F2:70:3C:0C:83:53:31:CF:9C:95:AD:6F:0B:BB:50:CC:B9:D2:20:3D:D2:63:D6:21:DA:96:B5:51:B8:1D:AC:38:1E:CB:CC:14:44:DA:83:7D:0F:75:7B:05:10:07:76:8B:A6:D6:0A:91:F5:50:69:E7:3C:AC:C8:27:B4:F8:31:01:FC:3E:33:7C:E3:C4:83:37:38:43:63:59:04:29:6A:73:BF:1B:BB:55:E8:07:26:19:31:29:CC:BD:F8:9F:90:E6:CF:19:03:CF:19:0D:C8:B7:3F:E1:D5:10:AA:C2:62:CE:5E:D1:FC:43:B5:4F:10:36:1E:E9:17:8B:B9:2C:74:A1:D0:9D:73:0E:D0:72:47:94:3F:A3:F5:C3:01:44:07:78:06:05:05:4F:8A:46:E4:75:92:36:60:41:AB:1E:40:FC:93:F8:DA:AA:7D:CE:4C:CB:6A:FD:C6:4A:12:FD:A9:9A:6B:6D:85:0C:6E:72:C9:AD:BA:6E:8A:A3:8B:CF:1F:18:45:40:17:D4:4E:79:8B:A7:FF:A8:8F:42:DF:85:AC:66:97:84:35:BF:4A:90:64:2D:4F:DD:84:D5:74:E1:68:72:8D:37:29:93:E2:2E:00:2C:3D:A1:18:8A:F8:05:7E:BE:10:73:02:26:31:18:59:D6:73:AF:BE:46:5F:CD:14:E6:02:D4:72:7A:28:44:A3:A8:BB:91:4C:45:45:D3:98:78:7A:4E:A4:33:46:07:D6:CB:08:B2:18:E3:0A:E9:9F:B1:E7:BD:34:05:26:09:12:3D:B5:77:65:F0:09:74:89:B4:0E:94:4C:23:9D:49:A8:0A:F3:83:A4:68:0F:0C:FB:89:B5:D4:ED:E0:72:A6:6B:A6:4A:FB:2B:DE:67:3D:D8:AA:02:67:B6:D8:93:CE:21:46:47:B9:95:C0:FE:CB:04:79:65:71:27:CC:C9:CD:73:B5:24:81:7E:EC:5C:20:6C:DF:42:0B:26:84:B9:F0:4F:FF:1A:C7:78:E3:8F:00:20:63:AC:36:2E:8B:64:75:07:C5:2B:22:D3:4D:AB:43:BE:95:11:9F:B5:07:66:AD:9F:C1:28:75:02:03:01:00:01

Subject Key Identifier *E5:45:7F:C0:9B:7E:1F:7F:C7:5E:A7:77:36:23:87:0A:BC:C9:06:2E*

Basic Constraints *IsCA: true*

Authority Key Identifier *C7:6E:67:F0:A8:13:17:96:11:DC:20:38:A7:79:0A:61:CA:6F:1B:C7*

CRL Distribution Points *http://crl.yousign.fr/crl/yousignsasroot2ca.crl*

http://crl2.yousign.fr/crl/yousignsasroot2ca.crl

http://crl3.yousign.fr/crl/yousignsasroot2ca.crl

Key Usage: *keyCertSign - cRLSign*

Thumbprint algorithm: *SHA-256*

Thumbprint: *74:31:87:05:63:64:75:2B:DA:2E:BA:D4:68:83:7C:A0:8E:61:58:41:D2:12:FA:AD:A2:DA:9A:F4:9A:56:9A:49*

X509SubjectName

Subject C: *FR*

Subject ST: *CALVADOS*

Subject L: *CAEN*

Subject O: *YOUSIGN SAS*

Subject OU: *794513986*

Subject CN: *YOUSIGN SAS - SIGN2 CA*

X509SKI

X509 SK I *5UV/wJt+H3/HXqd3NiOHCrzJBi4=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2017-10-31T23:00:00Z*

TSP Service Definition URI

URI *[en]* *https://yousign.fr/fr/public/document*

URI *[fr]* *https://yousign.fr/fr/public/document*

17 - TSP: AR24

TSP Name

Name *[en]* *AR24*

Name *[fr]* *AR24*

TSP Trade Name

Name *[en]* *VATFR-79809480122*

Name *[fr]* *VATFR-79809480122*

PostalAddress

Street Address *[en]* *85 Boulevard de Courcelles*

Locality *[en]* *Paris*

Postal Code *[en]* *75008*

Country Name *[en]* *FR*

PostalAddress

Street Address *[fr]* *85 Boulevard de Courcelles*

Locality *[fr]* *Paris*

Postal Code *[fr]* *75008*

Country Name *[fr]* *FR*

ElectronicAddress

URI *https://www.ar24.fr*

URI *https://www.ar24.fr*

URI *mailto:contact@ar24.fr*

URI *mailto:contact@ar24.fr*

TSP Information URI

URI *[en]* *https://www.ar24.fr/certifications/*

URI *[fr]* *https://www.ar24.fr/certifications/*

17.1 - Service (granted): AR24

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/EDS/Q*

Service type description *[en]* *An electronic delivery service providing qualified electronic deliveries.*

[fr] *Un service de livraison électronique fournissant des livraisons électroniques qualifiées.*

Service Name

Name *[en]* *AR24*

Name *[fr]* *AR24*

Service digital identities

Certificate fields details

Version: *3*

Serial Number: *171687144144457006000421069396098948557*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIHUjCCBTqgAwIBAgIRAIEpvb8dG+eehjJcxqUEHc0wDQYJKoZIhvcNAQELBQAwezELMAkGA1UE
BhMCRlIxEjAQBgNVBAoMCURISU1ZT1RJUzEcMBoGA1UECwwTMDAwMiA0ODE0NjMwODEwMDAzNjEd
MBsGA1UEYQwUTlRSRlItNDgxNDYzMDgxMDAwMzYxGzAZBgNVBAMMEkNlcnRpZ25hIEVudGl0eSBD
QTAeFw0xNzA5MDYxNDUyMDBaFw0yMDA5MDUxNDUyMDBaMIGOMQswCQYDVQQGEwJGUjENMAsGA1UE
CgwEQVIyNDEcMBoGA1UECwwTMDAwMiA4MDk0ODAxMjIwMDAxMzEdMBsGA1UEYQwUTlRSRlItODA5
NDgwMTIyMDAwMTMxHzAdBgNVBAMMFkFSMjQgLSBBUjI0IENBQ0hFVCBMUkUxEjAQBgNVBAUTCVNU
NjM1NjAwMjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKmlmaOmXLsgbG7GZOPvV70a
m1rjo06Bz9D5Qs+jG7yMtIu/QDTwIl6DqwrBEeLixm99D84fD39vD0ud546MoAchLXvGF10dvWqh
P/gmKo+WNnh07LG1rgl4ZOgvLHdoUMZf2g9J61WFG4pOqCZ9JuT7QQlG2pxBvYuOmzWaUFimKYYi
+CoSXk3kxBV8y+czKSE41OLPFKDkaZr4Ifn289/j0r5ec1k6eyCb4uHjOvEGrnfjGUFSf6yKIyf6
Bkd6R7XAeUW/vBnrG9v2OvHcnxTKWWgN53ujRxqbq5lpH4SuADbXooLuDXbfPDYLm+DCHIWsqDWy
ISdcNVLzwMKeYpkCAwEAAaOCArswggK3MAkGA1UdEwQCMAAwDgYDVR0PAQH/BAQDAgbAMBMGA1Ud
JQQMMAoGCCsGAQUFBwMEMGEGA1UdHwRaMFgwKaAnoCWGI2h0dHA6Ly9jcmwuY2VydGlnbmEuZnIv
ZW50aXR5Y2EuY3JsMCugKaAnhiVodHRwOi8vY3JsLmRoaW15b3Rpcy5jb20vZW50aXR5Y2EuY3Js
MIHcBggrBgEFBQcBAQSBzzCBzDA0BggrBgEFBQcwAoYoaHR0cDovL2F1dG9yaXRlLmNlcnRpZ25h
LmZyL2VudGl0eWNhLmRlcjA2BggrBgEFBQcwAoYqaHR0cDovL2F1dG9yaXRlLmRoaW15b3Rpcy5j
b20vZW50aXR5Y2EuZGVyMCwGCCsGAQUFBzABhiBodHRwOi8vZW50aXR5Y2Eub2NzcC5jZXJ0aWdu
YS5mcjAuBggrBgEFBQcwAYYiaHR0cDovL2VudGl0eWNhLm9jc3AuZGhpbXlvdGlzLmNvbTAdBgNV
HQ4EFgQUFKT+RNsuPtq0hwhgT8IdfDH56aQwHwYDVR0jBBgwFoAUpT8eJExs+IvSG3KYRlDK6IZV
udgwGgYDVR0RBBMwEYEPY29udGFjdEBhcjI0LmZyMEoGA1UdIARDMEEwPwYLKoF6AYExAgYBBAEw
MDAuBggrBgEFBQcCARYiaHR0cHM6Ly93d3cuY2VydGlnbmEuZnIvYXV0b3JpdGVzLzCBmgYIKwYB
BQUHAQMEgY0wgYowCAYGBACORgEBMAgGBgQAjkYBBDATBgYEAI5GAQYwCQYHBACORgEGAjBfBgYE
AI5GAQUwVTAqFiRodHRwczovL3d3dy5jZXJ0aWduYS5mci9lbi9hdXRvcml0ZXMTAkVOMCcWIWh0
dHBzOi8vd3d3LmNlcnRpZ25hLmZyL2F1dG9yaXRlcxMCRllwDQYJKoZIhvcNAQELBQADggIBAMWN
mKZvrXBfqbMYxUOhYO2SRyXDqYMEnpsYkoMLw6AVrtgLhiILyQDo6k6qIGbFbsSs01CMWrhBq73G
6OJoR9idmKPQ3cvzbpPTOrLqZ3BmEMf0DrlPG9yohIe1kPosn6cHhmVwNxX/hmTeKJw07tujx+p4
L0o+aL3meh3rFA0fzMOgO620gxzsc5xYucORUZy0prAbilwDD4T0kcC7CEyYpgWkYPVmzKkdWtR+
EomsRQWnIMhhM6d+GMJ+5eqd1TlFtK9zrXBShzw3dG+KRsVUl2Q396s49Xiuj6L86pOeedRosbBo
/KmtrIuYZJj2nKzW9GzPR1iXc/mX0hirlVcNsCmzrEh2MQxOkB7YmeFjygVoNKN2MB4paqAvkXe2
BuRxfHuSUlcRdLsXs9W1fwK3rwQg2XuQ+X0OKzPaooaH1NGPv0EBHbYLi7RxwXSY+YoTgteqmFX2
y/Ez3yukYcLSOj4Fsi2zveZgEMeQ+sNOHnrBxDj45KROlekNbBuonZaI4sgOLZUm8lEqDj+mFVl6
sdOahX2VIUizISJWpZcx/luHSDES+hM0zAJ+p5mkfcVMt7mMjPBIOXpgNb2sGnXSjchQUUBimzqQ
Mpu3+pVvta/2WZogW311y5JlRkbl9gaCSQI3r3t8b453aMn28CDOrFb3pMKg242NMZh203GZ

-----END CERTIFICATE-----

Signature algorithm:	*SHA256withRSA*
Issuer CN:	*Certigna Entity CA*
Issuer 2.5.4.97:	*NTRFR-48146308100036*
Issuer OU:	*0002 48146308100036*
Issuer O:	*DHIMYOTIS*
Issuer C:	*FR*
Subject SERIAL NUMBER:	*ST6356002*
Subject CN:	*AR24 - AR24 CACHET LRE*
Subject 2.5.4.97:	*NTRFR-80948012200013*
Subject OU:	*0002 80948012200013*
Subject O:	*AR24*

Subject C: *FR*

Valid from: *Wed Sep 06 16:52:00 CEST 2017*

Valid to: *Sat Sep 05 16:52:00 CEST 2020*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:A9:A5:99:A3:A6:5C:BB:20:6C:6E:C6:64:E3:EF:57:BD:1A:9B:5A:E3:A3:4E:81:CF:D0:F9:42:CF:A3:1B:BC:8C:B4:8B:BF:40:34:F0:22:5E:83:AB:0A:C1:11:E2:E2:C6:6F:7D:0F:CE:1F:0F:7F:6F:0F:4B:9D:E7:8E:8C:A0:07:21:2D:7B:C6:17:5D:1D:BD:6A:A1:3F:F8:26:2A:8F:96:36:78:74:EC:B1:B5:AE:09:78:64:E8:2F:2C:77:68:50:C6:5F:DA:0F:49:EB:55:85:1B:8A:4E:A8:26:7D:26:E4:FB:41:09:46:DA:9C:41:BD:8B:8E:9B:35:9A:50:58:A6:29:86:22:F8:2A:12:5E:4D:E4:C4:15:7C:CB:E7:33:29:21:38:D4:E2:CF:14:A0:E4:69:9A:F8:21:F9:F6:F3:DF:E3:D2:BE:5E:73:59:3A:7B:20:9B:E2:E1:E3:3A:F1:06:AE:77:E3:19:41:52:7F:AC:8A:23:27:FA:06:47:7A:47:B5:C0:79:45:BF:BC:19:EB:1B:DB:F6:3A:F1:DC:9F:14:CA:59:68:0D:E7:7B:A3:47:1A:9B:AB:99:69:1F:84:AE:00:36:D7:A2:82:EE:0D:76:DF:3C:36:0B:9B:E0:C2:1C:85:AC:A8:35:B2:21:27:5C:35:52:F3:C0:C2:9E:62:99:02:03:01:00:01

Basic Constraints *IsCA: false*

Extended Key Usage *id_kp_emailProtection*

CRL Distribution Points *http://crl.certigna.fr/entityca.crl*

http://crl.dhimyotis.com/entityca.crl

Authority Info Access *http://autorite.certigna.fr/entityca.der*

http://autorite.dhimyotis.com/entityca.der

http://entityca.ocsp.certigna.fr

http://entityca.ocsp.dhimyotis.com

Subject Key Identifier *14:A4:FE:44:DB:2E:3E:DA:B4:87:08:60:4F:C2:1D:7C:31:F9:E9:A4*

Authority Key Identifier *A5:3F:1E:24:4C:6C:F8:8B:D2:1B:72:98:46:50:CA:E8:86:55:B9:D8*

Subject Alternative Name *contact@ar24.fr*

Certificate Policies *Policy OID: 1.2.250.1.177.2.6.1.4.1*

CPS pointer: https://www.certigna.fr/autorites/

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*

id_etsi_qcs_QcSSCD

Key Usage: *digitalSignature - nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *55:5D:F3:EE:E6:D3:D8:07:A2:B5:F4:11:C7:4F:B1:A7:73:86:E0:E5:B1:A7:DD:0D:C4:A2:14:72:F9:7B:97:6A*

X509SubjectName

X509 SK I *FKT+RNsuPtq0hwhgT8IdfDH56aQ=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en]* *undefined.*

[fr] *undefined.*

Status Starting Time *2018-04-01T00:00:00Z*

TSP Service Definition URI

URI *[en]* *https://www.ar24.fr/certifications/*

URI *[fr]* *https://www.ar24.fr/certifications/*

18 - Signature node - Id: id-f7798ee8d2801e2c7391e97706f063a8

Signing Time *2018-06-29T10:11:21Z*

TSL Scheme Operator certificate fields details

Version: *3*

Serial Number: *149235040025528022361030584694016566270482 7*

X509 Certificate -----BEGIN CERTIFICATE-----

MIIFQzCCBCugAwIBAgISESGfqFZFHUOLR7zSSJGOugS7MA0GCSqGSIb3DQEBCwUAMIGXMQswCQYD
VQQGEwJGUjEwMC4GA1UECgwnQWdlbmNlIE5hdGlvbmFsZSBkZXMgVGl0cmVzIFPDqWN1cmlzw6lz
MRcwFQYDVQQLDA4wMDAyIDEzMDAwMzI2MjExMC8GA1UEAwwoQXV0b3JpdMOpIGRlIENlcnRpZmlj
YXRpb24gUGVyc29ubmVzIEFBRTEKMAgGA1UEBRMBMjAeFw0xNjEwMDUxMDMwMzBaFw0xOTEwMDUx
MDMwMzBaMHsxCzAJBgNVBAYTAkZSMQ4wDAYDVQQKDAVBTlNTSTEXMBUGA1UECwwOMDAwMiAxMzAw
MDc2NjkxIjAgBgNVBAMMGVlhbm4gVG91cmRvdCAzMzEwMDAyOTk4dHkxDTALBgNVBCoMBFlhbm4x
EDAOBgNVBAQMB1RvdXJkb3QwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC+t2D8YV04
ZkNdltdNp3mMpKoYIW4K+yI8JIAbYdPmzVvFhD5HGxsDtlopNHnkXAdguJ14CehLQaw4Pb/fk6Bs
n8dvg6GwJgQLNodOTUSaAFkDCiKB76n9rGwQ1qNTVuHb0UjO0a8mQTMJfztaFFnADxCg8Tpmy6Au
NcyQS08XBRirWfY7uWa2wZOaNApWt+PkNrPRVsy4CoiE4RrJWjUR31uKJ/WL+J7Bjy/0kbbA/gTt
jDgYQ83UIpIfdlp+ETeIvx6SeDJbxyd50tDFVuzCGVcDzSbfDFkkIK4b2iqbgjHEkzjEQhWNfpWJ
R5Kp4dbN7WFeMgD21fvyLgtVHdr/AgMBAAGjggGiMIIBnjAJBgNVHRMEAjAAMBgGA1UdIAQRMA8w
DQYLKoF6AYFIAwECAwEwRwYDVR0fBEAwPjA8oDqgOIY2aHR0cDovL2NybC5hbnRzLmdvdXYuZnIv
YW50c2F2My9hY19wZXJzb25uZXNfYWFlXzIuY3JsMIGUBggrBgEFBQcBAQSBhzCBhDA/BggrBgEF
BQcwAYYzaHR0cDovL29jc3AuYW50cy5nb3V2LmZyL2FudHNhdjMvYWNfcGVyc29ubmVzX2FhZV8y
MEEGCCsGAQUFBzAChjVodHRwOi8vc3AuYW50cy5nb3V2LmZyL2FudHNhdjMvYWNfcGVyc29ubmVz
X2FhZV8yLmNlcjAOBgNVHQ8BAf8EBAMCBkAwIgYIKwYBBQUHAQMEFjAUMAgGBgQAjkYBATAIBgYE
AI5GAQQwIwYDVR0RBBwwGoEYeWFubi50b3VyZG90QHNzaS5nb3V2LmZyMB0GA1UdDgQWBBTZMP44
ZRsN5vyPbhTLXJTaA1wR4zAfBgNVHSMEGDAWgBTay3b6httsUMIOPmOB4q0MfAiB9jANBgkqhkiG
9w0BAQsFAAOCAQEAf3O0aggl1NMr3eUMLV70erYIY/yD8UoAclC5fSPQOQbVQ3pfpBVTqA137wzw
yVhea/g6mwSzqOrhlYP/1YmDO/Pbxk+WVKAnJf4M9BAqJ4FeN7BkiAE9n6EyfXxm7O93g+Boai/4
iv2R45v5BABAbeLck4ekoyCQrhM+kk0CiclQCB5r6HH2bfKohwKIYpud6bY8w1hbHMavOOMKj3WI
Kma9aaiLb5qUCjxqf/s7hqU9o3F3NC1GzBFqniZa9/zEKmyjFBnm35IaOksQ4MjaJp/YjDNx5G2K
0d8pYX14WbFzzgM9JEWYff4yhs4QQrEH8Qt37AjETuzmBBA8NpO1LA==

-----END CERTIFICATE-----

Signature algorithm: *SHA256withRSA*

Issuer SERIAL NUMBER: *2*

Issuer CN: *Autorité de Certification Personnes AAE*

Issuer OU: *0002 130003262*

Issuer O: *Agence Nationale des Titres Sécurisés*

Issuer C: *FR*

Subject SURNAME: *Tourdot*

Subject GIVEN NAME: *Yann*

Subject CN: *Yann Tourdot 3310002998ty*

Subject OU: *0002 130007669*

Subject O: *ANSSI*

Subject C: *FR*

Valid from: *Wed Oct 05 12:30:30 CEST 2016*

Valid to: *Sat Oct 05 12:30:30 CEST 2019*

Public Key:

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:BE:B7:60:FC:61:5D:38:66:43:5D:96:D7:4D:A7:79:8C:A4:AA:18:21:6E:0A:FB:22:3C:24:80:1B:61:D3:E6:CD:5B:C5:84:3E:47:1B:1B:03:B6:5A:29:34:79:E4:5C:07:60:B8:9D:78:09:E8:4B:41:AC:38:3D:BF:DF:93:A0:6C:9F:C7:6F:83:A1:B0:26:04:0B:36:87:4E:4D:44:9A:00:59:03:0A:22:81:EF:A9:FD:AC:6C:10:D6:A3:53:56:E1:DB:D1:48:CE:D1:AF:26:41:33:09:7F:3B:5A:14:59:C0:0F:10:A0:F1:3A:66:CB:A0:2E:35:CC:90:4B:4F:17:05:18:AB:59:F6:3B:B9:66:B6:C1:93:9A:34:0A:56:B7:E3:E4:36:B3:D1:56:CC:B8:0A:88:84:E1:1A:C9:5A:35:11:DF:5B:8A:27:F5:8B:F8:9E:C1:8F:2F:F4:91:B6:C0:FE:04:ED:8C:38:18:43:CD:D4:22:92:1F:76:5A:7E:11:37:88:BF:1E:92:78:32:5B:C7:27:79:D2:D0:C5:56:EC:C2:19:57:03:CD:26:DF:0C:59:24:20:AE:1B:DA:2A:9B:82:31:C4:93:38:C4:42:15:8D:7E:95:89:47:92:A9:E1:D6:CD:ED:61:5E:32:00:F6:D5:FB:F2:2E:0B:55:1D:DA:FF:02:03:01:00:01

Basic Constraints *IsCA: false*

Certificate Policies *Policy OID: 1.2.250.1.200.3.1.2.3.1*

CRL Distribution Points *http://crl.ants.gouv.fr/antsav3/ac_personnes_aae_2.crl*

Authority Info Access *http://ocsp.ants.gouv.fr/antsav3/ac_personnes_aae_2*

http://sp.ants.gouv.fr/antsav3/ac_personnes_aae_2.cer

QCStatements - crit. = false *id_etsi_qcs_QcCompliance*

id_etsi_qcs_QcSSCD

Subject Alternative Name *yann.tourdot@ssi.gouv.fr*

Subject Key Identifier *D9:30:FE:38:65:1B:0D:E6:FC:8F:6E:14:CB:5C:94:DA:03:5C:11:E3*

Authority Key Identifier *DA:CB:76:FA:86:DB:6C:50:C2:0E:3E:63:81:E2:AD:0C:7C:08:81:F6*

Key Usage: *nonRepudiation*

Thumbprint algorithm: *SHA-256*

Thumbprint: *FB:2B:DF:5B:44:99:D8:05:7C:F8:22:69:09:F9:B3:DD:D2:6C:13:1E:E9:27:3A:E0:61:71:57:04:97:E5:42:86*

ANNEXE 5

Référentiel d'exigences

Historique des versions		
Date	**Version**	**Evolution du document**
	1.0	Publication de la première version du référentiel d'exigences

Avant-propos

Le présent référentiel est pris en application de l'article LP 41 de la loi du pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices, et de son arrêté d'application.

Le présent document est une copie adaptée de la documentation publiée par l'Agence nationale de la sécurité des systèmes d'information[1] (ANSSI), disponible sur son site internet www.ssi.gouv.fr.

Le texte fait des renvois à des documents publiés par l'ANSSI et à des organismes de normalisation, en ce qu'ils reflètent l'état de l'art en matière de sécurité de l'information.

Le référentiel est disponible en ligne sur le site internet www.dgen.pf, et sa mise à jour est assurée par la Direction générale de l'économie numérique.

L'opportunité de la mise à jour de ce document est évaluée par la Direction générale de l'économie numérique et peut notamment être le fait d'une évolution du cadre règlementaire lié à la [LOIDUPAYS] ou d'une évolution de l'état de l'art.

La date d'effet de chaque mise à jour et les modalités de transition le cas échéant sont précisées à chaque mise à jour.

Les compléments prévus par le référentiel doivent être replacés dans le contexte des normes européennes visées au présent document.

[1] L'ANSSI est un service à compétence nationale rattaché au Secrétaire général de la défense et de la sécurité nationale, l'autorité chargée d'assister le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale. Parmi ses nombreux objectifs, l'un deux consiste à promouvoir un espace de confiance pour les services en ligne. Elle y participe en ce sens notamment au travers de la règlementation (référentiels) et ses labels (certification des produits de sécurité et qualification des produits de sécurité et des prestataires de service de confiance).

Sommaire

I. Mise en conformité avec les exigences de la loi du pays relative à la dématérialisation des actes des autorités administratives et aux téléservices

I.1. Objet du document

La loi du pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices reconnaît des effets juridiques aux services de confiance, qualifiés ou non qualifiés.

Dans ce contexte, le présent document vise à renforcer la sécurité juridique des services de confiance mis en œuvre dans les systèmes d'information et téléservices proposés par les autorités administratives.

Il s'adresse aux autorités administratives qui souhaitent bénéficier des effets juridiques attachés aux services de confiance ainsi mis en œuvre.

Cette approche est complémentaire à la démarche de sécurité prévue par le Référentiel Général de Sécurité (RGS), mais, contrairement à cette dernière, elle n'est pas obligatoire pour les autorités administratives.

La loi du pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices fixe en outre les exigences que doivent respecter les services de confiance qualifiés.

Les acronymes utilisés dans le présent document sont les suivants :

PSCE	Prestataires de Services de Certification Electronique
RGS	Référentiel général de Sécurité
LCR	Liste des Certificats Révoqués
OCSP	*Online Certificate Status Protocol*
PSCo	Prestataire de services de confiance
PH	Politique d'horodatage
PSHE	Prestataire de service d'horodatage électronique
QSCD	*Qualified electronic Signature / Seal Creation Device*
CCRA	*Common Criteria Recognition Agreement*
CESTI	*Centre d'Evaluation de la Sécurité des Technologies de l'Information*
SOG-IS	*Senior Officials Group – Information systems Security*
OID	*Object Identifier*
URL	*Uniform Resource Locator*
HTTP	*hypertext transfer protocol*
LDAP	*Lightweight Directory Access Protocol*
CSPN	Certification de Sécurité de Premier Ministre
WORM	*Write Once Read Many*
DCSQ	*Dispositif de Création de Signature électronique Qualifié*
DCCQ	*Dispositif de Création de Cachet électronique Qualifié*

I.2. Déclinaisons techniques des exigences fixées par la loi du pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices

Pour les déclinaisons techniques relatives aux exigences, la loi du pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices opère des renvois à des normes, conformément à son article LP 41.

Certaines de ces normes existent déjà (notamment les normes ETSI en matière de profils de signature), d'autres sont encore en cours d'élaboration.

Dans ce cadre, les chapitres IV. et suivants du présent document précisent les normes et les modalités techniques permettant d'assurer le respect des exigences de la loi du pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices pour les services de confiance qualifiés.

I.3. Règles relatives au renforcement de la sécurité juridique des services de confiance

Le [RE] prévoit des exigences pour les services de confiance relatifs à la signature électronique, au cachet électronique, à l'horodatage électronique et à l'envoi recommandé électronique, ainsi que déclinés dans les chapitres suivants.
Ces exigences doivent être reprises dans les conditions d'utilisation des services mis à disposition par les prestataires de services de confiance.

I.3.1. Règles relatives aux services de confiance de signatures et de cachets électroniques

I.3.1.1. Délivrance de certificats qualifiés de signature électronique et de cachet électronique

Les certificats qualifiés de signature électronique permettent d'attester de l'identité des personnes physiques auxquelles ils ont été délivrés, lorsque celles-ci agissent en tant que signataires.

Les certificats qualifiés de cachet électronique permettent d'attester de l'identité des personnes morales auxquelles ils ont été délivrés, lorsque celles-ci agissent en tant que créateurs de cachets.

Les règles relatives à ces services de confiance sont énoncées au IV. du présent document.

I.3.1.2. Validation qualifiée des signatures électroniques qualifiées et des cachets électroniques qualifiés

Un service de validation qualifié des signatures électroniques qualifiées ou cachets électroniques qualifiés permet de garantir la sécurité juridique d'une signature ou d'un cachet qualifié en fournissant une preuve de validation par un tiers qualifié.

Les règles relatives à ce service de confiance sont énoncées au VI. du présent document.

I.3.1.3. Conservation qualifiée des signatures électroniques qualifiées et des cachets électroniques qualifiés

Un service de conservation qualifié des signatures électroniques qualifiées ou cachets électroniques qualifiés permet d'étendre la fiabilité de ceux-ci au-delà de leur période de validité technologique.

Les règles relatives à ce service de confiance sont énoncées au VII. du présent document.

I.3.2. Règles relatives à l'horodatage électronique

L'horodatage électronique qualifié permet d'attester que des données sous forme électronique existent à un instant donné. Un tel procédé peut être utilisé pour apposer une date certaine d'expédition ou de réception d'un courrier mais aussi plus largement pour attester de l'existence d'une donnée à un instant, ou de la date d'un acte réalisé par voie électronique.

Cet horodatage fera foi devant les Tribunaux en cas de contestation.

Les règles relatives à ce service de confiance sont énoncées au V. du présent document.

I.3.3. Règles relatives à l'envoi recommandé électronique

L'envoi recommandé électronique qualifié permet de transmettre des données entre tiers par voie électronique en fournissant des preuves concernant le traitement des données transmises, y compris la preuve de leur envoi et de leur réception, et en protégeant ces données contre les risques de perte, de vol, d'altération ou de toute modification non autorisée.

Les règles relatives à ce service de confiance sont énoncées au VIII. du présent document.

I.4. Qualification des prestataires de services de confiance

Les autorités administratives recourent à des prestataires de services de confiance qualifiés selon [eIDAS] et dans les conditions de l'[ARRETE].

De ce fait, en Polynésie française, un PSCo souhaitant proposer les services de confiance visés à la section VI de la [LOIDUPAYS] doit au préalable avoir obtenu la qualification délivrée sur la base de [eIDAS].

Dès lors, un PSCo qualifié en Polynésie française conformément à l'article LP 40 de la [LOIDUPAYS] respecte les exigences prévues par le présent document.

Le chapitre II. du présent document traite des déclinaisons techniques des exigences règlementaires applicables aux PSCo.

Il convient de prévoir des dispositions générales avec la responsabilité des prestataires de services de confiance et leur responsabilité (charge de la preuve).

I.5. Transition [RGS] vers [eIDAS]

Un PSCo déjà qualifié [RGS] bénéficie d'une facilité de qualification sur la base d'[eIDAS].

En Polynésie française, un PSCo déjà qualifié [RGS] et souhaitant proposer les services de confiance prévus à la section VI de la [LOIDUPAYS] doit au préalable avoir obtenu la qualification délivrée à travers la procédure de transition sur la base de [eIDAS] et de la note [PSCO_QUALIF].

I.6. Certification des dispositifs de création des signatures et des cachets électroniques

Le chapitre IX. du présent document porte sur la certification des dispositifs de création de signature qualifiés au sens de l'article LP 23 de la [LOIDUPAYS] et de cachet électronique qualifié au sens de l'article LP 30 de la [LOIDUPAYS].

En effet, la [LOIDUPAYS] prévoit que pour créer une signature électronique ou un cachet électroniques dits « qualifiés », les dispositifs de création de signature électronique et de création de cachets électronique doivent eux-mêmes être qualifiés.

Les exigences applicables à ces dispositifs qualifiés sont exprimées dans l'annexe II de la [LOIDUPAYS].

Conformément à l'article LP 40 de la [LOIDUPAYS], les dispositifs de création des signatures et des cachets électroniques sont certifiés selon [eIDAS] et dans les conditions de l'[ARRETE].

II. Prestataires de services de confiance qualifiés

II.1 Cadre juridique

Les prestataires de services de confiance qualifiés, respectant les exigences spécifiées au II.2 du présent document ainsi que les exigences spécifiques à chaque service de confiance qualifiés qu'ils fournissent, bénéficient des effets juridiques prévus par la [LOIDUPAYS] pour les services de confiance qualifiés.

Ces effets juridiques sont précisés dans les chapitres du présent document applicables à chacun des services de confiance qualifiés.

II.2. Exigences relatives aux prestataires de services de confiance qualifiés

Les exigences visées par la [LOIDUPAYS] concernant les prestataires de services de confiance qualifiés sont les suivantes :

- **Art. LP 35, II, 4° :** Expertise, fiabilité, expérience et qualification des personnels et sous-traitants ;
- **Art. LP 35, II, 5° :** Maintien de ressources financières suffisantes et/ou assurance responsabilité ;
- **Art. LP 35, II, 6° :** Information des conditions et limites d'utilisation des services ;
- **Art. LP 35, II, 7° :** Utilisation de produits et systèmes fiables pour le stockage des données ;
- **Art. LP 35, II, 8° :** Utilisation de systèmes fiables pour le stockage des données ;
- **Art. LP 35, II, 9° :** Mesures contre la falsification et le vol des données ;
- **Art. LP 35, II, 12° :** Traitement licite des données à caractère personnel ;
- **Art. LP 35, I 1° :** Gestion des risques ;
- **Art. LP 35, I 2°** : Notification des incidents.

Le respect de la norme [EN_319_401] et des compléments précisés au II.3 du présent document permet d'apporter une présomption de conformité à ces exigences.

Note : L'article LP 35, II 7° fait également l'objet de précisions dans les référentiels d'exigences spécifiques applicables à chaque service de confiance.

II.3 Compléments à la norme [EN_319_401]

II.3.1. Compléments relatifs aux systèmes fiables pour le stockage des données

Le PSCo doit utiliser des systèmes fiables pour stocker les données qui lui sont fournies, sous une forme vérifiable de manière à ce que :

- les données ne soient publiquement disponibles pour des traitements qu'après avoir obtenu le consentement de la personne concernée par ces données ;
- seules des personnes autorisées puissent introduire et modifier les données conservées ;
- l'authenticité de ces données puisse être vérifiée.

II.3.2. Compléments au chapitre 5 de la norme [EN_ 319_401] : « Risk Assessment »

Le PSCo doit effectuer une analyse de risques sur le système d'information utilisé pour mettre en œuvre le service de confiance et procéder à son homologation conformément au guide [HOMOLOGATION]. Cette

homologation est réalisée préalablement à la fourniture du service de confiance qualifié puis révisée au moins tous les deux ans.

Le PSCo doit évaluer l'opportunité de mettre à jour l'analyse de risques tous les ans.

Le PSCo doit mettre à jour l'analyse de risques à chaque modification ayant un impact important sur le service de confiance fourni, notamment en cas de modification des politiques ou pratiques relatives à la fourniture du service.

L'analyse de risque et la décision d'homologation doivent être jointes au rapport d'évaluation de la conformité transmis lors de la demande de qualification.

II.3.3. Compléments au chapitre 7 de la norme [EN_319_401] : « TSP Management and Operation »

§7.2.i : « *Human resources* »

Le PSCo doit mettre en œuvre tous les moyens légaux dont il peut disposer pour s'assurer de l'honnêteté et de l'éthique de ses personnels. Ces personnels ne doivent notamment pas avoir de condamnation de justice en contradiction avec leurs attributions.

A ce titre, l'employeur peut demander à ses personnels la communication d'une copie du bulletin n°3 de leur casier judiciaire. L'employeur peut décider en cas de refus de communiquer cette copie ou en cas de présence de condamnation de justice incompatible avec les attributions de la personne, de lui retirer ces attributions.

Ces vérifications doivent être menées préalablement à l'affectation à un rôle de confiance et revues régulièrement (au minimum tous les 3 ans).

§ 7.4. : « *Access control* »

Il est recommandé au PSCo d'appliquer l'ensemble des règles définies dans le guide d'hygiène informatique [GH] publié par l'ANSSI. A défaut, le PSCo doit mettre en place des mesures permettant de couvrir les risques identifiés.

Dans tous les cas, l'application des règles suivantes est obligatoire :

- le PSCo élabore et tient à jour un schéma d'architecture précis du système d'information du service de confiance. Ce schéma doit notamment identifier l'ensemble des interconnexions du système d'information du service de confiance (règle n° 1 du [GH]) ;
- le PSCo interdit la connexion d'équipements personnels au système d'information du service de confiance (règle n° 5 du [GH]) ;
- le PSCo met en place des réseaux cloisonnés (règle n° 21 du [GH]) ;
- le PSCo interdit l'accès sans fil au système d'information du service de confiance (règle n° 22 du [GH]) ;
- le PSCo interdit tout accès à Internet depuis les comptes d'administration (règle n° 28 du [GH]) ;
- le PSCo dispose d'un réseau d'administration dédié, l'ensemble des opérations d'administration devant être exclusivement réalisées depuis ce réseau (règle n° 29 du [GH]) ;
- Le PSCo n'autorise l'accès à distance au réseau d'entreprise, y compris pour l'administration du réseau, que depuis des postes de l'entreprise qui mettent en œuvre des mécanismes

d'authentification forte et protégeant l'intégrité et la confidentialité des échanges à l'aide de moyens robustes (règle n° 31 du [GH]) ;
- le PSCo contacte sans délai l'ANSSI pour tout incident relatif au service de confiance (règle n° 37 du [GH]) selon les modalités décrites dans le document [QUALIF_SERV].

§7.9 : « *Incident management* »

Le PSCo doit notifier à l'ANSSI dans un délai maximal de 24 heures après en avoir eu connaissance toute atteinte à la sécurité ou toute perte d'intégrité ayant une incidence importante sur le service de confiance fourni ou sur les données à caractère personnel qui y sont conservées.

Cette notification est réalisée au moyen du formulaire mis en ligne sur le site de l'ANSSI, selon les modalités définies dans [QUALIF_SERV].

II.3.4. Compléments relatifs à la certification des modules cryptographiques

Les fonctions cryptographiques sensibles[2] doivent être mises en œuvre dans des modules cryptographiques répondant aux critères définis dans le tableau ci-dessous[3] :

Labellisation	Schéma	Référentiel	Commentaire / modalités
Certifications Critères Communs[4]	**ANSSI**	Profils de protection reconnus par l'ANSSI, référencés sur le site www.ssi.gouv.fr	Présomption de conformité à l'exigence d'utilisation de produits fiables
Certification Critères Communs[3]	**SOG-IS**	Profils de protection HSM[5] recommandés sur le site www.sogis.org	Présomption de conformité à l'exigence d'utilisation de produits fiables
Certification Critères Communs[3]	**SOG-IS**	Cible de sécurité vérifiée par l'ANSSI comme étant comparable en terme d'assurance avec les profils de protection reconnus par l'ANSSI et conforme aux exigences de la [LOIDUPAYS].	Présomption de conformité à l'exigence d'utilisation de produits fiables
Certification Critères Communs[3]	**CCRA**	Cible de sécurité vérifiée par l'ANSSI comme étant comparable en terme d'assurance avec les profils de protection reconnus par l'ANSSI et conforme aux exigences de la [LOIDUPAYS].	L'ANSSI demande à ce que les travaux correspondant aux augmentations non reconnues dans le cadre du CCRA soient réalisés dans un schéma du SOG-IS (avec fourniture du rapport technique d'évaluation au CESTI en charge de l'évaluation et au centre de certification).
Autre		Le demandeur doit fournir un argumentaire visant à démontrer à l'ANSSI que sa méthode d'évaluation, le laboratoire utilisé, le référentiel d'évaluation, etc. sont de même niveau qu'une certification	

[2] Les chapitres suivants précisent les fonctions cryptographiques sensibles concernées selon le cas.
[3] Dans le cas particulier des fonctions de signature électronique qualifiée ou de cachet électronique qualifié, le dispositif de création de signature ou de cachet électronique qualifié utilisé doit être certifié conformément à la [LOIDUPAYS].
[4] La certification selon les Critères Communs doit avoir une ancienneté inférieure à 10 ans.
[5] L'ANSSI vérifiera que le profil de protection est bien approprié pour le cas d'usage prévu du module cryptographique au sein de l'environnement du PSCo.

	Critères Communs réalisées dans le cadre du SOG-IS selon l'un des profils de protection reconnus par l'ANSSI. Le rapport d'évaluation doit être fourni à l'ANSSI pour analyse. L'ANSSI se réserve le droit de demander des analyses complémentaires au frais du demandeur dans un laboratoire agréé et reconnu compétent pour ce type de produit au sein du SOG-IS.

Les chapitres suivants consacrés à chaque type de service de confiance qualifié précisent les fonctions cryptographiques sensibles concernées selon les cas.

II.3.5. Compléments relatifs aux algorithmes et mécanismes cryptographiques

Les algorithmes et mécanismes cryptographiques mis en œuvre doivent être conformes aux spécifications du document [SOGIS-CRYPTO].

Pour les modules cryptographiques employés par le PSCO, certifiés conformément aux dispositions du II.3.4. du présent document, la vérification de la conformité à cette exigence nécessite, dans le cadre de leur certification :

- Une analyse théorique des mécanismes cryptographiques mis en œuvre ;
- Et une expertise de l'implémentation de ces mécanismes dans le module cryptographique.

II.3.6. Langue des documents publiés par le PSCo

Les documents publiés par le PSCo à destination du public (conditions générales d'utilisation et politiques relatives à la fourniture des services) doivent être rédigés en langue française.

En complément, il est recommandé qu'une version rédigée en langue anglaise de ces documents soit mise à disposition du public.

II.4. Tableau récapitulatif des exigences

Exigences	**Clauses applicables des normes européennes**	**Sections applicables du présent document**
(LP 35, II, 4°) Expertise, fiabilité, expérience et qualification des personnels et sous-traitants	[EN_319_401] Clause 7.2	III.3.3
(LP 35, II, 5°) Maintient de ressources financières suffisantes et/ou assurance responsabilité	[EN_319_401] Clauses 7.1.1	*Pas de complément à la norme*
(LP 35, II, 6°) Information des conditions et limites d'utilisation des services	[EN_319_401] Clause 6.2	*Pas de complément à la norme*
(LP 35, II, 7°) Utilisation de systèmes et produits fiables	[EN_319_401] Clause 7.7	II.3.4. et II.3.5

(LP 35, II 8°) Utilisation de systèmes fiables pour le stockage des données	*Non couvert*	II.3.1 et II.3.3
(LP 35, II 9°) Mesures contre la falsification et le vol des données	[EN_319_401] Clauses 7.6 et 7.7	*Pas de complément à la norme*
(LP 35, II 12°) Traitement licite des données à caractère personnel	[EN_319_401] Clause 7.13	*Pas de complément à la norme*
(LP 35, I 1°	[EN_319_401] Clauses 5, 6.3 et 7.1 à 7.8	II.3.2 et II.3.3.
(LP 35, I 2°	[EN_319_401] Clause 7.13	II.3.3.

III. Transitions [RGS] relatives aux services de délivrance de certificats qualifiés de signature électronique et de cachet électronique et aux services d'horodatage électronique

Le présent chapitre décrit les modalités de transition de la qualification [RGS] vers la qualification visée à l'article LP 40 de la [LOIDUPAYS], c'est-à-dire la qualification [eIDAS], des services de délivrance de certificats qualifiés de signature électronique et de cachet électronique et aux services d'horodatage électronique.

III.1. Transitions [RGS] relatives aux services de délivrance de certificats qualifiés de signature électronique et de cachet électronique

III.1.1. Cadre juridique

Les certificats qualifiés de signature électronique et de cachet électronique délivrés par un PSCo qualifié [RGS] respectant les exigences spécifiées au III.2 du présent document sont présumés satisfaire aux exigences, respectivement, de l'annexe I et de l'annexe III de la [LOIDUPAYS].

Les signatures électroniques avancées, reposant sur un certificat qualifié, et créées à l'aide d'un dispositif de création de signature électronique qualifié, sont des signatures électroniques qualifiées, bénéficiant des effets juridiques prévus à l'article LP 23 de la [LOIDUPAYS].

Les cachets électroniques avancés, reposant sur un certificat qualifié, et créés à l'aide d'un dispositif de création de cachet électronique qualifié, sont des cachets électroniques qualifiés, bénéficiant des effets juridiques prévus à l'article LP 30 de la [LOIDUPAYS].

III.1.2 Principe de transition

Le principe de transition n'est applicable qu'aux PSCE ayant déjà fait l'objet d'une qualification selon le [RGS], préalablement à la demande de qualification selon [eIDAS].

Un PSCE, qualifié selon le [RGS], peut prétendre à la qualification selon [eIDAS] sous les conditions suivantes :

- L'offre de délivrance de certificats du PSCE est qualifiée selon le [RGS] au niveau (**) ou (***) ;
- L'offre de délivrance de certificats du PSCE respecte les exigences visées aux paragraphes I à V de la section VI et aux annexes I et III de la [LOIDUPAYS] non couvertes par le [RGS] et spécifiées au III.3 du présent document.

Conformément au I.5, en Polynésie française, un PSCo déjà qualifié [RGS] et souhaitant proposer des services de délivrance de certificat électronique prévus à la section VI de la [LOIDUPAYS] doit au préalable avoir obtenu la qualification délivrée sur la base de [eIDAS] et des dispositions de transition en vigueur en métropole.

III.1.3. Exigences supplémentaires à celles du [RGS]

Le respect des règles définies ci-après permet d'apporter une présomption de conformité aux exigences supplémentaires à celles du [RGS].

III.1.3.1. Compléments relatifs à la vérification de l'identité du demandeur

La vérification de l'identité de la personne physique, ou du représentant autorisé de la personne morale, à laquelle le PSCo délivre un certificat qualifié peut être réalisée, conformément aux règles du [RGS] pour le niveau 2 étoiles, soit :

- lors d'un face à face, en présence physique de la personne ; ou
- sous forme dématérialisée à condition que la demande soit signée à l'aide d'un procédé de signature électronique conforme au minimum aux exigences du niveau (**) décrites dans le document [RGS_A1], que la signature soit vérifiée et valide au moment de l'enregistrement, et que le certificat sur lequel repose cette signature électronique soit un certificat qualifié selon les articles LP 25 et LP 32 de la [LOIDUPAYS].

III.1.3.2. Compléments relatifs au statut de révocation des certificats

Le PSCE doit assurer la disponibilité du statut de révocation à tout moment et au-delà de la période de validité du certificat.

Afin de répondre à cette exigence, il est recommandé d'appliquer les règles suivantes, selon le cas :

1) Après l'expiration du certificat qualifié :
   a. Si le PSCE assure la publication d'une LCR, celle-ci devrait :
      i. Comporter l'extension « *ExpiredCertsOnCRL* », comme prévu par la recommandation ITU-T X.509 ;
      ii. Et contenir les numéros de série de l'ensemble des certificats révoqués, y compris les certificats étant arrivés à expiration après leur révocation.
   b. Si le PSCE met en œuvre un répondeur OCSP, celui-ci devrait :
      i. Comporter l'extension « *archive cutoff* », comme prévu par la [RFC 6960], avec une date identique à la date de début de validité du certificat de l'AC ;
      ii. Et maintenir disponible le statut de révocation du certificat après son expiration.
2) Si la clé de l'AC émettrice du certificat qualifié est sur le point d'expirer :
   a. L'ensemble des certificats non-expirés émis par cette AC devraient être révoqués ;
   b. Et si le PSCE assurait la publication d'une LCR, une dernière LCR devrait être publiée, celle-ci ayant une fin de validité positionnée au 31 décembre 9999, 23h59m59s (« *99991231235959Z* »);
   c. Et si le PSCE assurait un service de répondeur OCSP, une dernière réponse OCSP devrait être pré-générée pour chaque certificat émis, cette réponse ayant une fin de validité positionnée au 31 décembre 9999, 23h59m59s (« *99991231235959Z* »).
3) Lorsque le PSCE cesse de fournir le service de confiance qualifié, sans le transférer vers un autre PSCE qualifié :
   a. Les méthodes applicables au cas n°2 sont applicables dans ce cas. En complément, le PSCE n'est pas tenu de maintenir la publication des LCR ni de maintenir le service OCSP, mais les LCR et/ou réponses OCSP produites devraient être mises à disposition des clients du PSCE dans des conditions permettant de garantir leur intégrité.

Dans tous les cas, le PSCE doit rendre publique les mesures mises en œuvre pour répondre à l'exigence.

III.1.3.3 Compléments relatifs aux profils des certificats

Les exigences suivantes s'appliquent aux profils de certificats en complément de celles du [RGS] :

- L'extension « *QCStatements* » doit être valorisée de manière à indiquer, au moins sous une forme adaptée au traitement automatisé[6], que :
    - Le certificat a été délivré comme certificat qualifié de signature électronique et de cachet électronique ;
    - Le cas échéant, les données de création de signature ou de cachet électronique, associées aux données de validation de la signature ou du cachet électronique, se trouvent dans un dispositif de création de signature ou de cachet électronique qualifié ; et

Note : Pour les services visés aux VI., VII. et VIII., l'extension « *QCStatements* » doit être valorisée conformément aux prescriptions du présent chapitre.

- le chemin d'accès vers le lieu de publication du certificat de l'AC doit être renseigné dans le certificat lui-même, par le biais de l'extension « *AuthorityInformationAccess* ». III.1.4. Tableau récapitulatif des exigences

Exigences	Chapitres applicables du [RGS]	Sections applicables du présent document
(Art. LP 35, II 1°) Vérifications de l'identité du demandeur	[RGS_A2] III [RGS_A3] III	III.1.3.1
(Art. LP 35, II 3°) Accès automatisé, disponible à tout moment, fiable, gratuit et efficace au statut de révocation du certificat (y compris après sa fin de validité).	[RGS_A2] IV10.2 [RGS_A3] IV10.2	III.1.3.2
Certificats qualifiés de signature électronique **(Renvoi à l'annexe I de la [LOIDUPAYS])**	[RGS_A4] II.2	III.1.3.3
Certificats qualifiés de cachet électronique **(Renvoi à l'annexe III de la [LOIDUPAYS])**	[RGS_A4] II. 3	III.1.3.3
(Art. LP 25, 2° et LP 32, 2°) Aspect relatifs à la révocation	[RGS_A2] IV.9 [RGS_A3] IV.9	III.1.3.2

III.2. Transitions [RGS] relatives aux services d'horodatage électronique

III.2.1. Cadre juridique

Les services d'horodatage électronique qualifiés bénéficient des effets juridiques définis à l'article LP 36 de la [LOIDUPAYS].

III.2.2. Principe de transition

Le principe de transition n'est applicable qu'aux services d'horodatage électronique ayant déjà fait l'objet d'une qualification selon le [RGS], préalablement à la demande de qualification selon [eIDAS].

Conformément au I.5, en Polynésie française, un PSCo déjà qualifié [RGS] et souhaitant proposer des services d'horodatage électronique prévus à la section VI de la [LOIDUPAYS] doit au préalable avoir obtenu la qualification délivrée sur la base de [eIDAS] et des dispositions de transition en vigueur en métropole.

[6] La norme [EN_319_412-5] définit les règles permettant d'indiquer ces deux informations dans les certificats qualifiés de manière interopérable.

IV. Services de délivrance de certificats qualifiés de signature électronique et de cachet électronique

IV.1. Cadre juridique

Les certificats qualifiés de signature électronique et de cachet électronique délivrés par un PSCo respectant les exigences spécifiées au IV.2 du présent document sont présumés satisfaire aux exigences, respectivement, de l'annexe I et de l'annexe III de la [LOIDUPAYS].

Les signatures électroniques avancées, reposant sur un certificat qualifié, et créées à l'aide d'un dispositif de création de signature électronique qualifié, sont des signatures électroniques qualifiées, bénéficiant des effets juridiques prévus à l'article LP 23 de la [LOIDUPAYS].

Les cachets électroniques avancés, reposant sur un certificat qualifié, et créés à l'aide d'un dispositif de création de cachet électronique qualifié, sont des cachets électroniques qualifiés, bénéficiant des effets juridiques prévus à l'article LP 30 de la [LOIDUPAYS].

IV.2. Exigences relatives aux services de délivrance de certificats qualifiés de signature électronique et de cachet électronique

Les exigences visées par la [LOIDUPAYS] concernant les services de délivrance de certificats qualifiés de signature électronique et de cachet électronique sont les suivantes :

- **LP 25, 2° et LP 32, 2° :** Aspect relatifs à la révocation ;
- **LP 35, II 1° :** Vérification de l'identité et des attributs spécifiques de la personne
- **LP 35, II 2° :** Révocation du certificat (avec obligation de publication dans les 24h) ;
- **LP 35, II 3° :** Accès fiable, gratuit et efficace au statut de révocation du certificat (y compris après sa fin de validité) ;
- **LP 35, II 7° :** Utilisation des systèmes et des produits fiables ;
- **LP 35, II 8° :** Conservation des informations délivrées et reçues par le prestataire de services de confiance ;
- **LP 35, II 11° :** Continuité de service suite à l'arrêt d'activité de délivrance de certificats qualifiés ;
- **LP 35, II 13° :** Base de données relative aux certificats émis ;
- **Annexe I** : Exigences applicables aux certificats qualifiés de signature électronique ;
- **Annexe III** : Exigences applicables aux certificats qualifiés de cachet électronique.

Le respect de la norme [EN_319_411-2] et des compléments précisés dans le IV.3 du présent document permet d'apporter une présomption de conformité des services de délivrance des certificats électroniques à ces exigences.

IV.3. Compléments à la norme [EN_319_411-2]

IV.3.1. Compléments relatifs à la vérification de l'identité du demandeur

La vérification de l'identité de la personne physique ou morale à laquelle le PSCo délivre un certificat qualifié est réalisée soit :

1. par la présence en personne de la personne physique ou du représentant autorisé de la personne morale ; ou
2. au moyen d'un certificat de signature électronique qualifié pour une personne physique, ou d'un certificat de cachet électronique qualifié pour une personne morale, délivré conformément au point 1 ci-dessus.

Note : les informations relatives à l'identité du demandeur et portées dans le certificat électronique doivent correspondre exactement aux informations portées sur les éléments présentés dans le cadre de la vérification d'identité. *Par exemple, pour une personne physique, la troncature du prénom ou du nom, ou l'emploi d'un prénom ou d'un nom ne figurant pas sur l'élément d'identification présenté, ne sont pas acceptables.*

Les paragraphes IV.3.1.1 à IV.3.1.2 ci-dessous précisent, selon la méthode retenue par le PSCE, les modalités applicables à la vérification de l'identité du demandeur.

IV.3.1.1 Exigences applicables à la vérification de l'identité lors d'un face à face

Lors du face à face, la personne physique ou le représentant de la personne morale doit présenter un document officiel d'identité avec photographie (carte nationale d'identité, passeport, titre de séjour ou autre document relatif au séjour) qui sera vérifié par le personnel du PSCo qualifié. Cette vérification doit permettre d'établir :

- Que le visage de la personne physique ou du représentant autorisé de la personne morale correspond à la photographie portée sur le document officiel d'identité présenté ; et
- Que ce document soit bien dans sa période de validité, et qu'il n'est pas déclaré perdu, volé ou révoqué par une source disponible publiquement ; et
- Que ce document ne paraisse pas contrefait et ne présente pas de signe de falsification[7].

Pour les organismes publics ou privés délivrant des certificats qualifiés à leurs personnels pour couvrir leurs propres besoins, la preuve d'identité peut être apportée par la présentation d'une carte d'identité professionnelle avec photographie, ou par la vérification de l'identité du demandeur dans une base de données interne préétablie, comportant la photographie, et dont la constitution repose sur des processus formalisés et audités.

IV.3.1.2 Exigences applicables à la vérification de l'identité par le biais d'un certificat de signature électronique qualifié ou de cachet électronique qualifié

Un document, relatif à la manifestation du consentement du demandeur pour la délivrance du certificat, doit avoir été signé à l'aide d'une signature électronique avancée reposant sur un certificat qualifié, ou cacheté à l'aide d'un cachet électronique avancé reposant sur un certificat qualifié.

Il est recommandé que ce document soit la demande de certificat déposée électroniquement auprès du PSCo, et comportant l'ensemble des informations nécessaires à la délivrance du certificat.

Le PSCE doit s'assurer que le certificat de signature électronique qualifié ou de cachet électronique qualifié a été délivré selon la méthode décrite au IV.3.1.1.

Exemple : un PSCE peut accepter que la vérification d'identité du demandeur lors du premier renouvellement d'un certificat de signature électronique qualifié ou de cachet électronique qualifié puisse être réalisée via le recours au certificat qualifié précédemment délivré par ce PSCE, sous réserve que la vérification d'identité pour la délivrance initiale ait été réalisée conformément aux modalités précisées au IV.3.1.1. Lors du second renouvellement, en revanche, la vérification de l'identité devra être réalisée selon les mêmes modalités que la délivrance initiale.

[7] La vérification de l'authenticité d'un document d'identité se fait généralement au moyen d'une inspection physique des caractéristiques de sécurité de ce document. *Parmi les exemples de caractéristiques de sécurité figurent les filigranes, les encres, les hologrammes, la micro-impression, etc.* Le registre en ligne de documents authentiques d'identité et de voyage PRADO (disponible à l'adresse www.consilium.europa.eu/prado/fr) recense les caractéristiques de sécurité des documents d'identité que les Etats membres de l'Union européenne ont souhaité rendre publiques.

Le PSCE doit mettre en œuvre un processus de validation de la signature ou du cachet répondant aux exigences prévues à l'article LP 27 de la [LOIDUPAYS], appliqués *mutatis mutandis* pour le cachet. Si le PSCE exige une signature qualifiée ou un cachet qualifié, il est recommandé d'avoir recours à un service de validation qualifié des signatures ou des cachets électroniques qualifiés.

Si la création de la signature électronique avancée ou du cachet électronique avancé par le demandeur est mise en œuvre par le biais de moyens fournis par le PSCE, il est recommandé de respecter les bonnes pratiques suivantes :

- le format de la signature ou du cachet électronique est l'un de ceux prévus par les normes référencées dans l'annexe 2 du présent document ;
- la signature ou le cachet électronique fait l'objet d'un horodatage qualifié permettant de garantir sa date présumée de création.

Il convient de prévoir les cas de défaillance du PSCO avec sa responsabilité et une procédure d'escalade.

IV.3.2. Compléments relatifs à la constitution et la conservation du dossier de demande

Pour un certificat qualifié de signature électronique, sous la responsabilité d'une personne physique, le dossier d'enregistrement doit au moins comprendre :

- Une demande de certificat manuscrite ou électronique datée de moins de 3 mois et signée par le demandeur, comprenant l'ensemble des éléments nécessaires à la délivrance du certificat ;
- Les conditions générales d'utilisation, dans leur version en vigueur, signées par le demandeur.

La demande de certificat et les conditions générales d'utilisation doivent être :

- Signées au moyen d'une signature manuscrite ; ou
- Signées électroniquement au moyen d'une signature avancée.

Dans le second cas, il est recommandé que le certificat de signature électronique soit un certificat qualifié.
Pour un certificat qualifié de cachet électronique, sous la responsabilité d'une personne morale, le dossier d'enregistrement doit au moins comprendre :

- Une demande de certificat manuscrite ou électronique datée de moins de 3 mois et signée par un représentant autorisé de la personne morale, comprenant l'ensemble des éléments nécessaires à la délivrance du certificat ;
- Les conditions générales d'utilisation, dans leur version en vigueur, datées et signées conformément à la clause 6.3.4 de la norme [EN_319_411-2] ;
- Pour une entreprise, toute pièce, valide lors de la demande de certificat, attestant de l'existence et de l'identification unique de l'entreprise qui figurera dans le certificat ;
- Pour une entreprise, tout document attestant de la qualité demandeur de certificat ;
- Pour une administration, une pièce, valide au moment de l'enregistrement, portant délégation ou subdélégation de l'autorité responsable de la structure administrative.

La demande de certificat et les conditions générales d'utilisation doivent être :

- Signées au moyen d'une signature manuscrite ; ou
- Signées électroniquement au moyen d'une signature avancée ; ou
- Cachetées électroniquement au moyen d'un cachet avancé.

Dans les deux derniers cas, il est recommandé que le certificat de signature électronique ou de cachet électronique soit un certificat qualifié.

Les dossiers d'enregistrement doivent être conservés pendant sept (7) ans après la fin de validité du certificat faisant l'objet de la demande.

IV.3.3. Compléments relatifs à l'utilisation des systèmes et des produits fiables

Les modules cryptographiques employés pour signer les certificats des autorités de certification, les certificats des demandeurs, les réponses OCSP et les LCR, et pour générer les clés privées des autorités de certification et les clés privées des demandeurs le cas échéant, doivent respecter les règles spécifiées dans le document [PSCO_QUALIF].

IV.3.4. Compléments relatifs au statut de révocation des certificats

Il est recommandé de mettre en œuvre un répondeur OCSP. Si le PSCE ne met pas en œuvre de répondeur OCSP, alors il doit assurer la publication d'une LCR.

Dans le cas où le PSCE met à disposition le statut de révocation des certificats à la fois via la publication d'une LCR et la mise en œuvre d'un répondeur OCSP, la norme [EN_319_411-2] prévoit une cohérence, sur la durée, des informations fournies par ces deux moyens. Le respect de cette exigence ne doit pas empêcher un répondeur OCSP d'utiliser le statut « *unknown* » ou « *revoked* » en cas de requête portant sur un certificat non connu, conformément au chapitre 2.2 de la [RFC_6960].

IV.3.5. Compléments relatifs à l'accessibilité du statut de révocation au-delà de la fin de validité

Le PSCE doit assurer et garantir la disponibilité du statut de révocation à tout moment et au-delà de la période de validité du certificat.

Afin de répondre à cette exigence, il est recommandé d'appliquer les règles suivantes, selon le cas :

1. Après l'expiration du certificat qualifié :
    a. Si le PSCE assure la publication d'une LCR, celle-ci devrait :
        i. Comporter l'extension « *ExpiredCertsOnCRL* », comme prévu par la recommandation ITU-T X.509 ; et
        ii. Contenir les numéros de série de l'ensemble des certificats révoqués, y compris les certificats étant arrivés à expiration après leur révocation.
    b. Si le PSCE met en œuvre un répondeur OCSP, celui-ci devrait :
        i. Comporter l'extension « *archive cutoff* », comme prévu par la [RFC 6960], avec une date identique à la date de début de validité du certificat de l'AC ; et
        ii. Maintenir disponible le statut de révocation du certificat après son expiration.
2. Si la clé de l'AC émettrice du certificat qualifié est sur le point d'expirer :
    a. L'ensemble des certificats non-expirés émis par cette AC devraient être révoqués ; et
    b. Si le PSCE assurait la publication d'une LCR, une dernière LCR devrait être publiée, celle-ci ayant une fin de validité positionnée au 31 décembre 9999, 23h59m59s (« *99991231235959Z* »); et
    c. Si le PSCE assurait un service de répondeur OCSP, une dernière réponse OCSP devrait être pré-générée pour chaque certificat émis, cette réponse ayant une fin de validité positionnée au 31 décembre 9999, 23h59m59s (« *99991231235959Z* »).
3. Lorsque le PSCE cesse de fournir le service de confiance qualifié, sans le transférer vers un autre PSCE qualifié :
    a. Les méthodes applicables au cas n°2 sont applicables dans ce cas ; et

b. Le PSCE n'est pas tenu de maintenir la publication des LCR ni de maintenir le service OCSP, mais les LCR et/ou réponses OCSP produites devraient être mises à disposition des clients du PSCE dans des conditions permettant de garantir leur intégrité.

Dans tous les cas, le PSCE doit rendre publique les mesures mises en œuvre pour répondre à l'exigence.

IV.3.6. Compléments relatifs à la crypto-période des clés privées

Les bi-clés doivent être périodiquement renouvelées afin de minimiser les possibilités d'attaques cryptographiques.

Il est recommandé que la durée de vie des bi-clés correspondant aux certificats qualifiés de signature électronique et de cachet électronique n'excède pas les durées indiquées dans le tableau suivant :

Type de certificat	**Durée maximale de validité**
Signature électronique (Personne physique)	La durée maximale de validité doit être fonction de la taille de clé, conformément aux règles de la clause 9.3 du standard
Cachet électronique (Personne morale)	

IV.3.7. Compléments relatifs à la durée de validité des certificats

La durée de validité d'un certificat qualifié ne peut excéder la durée de validité restante du certificat de l'autorité de certification émettrice.

IV.3.8. Compléments relatifs au cumul des usages de clés

Il est recommandé d'appliquer les règles suivantes :

- Les certificats qualifiés de signature électronique devraient contenir l'usage de clé *nonRepudiation* (aussi appelé *contentCommitment)* à l'exclusion de tout autre ;
- Les certificats qualifiés de cachet électronique devraient contenir les usages de clés *digitalSignature* et/ou *nonRepudiation* à l'exclusion de tout autre.

IV.4. Tableau récapitulatif des exigences

Exigences	**Clauses applicables des normes européennes**	**Sections applicables du présent document**
(LP 35, 1°) Vérification de l'identité et des attributs spécifiques de la personne physique ou morale	[EN_319_411-2] Clauses 6.2.2 et 6.2.3	IV.3.1
(LP 35, 2°) Révocation du certificat (avec obligation de publication dans les 24h) ;	[EN_319_411-2] Clause 6.2.4	IV.3.4
(LP 35, 3°) Accès fiable, gratuit et efficace au statut de révocation du certificat (y compris après sa fin de validité).	[EN_319_411-2] Clause 6.3.10	IV.3.5
Certificats qualifiés de signature électronique **(Renvoi à l'annexe I de la [LOIDUPAYS])**	[EN_319_411-2] Clause 6.6.1	Annexe 3 (et IV.3.6 à IV.3.8)

Certificats qualifiés de cachet électronique **(Renvoi à l'annexe III de la [LOIDUPAYS])**		
(LP 25, 2° et LP 32, 2°) Aspect relatifs à la révocation	[EN_319_411-2] Clause 6.3.9	IV.3.4
(LP 35, II 7°) Utilisation des systèmes et des produits fiables	[EN_319_411-2] Clause 6.5	IV.3.3
LP 35, II 10°) Conservation des informations délivrées et reçues par le prestataire de services de confiance	[EN_319_411-2] Clauses 6.4.5 et 6.4.6	IV.3.2
LP 35, II 11°) Continuité de service suite à l'arrêt d'activité du prestataire de services de confiance	[EN_319_411-2] Clause 6.4.9	IV.3.2
LP 35, II 13°) Base de données relative aux certificats émis	[EN_319_411-2] Clause 6.1	*Pas de complément à la norme*

V. Services d'horodatage électronique qualifiés

V.1. Cadre juridique

Les services d'horodatage électronique qualifiés, respectant les exigences spécifiées au V.2 du présent document, bénéficient des effets juridiques définis à l'article LP 36 de la [LOIDUPAYS].

Note : Le procédé d'horodatage électronique conforme aux exigences du RGS bénéficie des effets juridiques prévus à l'alinéa 2 de l'article LP 36 de la [LOIDUPAYS].

V.2. Exigences relatives aux services d'horodatage électronique qualifiés

Les exigences visées par la [LOIDUPAYS] concernant les services d'horodatage électronique qualifiés sont les suivantes :

- **Art. LP 35, II 7° :** Utilisation des systèmes et des produits fiables ;
- **Art. LP 35, II 10° :** Conservation des informations délivrées et reçues par le prestataire de services de confiance ;
- **Art. LP 35, 11° :** Plan d'arrêt d'activité d'un service d'horodatage électronique ;
- **Art. LP 37, 1° :** Lien entre date, heure, et données ;
- **Art. LP 37, 2° :** Fondation sur une horloge exacte reliée à l'UTC ;
- **Art. LP 37, 3° :** Signature ou cachet électronique avancé, ou méthode équivalente.

Le respect de la norme [EN_319_421] et des compléments précisés au V.3 du présent document, permet d'apporter une présomption de conformité à ces exigences.

V.3. Compléments à la norme [EN_319_421]

V.3.1 Compléments relatifs à la certification des modules cryptographiques

Les modules cryptographiques employés pour générer les bi-clés de l'unité d'horodatage et pour signer les contremarques de temps doivent être conformes aux règles définies au II.3.4. du présent document

V.3.2 Compléments relatifs à la protection des modules d'horodatage

Le lien entre la date et l'heure et les données est établi au moyen d'un module d'horodatage composé d'une application d'horodatage et d'un module cryptographique.

Si l'application d'horodatage est embarquée dans le module cryptographique, alors l'application d'horodatage doit avoir fait l'objet au minimum d'une CSPN selon une cible de sécurité vérifiée par l'ANSSI. Il est recommandé que l'application d'horodatage ait fait l'objet d'une certification selon les Critères Communs selon le profil de protection [CEN_419_231] ou [PP_HORODAT].

Si l'application d'horodatage n'est pas embarquée dans le module cryptographique (par exemple, l'application d'horodatage fonctionne sur un serveur lui-même connecté au module cryptographique), alors le PSHE doit démontrer la mise en place de mesures techniques et organisationnelles permettant de réduire les risques pesant sur le module d'horodatage. Il est recommandé que l'application d'horodatage ait fait l'objet d'une CSPN selon une cible de sécurité vérifiée par l'ANSSI.

V.3.3. Compléments relatifs à la conservation des données

Le PSHE doit conserver pendant une durée minimale de sept (7) ans après l'expiration de chaque jeton d'horodatage toutes les informations pertinentes concernant les données délivrées et reçues, notamment afin de pouvoir fournir des preuves en justice. Le PSHE précise dans ses conditions générales d'utilisation la durée de conservation effectivement appliquée ainsi que, le cas échéant, les modalités de réversibilité et de portabilité.

V.4. Tableau récapitulatif des exigences

Exigences	Clauses applicables des normes européennes	Sections applicables du présent document
(Art. LP 35, II 7°) Utilisation des systèmes et des produits fiables ;	[EN_319_421] Clauses 7.6.2 et 7.6.3	V.3.1 et V.3.2
(Art. LP 35, II 10°) Conservation des informations délivrées et reçues par le prestataire de services de confiance ;	[EN_319_421] Clause 7.12	V.3.3
(Art. LP 35, II 11°) Continuité de service suite à l'arrêté d'activité du prestataire de services de confiance ;	[EN_319_421] Clause 7.14	*Pas de complément à la norme*
(Art. LP 37, 1°) Lien entre date, heure, et données ;	[EN_319_421] Clauses 7.6.3 et 7.7.1	V.3.2
(Art. LP 37, 2°) Fondation sur une horloge exacte reliée à l'UTC	[EN_319_421] Clauses 7.7.1 et 7.7.2	*Pas de complément à la norme*
(Art. LP 37, 3°) Signature ou cachet électronique avancé, ou méthode équivalente	[EN_319_421] Clause 7.7.1	V.3.1

VI. Services de conservation qualifiés des signatures et des cachets électroniques qualifiés

VI.1. Cadre juridique

Les services de conservation qualifiés des signatures électroniques qualifiées et des cachets électroniques qualifiés mis en œuvre par un PSCo respectant les exigences spécifiées au VI.2 du présent document permettent d'apporter une sécurité juridique concernant la validité, sur la durée, des signatures électroniques qualifiées et des cachets électroniques qualifiés.

VI.2. Exigences relatives aux services de conservation qualifiés des signatures et des cachets électroniques qualifiés

Les exigences visées par la [LOIDUPAYS] concernant les services de conservation qualifiés des signatures et des cachets électroniques qualifiés sont les suivantes :

- **Art. LP 29 :** Utilisation de procédures et technologies permettant d'étendre la fiabilité des signatures électroniques qualifiées ;
- **Art. LP 34 :** Application mutatis mutandis de l'article LP 29 de la LOIDUPAYS] à la conservation des cachets électroniques qualifiés ;
- **Art. LP 35, II 7° :** Utilisation des systèmes et des produits fiables ;
- **Art. LP 35, II 10° :** Conservation des informations délivrées et reçues par le prestataire de services de confiance ;
- **Art. LP 35, II 11° :** Plan d'arrêt d'activité d'un service de conservation des signatures électroniques et des cachets électroniques ;

Le respect des exigences de la norme [EN_319_401] relatives à la conservation des preuves et au plan d'arrêt d'activité, des exigences applicables[8] des exigences applicables des normes [NF_Z42-013] ou [EN_319_102-1] selon l'approche retenue par le PSCo et des compléments précisés au VI.3 du présent document, permet d'apporter une présomption de conformité à ces exigences.

Note : Deux approches sont reconnues pour assurer la conservation des signatures et cachets électroniques qualifiés :

- Une approche systémique reposant sur la protection en intégrité d'un système d'archivage électronique dans lequel seront conservés les signatures et cachets électroniques qualifiés. Dans ce cas la norme française [NF_Z42-013] (équivalente à la norme internationale [ISO_14641-1]) est la norme de référence ; ou
- Une approche spécifique reposant sur la protection en intégrité, unitairement, de chaque signature ou cachet électronique qualifié faisant l'objet d'une conservation, par le biais d'une extension régulière de la signature ou du cachet ou d'une capture régulière des informations de validation.

Le présent chapitre précise ainsi, en fonction de l'approche retenue, les exigences applicables.

VI.3. Compléments aux normes [NF_Z42-013] et [EN_319_102-1]

[8] Le point V.3 du présent chapitre précise, selon la méthode de conservation retenue par le PSCo, les exigences applicables.

VI.3.1. Compléments relatifs à l'utilisation de systèmes et produits fiables

Les modules cryptographiques employés pour les opérations nécessaires au service de conservation qualifié, notamment les opérations de création de signature électronique, de création de cachet électronique, ou d'horodatage le cas échéant, doivent respecter les règles spécifiées dans le document [PSCO_QUALIF].

VI.3.2. Compléments relatifs à la conservation des informations délivrées et reçues

Les exigences de la clause 7.10 de la norme [EN_319_401] s'appliquent.

Lorsque le service de conservation qualifié s'appuie sur une approche de type archivage électronique (voir le chapitre II.3.4 du présent document), les exigences de la clause 5.6 de la norme [NF_Z42-013] sont applicables. D'autres méthodes peuvent être acceptées sous réserve qu'elles apportent un niveau d'assurance équivalent.

Le prestataire de service de conservation qualifié doit conserver pendant une durée au moins égale à la durée de conservation des signatures ou cachets électroniques qualifiés, toutes les informations pertinentes concernant les données délivrées et reçues, notamment à fin de pouvoir fournir des preuves en justice. Le prestataire de service de conservation qualifié précise dans ses conditions générales d'utilisation, le cas échéant, la durée supplémentaire de conservation des preuves (au-delà de la durée de conservation des signatures et cachets électroniques qualifiés) effectivement appliquée ainsi que les modalités de réversibilité et de portabilité.

VI.3.3. Compléments relatifs à la continuité de service et à l'arrêt d'activité du PSCo

Les exigences de la clause 7.12 de la norme [EN 319 401] s'appliquent.

Le PSCo doit prévoir des modalités de réversibilité permettant de garantir l'intégrité et l'exploitabilité de l'ensemble des éléments reversés, soit vers le demandeur initial, soit vers un autre prestataire de services de conservation qualifié avec l'accord express du demandeur initial.

Ces éléments doivent être lisibles et intelligibles par leur destinataire, et doivent être dans un format permettant leur bonne exploitation :

- Si les éléments reversés sont dans un format non standard, le PSCo doit fournir les spécifications correspondantes et si nécessaire les outils permettant leur lecture ;
- En complément, si ces éléments font l'objet d'une protection en intégrité au moyen d'horodatages ou de cachets électroniques, il doit être possible pour le destinataire de valider ces horodatages ou ces cachets, ce qui suppose et le recours à des certificats électroniques pour lesquels le statut de révocation, la chaine de confiance et la politique de certification sont accessibles (par exemple, il peut s'agit du certificat électronique identifiant le service dans la liste de confiance).

La fiabilité des signatures et cachets électroniques qualifiés ne doit pas être affectée par cette réversibilité.

Note : Le PSCo peut refuser la conservation de signatures ou cachets électroniques fournis dans des formats propriétaires, s'il estime qu'il ne lui est pas possible d'assurer leur lisibilité dans le temps.

VI.3.4. Compléments relatifs aux procédures et technologies mises en œuvre pour étendre la fiabilité des signatures et cachets électroniques qualifiés

Le PSCo peut choisir d'assurer la conservation des signatures et cachets électroniques qualifiés :

- soit via le recours à un archivage électronique, permettant de garantir l'intégrité des signatures et cachets électroniques qualifiés archivés ;
- soit via le recours, de manière régulière, à une extension des signatures et cachets électroniques qualifiés ou à une capture des informations permettant, au-delà de la période de validité technologique, de valider ces signatures et cachets électroniques.

Le PSCo peut utiliser d'autres techniques, pourvu qu'il démontre que celles-ci répondent à un niveau de sécurité similaire aux deux précédentes.

Quelle que soit la méthode retenue, il est recommandé que le PSCo assure la conservation du document faisant l'objet de la signature ou du cachet électronique, dans les mêmes conditions de protection en intégrité, notamment pour pallier au risque d'affaiblissement de la fonction de calcul d'empreinte liant le document et la signature ou le cachet.

VI.3.4.1 Compléments relatifs à l'archivage des signatures et cachets électroniques qualifiés

Si le PSCo met en œuvre un archivage électronique, les exigences de la norme [NFZ_42-013] s'appliquent. Le respect des exigences additionnelles définies dans la clause 4.2 de cette norme n'est pas demandé.

Le PSCo doit également respecter les prescriptions du guide [GA_Z42-019].

Lorsque le PSCo a recours à des supports réinscriptibles ou à des supports de type WORM logiques, les enregistrements doivent faire l'objet d'un horodatage électronique régulier, à une périodicité définie en fonction des résultats de l'analyse des risques et de l'état de l'art de la cryptographie. Il est recommandé que cet horodatage électronique soit qualifié.

Préalablement à son archivage, il est recommandé que la signature ou le cachet électronique qualifié fasse l'objet d'une validation par le prestataire de services de conservation qualifié, répondant aux exigences applicables aux services de validation qualifiés, tels que décrites au VII. de la présente note.

Le prestataire de services de conservation qualifié peut s'appuyer sur un prestataire de services de validation qualifié pour réaliser cette opération. Dans ce cas, la signature avancée ou le cachet électronique avancé, apposé par le prestataire de services de validation qualifié sur le rapport de validation, doit être vérifié avant l'archivage de la signature électronique qualifiée ou du cachet électronique qualifié.

Le résultat de la validation doit être archivé avec la signature ou le cachet électronique qualifié.

Note : Le PSCo peut ne pas appliquer cette recommandation. Il doit dans ce cas s'assurer que les utilisateurs du service sont bien informés de cette limitation et des risques induits par l'absence de validation initiale sur la fiabilité des signatures et cachets électroniques qualifiés conservés. Le PSCo doit également pouvoir conserver, en complément des signatures et cachets électroniques qualifiés et dans les mêmes conditions de maintien d'intégrité, tous éléments additionnels transmis par le demandeur et concourant à prouver la validité de la signature ou du cachet électronique qualifié conservé.

VI.3.4.2 Compléments relatifs à l'extension des signatures électroniques

Si le PSCo met en œuvre une extension régulière des signatures et cachets électroniques qualifiés, le processus décrit dans la clause 4.3.5 de la norme [EN_319_102-1] doit être appliqué.

La validation de la signature ou du cachet électronique qualifié doit répondre aux exigences applicables aux services de validation qualifiés, tels que décrites au VII du présent document.

Il est recommandé que le format des signatures et cachets électroniques qualifiés ayant fait l'objet de cette extension soit l'un de ceux prévus par les standards référencées à l'annexe II de la présente note

Le PSCo peut, comme alternative à l'extension des signatures ou cachets électroniques qualifiés conservés, capturer régulièrement les informations nécessaires à leur validation (, informations relatives au statut de révocation). Il doit dans ce cas garantir l'intégrité et l'exploitabilité de ces éléments avec un niveau d'assurance au moins égal à celui permis par le mécanisme d'extension.

V.4. Tableau récapitulatif des exigences

Exigences	Clauses applicables des normes EN et ISO	Sections applicables du présent document
(Art. LP 29) Utilisation de procédures et technologies permettant d'étendre la fiabilité des signatures électroniques qualifiées	[NF_Z42-013] [GA_Z42-019] *(archivage électronique)* [EN_319_102-1] Clause 4.3.5 *(extension des signatures et cachets électroniques)*	VI.3.4.
(Art. LP 34) Application mutatis mutandis de l'article LP 29 à la conservation des cachets électroniques qualifiés.		
(LP 35, II 7°) Utilisation des systèmes et des produits fiables	[EN_319_401] Clause 7.7	VI.3.1
(Art. LP 35, II 10°) Conservation des informations délivrées et reçues par le prestataire de services de confiance ;	[EN_319_401] Clause 7.10 [NF_Z42_013] V.6et [GA_Z42-019] (*archivage électronique*)	VI.3.2
(Art. LP 35, II 11°) Continuité de service suite à l'arrêté d'activité du prestataire de services de confiance ;	[EN_319_401] Clause 7.12	VI.3.3

VII. Services de validation qualifiés des signatures électroniques qualifiées et des cachets électroniques qualifiés

VII.1. Cadre juridique

Les services de validation qualifiés des signatures électroniques qualifiées et des cachets électroniques qualifiés mis en œuvre par un PSCo respectant les exigences spécifiées au VII.2 du présent document permettent d'apporter une sécurité juridique concernant la validité des signatures électroniques qualifiées et des cachets électroniques qualifiés.

VII.2. Exigences relatives aux services de validation qualifiés des signatures électroniques qualifiées et des cachets électroniques qualifiés

Les exigences visées par la [LOIDUPAYS] concernant les services d'horodatage électronique qualifiés sont les suivantes :

- **Art. LP 27, 1° :** Le certificat sur lequel repose la signature était, au moment de la signature, un certificat qualifié de signature électronique conforme à l'annexe I ;
- **Art. LP 27, 2° :** Le certificat qualifié a été délivré par un prestataire de services de confiance qualifié et était valide au moment de la signature ;
- **Art. LP 27, 3° :** Les données de validation de la signature correspondent aux données communiquées à la partie utilisatrice ;
- **Art. LP 27, 4° :** L'ensemble unique de données représentant le signataire dans le certificat est correctement fourni à la partie utilisatrice ;
- **Art. LP 27, 5° :** La signature électronique a été créée par un dispositif de création de signature électronique qualifié ;
- **Art. LP 27, 6° :** L'intégrité des données signées n'a pas été compromise ;
- **Art. LP 27, 7° :** Les exigences relatives à la signature électronique avancée (art.26) ont été satisfaites au moment de la signature ;
- **Art. LP 28, 2° :** Fourniture aux parties utilisatrices du résultat du processus de validation, signé ou cacheté électroniquement par le prestataire ;
- **Art. LP 34 :** Application mutatis mutandis des articles LP 27 et LP 28 de la [LOIDUPAYS] à la validation des cachets électroniques qualifiés ;
- **Art. LP 35, II 7° :** Utilisation de systèmes et produits fiables, sécurité et fiabilité des processus ;
- **Art. LP 35, II 10° :** Conservation des données d'un service de validation des signatures électroniques et des cachets électroniques ;
- **Art. LP 35, II 11° :** Plan d'arrêt d'activité d'un service de validation des signatures électroniques et des cachets électroniques ;

Le respect des exigences de la norme [EN_319_401] relatives à la conservation des données et au plan d'arrêt d'activité, du processus de validation défini dans la norme [EN_319_102] et des compléments précisés au VII.3 du présent document, permet d'apporter une présomption de conformité à ces exigences.

VII.3. Compléments à la norme [EN_319_102]

VII.3.1 Compléments relatifs à la fourniture du résultat de la validation d'une signature ou d'un cachet électronique qualifié

Le processus de validation doit permettre de fournir à la partie utilisatrice le résultat du processus de validation, de manière automatisée, fiable, efficace et portant la signature électronique avancée ou le cachet électronique avancé du prestataire fournissant le service de validation qualifié.

La norme [EN_319_102] précise que le résultat du processus de validation est fourni via un rapport de validation permettant l'étude détaillée des décisions prises durant la phase de validation et la justification du statut de validation.

Le PSCo doit permettre l'accès au service de validation de signature ou de cachet, et la mise à disposition des parties utilisatrices de ce rapport de validation, de manière automatisée.

Afin de garantir la bonne interprétation du rapport de validation, le PSCo doit également rendre publique sa politique de validation des signatures électroniques qualifiées ou des cachets électroniques qualifiés.

VII.3.2 Compléments relatifs à la signature ou au cachet du rapport de validation

Le processus de validation doit permettre de fournir à la partie utilisatrice le résultat du processus de validation, de manière automatisée, fiable, efficace et portant la signature électronique avancée ou le cachet électronique avancé du prestataire fournissant le service de validation qualifié.

Exigence : Les modules cryptographiques employés pour apposer la signature électronique avancée ou le cachet électronique avancé du prestataire sur le rapport de validation de signature électronique qualifiée, ou de cachet électronique qualifié, doivent être conformes aux règles définies au II.3.4. du présent document. Il est recommandé que le certificat sur lequel repose cette signature électronique ou ce cachet électronique soit un certificat qualifié.

VII.3.3. Compléments relatifs à la protection des applications de validation

Le prestataire de service de validation qualifié doit démontrer la mise en place de mesures techniques et organisationnelles permettant de réduire les risques pesant sur l'application utilisée pour la validation.

Exigence : Il est recommandé que l'application de validation de signature ou de cachet ait fait l'objet d'une Certification de Sécurité de Premier Niveau (CSPN) selon une cible de sécurité vérifiée par l'ANSSI.

VII.3.4. Compléments relatifs à la conservation des informations délivrées et reçues

Les exigences de la clause 7.10 de la norme [EN_319_401] s'appliquent.

Le prestataire de service de validation qualifié doit conserver pendant une durée minimale de sept (7) ans après la date de validation de la signature électronique qualifiée ou du cachet électronique qualifié toutes les informations pertinentes concernant les données délivrées et reçues, notamment à fin de pouvoir fournir des preuves en justice. Le prestataire de service de validation qualifié précise dans ses conditions générales d'utilisation la durée de conservation effectivement appliquée ainsi que les modalités de réversibilité et de portabilité.

Exigence : Toutes les informations pertinentes, transmises par le demandeur ou recueillies électroniquement pour la validation de la signature électronique ou du cachet électronique, doivent être conservées pendant sept (7) ans, dont au moins :

- La date et l'heure de la validation de la signature ou du cachet électronique qualifié ;
- Les données fournies par le demandeur pour la validation de signature ou de cachet (valeur de la signature électronique ou du cachet électronique si celle-ci est séparable du document signé ou représentation unique du document signé dans le cas contraire) ainsi que l'identité du demandeur si celui-ci a fait l'objet d'une identification pour l'accès au service ;
- Les données externes (listes de confiance, listes de certificats révoqués, réponses OCSP, …) utilisées pour valider la signature ou le cachet ;
- Le rapport contenant le résultat de la validation de la signature ou du cachet électronique qualifié.

VII.3.5. Compléments relatifs à la continuité de service et à l'arrêt d'activité du PSCo

Les exigences des clauses 7.11 et 7.12 de la norme [EN 319 401] s'appliquent.

En cas de cessation d'activité, le PSCo doit détruire les clés privées utilisées pour signer les rapports de validation.

VII.3.6. Compléments relatifs à la date et l'heure présumées de la création de la signature électronique et du cachet électronique qualifiés

Le processus de validation doit permettre d'attester que :

- le certificat sur lequel repose la signature ou le cachet, était, au moment de la signature ou de la création de cachet, un certificat de signature électronique qualifié ou un certificat de cachet électronique qualifié ;
- le certificat qualifié a été délivré par un PSCo qualifié et était valide au moment de la signature ou de la création de cachet.

Cette exigence impose la connaissance de la date et de l'heure de la création de la signature électronique qualifiée ou du cachet électronique qualifié afin de pouvoir vérifier :

- que le certificat était bien dans sa période de validité ;
- que le certificat n'était pas révoqué.

Exigence : La date et l'heure de référence pour la validation sont la date et l'heure auxquelles la signature électronique ou le cachet électronique est fourni au service de validation dans les cas suivants :

- Il n'y a pas de date et d'heure associées à la signature ou au cachet ; ou
- la date et l'heure se trouvent dans la signature ou le cachet sous la forme d'attributs renseignés par le signataire.

Si la date et l'heure sont associées à la signature ou au cachet au moyen d'un horodatage électronique non qualifié, il appartient au prestataire de service de validation qualifié d'accepter ou non comme référence de validation cette date et cette heure. En cas de non-acceptation, la date et l'heure de référence sont celles du moment de la validation. Le PSCo doit rendre publique sa politique d'acceptation des horodatages non qualifiés (incluant les modalités de vérification des jetons d'horodatage électronique).

Si la date et l'heure sont associées à la signature ou au cachet grâce à un horodatage électronique qualifié, cette date et cette heure sont prises comme référence pour la validation. Le PSCo doit mener l'ensemble des opérations techniques nécessaires à la validation du jeton d'horodatage, dont notamment les vérifications relatives à la cryptographie (vérification de l'empreinte et de la signature figurant dans le jeton d'horodatage).

VII.3.7 Compléments relatifs à la qualité des informations de révocation

Le service de validation doit systématiquement solliciter les informations les plus récentes mises à disposition par l'autorité de certification émettrice du certificat qualifié. Si cette autorité met à disposition un service de répondeur OCSP, il est recommandé de s'appuyer sur celui-ci.

VII.3.8 Compléments relatifs au statut qualifié du certificat de signature ou de cachet et du dispositif de création de signature ou de cachet

Le processus de validation doit permettre d'attester que :

- Le certificat sur lequel repose la signature ou le cachet, était, au moment de la signature ou de la création de cachet, un certificat de signature électronique qualifié ou un certificat de cachet électronique qualifié ;
- La signature électronique ou le cachet électronique a été créé par un dispositif de création de signature / cachet électronique qualifié.

Exigence : La présence des extensions de certificat suivantes, valorisées de la manière prévue par la norme [EN_319_412-5], doit être vérifiée :

- *« id-etsi-qcs-QcCompliance » ;*
- *« id-etsi-qcs-QcSSCD ».*

La présence de l'extension « *id-etsi-qcs-QcType* » et sa bonne valorisation devraient être vérifiées, mais, l'absence de cette extension ne devrait pas entrainer un rejet de la signature ou du cachet.

VII.3.9 Compléments relatifs à la vérification du statut qualifié du prestataire de services de confiance ayant délivré le certificat de signature ou de cachet

Le processus de validation doit permettre d'attester que :

- le certificat sur lequel repose la signature ou le cachet, était, au moment de la signature ou de la création de cachet, un certificat de signature électronique qualifié ou un certificat de cachet électronique qualifié ;
- le certificat qualifié a été délivré par un PSCo qualifié et était valide au moment de la signature ou de la création de cachet.

Exigence : Cette vérification doit :

- Prendre comme référence la date et l'heure de début de validité figurant dans le certificat qualifié pour déterminer si, à la date présumée de délivrance du certificat, le PSCo ayant délivré le certificat était qualifié ;
- Prendre comme référence la date et l'heure identifiées conformément aux règles au VII.3.6 du présent document, pour déterminer si à, la date présumée de création de la signature ou du cachet, le PSCo ayant délivré le certificat était qualifié ;
- Exploiter si nécessaire les informations sur les historiques des statuts des services de confiance

qualifiés dans les listes de confiance, conformément aux clauses 5.5.9, 5.5.10 et 5.6 de la norme [EN_119_612].

VII.3.10 Compléments relatifs à l'identité du signataire ou du créateur de cachet

Le processus de validation permet d'attester que :

- L'ensemble unique de données représentant le signataire dans le certificat est correctement fourni à la partie utilisatrice ;
- L'utilisation d'un pseudonyme est clairement indiquée à la partie utilisatrice, si un pseudonyme a été utilisé au moment de la signature.

Exigence : La présence du champ « Subject », valorisé de la manière prévue par les normes [EN_319_412-2] et [EN_319412-3], doit être vérifiée[9].

L'identité extraite du champ « Subject », et une mention relative à l'utilisation d'un pseudonyme le cas échéant, doit être précisée dans le rapport de validation.

VII.4. Tableau récapitulatif des exigences

Exigences	Clauses applicables des normes européennes	Sections applicables du présent document
(Art. LP 27, 1°) Qualification du certificat au moment de la signature	[EN_319_102] Clauses 5.2.6, 5.6.2	VII.3.6 et VI.3.8
(Art. LP 27, 2°) Délivrance du certificat par un PSCo qualifié et validité au moment de la signature	[EN_319_102] Clauses 5.2.5, 5.2.6, 5.6.2	VII.3.6, VII.3.7 et VII.3.9
(Art. LP 27, 3°) Correspondance des données de validation de la signature aux données communiquées à la partie utilisatrice	[EN319102] Clause 5.2.7	*Pas de complément à la norme*
(Art. LP 27, 4°) Fourniture correcte à la partie utilisatrice de l'ensemble unique de données représentant le signataire dans le certificat	[EN319102] Clause 5.2.3	VII.3.10
(Art. LP 27, 5°) Création de la signature électronique par un dispositif de création de signature électronique qualifié	*Non couvert*	VII.3.8
(Art. LP 27, 6°) Non compromission de l'intégrité des données signées	[EN_319_102] Clause 5.2.7	*Pas de complément à la norme*
(Art. LP 27, 7°) Respect des exigences relatives à la signature électronique avancée	*Non couvert*	*Considéré comme couvert par les autres points de contrôle*
(Art. LP 28, 2°) Fourniture aux parties utilisatrices du résultat du processus de validation, signé ou cacheté électroniquement par le prestataire	*Non couvert*	VII.3.1 et VII.3.2
(Art. LP 34) Application mutatis mutandis des articles LP 27 et LP 28 à la validation des cachets électroniques qualifiés.		
(Art. LP 35, II 7°) Utilisation des systèmes et des produits fiables ;	[EN_319_401] Clause 7.7	VII.3.2 et VII.3.3

[9] Ces normes représentent une bonne pratique mais ne sont pas d'application obligatoire. Le processus de validation doit pouvoir tolérer des écarts à celles-ci tant que l'exigence de la [LOIDUPAYS] est remplie. *A titre d'exemple, un certificat de signature électronique qualifié pourrait contenir un attribut commonName, mais pas d'attribut givenName ou surname.*

(Art. LP 35, II 10°) Conservation des informations délivrées et reçues par le prestataire de services de confiance ;	[EN_319_401] Clause 7.0	VII.3.4
(Art. LP 35, II 11°) Continuité de service suite à l'arrêté d'activité du prestataire de services de confiance ;	[EN_319_401] Clause 7.12	VII.3.5

VIII. Services d'envoi recommandé électronique qualifiés

VIII.1 Cadre juridique

Les services d'envoi recommandé électronique qualifiés, respectant les exigences spécifiées au VIII.2 du présent document, bénéficient des effets juridiques définis à l'article LP 38 la [LOIDUPAYS].

VIII.2. Exigences relatives aux services d'envoi recommandé électronique qualifiés

Les exigences visées par la [LOIDUPAYS] concernant les services d'envoi recommandé électronique qualifiés :

- **Art. LP 35, II 7° :** Utilisation de systèmes et produits fiables, sécurité et fiabilité du processus ;
- **Art. LP 35, II 10° :** Conservation des informations délivrées et reçues dans le cadre d'envoi recommandé électronique ;
- **Art. LP 35, II 11° :** Continuité de service suite à l'arrêt d'activité d'envoi recommandé électronique ;
- **Art. LP 39, 1° :** Les services sont fournis par un ou plusieurs prestataires de services de confiance qualifiés ;
- **Art. LP 39, 2° :** Le service doit garantir l'identification de l'expéditeur avec un degré de confiance élevé ;
- **Art. LP 39, 3° :** Le service doit garantir l'identification du destinataire avant la fourniture ;
- **Art. LP 39, 4° :** L'envoi et la réception de données sont sécurisés par une signature électronique avancée ou par un cachet électronique avancé d'un prestataire de services de confiance qualifié de manière à exclure toute possibilité de modification indétectable des données ;
- **Art. LP 39, 5° :** Toute modification des données nécessaire pour l'envoi ou la réception de celles-ci est clairement signalée à l'expéditeur et au destinataire des données ;
- **Art. LP 39, 6° :** La date et l'heure d'envoi, de réception et toute modification des données sont indiquées par un horodatage électronique.

Le respect des exigences de la norme [EN_319_401] relatives à la conservation des données et au plan d'arrêt d'activité, des exigences applicables[10] du standard [TS_102_640-3], et des compléments précisés au VIII.3 du présent document, permet d'apporter une présomption de conformité à ces exigences.

Note : Le service d'envoi recommandé électronique doit également correspondre à la définition de la [LOIDUPAYS], telle que précisée à l'article LP 1, 29°) :
« *Un service qui permet de transmettre des données entre des tiers par voie électronique, qui fournit des preuves concernant le traitement des données transmises, y compris la preuve de leur envoi et de leur réception, et qui protège les données transmises contre les risques de perte, de vol, d'altération ou de toute modification non autorisée*. »

[10] Le standard [TS_102_640-3] traite de l'envoi de courriers électroniques recommandés, et référence des versions obsolètes de normes et standards. Les exigences de ce standard doivent être adaptées au contexte de l'envoi recommandé électronique qualifié, et à l'état de l'art de la normalisation.

VIII.3. Compléments à la norme [TS_102_640-3]

VIII.3.1 Compléments relatifs aux preuves d'envoi et de réception

Conformément à l'article LP 1, 29°) de la [LOIDUPAYS], on entend par « service d'envoi recommandé électronique », un service qui permet de transmettre des données entre des tiers par voie électronique, qui fournit des preuves concernant le traitement des données transmises, y compris la preuve de leur envoi et de leur réception, et qui protège les données transmises contre les risques de perte, de vol, d'altération ou de toute modification non autorisée.

Il est ainsi attendu qu'un service d'envoi recommandé électronique qualifié mette à disposition de l'expéditeur les preuves d'envoi et de réception, de manière automatisée, fiable et efficace.

Les conditions générales d'utilisation du service d'envoi recommandé électronique qualifié doivent préciser les modalités de mise à disposition de ces preuves.

VIII.3.2 Compléments relatifs à l'utilisation de systèmes et produits fiables

Les modules cryptographiques employés pour les opérations nécessaires au service d'envoi recommandé électronique qualifié, notamment les opérations de création de cachet électronique, ou d'horodatage électronique le cas échéant, doivent respecter les règles spécifiées dans le document [PSCO_QUALIF].

VIII.3.3 Compléments relatifs à la conservation des informations délivrées et reçues

Les exigences de la clause 7.10 de la norme [EN_319_401] et de la clause 6.5 du standard [TS_102_640-3] s'appliquent.

Le prestataire de service d'envoi recommandé électronique qualifié doit conserver pendant une durée minimale de sept (7) ans après la date d'envoi et de réception des données toutes les informations pertinentes concernant les données délivrées et reçues, notamment à fin de pouvoir fournir des preuves en justice. Le PSCo précise dans ses conditions générales d'utilisation la durée de conservation effectivement appliquée ainsi que les modalités de réversibilité et de portabilité.

Les données à conserver sont au moins :

- L'identité de l'expéditeur du recommandé électronique ;
- Une preuve de validation de l'identité de l'expéditeur ;
- Une référence au document faisant l'objet de la demande d'envoi recommandé électronique ;
- Les jetons d'horodatage électronique qualifié correspondant à la date et heure d'envoi, de réception et de modification des données le cas échéant ;
- L'identité du destinataire du recommandé électronique ;
- Une preuve de validation de l'identité du destinataire ;
- Les données relatives à la sécurisation de l'envoi (cachets électroniques).

VIII.3.4 Compléments relatifs à la continuité de service et à l'arrêt d'activité du PSCo

Les exigences de la clause 7.12 de la norme [EN_319_401] s'appliquent.

VIII.3.5 Compléments relatifs à la fourniture du service par des prestataires de services de confiance qualifiés

Si le service est fourni par plusieurs prestataires de services de confiance qualifiés, l'expéditeur et le destinataire de l'envoi recommandé électronique doivent être informés de l'identité de l'ensemble des PSCo qualifiés contribuant au service.

Chaque PSCo doit s'assurer, sur une base régulière et au moyen des listes de confiance publiées par les Etats membres, du maintien de la qualification des PSCo partenaires.

VIII.3.6 Compléments relatifs à l'identification de l'expéditeur

VIII.3.6.1. Vérification initiale de l'identité de l'expéditeur

Le service d'envoi recommandé électronique qualifié doit garantir l'identification de l'expéditeur avec un degré de confiance élevé.

Pour la vérification d'identité de l'expéditeur, les exigences définies au IV.3.1 du présent document s'appliquent mutatis mutandis à l'envoi recommandé électronique.

VIII.3.6.2. Identification et authentification de l'expéditeur

Postérieurement à cette vérification d'identité, le prestataire de service d'envoi recommandé électronique peut attribuer un moyen d'authentification à l'expéditeur ou au destinataire, qu'il pourra utiliser pour s'authentifier à chaque envoi.

Dans ce cas, les méthodes d'authentification décrites dans les points 6.3.b à 6.3.f du standard [TS_102_640-3] sont acceptables. La méthode décrite au point 6.3.a de ce standard n'est pas acceptable.

L'authentification doit être forte (via l'emploi de deux facteurs distincts), et le mécanisme d'authentification mis en œuvre doit être dynamique. Il est recommandé que le moyen d'identification fasse au minimum l'objet d'une CSPN.

Le moyen d'authentification doit être sous le contrôle exclusif de l'utilisateur, et mettre en œuvre des contrôles de sécurité de sorte qu'il soit hautement improbable que des activités telles que les tentatives de décryptage, l'écoute, l'attaque par rejeu ou la manipulation d'une communication par un attaquant ayant un potentiel d'attaque modéré puissent nuire aux mécanismes d'authentification.

Dans le cas où le moyen d'identification repose sur l'utilisation un certificat de signature ou de cachet électronique, il est recommandé que ce certificat soit qualifié.

Note : Ce moyen d'identification peut être délivré par un autre organisme que le prestataire de services d'envoi recommandé électronique qualifié.

Si le PSCo n'attribue pas de moyen d'identification à l'expéditeur, la vérification d'identité doit être réalisée à chaque envoi dans les conditions décrites au VIII.3.6.1 ci-dessus.

VIII.3.7. Compléments relatifs à l'identification du destinataire

VIII.3.7.1. Vérification initiale de l'identité du destinataire

Le service d'envoi recommandé électronique qualifié doit garantir l'identification du destinataire avant la fourniture des données. Pour la vérification d'identité du destinataire, il est recommandé lorsque cela est possible d'appliquer les mêmes exigences que pour l'identification de l'expéditeur. A défaut, cette vérification d'identité doit au minimum respecter les exigences du chapitre 2.1 du règlement [RE_2015_1502] pour le niveau substantiel.

VIII.3.7.2. Identification et authentification du destinataire

Postérieurement à la vérification d'identité, le prestataire de service d'envoi recommandé électronique qualifié peut attribuer un moyen d'identification au destinataire, qu'il pourra utiliser pour s'authentifier à chaque réception. Les exigences et recommandations applicables au moyen d'identification de l'expéditeur sont applicables au moyen d'identification du destinataire.

Note : Ce moyen d'identification peut être délivré par un autre organisme que le prestataire de services d'envoi recommandé électronique qualifié.

Si le PSCo n'attribue pas de moyen d'identification au destinataire, la vérification d'identité doit être réalisée à chaque réception dans les conditions décrites au VIII.3.7.1 ci-dessus.

VIII.3.8. Compléments relatifs à la sécurisation des envois et réceptions par un cachet électronique

Les exigences définies à la clause 6.4 du standard [TS_102_640-3] s'appliquent.

Les modules cryptographiques employés pour apposer le cachet électronique avancé sécurisant l'envoi et la réception des données doivent être conformes aux règles définies au II.3.4. du présent document.

Il est recommandé que le certificat sur lequel repose ce cachet électronique soit un certificat qualifié au titre de l'article LP 32 de la [LOIDUPAYS].

Si le cachet électronique avancé est apposé–par un PSCo qualifié distinct du prestataire de services d'envoi recommandé électronique qualifié, ce dernier doit vérifier la validité de ce cachet.

Note : La [LOIDUPAYS] prévoit que l'envoi et la réception puissent être sécurisés au moyen d'une signature électronique avancée ou d'un cachet électronique avancé du PSCo qualifié. Pour autant, en France métropolitaine et en Polynésie française, les PSCo qualifiés étant nécessairement des personnes morales, seule la sécurisation par le biais d'un cachet électronique avancé devrait être mise en œuvre.

VIII.3.9 Compléments relatifs au signalement des modifications de données

Le service d'envoi recommandé électronique qualifié doit signaler clairement toute modification des données nécessaire pour l'envoi ou la réception de celles-ci à l'expéditeur et au destinataire des données.

Le PSCo précise dans ses conditions générales d'utilisation les moyens utilisés pour le signalement de ces modifications.

VIII.3.10 Compléments relatifs à l'horodatage électronique qualifié

La date et l'heure d'envoi, de réception et toute modification des données doivent être indiquées par un horodatage électronique qualifié.

Le prestataire de service d'envoi recommandé électronique qualifié peut s'appuyer sur un prestataire de service d'horodatage qualifié distinct pour réaliser cette opération. Dans ce cas, la validité du jeton d'horodatage électronique qualifié doit être systématiquement vérifiée.

VIII.4. Tableau récapitulatif des exigences

Exigences	Clauses applicables des normes européennes	Sections applicables du présent document
(Art. LP 1, 29°) Définition de l'envoi recommandé électronique	*Non couvert*	VIII.3.1
(Art. LP 35, II 7°) Utilisation des systèmes et des produits fiables ;	[EN_319_401] Clause 7.7 [TS_102_640-3] Clause 6.4.3	VIII.3.2
(Art. LP 35, II 10°) Conservation des informations délivrées et reçues par le prestataire de services de confiance ;	[EN_319_401] Clause 7.10 [TS_102_640-3] Clause 6.5	VIII.3.3
(Art. LP 35, II 11°) Continuité de service suite à l'arrêté d'activité du prestataire de services de confiance ;	[EN_319_401] Clause 7.12	VIII.3.4
(Art. LP 39, 1°) Les services sont fournis par un ou plusieurs prestataires de services de confiance qualifiés	*Non couvert*	VIII.3.5
(Art. LP 39, 2°) Le service doit garantir l'identification de l'expéditeur avec un degré de confiance élevé	[TS_102_640-3] Clause 6.3	VIII.3.6
(Art. LP 39, 3°) Le service doit garantir l'identification du destinataire avant la fourniture	[TS_102_640-3] Clause 6.3	VIII.3.7
(Art. LP 39, 4°) L'envoi et la réception de données sont sécurisés par une signature électronique avancée ou par un cachet électronique avancé d'un prestataire de services de confiance qualifié de manière à exclure toutN possibilité de modification indétectable des données	[TS_102_640-3] Clause 6.4	VIII.3.8

(Art. LP 39, 5°) Toute modification des données nécessaire pour l'envoi ou la réception de celles-ci est clairement signalée à l'expéditeur et au destinataire des données	*Non couvert*	VIII.3.9
(Art. LP 39, 6°) La date et l'heure d'envoi, de réception et toute modification des données sont indiquées par un horodatage électronique qualifié.	*Non couvert*	VIII.3.10

IX. Dispositifs de création de signature / cachet électronique qualifiés

IX.1. Cadre juridique

Les dispositifs de création de signature / cachet électronique qualifiés certifiés conformément à la présente procédure sont présumés satisfaire aux exigences de l'annexe II de la [LOIDUPAYS]

Les signatures électroniques avancées, reposant sur un certificat qualifié, et créées à l'aide d'un dispositif de création de signature électronique qualifié, sont des signatures électroniques qualifiées, bénéficiant des effets juridiques prévus à l'article LP 23 de la [LOIDUPAYS]

Les cachets électroniques avancés, reposant sur un certificat qualifié, et créés à l'aide d'un dispositif de création de cachet électronique qualifié, sont des cachets électroniques qualifiés, bénéficiant des effets juridiques prévus à l'article LP 30 de la [LOIDUPAYS]

IX.2 Exigences relatives aux dispositifs de création de signature / cachet électronique qualifiés

Les produits permettant la signature électronique qualifiée et le cachet électronique qualifié sont définis ainsi à l'article LP 1er de la [LOIDUPAYS] :

- « « dispositif de création de signature électronique », un dispositif logiciel ou matériel configuré servant à créer une signature électronique » ;
- « « dispositif de création de signature électronique qualifié », un dispositif de création de signature électronique qui satisfait aux exigences énoncées à l'annexe 2 » ;
- « « dispositif de création de cachet électronique », un dispositif logiciel ou matériel configuré utilisé pour créer un cachet électronique » ;
- « « dispositif de création de cachet électronique qualifié », un dispositif de création de cachet électronique qui satisfait mutatis mutandis aux exigences énoncées à l'annexe 2 ».

Les exigences visées par l'annexe II de la [LOIDUPAYS] concernant les dispositifs de création de signature / cachet électronique qualifiés sont les suivantes :

- Les dispositifs de création de signature électronique qualifiés garantissent au moins, par des moyens techniques et des procédures appropriés, que :
    - La confidentialité des données de création de signature électronique utilisées pour créer la signature électronique est suffisamment assurée ;
    - Les données de création de signature électronique utilisées pour créer la signature électronique ne peuvent être pratiquement établies qu'une seule fois ;
    - L'on peut avoir l'assurance suffisante que les données de création de signature électronique utilisées pour créer la signature électronique ne peuvent être trouvées par déduction et que la signature électronique est protégée de manière fiable contre toute falsification par les moyens techniques actuellement disponibles ;
    - Les données de création de signature électronique utilisées pour créer la signature électronique peuvent être protégées de manière fiable par le signataire légitime contre leur utilisation par d'autres.
- Les dispositifs de création de signature électronique qualifiés ne modifient pas les données à signer et n'empêchent pas la présentation de ces données au signataire avant la signature.

- La génération ou la gestion de données de création de signature électronique pour le compte du signataire peut être seulement confiée à un prestataire de services de confiance qualifié.
- Sans préjudice du paragraphe 1, point d), un prestataire de services de confiance qualifié gérant des données de création de signature électronique pour le compte d'un signataire ne peut reproduire les données de création de signature électronique qu'à des fins de sauvegarde, sous réserve du respect des exigences suivantes :
    - le niveau de sécurité des ensembles de données reproduits doit être équivalent à celui des ensembles de données d'origine ;
    - le nombre d'ensembles de données reproduits n'excède pas le minimum nécessaire pour assurer la continuité du service.

Les exigences de cette annexe 2 s'appliquent, mutatis mutandis, aux dispositifs de création de cachet électronique qualifiés.

La certification de conformité à ces exigences est réalisée conformément à la décision d'exécution [eIDAS_DE_QSCD].

Pour les DCSQ ou DCCQ pour lesquels les données de création de signature ou de cachet électronique sont contenues dans un environnement sous le contrôle de l'utilisateur, la certification de conformité repose sur les normes référencées dans l'annexe I de l'acte d'exécution.

Pour les DCSQ ou DCCQ pour lesquels les données de création de signature ou de cachet électronique sont gérées par un fournisseur de services de confiance qualifié pour le compte du signataire ou du créateur de cachet, la certification de conformité repose sur le processus prévu au IX3.2 du présent document.

IX.3. Modalités de certification de la conformité des DCSQ et DCCQ

IX.3.1 DCSQ et DCCQ mis en œuvre sous le contrôle exclusif de l'utilisateur

Le certificat de conformité complet du DCSQ ou DCCQ est délivré s'il est vérifié, dans le cadre du processus [QUALIF_PROD], que :

- Le système ou le produit dans lequel est mis en œuvre la clé privée de signature ou de cachet a été certifié dans le cadre de l'accord européen de reconnaissance mutuelle du SOG-IS3 sur la base de l'un des profils de protection référencés dans la décision n° 2016/650 ;
- **et**
- La cryptographie répond aux règles définies dans le document « SOG-IS Crypto Evaluation Scheme ».

IX.3.2 DCSQ et DCCQ mis en œuvre par un PSCo qualifié pour le compte de l'utilisateur

Le certificat de conformité partiel du produit est délivré s'il est vérifié, dans le cadre du processus [QUALIF_PROD], que :

- Le système ou le produit dans lequel est mis en œuvre la clé privée de signature ou de cachet a été certifié dans le cadre de l'accord européen de reconnaissance mutuelle du SOG-IS 3 sur la base de

l'un des profils de protection référencés par l'ANSSI ou référencés par le SOG-IS et applicables à ce type de dispositif, ou sur la base d'une cible de sécurité validée par l'ANSSI ;

- **et**

- Les systèmes ou les produits concourant à protéger cette clé privée contre une utilisation par d'autres que le signataire ou le créateur de cachet légitime, ont été certifiés conformément à une stratégie définie préalablement avec l'ANSSI.

- **et**

- La cryptographie répond aux règles définies dans le document « SOG-IS Crypto Evaluation Scheme »

Le certificat de conformité complet du DCSQ ou DCCQ est délivré s'il est vérifié, dans le cadre du processus [QUALIF_SERV], que :

- Le système ou le produit est mis en œuvre dans l'environnement d'un prestataire de services de confiance qualifié, figurant dans la liste de confiance de l'un des Etats membres de l'Union européenne ;

- **et**

- Ce prestataire de services de confiance qualifié met en œuvre le produit ou le système conformément aux restrictions d'usage figurant dans son rapport de certification [CC] ;

- **et**

- Ce prestataire de services de confiance qualifié respecte les exigences formulées au point 4 de l'annexe II du règlement eIDAS ;

- **et**

- Ce prestataire de services de confiance qualifié respecte les exigences du règlement précisées à l'article 19, et en particulier dispose d'une analyse de risques à jour couvrant la mise en œuvre du produit ou système au sein de son environnement.

Annexe 1 : Références documentaires

Renvoi	Document
[LOIDUPAYS]	Loi du pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices
[ARRETE]	Arrêté relatif à la dématérialisation des actes administratifs et aux téléservices
[eIDAS]	Règlement n° 910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive n°1999/93/CE.
[eIDAS_DE_QSCD]	Décision d'exécution (UE) n° 2016/650 de la commission du 25 avril 2016 établissant des normes relatives à l'évaluation de la sécurité des dispositifs qualifiés de création de signature électronique et de cachet électronique conformément à l'article 30, paragraphe 3, et à l'article 39, paragraphe 2, du règlement (UE) n° 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur
[PSCO_QUALIF]	Prestataires de services de confiance qualifiés - Critères d'évaluation de la conformité au règlement eIDAS, version en vigueur. Disponible sur http://www.ssi.gouv.fr
[QUALIF_PROD]	Processus de qualification d'un produit, version en vigueur. Disponible sur http://www.ssi.gouv.fr
[QUALIF_SERV]	Processus de qualification d'un service, version en vigueur. Disponible sur http://www.ssi.gouv.fr
[HOMOLOGATION]	Annexe D du RGS : L'homologation de sécurité en neuf étapes simples, version en vigueur.
[GH]	Guide d'hygiène informatique. Disponible sur http://www.ssi.gouv.fr
[SOGIS-CRYPTO]	SOG-IS Crypto Evaluation Scheme - Agreed Cryptographic Mechanisms - Version 1.0 – May 2016 Disponible sur http://sogis.org
[TS_119_312]	ETSI TS 119 312 V1.1.1 (2014-11) : Electronic Signatures and Infrastructures (ESI); Cryptographic Suites Disponible sur : http://www.etsi.org
[TS_103_171]	ETSI TS 103 171 V2.1.1 (2012-03) Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile
[TS_103_172]	ETSI TS 103 172 V2.2.2 (2013-04) Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile
[TS_103_173]	ETSI TS 103 173 V2.2.1 (2013-04) Electronic Signatures and Infrastructures (ESI); CAdES Baseline Profile
[TS_103_174]	ETSI TS 103 174 V2.2.1 (2013-06) Electronic Signatures and Infrastructures (ESI); ASiC Baseline Profile
[TS_102_640-3]	ETSI TS 102 640-3 V2.1.2 (2011-09) : Technical Specification Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 3: Information Security Policy Requirements for REM Management Domains
[EN_319_411-2]	ETSI EN 319 411-2 V2.1.1 (2016-02) : Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
[EN_319_412-1]	ETSI EN 319 412-1 V1.1.1 (2016-02) : Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures Disponible sur : http://www.etsi.org
[EN_319_412-5]	ETSI EN 319 412-5 V2.1.1 (2016-02) : Part 5: QCStatements
[EN_319_421]	ETSI EN 319 421 v1.1.1 (2016-03), Electronic Signatures and Infrastructures (ESI) ; Policy and

	Security Requirements for Trust Service Providers issuing Time-Stamps. Disponible sur : http://www.etsi.org
[EN_319_412-2]	ETSI EN 319 412-2 V2.1.1 (2016-02) : Part 2: Certificate profile for certificates issued to natural persons
[EN_319_102]	Draft ETSI EN 319 102-1 V1.0.0 (2015-07) : Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation
[EN_319_102-1]	ETSI EN 319 102-1 V1.1.1 (2016-05) Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation
[NF_Z42-013]	NF Z42-013 (mars 2009) : Archivage électronique Spécifications relatives à la conception et à l'exploitation de systèmes informatiques en vue d'assurer la conservation et l'intégrité des documents stockés dans ces systèmes.
[GA_Z42-019]	Guide d'application de la NF Z 42-013 (juin 2010).
[ISO_14641-1]	ISO 14641-1 (2012-02-01) : Electronic archiving Part 1 : Specifications concerning the design and the operation of an information system for electronic information preservation
[PP_HORODAT]	Profil de protection, Système d'horodatage, référence PP-SH-CCv3.1, version 1.7 du 18 juillet 2008. Disponible sur http://www.ssi.gouv.fr
[CEN_419_231]	Protection profile for trustworthy systems supporting time stamping, 2015-11-02. Disponible sur : http://www.etsi.org *Ce document est encore à l'état de projet.*
[RFC_6960]	Internet Engineering Task Force (IETF) - Request for Comments : 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
[RGS]	Référentiel général de sécurité version 1.0 Disponible sur http://www.ssi.gouv.fr
[RGS_A1]	Annexe A1 au RGSv1.0 : Règles relatives à la mise en œuvre des fonctions de sécurité basées sur l'emploi de certificats électroniques.
[RGS_A2]	Annexe A2 au RGSv1.0 : Politique de Certification Type – certificats électroniques de personne
[RGS_A3]	Annexe A3 au RGSv1.0 : Politique de Certification Type – certificats électroniques de services applicatifs
[RGS_A4]	Annexe A4 au RGSv1.0 : Profils de certificats / LCR / OCSP et algorithmes cryptographiques
[RGS_A5]	Annexe A5 du RGSv1.0, Politique d'Horodatage Type

Annexe 2 Liste des spécifications techniques recommandées relatives aux signatures et cachets électroniques avancés

Les normes figurant à la présente annexe sont les normes de référence en vigueur pour les formats de signatures électroniques avancés. Établir de tels formats de référence vise notamment à améliorer l'interopérabilité transfrontalière des procédures électroniques.

Les signatures électroniques avancées et les cachets électroniques avancés sont similaires du point de vue technique. Par conséquent, les normes applicables aux formats des signatures électroniques avancées s'appliquent *mutatis mutandis* aux formats des cachets électroniques avancés.

2.1. Liste des spécifications techniques relatives aux signatures électroniques avancées XML, CMS ou PDF et au conteneur de signature associé

Les formats de référence relatifs aux signatures électroniques avancées et aux signatures électroniques avancées reposant sur un certificat qualifié sont XML, CMS ou PDF au niveau de conformité B, T ou LT, ou au moyen d'un conteneur de signature associé.

Les normes de référence en vigueur relatives à signatures électroniques avancées sont les spécifications techniques ETSI suivantes, à l'exception de leur clause 9 :

XAdES Baseline Profile	ETSI TS 103171 v.2.1.1 (1)
CAdES Baseline Profile	ETSI TS 103173 v.2.2.1 (2)
PAdES Baseline Profile	ETSI TS 103172 v.2.2.2 (3)

(1) http://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf
(2) http://www.etsi.org/deliver/etsi_ts/103100_103199/103173/02.02.01_60/ts_103173v020201p.pdf
(3) http://www.etsi.org/deliver/etsi_ts/103100_103199/103172/02.02.02_60/ts_103172v020202p.pdf

Les normes de référence en vigueur relatives au conteneur de signature sont les spécifications techniques ETSI suivantes :

Associated Signature Container Baseline Profile	ETSI TS 103174 v.2.2.1 (1)

(1) http://www.etsi.org/deliver/etsi_ts/103100_103199/103174/02.02.01_60/ts_103174v020201p.pdf

2.2. Liste des spécifications techniques relatives aux cachets électroniques avancés XML, CMS ou PDF et au conteneur de cachet associé

Les formats de référence relatifs aux cachets électroniques avancés et aux cachets électroniques avancés reposant sur un certificat qualifié sont XML, CMS ou PDF au niveau de conformité B, T ou LT, ou au moyen d'un conteneur de signature associé.

Les normes de référence en vigueur relatives aux cachets électroniques avancés sont les spécifications techniques ETSI suivantes, à l'exception de leur clause 9 :

XAdES Baseline Profile	ETSI TS 103171 v.2.1.1

CAdES Baseline Profile	ETSI TS 103173 v.2.2.1
PAdES Baseline Profile	ETSI TS 103172 v.2.2.2

Les normes de référence en vigueur relatives au conteneur de cachet associé sont les spécifications techniques ETSI suivantes :

Associated Seal Container Baseline Profile	ETSI TS 103174 v.2.2.1

Annexe 3 : Profils de certificats recommandés

Les tableaux suivants présentent quatre types de profils de certificats permettant d'apporter une présomption de conformité aux exigences de la loi du pays n° 2017-30 du 2 novembre 2017. Il est recommandé aux PSCE de respecter ces profils de certificats. Dans le cas contraire, le PSCE doit démontrer le respect des exigences applicables des annexes I et III de la loi du pays n° 2017-30 du 2 novembre 2017.

Par exemple, un PSCE pourrait, pour les certificats de signature électronique qu'il émet, ne pas utiliser les attributs givenName et surname pour identifier ses porteurs, et utiliser uniquement l'attribut commonName. Dans ce cas, la structure du commonName doit permettre d'identifier sans ambiguïté le nom du demandeur du certificat.

Les certificats peuvent contenir d'autres champs ou extensions que ceux définis ci-dessous, en conformité avec la [RFC 5280].

3.1. Socle commun à tous les profils de certificats

<table>
<tr><th>Champ</th><th>Valeur</th></tr>
<tr><td>Version</td><td>2 (=version 3)</td></tr>
<tr><td>Serial number</td><td>Unique pour chaque certificat généré au sein du domaine d'une AC.</td></tr>
<tr><td>Key Size</td><td>Longueur de la clé, conforme aux règles du II.3.4 du présent document.</td></tr>
<tr><td>Issuer DN</td><td>
<table>
<tr><th>Attribut</th><th>Valeur</th></tr>
<tr><td>countryName</td><td>Nom du pays de l'autorité compétente auprès de laquelle le prestataire est officiellement enregistré (tribunal de commerce, ministère, …).</td></tr>
<tr><td>organiszationName</td><td>Nom officiel complet du prestataire tel qu'enregistré auprès des autorités compétentes[11]</td></tr>
<tr><td>organizationIdentifier</td><td>Numéro d'immatriculation officiel du prestataire conformément à [EN_319_412-1] clause 5.1.4.</td></tr>
<tr><td>commonName</td><td>Nom significatif du prestataire ou du service de délivrance de certificats</td></tr>
</table>
</td></tr>
<tr><td>NotBefore</td><td>Date de début de validité du certificat, conformément aux règles des chapitres IV.3.6 et IV.3.7</td></tr>
<tr><td>NotAfter</td><td>Date de fin de validité du certificat, conformément aux règles des chapitres IV.3.6 et IV.3.7</td></tr>
<tr><td>Subject</td><td>Voir les règles applicables à chaque type de certificat, dans les annexes 3.2 et 3.3.</td></tr>
<tr><td>Public Key Algorithm</td><td>Algorithme de clé publique conforme aux règles du II.3.4 du présent document.</td></tr>
<tr><td>Public-Key</td><td>Clé publique.</td></tr>
</table>

Extension	**Obligatoire**	**Critique**	**Valeur**
Basic Constraints	Oui	Non	« *CA:false* »
Certificate Policies	Oui	Non	Identifiant de la Politique de Certification applicable
CRL Distribution Points	Conditionnel	Non	Point de publication des listes de certificats révoqués. En cas d'absence d'un service OCSP : − un point de distribution des LCR est requis ; − le point de publication des LCR doit faire référence à une LCR publiée. Au moins une des LCR publiées doit être accessible selon le

[11] A titre dérogatoire, une représentation non ambigüe du nom officiel du prestataire peut également être utilisée (par exemple, une abréviation reconnue et largement utilisée du nom officiel).

<table>
<tr><td></td><td></td><td></td><td>protocole http ou LDAP.</td></tr>
<tr><td>Authority Information Access</td><td>Oui</td><td>Non</td><td>Renseignement de l’extension « Authority Information Access » :
– accessMethod OID valorisé à « id-ad-caIssuers » ;
– accessLocation valorisé avec le chemin d’accès au certificat de l’AC (URL http de téléchargement du certificat de l’AC).

En complément, si un répondeur OCSP est mis en œuvre :
– accessMethod OID valorisé à « id-ad-ocsp » ;
– accessLocation valorisé avec le chemin d’accès au répondeur OCSP (obligatoire si aucune LCR n’est publiée).</td></tr>
<tr><td>Key Usage</td><td>Oui</td><td>Oui</td><td>Voir les règles applicables à chaque type de certificat, dans les annexes 3.2 et 3.3.</td></tr>
<tr><td>QCStatements</td><td>Oui</td><td>Non</td><td>Cette extension doit être conforme à [EN_319_412-5]
<table>
<tr><th>Extension</th><th>Présente</th><th>Commentaire</th></tr>
<tr><td>esi4-qcStatement-1</td><td>Oui</td><td>Indication que le certificat émis est qualifié, via la valeur “ id-etsi-qcsQcCompliance”.</td></tr>
<tr><td>esi4-qcStatement-2</td><td>Cond.</td><td>Extension optionnelle, décrite dans la norme [EN_319_ 412-5].</td></tr>
<tr><td>esi4-qcStatement-3</td><td>Cond.</td><td>Extension optionnelle, décrite dans la norme [EN_319_ 412-5].</td></tr>
<tr><td>esi4-qcStatement-4</td><td>Cond.</td><td>Voir les règles applicables à chaque type de certificat, dans les annexes 3.2 et 3.3.</td></tr>
<tr><td>esi4-qcStatement-5</td><td>Opt.</td><td>Extension optionnelle, décrite dans la norme [EN_319_ 412-5].</td></tr>
<tr><td>esi4-qcStatement-6</td><td>Oui</td><td>Voir les règles applicables à chaque type de certificat, dans les annexes 3.2 et 3.3.</td></tr>
</table></td></tr>
<tr><td>Subject Alternative Name</td><td>Conditionnel</td><td>Non</td><td>Voir les règles applicables à chaque type de certificat, dans les annexes 3.2 et 3.3.</td></tr>
<tr><td>Subject Key Identifier</td><td>Oui</td><td>Non</td><td>Identifiant de la clé publique contenue dans le certificat.</td></tr>
<tr><td>Authority Key Identifier</td><td>Oui</td><td>Non</td><td>Identifiant de la clé publique de l'AC émettrice.</td></tr>
</table>

3.2. Compléments relatifs aux certificats qualifiés de signature électronique

<table>
<tr><th>Champ</th><th>Valeur</th></tr>
<tr><td>Subject DN</td><td>
<table>
<tr><th>Attribut</th><th>Valeur</th></tr>
<tr><td>countryName</td><td>Nom de pays, spécifiant le contexte général dans lequel les autres attributs doivent être interprétés. Le PSCE doit expliquer dans sa politique de certification la valorisation de cet attribut.</td></tr>
<tr><td>organizationName</td><td>(Obligatoire si le certificat est délivré au porteur dans le cadre de son appartenance à une entité donnée, interdit sinon) Nom officiel complet de l’entité dont dépend le
porteur tel qu'enregistré auprès des autorités compétentes.</td></tr>
<tr><td>organizationIdentifier</td><td>(Obligatoire si le certificat est délivré au porteur dans le cadre de son appartenance à une entité donnée, interdit sinon) Numéro d’immatriculation officiel de l’entité dont
dépend le porteur conformément à [EN_319_412-1] clause 5.1.4.</td></tr>
<tr><td>serialNumber</td><td>(Optionnel) Elément complémentaire permettant de distinguer les homonymes</td></tr>
</table>
En cas d’utilisation de l’état civil du porteur :
<table>
<tr><th>Attribute</th><th>Value</th></tr>
<tr><td>givenName</td><td>Prénom usuel ou prénoms de l’état civil du porteur.</td></tr>
<tr><td>Surname</td><td>Nom de l'état civil ou nom d’usage du porteur</td></tr>
<tr><td>commonName</td><td>Nom complet du porteur tel qu’il devrait être affiché par les applications.
Il est recommandé d’indiquer le prénom usuel, suivi d'un espace, suivi du
nom de l'état civil ou, le cas échéant, du nom d’usage du porteur.</td></tr>
</table>
Ou en cas d’utilisation d’un pseudonyme :
<table>
<tr><th>Attribute</th><th>Value</th></tr>
<tr><td>Pseudonym</td><td>Pseudonyme du porteur</td></tr>
<tr><td>commonName</td><td>Pseudonyme du porteur</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Extension</th><th>Obligatoire</th><th>Critique</th><th>Valeur</th></tr>
<tr><td>Key Usage</td><td>Oui</td><td>Oui</td><td>Usages de clé conformes au chapitre IV.3.5 du présent document : nonRepudiation</td></tr>
<tr><td>QCStatements</td><td>Oui</td><td>Non</td><td>
<table>
<tr><th>Extension</th><th>Présente</th><th>Commentaire</th></tr>
<tr><td>esi4-qcStatement-4</td><td>Cond.</td><td>Indique que la clé privée correspondante est stockée dans un dispositif sécurisé de création de signature électronique.
Valeur « id-etsi-qcs-QcSSCD »</td></tr>
<tr><td>esi4-qcStatement-6</td><td>Oui</td><td>Indication que le certificat est un certificat qualifié de signature électronique.
Valeur « id-etsi-qct-esign ».</td></tr>
</table>
</td></tr>
<tr><td>Subject Alternative Name</td><td>Non</td><td>Non</td><td>Cette extension ne devrait pas être présente.</td></tr>
</table>

3.3. Compléments relatifs aux certificats qualifiés de cachet électronique

<table>
<tr><th>Field</th><th>Value</th></tr>
<tr><td>Subject DN</td><td>
<table>
<tr><th>Attribute</th><th>Value</th></tr>
<tr><td>countryName</td><td>Nom du pays de l'autorité compétente auprès de laquelle l’entité responsable du certificat est officiellement enregistrée (tribunal de commerce, ministère, …).</td></tr>
<tr><td>organizationIdentifier</td><td>Numéro d’immatriculation officiel de l’entité responsable du certificat conformément à [EN_319_412-1] clause 5.1.4</td></tr>
<tr><td>organizationName</td><td>Nom officiel complet de l’entité responsable du certificat, tel qu’enregistré auprès des autorités compétentes</td></tr>
<tr><td>commonName</td><td>Nom significatif du service mettant en œuvre le cachet</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Extension</th><th>Obligatoire</th><th>Critique</th><th>Valeur</th></tr>
<tr><td>Key usage</td><td>Oui</td><td>Oui</td><td>Usages de clé conformes au chapitre IV.3.5 du présent document : digitalSignature et/ou nonRepudiation</td></tr>
<tr><td>qCStatements</td><td>Oui</td><td>Non</td><td>
<table>
<tr><th>Extension</th><th>Présente</th><th>Commentaire</th></tr>
<tr><td>esi4-qcStatement-4</td><td>Cond.</td><td>Indique que la clé privée correspondante est stockée dans un dispositif sécurisé de création de signature électronique (QSCD)
Valeur « id-etsi-qcs-QcSSCD »</td></tr>
<tr><td>esi4-qcStatement-6</td><td>Oui</td><td>Indication que le certificat est un certificat qualifié de signature électronique.
Valeur « id-etsi-qct-eseal ».</td></tr>
</table>
</td></tr>
<tr><td>Subject Alternative Name</td><td>Non</td><td>Non</td><td>Cette extension ne devrait pas être présente</td></tr>
</table>

ANNEXE 6

Référentiel Général d'Accessibilité pour les Administrations de la Polynésie française

RGAA PF

Introduction

Historique des versions		
Date	**Version**	**Évolution du document**
	1.0	Publication de la première version du Référentiel Général d'Accessibilité pour les Administrations de la Polynésie française (RGAA PF)

Introduction au RGAA PF

1. Introduction

1.1 Présentation générale

Le présent référentiel est pris en application des dispositions de l'arrêté relatif à la dématérialisation des actes des autorités administratives et aux téléservices, et des articles LP 34 et suivants de la loi du pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices.

Ce référentiel, à forte dimension technique, offre une traduction opérationnelle des critères d'accessibilité issus des règles internationales ainsi qu'une méthodologie pour vérifier la conformité à ces critères.

Si le réseau Internet et les ressources du Web ne sont pas accessibles aux personnes handicapées et aux personnes âgées, cela constitue un facteur d'exclusion supplémentaire qui peut aggraver une situation de handicap ou des situations de fragilité.

La **Web Accessibility Initiative (WAI)** définit l'accessibilité numérique[1] comme suit :

> « L'accessibilité du Web signifie que les personnes en situation de handicap peuvent utiliser le Web. Plus précisément, qu'elles peuvent percevoir, comprendre, naviguer et interagir avec le Web, et qu'elles peuvent contribuer sur le Web. L'accessibilité du Web bénéficie aussi à d'autres, notamment les personnes âgées dont les capacités changent avec l'âge.
>
> L'accessibilité du Web comprend tous les handicaps qui affectent l'accès au Web, ce qui inclut les handicaps visuels, auditifs, physiques, de parole, cognitifs et neurologiques. »

La principale mission que s'est donnée la WAI est de proposer des solutions techniques pour rendre le Web accessible aux personnes handicapées.

Ces recommandations nommées **règles d'accessibilité pour les contenus Web** ou **WCAG**[2] (pour l'anglais **Web Content Accessibility Guidelines**) émises et actualisées par la WAI constituent aujourd'hui un consensus technique, suivi par les praticiens du domaine et transposées en tant que norme ISO6 depuis le 26 octobre 2012.

1.2 Responsabilité du document

Le RGAA de la Polynésie française (RGAA PF) est une copie adaptée de la version 3.2017 du RGAA de l'Etat.

Le RGAA PF et son contenu sont gérés par la Direction générale de l'économie numérique.

Le présent référentiel ainsi que les annexes sont disponibles en ligne sur le site Internet du service public d'accès au droit en Polynésie française (www.lexpol.pf).

[1] Traduction française de la définition de la WAI. Source : https://www.w3.org/WAI/intro/accessibility.php

[2] Il s'agit des WGAC 2.0, dont vous pouvez consulter la traduction française agréée sur le site du W3C. Source : https://www.w3.org/Translations/WCAG20-fr/

1.3 Organisation du document

Le présent document se découpe comme suit :

- Les WCAG 2.0 et leur traduction : présentation des WCAG 2.0 sur lesquels se base le RGAA ;
- Présentation du référentiel technique avec ses 6 sections :
    - Liste des critères et des tests ;
    - Glossaire ;
    - Cas particuliers ;
    - Notes techniques ;
    - Base de référence ;
    - Références.

Un guide d'accompagnement vient compléter cette introduction.

2. Les règles pour l'accessibilité des contenus Web (WCAG 2.0) et leur traduction

Les règles pour l'accessibilité des contenus Web, qui sont proposées à travers ce référentiel, reposent sur les **WCAG 2.0** (**Web Content Accessibility Guidelines 2.0**), rédigées par la WAI.

Les WCAG 2.0 adoptent une approche thématique proposant 12 règles structurantes selon 4 principes fondamentaux :

2.1 Principe 1 : Perceptible

1. Proposer des équivalents textuels à tout contenu non textuel qui pourra alors être présenté sous d'autres formes selon les besoins de l'utilisateur : grands caractères, braille, synthèse vocale, symboles ou langage simplifié ;
2. Proposer des versions de remplacement aux média temporels ;
3. Créer un contenu qui puisse être présenté de différentes manières sans perte d'information ni de structure (par exemple avec une mise en page simplifiée) ;
4. Faciliter la perception visuelle et auditive du contenu par l'utilisateur, notamment en séparant le premier plan de l'arrière-plan.

2.2 Principe 2 : Utilisable

1. Rendre toutes les fonctionnalités accessibles au clavier ;
2. Laisser à l'utilisateur suffisamment de temps pour lire et utiliser le contenu ;
3. Ne pas concevoir de contenu susceptible de provoquer des crises ;
4. Fournir à l'utilisateur des éléments d'orientation pour naviguer, trouver le contenu et se situer dans le site.

2.3 Principe 3 : Compréhensible

1. Rendre le contenu textuel lisible et compréhensible ;
2. Faire en sorte que les pages apparaissent et fonctionnent de manière prévisible ;
3. Aider l'utilisateur à éviter et à corriger les erreurs de saisie.

2.4 Principe 4 : Robuste

1. Optimiser la compatibilité avec les agents utilisateurs actuels et futurs, y compris les technologies d'assistance.

La version des WCAG sur laquelle s'appuie le RGAA PF est la version WCAG 2.0 du 11 décembre 2008.

L'Association BrailleNet a coordonné le travail de traduction pour la version en français. La traduction française des WCAG 2.0 a été validée le 24 avril 2009 comme traduction autorisée par le comité francophone de traduction et a été agréée par le W3C le 25 juin 2009.

Cette traduction est disponible à l'adresse suivante :
http://www.w3.org/Translations/WCAG20-fr/

Vous y trouverez également traduite la liste des critères de succès qui ont une portée normative.

3. Le référentiel technique

3.1. Généralités

Le référentiel technique du RGAA PF est une reproduction du référentiel technique de l'Etat, dont la licence Licence Ouverte autorise la reproduction, la redistribution, l'adaptation, à condition de citer la paternité du document original.

Ce référentiel technique s'appuie lui-même sur le référentiel AccessiWeb de l'association BrailleNet dont la licence d'utilisation autorise d'en faire des copies modifiées à condition de citer la source du document original.

La version 1 du RGAA PF est donc une version adaptée du référentiel AccessiWeb HTML5/ARIA dans sa version de travail.

Le référentiel technique du RGAA PF est un document unique composé de cinq sections.

Ce document ou un lien vers celui-ci est à inclure en annexe du cahier des charges de toute opération de mise en œuvre ou de refonte de contenus web.

3.2. Liste des critères

Les critères de succès WCAG ont été traduits de façon opérationnelle sous la forme d'une liste de critères et de tests à respecter.

La méthodologie associée à ce nouveau référentiel est structurée selon les règles suivantes :

- Un critère ou un test pose une question ;
- Un critère ou un test ne pose qu'une question et n'attend qu'une réponse (note : pour un test cette règle peut avoir certaines exceptions) ;
- Lorsque la réponse est positive cela signifie que le critère est conforme ;
- Un critère est lié à un ou plusieurs critères WCAG dont le niveau est alors déduit du niveau WCAG le plus bas ;

- Un test ou une condition de test est lié à une technique WCAG ou à un élément de la spécification HTML (ou des notes associées) au moins.

La liste des critères est précédée d'un mode d'emploi expliquant comment utiliser le référentiel dans un contexte technique basé sur une version antérieure à HTML5.

La liste des critères est structurée en 13 thématiques :

1. Images
2. Cadres
3. Couleurs
4. Multimédia
5. Tableaux
6. Liens
7. Scripts
8. Éléments obligatoires
9. Structuration de l'information
10. Présentation de l'information
11. Formulaires
12. Navigation
13. Consultation

Pour chaque thématique, un encart introductif indique :

- Le ou les principes WCAG associés à la thématique parmi les quatre disponibles : perceptible, utilisable, compréhensible, robuste ;
- La recommandation générale d'accessibilité sous la forme d'une ou deux phrases résumant les objectifs de la thématique.

Puis vient la liste des critères qui peut être affichée selon deux vues : une liste générale des critères, et une liste détaillée avec les tests permettant de vérifier si le critère est satisfait.

Pour chaque critère se trouve le numéro du critère, le niveau WCAG auquel il est rattaché (A, double A ou triple A) et l'intitulé du critère sous la forme d'une question.

Dans la vue détaillée, vient ensuite l'encart technique avec la liste des tests qui énumère les techniques permettant de vérifier que le critère est respecté et le lien vers les notes techniques associées s'il y a lieu.

Enfin, un encart énumère les correspondances entre le référentiel technique du RGAA PF et les règles internationales WCAG 2.0 de la façon suivante :

- La liste des critères de succès WCAG 2.0 (volet normatif) attachés au critère RGAA PF ;
- La liste des techniques suffisantes et échecs (volet non-normatif) de WCAG 2.0 associés aux tests RGAA PF.

3.3. Glossaire

Pour préciser et aider à la compréhension du référentiel technique, un glossaire permet de définir certains termes.

Chaque terme défini dans le glossaire est lié directement depuis la liste des critères. Les définitions font partie intégrante du référentiel et ont une valeur normative.

3.4. Cas particuliers

Plusieurs critères RGAA PF font référence à des cas particuliers permettant de préciser l'objectif du critère et la façon dont il doit être appliqué en excluant les cas qui ne relèvent pas de l'application dudit critère. Ce document liste l'ensemble des cas particuliers pour lesquels le critère concerné est non applicable.

3.5. Notes techniques

Les notes techniques donnent des explications pour la prise en charge de certains éléments HTML5 dont le support peut être variable et la manière dont le référentiel propose de les prendre en charge.

3.6. Base de référence

Avec l'arrivée de nouvelles technologies dont le support est variable selon les navigateurs, et la multiplication des plateformes de consultation, il n'est plus possible de faire une même interface qui soit à la fois moderne et accessible de façon universelle.

Or, l'accessibilité nécessite de faire des tests pour vérifier que le code produit est compatible avec les technologies utilisées par les personnes handicapées.

Le document « Base de référence » recense un ensemble de technologies sur lesquels il est requis de faire des tests pour assurer l'accès aux contenus par le plus grand nombre. Cette base de référence est applicable pour tout contenu soumis à la consultation du grand public ou lorsqu'il n'est pas possible de savoir quels outils seront utilisés pour accéder aux contenus (système d'exploitation, navigateur, technologie d'assistance).

Lorsque le site ou l'application est destinée à un public dont l'équipement est maîtrisé, les tests devront se faire sur une base de référence adaptée au contexte de l'environnement maîtrisé.

3.7. Références

Le référentiel technique du RGAA PF a été établi en utilisant un certain nombre de références et de sources documentaires. Le document « références » liste les références qui ont été utilisées.

ANNEXE 6 Bis

Référentiel Général d'Accessibilité pour les Administrations de la Polynésie française

RGAA PF

Guide d’accompagnement

Historique des versions		
Date	**Version**	**Évolution du document**
	1.0	Publication de la première version du guide d'accompagnement du Référentiel Général d'Accessibilité pour les Administrations de la Polynésie française (RGAA PF)

Sommaire :

1. Organisation du guide d'accompagnement

Le présent guide d'accompagnement est organisé en trois parties : l' « avant-propos », le « cadre d'accessibilité » et le « guide d'application du RGAA PF ».

Pour mémoire, le RGAA PF représente un ensemble cohérent de documents. Il est composé de trois documents :

- Le document « Introduction au RGAA PF » ;
- Le présent « Document d'accompagnement » ;
- Le « Référentiel technique », lui-même composé de 6 sections :
    - Liste des critères et des tests ;
    - Glossaire ;
    - Cas particuliers ;
    - Notes techniques ;
    - Base de référence ;
    - Références.

1.1. Avant-propos : problématique et vue d'ensemble du RGAA PF

L'avant-propos introduit la problématique de l'accessibilité et présente une vue d'ensemble du RGAA PF. Il vise à apporter des réponses concrètes à certaines questions qui peuvent se poser, sous forme de questions/réponses.

Il s'adresse en priorité aux décideurs et responsables des autorités administratives.

1.2. Cadre d'accessibilité : contexte, démarche et évolution du RGAA PF

Le cadre d'accessibilité présente le contexte qui a amené à élaborer le RGAA PF, ainsi que les principes adoptés pour sa conception, son évolution et le périmètre de ce document.

Il s'adresse aux directions et aux maîtrises d'ouvrage des autorités administratives œuvrant dans les domaines de l'organisation et des systèmes d'information.

1.3. Guide d'application du RGAA PF

Cette partie décrit les modalités d'application du RGAA PF : son périmètre d'application, les actions à mettre en œuvre dans le cadre d'une mise en accessibilité, la vérification de conformité des contenus et la déclaration de conformité.

Il s'adresse plus particulièrement aux chefs de projet, architectes et développeurs travaillant sur des projets Web relatifs à l'administration électronique.

2. Avant-propos : Problématique et vue d'ensemble du RGAA PF

Le RGAA PF (Référentiel général d'accessibilité pour les administrations de la Polynésie française) a pour objectif de qualifier l'accessibilité des contenus et applications des téléservices présentés sous forme numérique et consultables à travers un navigateur Web, quel que soit le support.

Dans sa version actuelle, il guide les autorités administratives dans l'adoption et la mise en œuvre de bonnes pratiques assurant l'accessibilité de ces contenus Web, quelles que soient leurs aptitudes physiques ou mentales. Pour ce faire, il met à disposition un référentiel technique permettant de vérifier le respect effectif des normes et de mesurer la conformité des contenus Web des téléservices au regard des standards internationaux.

2.1. Déficiences, incapacité et handicap : une question de contexte

L'Organisation mondiale de la santé, dans sa première définition de 1980[1], faisait une distinction entre les notions de déficience, d'incapacité et de handicap.

Les déficiences sont des écarts de fonctionnement d'un organe ou d'un sens par rapport au fonctionnement normal de cet organe. Les principales déficiences sont de trois types :

- Sensorielles ;
- Mentales ;
- Motrices.

Ces déficiences peuvent conduire à des incapacités, c'est-à-dire des impossibilités pour la personne déficiente de faire certaines actions.

Le handicap se définit quant à lui comme la perte ou la restriction pour un individu de participer à la vie de la collectivité à égalité avec les autres. La traduction française de la classification internationale du handicap parlait de « désavantage ».

Cette première définition, bien qu'intéressante, était insatisfaisante car elle centrait la problématique sur l'individu. La dernière définition de l'OMS, qui date de 2001[2], emploie « handicap » comme un terme générique pour les déficiences, les limitations de l'activité et restrictions à la participation. Le handicap est décrit comme l'interaction entre des sujets présentant une affection médicale et des facteurs personnels et environnementaux.

Le handicap est directement lié à un contexte, par exemple :

- Une personne paraplégique a une déficience motrice. Cette déficience n'induit pas obligatoirement de handicap pour se servir d'un ordinateur si seul le bas du corps est touché, mais induit un handicap pour accéder à certains bâtiments ou moyens de transport.

[1] Source : International classification of Impairments, Disabilities and Handicaps (OMS, 1980) – Lien : http://apps.who.int/iris/bitstream/10665/41003/1/9241541261_eng.pdf

[2] Définition issue de la classification internationale du fonctionnement, du handicap et de la santé.

- Certaines personnes déficientes auditives seront handicapées sans appareillage pour communiquer par téléphone, mais ne seront pas handicapées si elles savent lire et peuvent communiquer par courrier électronique ou SMS.
- Une personne sourde pratiquant la langue des signes est handicapée dans une assemblée d'entendants et, à l'inverse, une personne entendante est également handicapée dans une assemblée de personnes sourdes qui utilisent la langue des signes.

Tous les êtres humains peuvent être déficients à un moment ou à un autre de leur existence. Ces déficiences peuvent être présentes dès la naissance, mais également arriver plus tardivement et être liées à des maladies, à des accidents, à l'âge.

2.2. Le défaut d'accessibilité, générateur d'exclusion

C'est souvent un défaut d'accessibilité qui met le mieux en évidence le concept et l'intérêt de l'accessibilité.

Lorsqu'on met en place une application, un téléservice, si le dispositif n'est pas accessible, il créera de fait une inégalité de traitement entre les usagers pouvant y accéder et ceux ne le pouvant pas.

Dans la vie de tous les jours, le manque d'accessibilité de bâtiments publics ou privés par le simple fait de n'avoir que des escaliers comme seul moyen d'accès est l'un des exemples les plus flagrants de l'inégalité d'accès à une information ou un service qui existe entre des personnes présentant un handicap ou âgées et des personnes ne présentant pas de handicap.

Le défaut d'accessibilité existe aussi dans le monde des systèmes d'information. La mise en œuvre d'interfaces utilisateurs est souvent l'occasion d'observer des lacunes d'accessibilité notamment par l'absence de solutions alternatives pour pallier à diverses déficiences visuelles, auditives, motrices ou cognitives. Le contenu Web via les téléservices est particulièrement concerné puisqu'il met en œuvre de nombreux modes de diffusion (texte, audio, vidéo).

2.3. Comment résoudre un défaut d'accessibilité ?

Pour améliorer l'accessibilité, il est indispensable de prendre en compte l'ensemble des handicaps et de mettre en œuvre des normes et standards permettant d'améliorer l'accessibilité, et le cas échéant, des solutions alternatives permettant de mettre à disposition un même niveau d'information et des fonctionnalités similaires pour l'ensemble de la population.

Il ne s'agit pas de développer des solutions techniques spécifiques mais de permettre à toutes et à tous d'accéder aux mêmes contenus et fonctionnalités, quelle que soit la façon pour les utilisateurs du service d'utiliser l'ordinateur (au clavier seulement – sans souris –, avec des technologies spécifiques comme un clavier virtuel, un lecteur d'écran couplé à une plage braille…).

2.4. Domaine d'application du RGAA PF

Le RGAA PF met en œuvre un certain nombre de règles et standards et propose un ensemble de tests permettant de s'assurer de la conformité des contenus Web des téléservices aux dites règles.

2.5. Rendre le Web plus accessible

Des travaux ont été engagés sur le plan international pour améliorer l'accessibilité des contenus Web, avec l'initiative pour l'accessibilité du Web (**Web Accessibility Initiative - WAI**) lancée en 1999 par le **World Wide Web Consortium** (**W3C**).

La principale mission que s'est donnée la WAI est de proposer des solutions techniques pour rendre le Web accessible aux personnes handicapées. Ces recommandations nommées « **règles d'accessibilité pour les contenus Web** » ou **WCAG**[3] (pour l'anglais **Web Content Accessibility Guidelines**) émises et actualisées par la WAI constituent aujourd'hui un consensus technique, suivi par les praticiens du domaine et transposées en tant que norme ISO6 depuis le 26 octobre 2012.

Portant sur des technologies en constante évolution, le RGAA PF est un document vivant et qui devra connaître des actualisations régulières. La présente version expose l'état actuel des questions sur l'accessibilité des contenus Web via un téléservice.

Elle est destinée à appuyer les autorités administratives dans leurs choix stratégiques et techniques à travers la mise à disposition d'un référentiel technique comprenant une liste précise de critères d'accessibilité et de tests.

2.6. La chaîne de responsabilité de l'accessibilité numérique

Les règles techniques pour rendre des contenus numériques accessibles sont rarement complexes. La difficulté tient davantage au fait que l'accessibilité numérique ne peut se réaliser sans la participation de tous les acteurs impliqués dans la création, le maintien et l'utilisation des dispositifs numériques. Chaque acteur a ainsi une responsabilité à assumer.

2.6.1. La Polynésie française

Le rôle de la Polynésie française est de garantir l'accessibilité des téléservices mis en œuvre par une autorité administrative de la Polynésie française.

2.6.2. Donneur d'ordre - maîtrise d'ouvrage

La maîtrise d'ouvrage a un rôle de décision. Elle doit fixer comme prioritaire la livraison de produits conformes à la législation et non discriminants.

Le respect du RGAA PF doit faire l'objet d'une demande explicite dans tout cahier des charges concernant le choix d'un équipement numérique (site Web, application métier, logiciel en ligne…). Cette exigence doit faire partie des critères de sélection d'un candidat.

De même que le donneur d'ordre a la responsabilité de s'assurer que le produit livré est conforme au besoin exprimé, il a la responsabilité de vérifier l'accessibilité du produit livré. À charge pour lui de vérifier ou faire vérifier que les règles sont respectées.

Par ailleurs, en cas d'exigences contradictoires, il a le devoir d'arbitrer en faveur de l'accessibilité. Cela se traduit notamment par le fait de ne pas exiger de choses impossibles à rendre accessible ou d'accepter des compromis permettant de donner accès à tous aux mêmes contenus et fonctionnalités similaires sous une autre forme.

[3] Il s'agit des WCAG 2.0, dont vous pouvez consulter la traduction française agréée à l'adresse suivante : https://www.w3.org/Translations/WCAG20-fr/

Par exemple, si une charte graphique est imposée par le donneur d'ordre. Soit il s'assure en amont que cette charte est suffisamment contrastée, soit il accepte que soit proposée en plus de la charte graphique originale une version alternative avec des contrastes renforcés conforme aux exigences du RGAA PF.

Afin de s'assurer que le travail livré est conforme, il est vivement recommandé de confier la vérification de la conformité aux règles à un expert indépendant du service ou de l'organisme ayant réalisé l'ouvrage pour éviter les conflits d'intérêts. Cet expert peut être un membre formé de l'administration n'ayant pas directement travaillé sur le projet ou un prestataire extérieur.

2.6.3. Maîtrise d'œuvre

La maîtrise d'œuvre réalise le site, l'application ou le logiciel commandé.

Elle a le devoir de se former, voire de se faire accompagner si nécessaire, et de prendre en compte les règles d'accessibilité. Il est de sa responsabilité de livrer un travail conforme au RGAA PF.

En tant que professionnel ayant les connaissances utiles à l'appréciation des enjeux techniques, elle a le devoir d'alerter la maîtrise d'ouvrage si elle détecte des contraintes techniques insurmontables pour l'accessibilité ou nécessitant des compromis dans la conception ou les choix opérés.

2.6.4. Responsables éditoriaux

Dans le cas de contenus éditoriaux en ligne adossés à des téléservices, la mise à jour est souvent l'œuvre de plusieurs contributeurs pas nécessairement tous parfaitement formés. Le responsable éditorial a le devoir de former les contributeurs ou de mettre en place un dispositif pour prendre en compte l'accessibilité dans la mise à disposition de nouveaux contenus.

2.6.5. Utilisateurs et utilisatrices des services en ligne sur Internet

Cette section concerne uniquement les personnes accédant à un service en ligne sur Internet et pour lesquels il n'est pas possible de connaître précisément la configuration des outils donnant accès à Internet (système d'exploitation, navigateur, technologie d'assistance). En parallèle de la mise aux normes des contenus et fonctionnalités de ses services en ligne par l'administration, il est nécessaire que les utilisateurs mettent à jour leur navigateur et leur technologie d'assistance pour bénéficier des avancées techniques en matière d'accessibilité.

Par ailleurs, toute personne constatant un défaut d'accessibilité doit être en mesure de le signaler à l'administration concernée pour l'alerter et lui donner l'occasion d'améliorer l'accessibilité.

2.7. Questions - réponses

Cette section constitue une synthèse permettant de répondre aux questions pouvant se poser concernant l'application du RGAA PF.

2.7.1. Qu'est-ce que le RGAA PF ?

Le RGAA PF a pour objectif d'encadrer l'accessibilité des téléservices proposés par une autorité administrative relevant de la Polynésie française.

Dans sa version actuelle il constitue un référentiel de vérification du respect des standards internationaux WCAG 2 0.

Il a pour objectif de proposer des critères et des tests vérifiant que les règles d'accessibilité sont respectées.

Il ne constitue pas une nouvelle norme ou un nouveau standard mais offre une méthodologie et un cadre opérationnel pour permettre la vérification de la mise en œuvre des standards internationaux d'accessibilité.

2.7.2. Qui est concerné par l'obligation de mise aux normes ?

La loi du pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des autorités administratives et aux téléservices indique que sont concernés les téléservices mis en œuvre par une autorité administrative relevant de la Polynésie française.

2.7.3. Quels sont les documents du RGAA PF légalement opposables ?

Tous les documents du RGAA PF sont opposables, c'est-à-dire l'introduction au RGAA PF, le document d'accompagnement et le référentiel technique avec ses 5 parties.

2.7.4. Quel est le niveau d'accessibilité exigé ?

Le niveau attendu est le niveau double A (AA).

2.7.5. Quel est le délai de mise en conformité ?

Le délai de mise en conformité est de 3 ans.

2.7.6. En plus de la mise en conformité du site ou de l'application, y a-t-il des documents à publier pour remplir l'obligation légale ?

Deux documents[4] sont attendus :

- Une page d'aide à destination des utilisateurs, rédigée dans un langage non technique, pour les informer du niveau d'accessibilité de l'application ou des contenus et les aider à s'orienter. Cette page d'aide doit mentionner les coordonnées d'un contact au sein de l'administration en cas de difficulté ;
- Une déclaration de conformité, destinée à l'administration, qui fait état du niveau précis de conformité au RGAA PF et des dérogations déclarées et justifiées.

2.7.7 Quels sont les canaux traités par le RGAA PF ?

Dans sa version actuelle, il ne traite que l'accessibilité des applications et contenus Web d'un téléservice consultables depuis un navigateur Web.

[4] Des modèles de ces documents seront proposés au sein d'une section « ressources ». Cette section, non normative, fournira différents types de ressources administratives, techniques et pédagogiques pour accompagner les employeurs publics dans leurs démarches.

2.7.8 Le RGAA PF concerne-t-il aussi les applications mobiles ?

Les téléservices consultables depuis un navigateur Web sur un smartphone sont concernés.

En revanche, bien que les critères du référentiel technique soient applicables à de nombreux contenus au-delà des contenus Web, aucun test ne couvre les applications mobiles. Le RGAA PF est en effet une transposition des WCAG 2.0 pour lesquels aucune technique spécifiquement dédiée aux applications mobiles n'est prévue.

Des ressources complémentaires au RGAA PF, non normatives, seront mises à disposition pour améliorer l'accessibilité des contenus Web sur les plateformes mobiles.

2.7.9 Le RGAA PF est-il applicable pour rendre les postes de travail accessibles ?

Non, le référentiel technique du RGAA PF concerne uniquement les applications et contenus d'un téléservice disponibles via un navigateur Web. Cela inclut les applications métiers disponibles via ce canal, mais pas les logiciels en environnement de bureau.

2.7.10 Le RGAA PF impose-t-il des solutions techniques ?

La composante normative des WCAG, les critères de succès, a été pensée pour être indépendante de toute technologie afin d'assurer une compatibilité des recommandations avec les technologies actuelles et futures. C'est à la fois ce qui assure sa pérennité et ce qui rend son utilisation peu pratique car peu opérationnelle.

Les critères du référentiel technique du RGAA PF ne réfèrent pas non plus à une technologie, mais les tests associés visent explicitement des techniques d'implémentation servant à vérifier que le critère est respecté. Le travail de test pour vérifier la compatibilité avec l'accessibilité est ainsi en partie supporté par le référentiel, ce qui le rend particulièrement opérationnel mais nécessitera des mises à jour régulières pour intégrer les nouvelles techniques qui verront le jour (cf. les plateformes mobiles).

Les critères et les tests du référentiel technique RGAA PF sont normatifs. Toutefois, en cas d'absence de mise à jour du RGAA PF sous 2 ans pour prendre en compte de nouvelles techniques WCAG mises à disposition par le W3C, il est autorisé de créer ses propres tests en complément de ceux existant, à condition d'assurer la compatibilité avec les critères du référentiel technique et avec les technologies mentionnées dans la base de référence.

2.7.11. Le RGAA PF est-il exhaustif dans ses préconisations ?

Le RGAA PF propose un ensemble de critères techniques permettant d'assurer l'accessibilité des applications et contenus Web d'un téléservice. Toutefois, l'évolution des technologies et des outils les exploitant ne permet pas d'être totalement exhaustif dans les recommandations effectuées. C'est pour cette raison qu'il fera l'objet de mises à jour régulières.

2.7.12. Est-il autorisé d'utiliser un autre référentiel technique que celui préconisé par le RGAA PF pour vérifier la conformité aux WCAG 2.0 ?

L'usage d'un autre référentiel est autorisé, à une triple condition :

1. S'assurer qu'il est compatible avec le référentiel technique du RGAA PF ;
2. Produire une table de correspondance explicite entre les critères et tests du référentiel alternatif et ceux du référentiel technique du RGAA PF en vigueur ;
3. Produire une déclaration de conformité basée sur le référentiel technique du RGAA PF.

2.7.13. Quels sont les coûts liés à la mise aux normes d'accessibilité pour un dispositif numérique ?

De façon générale, lorsque la prise en compte de l'accessibilité est faite en amont, le coût est transparent, le temps passé étant lissé dans les différentes tâches inhérentes au projet. Ce cas général est à nuancer lorsque le site propose des contenus spécifiques nécessitant des aménagements particuliers (vidéos, mise à disposition de nombreux documents en téléchargement dont la production n'est pas maîtrisée…).

Le coût le plus important reste cependant celui du changement lorsque l'accessibilité n'a jamais été prise en compte. Dans ce cas, la démarche accessibilité peut nécessiter un effort et représenter un coût quelquefois non négligeable, extrêmement dépendant du contexte.

1. **Formation et communication** : selon le niveau initial des développeurs, graphistes, rédacteurs, ainsi que la nature des outils de production utilisés, il est quelquefois nécessaire de mettre en place des actions de sensibilisation et de formation permettant à tous les acteurs impliqués de connaître les bases de la démarche accessibilité. Il est également nécessaire de veiller à ce que l'ensemble des acteurs internes et externes soient informés des impératifs et des principes de l'accessibilité numérique ;
2. **Conseil et assistance** : le respect des règles d'accessibilité nécessite très fréquemment des arbitrages. Cette expertise peut également être nécessaire pour la production des cahiers des charges ou leur exploitation. Ces arbitrages se font généralement au cas par cas, et peuvent mobiliser une expertise interne ou externe ;
3. **Temps de développement et de mise en conformité** : la reprise des pages existantes pour la mise en conformité peut représenter une charge importante. Même si c'est plus rare, le temps initial de développement de pages accessibles peut également représenter un surcoût par rapport au développement des mêmes pages sans préoccupation spécifique en matière d'accessibilité. Bien que ce ne soit pas le cas le plus fréquent, cette étape peut nécessiter la production de contenus spécifiquement dédiés à l'accessibilité, notamment pour les vidéos (sous-titrage, transcription ou audiodescription par exemple) ;
4. **Recettes, audit, suivi** : les contenus des sites de grande ampleur sont très fréquemment actualisés. De nouvelles pages sont régulièrement mises en ligne et le contenu des pages existantes est régulièrement modifié. Chaque modification peut faire apparaître de nouvelles erreurs. Il est donc nécessaire d'introduire dans le processus de production et de maintenance des étapes de test, de recette, ou de validation des contenus produits ou mis à jour, ce qui peut représenter un coût supplémentaire, ou être intégré au processus de recette continu s'il existe ;
5. **Déclaration de conformité** : l'entité responsable du téléservice devra prévoir de publier une déclaration de conformité. Ceci suppose qu'un audit ait été fait, de préférence par un expert indépendant pouvant faire partie de l'administration ou d'une société privée tierce.

3. Partie 1 : Cadre d'accessibilité : Contexte, démarche et évolution du RGAA PF

3.1. Contexte et environnement

3.1.1. Les enjeux

3.1.1.1. La diversité des publics

Si le réseau Internet et les ressources du Web ne sont pas accessibles aux personnes handicapées et aux personnes âgées, cela constitue un facteur d'exclusion supplémentaire qui peut aggraver une situation de handicap ou des situations de fragilité.

De nombreux utilisateurs peuvent être amenés à opérer dans des contextes très différents de celui de l'internaute moyen :

- Ils peuvent ne pas être en mesure de voir, entendre, se mouvoir ;
- Ils peuvent avoir des difficultés à lire ou à comprendre le contenu textuel ;
- Ils peuvent être dans l'impossibilité d'utiliser un clavier ou une souris ;
- Ils peuvent être sujets à des crises d'épilepsie déclenchées par des animations ;
- Ils peuvent être dans l'incapacité de réaliser des tâches dans une limite de temps ou être perturbés par un environnement dont ils ne maîtrisent pas les changements.

Notons que les règles d'accessibilité du Web visent à rendre une même interface accessible à chacun quelles que soient ses capacités, en évitant la multiplication des supports, dans un esprit de conception universelle.

Or, la prise en compte du handicap intellectuel nécessite souvent de produire une version alternative des textes pour les simplifier, selon la méthode « Facile À Lire et à Comprendre »[5].

La prise en compte du handicap intellectuel consiste à faire simple tant sur le fond que sur la forme, ce qui peut s'avérer fort utile à tous les internautes :

- Penser ses contenus textuels dans un langage simple, utilisant des phrases courtes, des mots simples, des sigles explicités ;
- Illustrer les contenus avec des exemples concrets, des visuels explicites en rapport avec le sujet ;
- Structurer les pages et le texte dans un ordre logique et chronologique ;
- Privilégier la lisibilité et la clarté du texte par rapport aux effets graphiques ;
- Utiliser une mise en page claire et aérée faisant ressortir l'information essentielle.

Pour aller au-delà de la recommandation (double A), et s'assurer d'une véritable accessibilité de l'information textuelle, il est recommandé de se reporter à la méthode européenne du Facile à lire et à comprendre qui regroupe l'ensemble des préconisations pour écrire et présenter des informations faciles à lire et à comprendre.

3.1.1.2. La diversité des technologies

Au delà des capacités humaines, l'accélération des évolutions techniques a entraîné une diversité croissante des technologies permettant d'accéder au Web. Les utilisateurs peuvent ainsi être équipés très diversement :

[5] Note : Pour en savoir plus sur la méthode FALC, vous pouvez consulter le Guide du langage Facile à Lire et à Comprendre (PDF), disponible sur le site de l'UNAPEI à l'adresse suivante : http://www.unapei.org/IMG/pdf/Guide_ReglesFacileAlire.pdf

- Ils peuvent avoir un ordinateur de bureau doté des dernières versions de système d'exploitation, de navigateur et une technologie d'assistance à jour, ou des versions plus anciennes ;
- Ils peuvent se rendre sur Internet depuis un smartphone, une tablette ou un ordinateur portable ou de bureau, avec des systèmes d'exploitations et des navigateurs d'une grande variété ;
- Ils peuvent avoir un écran n'affichant que le texte, qu'un nombre réduit de couleurs, de petite taille ou avec une résolution particulière ;
- Ils peuvent avoir une version ancienne d'un logiciel de consultation, un logiciel entièrement différent de celui sur lequel les tests ont été faits, ou un système d'exploitation différent de ceux couramment utilisés ;
- Ils peuvent être amenés à se connecter depuis des terminaux mobiles, et accéder aux services en ligne en bas-débit ou avec des écrans de petite taille.

3.1.1.3. L'adaptation des contenus

Pour reprendre les quatre grands principes définis dans les règles internationales d'accessibilité des contenus Web, l'adaptation des contenus Web consiste à rendre les contenus perceptibles, compréhensibles, robustes et utilisables :

- Soit par la mise à disposition des contenus sous des formes utilisables dans certains contextes : le sous-titrage d'un film pour une personne déficiente auditive, un fichier son décrivant les textes affichés dans le film pour une personne déficiente visuelle…
- Soit par les technologies d'assistance permettant de restituer le contenu sous une forme perceptible par la personne (exemple : logiciel de lecture d'écran et restitution vocale des contenus).

Très souvent, c'est la combinaison de ces deux types de solution qui permettra aux utilisateurs d'accéder aux contenus.

Le respect des normes et standards de développement Web publiées par le **W3C** (**World Wide Web Consortium**) et la conformité technique des pages Web pourront grandement faciliter l'accès à de nombreux contenus pour toutes et tous, notamment les personnes handicapées et certaines personnes valides navigant dans des contextes variés.

Dans de très nombreux cas, la conformité technique sera toutefois largement insuffisante. C'est notamment le cas lorsque la nature du contenu le rend imperceptible par certaines personnes. Dans ce cas, il faudra prévoir des contenus de substitution, appelés aussi contenus alternatifs ou plus simplement « alternatives ».

Exemple : les équivalents textuels pour les images

Une personne non-voyante utilisera par exemple un logiciel appelé lecteur d'écran qui, couplé à une synthèse vocale ou une plage braille, restituera les informations disponibles. Or, si le texte est un contenu compatible avec les technologies d'assistance qui peuvent le traiter et le restituer à l'utilisateur, ce n'est pas le cas des images. Il est donc nécessaire de fournir un texte alternatif pour renseigner les personnes qui ne peuvent pas percevoir le sens véhiculé par l'image lorsque cette dernière apporte une information non présente dans le contexte. Ce recours, qui n'a de valeur ajoutée que lorsque l'image véhicule effectivement un sens, est un des éléments nécessaires pour qu'une page qui comporte des images signifiantes soit accessible.

Outre le bénéfice qu'en retirent les utilisateurs de lecteurs d'écran, ces alternatives sont également nécessaires pour certaines personnes en situation de handicap moteur. Une image sans alternative textuelle empêchera un logiciel de dictée vocale de repérer cette image puisqu'il se fie à l'alternative textuelle pour les identifier. En conséquence, une personne en situation de handicap moteur, qui ne peut utiliser ni clavier ni souris, ne pourra pas activer une image lien sans équivalent textuel.

À noter que les équivalents textuels peuvent également aider au référencement des pages d'un site puisque les robots de recherche peuvent utiliser ce texte quand ils indexent ces pages.

3.1.2. L'administration en ligne

Pour assurer l'accès aux services et informations mis en œuvre par le développement de l'administration en ligne, les autorités administratives doivent proposer des téléservices à l'ensemble de la population, quelles que soient ses aptitudes. Cet environnement doit également garantir les éléments suivants :

- Sécuriser l'accès à l'information et aux services ;
- Assurer la compatibilité avec les technologies d'assistance utilisées par les personnes handicapées (lecteurs d'écran, claviers virtuels, trackball…) ;
- Proposer des solutions alternatives pour les contenus non ou difficilement perceptibles.

Tous ces éléments contribuent à apporter des solutions nécessaires au développement de l'administration électronique, au sein des administrations, entre les administrations et les entreprises, ainsi qu'entre les administrations et les usagers.

Afin d'assurer une accessibilité maximale pour les applications et contenus Web des téléservices, il est nécessaire de respecter un ensemble de règles et de s'assurer que l'implémentation de ces règles fonctionne effectivement sur les technologies dont se servent les utilisateurs finaux, qu'ils soient en situation de handicap ou non. Le RGAA PF a été élaboré pour répondre à cette préoccupation.

3.2. Démarche adoptée

La méthode retenue est de favoriser le développement de l'accessibilité numérique en mettant en place un cadre de référence clair, pratique, opérationnel et pragmatique.

Le RGAA PF repose sur les principes suivants :

- Le document doit pouvoir être utilisé dans différents contextes (management, déploiement, formation, gestion de projet, développement, audit…). Des ressources non normatives associées à sa compréhension seront mise à disposition pour faciliter sa prise en main ;
- Le document s'appuie le plus strictement possible sur le standard international WCAG 2.0 et ses différents documents de déploiement ;
- Le RGAA PF concerne l'ensemble des autorités administratives ; aussi, le niveau d'exigence traduit dans les critères de succès du RGAA PF doit être adapté à l'ensemble des autorités administratives.

3.3. Modalités d'évolution du document

3.3.1. Évolution du document

Le RGAA PF est approuvé et modifié par arrêté pris en conseil des ministres.

Le RGAA PF est publié sur un site Web public, afin qu'il soit consultable par tous.

Des mises à jour régulières interviendront, afin de tenir compte des évolutions des technologies liées à l'accessibilité et des usages des autorités administratives.

Sa mise à jour est assurée par la Direction générale de l'économie numérique.

En cas d'absence de mise à jour du RGAA PF sous 2 ans pour prendre en compte de nouvelles techniques WCAG mises à disposition par le W3C, il est autorisé de créer ses propres tests en complément de ceux existant, dans les conditions définies ci-dessous.

3.3.1.1. Gestion des tests créés hors du cadre du RGAA PF en cas d'absence de mise à jour

3.3.1.1.1. Conditions de création de tests non prévus par le RGAA PF

Il y a trois conditions concernant la création de nouveaux tests non définis par la version applicable du RGAA PF en vigueur :

- L'absence de mise à jour du RGAA PF alors que les techniques WCAG ont été mises à jour entraîne des problèmes d'application de la norme ;
- La mise à jour des WCAG est intervenue depuis 2 ans au moins sans que le RGAA PF n'est été mis à jour ;
- Les nouveaux tests créés doivent assurer la compatibilité avec les critères du référentiel technique du RGAA PF et avec les technologies mentionnées dans la base de référence.

3.3.1.1.2. Traçabilité et documentation des tests créés en dehors du RGAA PF

Tout nouveau test doit être référencé dans une section dédiée intitulée « Tests créés hors du cadre RGAA PF » de la déclaration de conformité. Cette section doit lister les nouveaux tests créés, les critères du RGAA PF auxquels ils se rattachent, et les correspondances avec les critères de succès et techniques WCAG (avec un lien vers ces techniques).

La date de création de ces tests doit également être mentionnée.

3.3.1.1.3. Priorité à l'interprétation officielle du RGAA PF

Considérons le cas où de nouveaux tests auraient été créés en l'absence de mise à jour du RGAA PF prenant en charge de nouvelles techniques WCAG depuis plus de 2 ans, et que la publication d'une nouvelle version du RGAA PF prenant en charge ces mises à jour intervienne quelques mois après.

Ces nouveaux tests ne se justifiant plus, ils devront être retirés des futurs audits. Et c'est bien l'interprétation de la version officielle du RGAA PF qui doit primer sur tout test créé hors de ce cadre lorsque les techniques sont prises en charge.

3.3.2. Propriété et responsabilité

Le RGAA PF de la Polynésie française est une copie adaptée de la version 3.2017 du RGAA de l'Etat.

Le référentiel technique du RGAA PF est une reproduction du référentiel technique de l'Etat, dont la Licence Ouverte autorise la reproduction, la redistribution, l'adaptation, à condition de citer la paternité du document original.

Ce référentiel technique s'appuie lui-même sur le référentiel AccessiWeb de l'association BrailleNet dont la licence d'utilisation autorise d'en faire des copies modifiées à condition de citer la source du document original.

Le RGAA PF et son contenu sont gérés par la Direction générale de l'économie numérique.

Le présent référentiel ainsi que les annexes sont disponibles en ligne sur le site Internet du service public d'accès au droit en Polynésie française (www.lexpol.pf).

Le RGAA PF est placé sous licence ouverte. Vous êtes libres de :

- Reproduire, copier, publier et transmettre ces informations ;
- Diffuser et redistribuer ces informations ;
- Adapter, modifier, extraire et transformer ces informations, notamment pour créer des informations dérivées ;
- Exploiter ces informations à titre commercial, par exemple en les combinant avec d'autres informations, ou en l'incluant dans votre propre produit ou application.

Ces libertés s'appliquent sous réserve de mentionner la paternité de l'information d'origine : sa source et la date de sa dernière mise à jour. Le réutilisateur peut notamment s'acquitter de cette condition en indiquant un ou des liens hypertextes (URL) renvoyant vers le présent site et assurant une mention effective de sa paternité.

Cette mention de paternité ne doit ni conférer un caractère officiel à la réutilisation de ces informations, ni suggérer une quelconque reconnaissance ou caution par le producteur de l'information, ou par toute autre entité publique, du réutilisateur ou de sa réutilisation.

4. Partie 2 : Guide d'application du RGAA PF

4.1. Périmètre d'application du RGAA PF

4.1.1. Services concernés

Le RGAA PF concerne les autorités administratives de la Polynésie française mettant en œuvre des téléservices.

4.1.2. Contenus concernés

Sont concernés toutes les documents et applications Web d'un téléservice disponibles depuis un navigateur Web.

Par application Web, on entend toute application « métier » à laquelle on accède au moyen d'un navigateur Web et qui vise les usagers des téléservices (exemple : inscription aux concours, déclaration d'impôts…).

4.1.2.1. Cas des contenus mis en ligne sur des sites externes

Les contenus mis en ligne sur des sites externes sont le résultat d'une volonté du maître d'ouvrage d'atteindre le public via ces sites.

Il est recommandé de rendre ces contenus accessibles.

Exemple : un ministère qui met ses vidéos sur Daily Motion ou Youtube, pourrait créer un lien vers un contenu textuel accessible alternatif, selon le principe de la compensation. Il procédera de même s'il diffuse des contenus par l'intermédiaire de réseaux sociaux.

4.1.2.2. Cas des liens vers des documents téléchargeables publiés sur d'autres sites

La mise en place de liens externes vers des documents à télécharger peut se justifier par la nécessité de fournir des informations complémentaires relatives au contenu. Il s'agit d'un cas de dérogation autorisé décrit dans la section Liste des dérogations admises et principe de la compensation.

4.2. Modalités d'application du RGAA PF

L'objectif du RGAA PF est de donner aux autorités administratives mettant en place une démarche de mise en accessibilité des téléservices les moyens de pouvoir le faire dans les meilleures conditions possibles.

L'exigence d'accessibilité numérique doit être incluse dans les cahiers des charges d'appels d'offres.
Il est recommandé de mettre à la disposition des services concernés les ressources utiles.

L'appropriation du RGAA PF ne peut se concrétiser que par une démarche volontariste d'évolution de l'accessibilité des téléservices. Elle repose sur une procédure d'auto-évaluation (ou d'évaluation par un tiers selon les compétences disponibles localement) et sur une démarche de mise en accessibilité qui devra s'adapter au type de projet (création d'un nouveau téléservice, refonte d'un téléservice existant, amélioration continue, échantillonnage).

4.2.1. Niveaux de conformité aux normes d'accessibilité

La traduction française agréée des WCAG 2.0 indique :

> « Afin de répondre aux besoins de divers groupes et de différents contextes, trois niveaux de conformité ont été définis : A (le plus bas), AA et AAA (le plus élevé) ».

Les critères de succès ont donc été associés à l'un des niveaux A, AA et AAA sur la base de divers facteurs (liste des facteurs d'attribution du niveau WCAG).

Par ailleurs, le niveau AAA possède la particularité de ne pas s'appliquer à tous les contenus ou dans tous les contextes :

> « Il n'est pas recommandé de se fixer le niveau AAA comme objectif à l'échelle de sites entiers car il n'est pas possible de satisfaire à tous les critères de succès du niveau AAA pour certains contenus ».

Le niveau recommandé par l'Union européenne est le niveau double A (AA). C'est également le niveau attendu pour les sites concernés par le RGAA PF et à ce titre, pour être conforme au RGAA PF, il est nécessaire de valider l'ensemble des critères ayant un niveau WCAG déduit A et AA. Les critères de succès associés au niveau AAA peuvent être pris en compte dans certains contextes, lorsque cela est possible et pertinent.

Niveaux de conformité WCAG :

Niveau	Définition de la conformité	Critères
A	Pour une conformité de niveau A (le niveau minimal), la page Web satisfait à tous les critères de succès de niveau A ou une version de remplacement est fournie.	Critères de succès essentiels pouvant raisonnablement s'appliquer à toutes les ressources Web.
AA	Pour une conformité de niveau AA, la page Web remplit tous les critères de succès de niveau A et AA ou une version de remplacement conforme au niveau AA est fournie.	Critères de succès pouvant raisonnablement s'appliquer à toutes les ressources Web.
AAA	Pour une conformité de niveau AAA, la page Web remplit tous les critères de succès de niveau A, AA et AAA ou une version de remplacement conforme au niveau AAA est fournie.	Critères de succès ne s'appliquant pas à toutes les ressources Web.

4.2.2. Démarche de mise en accessibilité

L'objectif du RGAA PF est d'accompagner les démarches de mise en accessibilité par la fourniture des critères techniques à mettre en œuvre et des tests correspondants. En fonction du projet de mise en accessibilité, des objectifs d'accessibilité et des différentes phases du projet, le RGAA PF doit servir de référence en répondant aux questions d'accessibilité qui se posent dans différents contextes.

Le RGAA PF pourra notamment être utilisé dans les contextes suivants :

- La mise en œuvre d'un nouveau téléservice (refonte) : Cette approche consiste à prendre en compte les recommandations du RGAA PF du début à la fin du projet de création du site (analyse, production, mise en ligne, maintenance, vie du site).
- L'amélioration d'un téléservice existant et la réalisation de la déclaration de conformité : Cette approche consiste à évaluer l'accessibilité d'un site déjà en production, de façon à extraire des indicateurs, des résultats globaux, des recommandations opérationnelles, et des résultats pour le site et pour ses pages.

Concrètement, une démarche de prise en compte de l'accessibilité nécessite la mise en place d'engagements concrets. Inspirés de la norme ISO 9001 : 200823, voici quelques éléments à mettre en œuvre sans lesquels une démarche accessibilité ne peut réussir sur la durée.

4.2.2.1. Engagement de la direction

La direction de l'entité publique, c'est-à-dire les personnes ayant la responsabilité suffisante pour réaliser les actions suivantes, doit :

- Communiquer au sein de l'organisme l'importance à prendre en compte les règles d'accessibilité pour remplir sa mission de service public dans l'intérêt général et satisfaire les exigences réglementaires et légales ;
- Établir la politique d'accessibilité ;
- Assurer que des objectifs de conformité sont établis ;
- Suivre des indicateurs sur le niveau d'accessibilité ;
- Assurer la disponibilité des ressources.

4.2.2.2. Désignation d'un référent accessibilité

La direction doit nommer un membre de l'encadrement de l'organisme en tant que « référent accessibilité ». Ce référent qui, nonobstant d'autres responsabilités, doit avoir la responsabilité et l'autorité en particulier pour :

- Assurer que les processus nécessaires à la prise en compte de l'accessibilité sont établis, mis en œuvre et entretenus ;
- Rendre compte à la direction du niveau d'accessibilité et de tout besoin d'amélioration ;
- Assurer que la sensibilisation aux exigences d'accessibilité dans tout l'organisme est encouragée ;
- Être le point d'entrée unique sur les sujets d'accessibilité numérique.

4.2.2.3. Audits d'accessibilité réguliers

Seul un audit sur un échantillon représentatif de pages peut permettre de connaître le niveau de conformité du site ou de l'application au RGAA PF.

Cet audit est conduit sous la responsabilité du « référent accessibilité » de l'entité publique et doit se conformer aux points suivants :

- Il est réalisé sur au moins une partie du périmètre du site, et sur un échantillon représentatif de l'ensemble du système d'information selon une fréquence à définir ;
- Il revient à l'entité de veiller à la fiabilité de sa déclaration par tous moyens (recours à un prestataire externe, formation d'experts internes, audits croisés…) ;
- Il vise à produire un score de conformité pour les niveaux simple A et double A (AA) du RGAA PF sur un échantillon représentatif de pages Web ;
- Le résultat doit être remonté à la direction au minimum.

4.2.3. Principe d'aménagement raisonnable

La Convention relative aux droits des personnes handicapées (CRDPH) des Nations Unies, en même temps qu'elle consacre l'accessibilité comme un droit humain et crée une obligation d'action pour inclure les personnes handicapées, précise que cette action doit consister en des « aménagements raisonnables ».

La notion est définie à l'article 2 de la CRDPH comme suit :

> « On entend par "aménagement raisonnable" les modifications et ajustements nécessaires et appropriés n'imposant pas de charge disproportionnée ou indue apportés, en fonction des besoins dans une situation donnée, pour assurer aux personnes handicapées la jouissance ou l'exercice, sur la base de l'égalité avec les autres, de tous les droits de l'homme et de toutes les libertés fondamentales ».

Les standards WCAG 2.0 contiennent un certain nombre de règles techniques très précises qui peuvent être déployées facilement et même quelquefois être testées automatiquement. Notons toutefois que seuls 20 % des critères d'accessibilité semblent permettre une vérification de façon entièrement automatique.

De nombreux critères sont donc à vérifier manuellement, par une personne formée, notamment lorsqu'il s'agit de critères de pertinence. Il est important de comprendre la notion de pertinence qui n'est pas à entendre dans le sens d'optimisation, mais dans le sens de l'accès à l'information, ce qui constitue un critère qu'il est possible d'évaluer de façon objective. Ainsi, la qualité des alternatives apportées ne devrait pas être appréciée par l'auditeur qui doit se contenter de vérifier si l'accès à l'information est possible.

Ces deux types de recommandations (celles vérifiables automatiquement et celles devant faire l'objet d'un test manuel) doivent se déployer sur toutes les pages d'un site.

En pratique, il est difficile et extrêmement chronophage de tester l'intégralité des contenus au regard de l'intégralité des règles WCAG 2.0. La volonté de rendre un site totalement accessible sur l'intégralité de ses pages et pour l'intégralité des critères peut conduire à une débauche d'énergie qui peut s'avérer contre-productive.

Il va donc être nécessaire :

- De fixer des limites : analyser un échantillon de pages représentatives et non l'intégralité du site ;
- D'effectuer des arbitrages : déterminer les contenus et fonctionnalités essentiels du site ou de l'application qu'il n'est pas possible de ne pas rendre accessible, et décider dans quel cas une amélioration s'avère trop lourde ou contre-productive ;
- De planifier les opérations de façon à faire de l'accessibilité une démarche d'amélioration continue.

La première attente fondamentale des utilisateurs est de pouvoir accéder aux contenus et fonctionnalités des téléservices, mais pas nécessairement sous la même forme. Mettre en place des alternatives peut être un compromis acceptable à condition qu'elles fournissent le même niveau d'information et des fonctionnalités équivalentes.

4.2.4. La notion de « base de référence »

Avec le saut technologique opéré ces dernières années, il n'est pas possible de mettre à disposition une même version d'un service pour des technologies modernes, c'est-à-dire supportant les dernières évolutions techniques et majoritairement utilisées, et des technologies considérées aujourd'hui comme obsolètes.

L'accessibilité consiste à respecter un principe d'aménagement raisonnable, et le maintien de plusieurs versions d'une même interface n'est pas réalisable en pratique car complexe et excessivement coûteux à maintenir.

En parallèle de la mise aux normes des contenus et fonctionnalités de ses services en ligne par l'administration, il est nécessaire que les utilisateurs mettent à jour leur navigateur et leur technologie d'assistance pour bénéficier des avancées techniques en matière d'accessibilité.

La réalisation du référentiel technique a reposé sur un ensemble de tests pour vérifier leur compatibilité avec les navigateurs et technologies d'assistance. Étant donné la diversité des systèmes existant, les tests se sont concentrés sur les configurations majoritairement utilisées.

Il a été pris en compte l'existence de solutions libres et gratuites pour effectuer les tests afin de permettre aux utilisateurs souhaitant se mettre à jour de pouvoir le faire sans coût supplémentaire.

Cette base de référence est explicitée en détail dans une sous-section du référentiel technique. Elle concerne les cas où il n'est pas possible de connaître la configuration des postes de travail des utilisateurs (configuration des logiciels utilisés et leur version).

Dans le cas où le parc informatique est maîtrisé, on parle alors d'« environnement maîtrisé ». La base de référence pour les tests est alors constituée des logiciels utilisés dans cet environnement maîtrisé.

Notons que cette base de référence est un socle technique minimal sur lequel des tests doivent être effectués. Mais rien n'empêche de compléter cette base de référence, notamment si vous souhaitez étendre la compatibilité avec des technologies plus anciennes.

4.2.5. Déclaration de conformité

4.2.5.1. Principe

La « déclaration de conformité » est l'étape finale de la vérification de la conformité au RGAA PF ; elle est réalisée préalablement à la mise à disposition du téléservice en ligne et correspond à un engagement sur l'honneur de satisfaire à l'ensemble des tests (sauf dérogation dûment justifiée) ayant un niveau WCAG déduit A et AA dans la version du RGAA PF en vigueur.

Elle peut donc comporter des écarts en nombre limité au regard des tests du RGAA PF. Dans certains cas, le responsable du téléservice sera dans l'impossibilité matérielle de mettre en œuvre une partie des critères. Il sera alors possible de signaler les contenus correspondant comme non-accessibles.

En tout état de cause, les écarts devront être justifiés et expliqués suivant le principe de la dérogation (cf. section Liste des dérogations admises et principe de la compensation).

La mise en œuvre de ce principe de dérogation ne remet pas en question l'objectif de conformité totale aux tests du RGAA PF, mais elle permet aux administrateurs :

- De démontrer les avancées de leur démarche de mise en conformité ;
- De signaler les futures améliorations du site ;
- De montrer aux utilisateurs que les problèmes sont connus et anticipés ;
- De faire remonter aux autorités compétentes les problèmes de mise en œuvre sur le terrain ;
- De faciliter l'ajustement ou la mise en œuvre des actions de formation, de sensibilisation ou de mise à disposition d'outils.

4.2.5.2. Contenu de la déclaration

La déclaration de conformité porte au minimum sur la liste de pages suivantes du téléservice, lorsqu'elles existent :

- Page d'accueil (page constituant le point d'entrée principale du téléservice, elle est généralement accessible par une adresse de la forme http://www.urldusite.extension) ;
- Page contact (page contenant les informations de contact ou le ou les formulaires permettant de contacter directement le ou les responsables du téléservice) ;
- Page mentions légales ;
- Page politique d'accessibilité : outre les informations relatives à l'évolution globale de l'accessibilité du site, cette page contiendra les renseignements relatifs à la déclaration de conformité dont la liste des pages ou secteurs du service dérogeant aux exigences d'accessibilité, leur type de contenu et les solutions alternatives pour y accéder ;
- Page aide (page contenant les informations facilitant l'utilisation du téléservice, raccourcis claviers, éventuels, logiciels/plug-in nécessaires à la consultation du site). La page d'aide, obligatoire, doit mentionner les coordonnées d'un contact au sein de l'administration ;
- Page conditions générales d'utilisation du téléservice ;
- Page recherche (page dont l'objet principal est la mise à disposition d'un formulaire de recherche ou des résultats d'une recherche) ;
- Toutes les pages composant le processus d'un téléservice (un formulaire ou une transaction sur plusieurs pages).

S'ajoute à ces pages impératives un certain nombre de pages dans la liste suivante :

- Pages d'accès aux contenus ou fonctionnalités principaux (ex : rubriques de 1er niveau dans l'arborescence…) ;
- Pages représentatives des types de contenus disponibles sur le site (ex. : page contenant des tableaux de données, des éléments multimédias, des illustrations, des formulaires, etc.) ;
- Pages ayant le plus grand nombre de visiteurs.

Le choix exact des pages dans cette liste complémentaire et leur nombre nécessitent une appréciation humaine. Cette appréciation dépend des contenus et services, et de la capacité à mettre en œuvre le RGAA PF, dans votre environnement technique, en fonction de vos compétences et de vos ressources.

À noter que dans le cas d'application de type Single Page Application (SPA), toutes les pages requises dans l'échantillon décrites ci-dessus ne sont pas forcément présente. Il faudra alors ajuster l'échantillon pour le rendre représentatif.

Le RGAA PF ne fournit pas de format spécifique pour la déclaration de conformité mais précise les informations minimums à faire figurer, en se basant sur le principe de la déclaration de conformité WCAG 2.029 :

Date de réalisation ;
- Version du RGAA PF de référence ;
- Nom et adresse email du déclarant ;
- Technologies utilisées sur le site ;
- Liste des agents utilisateurs et technologies d'assistance utilisées pour vérifier l'accessibilité des contenus ;
- Liste des pages du site ayant fait l'objet de la vérification de conformité ;
- Résultat des tests et justification des dérogations.

4.2.5.3. Que vérifie-t-on ?

Le responsable d'un téléservice détermine un échantillon de pages représentatives dont certaines seront obligatoires au regard de la déclaration de conformité (cf section Contenu de la déclaration). La taille de cet échantillon peut varier suivant le nombre de pages, les contenus proposés, le nombre de formulaires, les processus transactionnels, etc.

L'administrateur du téléservice aura intérêt à choisir un échantillon de pages le plus représentatif possible, tout en veillant à ne pas provoquer une masse de travail exagérée pour la vérification. À titre indicatif, l'échantillon standard comprend généralement une quinzaine de pages.

Pour qu'une page soit déclarée conforme au RGAA PF, elle doit vérifier les éléments suivants :

- Le niveau double A (AA) doit être atteint ;
- La conformité (et le niveau de conformité) s'entend uniquement pour des pages Web complètes et ne peut être atteinte si une partie de la page Web est exclue ;
- Quand une page Web fait partie d'un ensemble représentant un processus (comme une succession d'étapes devant être complétées afin d'accomplir une activité), toutes les pages Web du processus sont conformes au moins au niveau spécifié. (La conformité à un certain niveau est impossible s'il existe une page de ce processus qui n'atteint pas au moins ce niveau) ;
- Si des technologies sont employées de manière non compatible avec l'accessibilité ou non-conforme, alors elles n'empêchent pas les utilisateurs d'accéder au reste de la page.

4.2.5.4. Comment vérifie-t-on la conformité au RGAA PF ?

Les actions à effectuer par le responsable de la vérification de la conformité au RGAA PF sont :

- Identification des pages composant l'échantillon : ce choix relèvera le plus souvent de décisions locales eu égard à la disparité des contextes et donc de la politique d'accessibilité définie. L'échantillon contient au minimum l'ensemble des pages obligatoires ;
- Réalisation des tests sur chacune des pages de l'échantillon ;
- Production d'un compte-rendu sous la forme d'une grille d'audit renseignée et/ou d'un rapport plus ou moins détaillé selon le besoin.

Pour le référentiel technique du RGAA PF, un critère peut désormais avoir l'un des 4 statuts suivants :

- Conforme ou validé : le critère est conforme ;
- Non-conforme ou invalidé : le critère est non-conforme ;
- Non applicable : le critère est non applicable ;
- Non testé : le critère est non testé (nouveau statut permettant de mesurer la progression de l'audit).

En plus de ces 4 statuts est créé un état particulier, traité à part, concernant les contenus dérogés. Cela se traduira par une colonne supplémentaire dans la grille d'audit permettant d'indiquer quand un contenu dérogé est présent et qu'il impacte des critères. Un même critère peut donc avoir un état dérogé quand il concerne un contenu dérogé, mais il reste applicable pour le reste des contenus de la page.

Cet état particulier viendra en complément des quatre premiers statuts et servira à signaler que des contenus dérogés sont applicables au critère et à conserver la trace de ces dérogations.

4.2.5.5. Mise en ligne de la déclaration

La déclaration sera accessible via le téléservice, par le biais d'une page dédiée ou au sein d'une autre page (aide/politique d'accessibilité/mentions légales/conditions générales d'utilisation).

4.2.5.6. Validité de la déclaration

La déclaration de conformité est considérée comme valide pour la version en cours du RGAA PF à la date de sa mise en ligne. Dès qu'une nouvelle version du RGAA PF sera publiée, la déclaration liée à une version antérieure ne sera plus valide. Les autorités administratives auront alors 18 mois pour se mettre en conformité avec la dernière version publiée.

Il est à noter qu'une déclaration de conformité peut être mise à jour à plusieurs reprises pour un même téléservice et une même version du RGAA PF, afin de mettre en évidence les efforts de mise en accessibilité et de mettre à jour le niveau atteint.

4.2.6. Liste des dérogations admises et principe de la compensation

À noter qu'une dérogation ne s'applique qu'à un contenu et non à un critère du RGAA PF. Une fois le contenu dérogé, il sort du champ de l'audit.

Lorsqu'il s'agit d'un contenu ou d'une fonctionnalité essentielle dans le cadre du téléservice, il ne peut y avoir de dérogation sans une alternative sophistiquée permettant d'apporter le même niveau d'information à l'utilisateur.

4.2.6.1. Dérogations prévues par WCAG 2.0

Les WCAG prévoient un certain nombre de cas permettant de déroger à l'accessibilité complète d'une page Web en faisant une déclaration de conformité partielle.

4.2.6.1.1. Contenus fournis par un tiers

Contenus générés par l'utilisateur : il peut arriver qu'il soit impossible lors de l'affichage original de savoir quel sera le contenu non contrôlé de ces pages. C'est le cas notamment des contenus générés par l'utilisateur, comme par exemple dans une application Web de courrier électronique, un blog, un article permettant l'ajout de commentaires par les utilisateurs ou toute application acceptant du contenu généré par l'utilisateur comme un wiki.

Contenus non contrôlés provenant de sources extérieures : un autre exemple fourni par WCAG concerne les pages, telles que celles d'un portail ou d'un site d'informations, composées d'une somme de contenus rédigés par de multiples contributeurs ou des sites insérant automatiquement, au fur et à mesure, du contenu provenant d'autres sites, tels que des publicités insérées automatiquement.

Ce cas de dérogation vaut également pour les liens vers des documents téléchargeables publiés sur d'autres sites, et dont le contenu n'est donc pas contrôlable (cf. Cas des liens vers des documents téléchargeables publiés sur d'autres sites).

Les contenus fournis par un tiers peuvent faire l'objet d'une dérogation. Une déclaration précise doit permettre de les identifier. La déclaration peut être sous la forme suivante :

> « Cette page n'est pas conforme, mais pourrait être conforme au RGAA PF niveau X si les parties suivantes, issues de sources non contrôlées, lui étaient retirées : [énumérer les parties concernées]. »

4.2.6.1.2. Langue

Une dérogation est également prévue dans les WCAG 2.0 lorsqu'une page n'est pas conforme et pourrait l'être si la compatibilité avec l'accessibilité était assurée pour toutes les langues utilisées dans la page. La déclaration s'énonce alors comme suit :

> « Cette page n'est pas conforme, mais serait conforme au RGAA PF au niveau X si la compatibilité avec l'accessibilité était assurée pour la (les) langue(s) suivante(s) : [énumérer les langues concernées]. »

4.2.6.2. Dérogations supplémentaires : contenus en téléchargement en nombre important

Il peut être excessivement coûteux et donc déraisonnable de mettre en conformité un nombre important d'archives en téléchargement.

Dans ce cas, une dérogation peut être faite pour les documents de plus de 2 ans. Cela ne vaut pas pour la production de nouveaux documents.

4.2.6.3. Mesures à prendre lorsqu'un contenu est dérogé

- Les contenus non accessibles doivent être signalés à l'utilisateur sur la page d'aide et dans la déclaration de conformité pour qu'il soit informé de la proportion des pages concernées et de leur localisation dans les rubriques du site ;
- Les dérogations en matière d'accessibilité doivent être expliquées et motivées dans le cadre de la déclaration de conformité ;
- Il est nécessaire de prévoir un canal permettant aux personnes handicapées ou qui détectent un problème dans ce domaine de pouvoir le signaler aux administrateurs du téléservice via un mécanisme accessible (adresse électronique ou formulaire).

La traçabilité de ces contenus dérogés devra également apparaître dans les grilles d'audit comme décrit à la section « Comment vérifie-t-on la conformité au RGAA PF ? ».

3. Une opportunité de mutualisation pour les autres données publiques en mettant en place un standard réutilisable par les collectivités territoriales qui souhaiteraient se lancer dans l'ouverture des données publiques.

ANNEXE 6 Ter

Référentiel Général d'Accessibilité pour les Administrations de la Polynésie française

RGAA PF

Référentiel technique

Historique des versions		
Date	**Version**	**Évolution du document**
	1.0	Publication de la première version du référentiel technique du Référentiel Général d'Accessibilité pour les Administrations de la Polynésie française (RGAA PF)

Liste détaillée des Critères

Mode d'emploi

Ce référentiel s'applique à tout contenu HTML (HTML4, XHTML1 et HTML5). Il utilise, pour certains tests une base de référence prenant en compte un ensemble de technologies d'assistance, de navigateurs et de systèmes d'exploitation sur lesquels l'accessibilité des composants d'interface développés par JavaScript doit être vérifiée notamment. Une description détaillée de la base de référence est disponible ici : base de référence.

Note importante pour tout contenu antérieur à la spécification HTML5 : Lorsque le code HTML de la page n'est pas du HTML5, les éléments HTML5 (balises et attributs) exigés par un critère ou test sont non applicables. Tous les autres critères ou tests restent applicables, y compris les dispositifs ARIA. Les critères et tests suivants sont non applicables :

- Critère 1.10 ;
- Critère 9.2 ;
- Test 11.10.1 (condition 2 relative à l'attribut HTML5 required).

Méthode de validation

Le niveau de conformité est établi au niveau des critères selon ces statuts :

- Conforme ou validé : le critère est conforme ;
- Non-conforme ou invalidé : le critère est non-conforme ;
- Non applicable : le critère est non applicable ;
- Non testé : le critère est non testé (nouveau statut permettant de mesurer la progression de l'audit).

Vous pouvez consulter, à ce sujet, le guide d'accompagnement : Comment vérifie-t-on la conformité au RGAA PF ?

1. Images

Principe WCAG : Perceptible

Recommandation :

Donner à chaque image porteuse d'information une alternative textuelle pertinente et une description détaillée si nécessaire. Lier les légendes à leurs images. Remplacer les images textes par du texte stylé lorsque c'est possible.

Critère 1.1 [A] Chaque image a-t-elle une alternative textuelle ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 1.1.1 : Chaque image (balise img) a-t-elle un attribut alt ?
- Test 1.1.2 : Chaque zone (balise area) d'une image réactive a-t-elle un attribut alt ?
- Test 1.1.3 : Chaque bouton de formulaire (balise inputavec l'attribut type="image") a-t-il un attribut alt ?
- Test 1.1.4 : Chaque zone cliquable d'une image réactive coté serveur est-t-elle doublée d'un lien dans la page ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.1.1

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : H36 - H37 - H53 - H24 - F65

Critère 1.2 [A] Pour chaque image de décoration ayant une alternative textuelle, cette alternative est-elle vide ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 1.2.1 : Chaque image (balise img) de décoration, sans légende, et ayant un attribut alt, vérifie-t-elle ces conditions ?
    - Le contenu de l'attribut altest vide (alt="") ;
    - L'image de décoration ne possède pas d'attribut title ;
    - La balise imgest dépourvue de rôle, propriété ou état ARIA visant à labelliser l'image (aria-label, aria-describedby, aria-labelledbypar exemple).
- Test 1.2.2 : Chaque zone non cliquable (balise areasans attribut href) de décoration, et ayant un attribut alt, vérifie-t-elle ces conditions ?
    - Le contenu de l'attribut altest vide (alt="") ;
    - La zone non cliquable ne possède pas d'attribut title ;
    - La balise areaest dépourvue de rôle, propriété ou état ARIA visant à labelliser l'image (aria-label, aria-describedby, aria-labelledbypar exemple).
- Test 1.2.3 : Chaque image objet (balise objectavec l'attribut type="image/…") de décoration, sans légende, vérifie-t-elle ces conditions ?
    - La balise objectpossède un attribut aria-hidden="true";
    - L'alternative textuelle entre <object>et </object>est vide ;
    - La balise objectou l'un de ses enfants est dépourvue de rôle, propriété ou état ARIA visant à labelliser l'image (aria-label, aria-describedby, aria- labelledby par exemple).

- Test 1.2.4 : Chaque image vectorielle (balise svg) de décoration, sans légende, vérifie-t-elle ces conditions ?
    - La balise svg possède un attribut aria-hidden="true";
    - Les balises titleet descsont absentes ou vides ;
    - La balise svgou l'un de ses enfants est dépourvue d'attribut title ;
    - La balise svgou l'un de ses enfants est dépourvue de rôle, propriété ou état ARIA visant à labelliser l'image vectorielle (aria-label, aria-describedby, aria-labelledby par exemple).
- Test 1.2.5 : Chaque image bitmap (balise canvas) de décoration, sans légende, vérifie-t-elle ces conditions ?
    - La balise canvaspossède un attribut aria-hidden="true";
    - Le contenu entre <canvas>et </canvas>est dépourvue de contenus textuels ;
    - La balise canvasou l'un de ses enfants est dépourvue de rôle, propriété ou état ARIA visant à labelliser l'image (aria-label, aria-describedby, aria-labelledby par exemple).
- Test 1.2.6 : Chaque image embarquée (balise embedavec l'attribut type="image/…") de décoration, sans légende, vérifie-t-elle ces conditions ?
    - La balise embedpossède un attribut aria-hidden="true";
    - La balise embedou l'un de ses enfants est dépourvue de rôle, propriété ou état ARIA visant à labelliser l'image (aria-label, aria-describedby, aria-labelledby par exemple).

Note technique : Consulter la note technique au sujet du rôle presentation.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.1.1 - 4.1.2

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : H67 - G196 - C9 - F39 - F38 - ARIA4 - ARIA10

Critère 1.3 [A] Pour chaque image porteuse d'information ayant une alternative textuelle, cette alternative est-elle pertinente (hors cas particuliers) ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 1.3.1 : Chaque image (balise img) porteuse d'information, ayant un attribut alt, vérifie-t-elle ces conditions (hors cas particuliers) ?
    - Le contenu de l'attribut altest pertinent ;
    - S'il est présent, le contenu de l'attribut titleest identique au contenu de l'attribut

alt ;
    - S'il est présent, le contenu de la propriété aria-labelest identique au contenu de l'attribut alt ;
    - S'il est présent, le contenu du passage de texte lié *via* la propriété aria-labelledbyest identique au contenu de l'attribut alt.
- Test 1.3.2 : Chaque zone (balise area) d'une image réactive porteuse d'information, ayant un attribut alt, vérifie-t-elle ces conditions (hors cas particuliers) ?
    - Le contenu de l'attribut altest pertinent ;
    - S'il est présent, le contenu de l'attribut titleest identique au contenu de l'attribut alt ;
    - S'il est présent, le contenu de la propriété aria-labelest identique au contenu de l'attribut alt ;
    - S'il est présent, le contenu du passage de texte lié *via* la propriété aria-labelledbyest identique au contenu de l'attribut alt.
- Test 1.3.3 : Chaque bouton associé à une image (balise inputavec l'attribut type="image"), ayant un attribut alt, vérifie-t-il ces conditions (hors cas particuliers) ?
    - Le contenu de l'attribut altest pertinent ;
    - S'il est présent, le contenu de l'attribut titleest identique au contenu de l'attribut alt ;
    - S'il est présent, le contenu de la propriété aria-labelest identique au contenu de l'attribut alt ;
    - S'il est présent, le contenu du passage de texte lié *via* la propriété aria-labelledbyest identique au contenu de l'attribut alt.
- Test 1.3.4 : Chaque image objet (balise objectavec l'attribut type="image/…") porteuse d'information vérifie-t-elle une de ces conditions (hors cas particuliers) ?
    - L'image objet est immédiatement suivie d'un lien adjacent permettant d'afficher une page ou un passage de texte contenant une alternative pertinente ;
    - Un mécanisme permet à l'utilisateur de remplacer l'image objet par un texte alternatif pertinent ;
    - Un mécanisme permet à l'utilisateur de remplacer l'image objet par une image possédant une alternative pertinente.
- Test 1.3.5 : Chaque image objet (balise objectavec l'attribut type="image/…") porteuse d'information, qui utilise une propriété aria-label, aria-labelledbyou un attribut title, vérifie-t-elle ces conditions (hors cas particuliers) ?
    - S'il est présent, le contenu de l'attribut titleest identique au contenu de l'attribut aria-label ;
    - S'il est présent, le contenu de l'attribut titleest identique au passage de texte lié par la propriété aria-labelledby.

- Test 1.3.6 : Chaque image embarquée (balise embed avec l'attribut type="image/…") porteuse d'information vérifie-t-elle une de ces conditions (hors cas particuliers) ?
    - L'image embarquée est immédiatement suivie d'un lien adjacent permettant d'afficher une page ou un passage de texte contenant une alternative pertinente ;
    - Un mécanisme permet à l'utilisateur de remplacer l'image embarquée par un texte alternatif pertinent ;
    - Un mécanisme permet à l'utilisateur de remplacer l'image embarquée par une image possédant une alternative pertinente.
- Test 1.3.7 : Chaque image embarquée (balise embed avec l'attribut type="image/…") porteuse d'information, qui utilise une propriété aria-label, aria-labelledbyou un attribut title, vérifie-t-elle ces conditions (hors cas particuliers) ?
    - S'il est présent, le contenu de l'attribut titleest identique au contenu de l'attribut aria-label ;
    - S'il est présent, le contenu de l'attribut titleest identique au passage de texte lié par la propriété aria-labelledby.
- Test 1.3.8 : Chaque image vectorielle (balise svg) porteuse d'information, en l'absence d'alternative, vérifie-t-elle ces conditions (hors cas particuliers) ?
    - La balise svgpossède un role="img";
    - La balise svgpossède une propriété aria-labeldont le contenu est pertinent et identique à l'attribut titles'il est présent ;
    - La balise svgpossède une balise descdont le contenu est pertinent et contient un passage de texte identique à la propriété aria-labelet à l'attribut titlede la balise svgs'il est présent.
- Test 1.3.9 : Pour chaque image vectorielle (balise svg) porteuse d'information et possédant une alternative, cette alternative est-elle correctement restituée par les technologies d'assistance ?
- Test 1.3.10 : Chaque image bitmap (balise canvas) porteuse d'information vérifie-t-elle une de ces conditions (hors cas particuliers) ?
    - Le contenu de l'alternative (contenu entre <canvas> et </canvas>) est pertinent ;
    - L'image bitmap est immédiatement suivie d'un lien adjacent permettant d'afficher une page ou un passage de texte contenant une alternative pertinente ;
    - Un mécanisme permet à l'utilisateur de remplacer l'image bitmap par un texte alternatif pertinent ;
    - Un mécanisme permet à l'utilisateur de remplacer l'image bitmap par une image possédant une alternative pertinente.
- Test 1.3.11 : Chaque image bitmap (balise canvas) porteuse d'information, qui utilise une propriété aria-label, aria-labelledbyou un attribut title, vérifie-t-elle ces conditions (hors cas particuliers) ?

- S’il est présent, le contenu de l’attribut titleest identique au contenu de l’attribut aria-label ;
- S’il est présent, le contenu de l’attribut titleest identique au passage de texte lié par la propriété aria-labelledby.

- Test 1.3.12 : Pour chaque image bitmap (balise canvas) porteuse d’information et possédant une alternative (contenu entre <canvas>et </canvas>), cette alternative est- elle correctement restituée par les technologies d’assistance ?
- Test 1.3.13 : Pour chaque image porteuse d’information et ayant une alternative textuelle, l’alternative textuelle est-elle courte et concise (hors cas particuliers) ?

Note technique : Consulter la note technique au sujet de l’attribut titlepour des images.

Note technique : Consulter la note technique au sujet des balises <title>dans les images vectorielles.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.1.1 - 4.1.2

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G94 - G95 - F30 - F71 - G196 - ARIA4

Critère 1.4 [A] Pour chaque image utilisée comme CAPTCHA ou comme image-test, ayant une alternative textuelle, cette alternative permet-elle d’identifier la nature et la fonction de l’image ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 1.4.1 : Chaque image (balise img) utilisée comme CAPTCHA ou comme image-test, ayant un attribut alt, vérifie-t-elle ces conditions ?
  - Le contenu de l’attribut altpermet de comprendre la nature et la fonction de l’image ;
  - S’il est présent, le contenu de l’attribut titleest identique au contenu de l’attribut alt ;
  - S’il est présent, le contenu de la propriété aria-labelest identique au contenu de l’attribut alt ;
  - S’il est présent, le contenu du passage de texte lié *via* la propriété aria-labelledbyest identique au contenu de l’attribut alt.
- Test 1.4.2 : Chaque zone (balise area) d’une image réactive utilisée comme CAPTCHA ou comme image-test, ayant un attribut alt, vérifie-t-elle ces conditions ?
  - Le contenu de l’attribut altpermet de comprendre la nature et la fonction de la zone ;
  - S’il est présent, le contenu de l’attribut titleest identique au contenu de l’attribut

alt ;

- S’il est présent, le contenu de la propriété aria-labelest identique au contenu de l’attribut alt ;
- S’il est présent, le contenu du passage de texte lié *via* la propriété aria-labelledby est identique au contenu de l’attribut alt.

- Test 1.4.3 : Chaque bouton associé à une image (balise inputavec l’attribut type="image") utilisée comme CAPTCHA ou comme image-test, ayant un attribut alt, vérifie-t-il ces conditions ?
  - Le contenu de l’attribut altpermet de comprendre la nature et la fonction du bouton ;
  - S’il est présent, le contenu de l’attribut titleest identique au contenu de l’attribut alt ;
  - S’il est présent, le contenu de la propriété aria-labelest identique au contenu de l’attribut alt ;
  - S’il est présent, le contenu du passage de texte lié *via* la propriété aria-labelledby est identique au contenu de l’attribut alt.
- Test 1.4.4 : Chaque image objet (balise objectavec l’attribut type="image/…") utilisée comme CAPTCHA ou comme image-test vérifie-t-elle une de ces conditions ?
  - L’image objet est immédiatement suivie d’un lien adjacent permettant d’afficher une page ou un passage de texte contenant une alternative permettant de comprendre la nature et la fonction de l’image ;
  - Un mécanisme permet à l’utilisateur de remplacer l’image objet par un texte alternatif permettant de comprendre la nature et la fonction de l’image ;
  - Un mécanisme permet à l’utilisateur de remplacer l’image objet par une image possédant une alternative permettant de comprendre la nature et la fonction de l’image.
- Test 1.4.5 : Chaque image objet (balise objectavec l’attribut type="image/…") utilisée comme CAPTCHA ou comme image-test, qui utilise une propriété aria-label, aria-labelledbyou un attribut title, vérifie-t-elle ces conditions ?
  - S’il est présent, le contenu de l’attribut titleest identique au contenu de l’attribut aria-label ;
  - S’il est présent, le contenu de l’attribut titleest identique au passage de texte lié par la propriété aria-labelledby.
- Test 1.4.6 : Chaque image embarquée (balise embedavec l’attribut type="image/…") utilisée comme CAPTCHA ou comme image-test vérifie-t-elle une de ces conditions ?
  - L’image embarquée est immédiatement suivie d’un lien adjacent permettant d’afficher une page ou un passage de texte contenant une alternative permettant de comprendre la nature et la fonction de l’image ;
  - Un mécanisme permet à l’utilisateur de remplacer l’image embarquée par un texte

alternatif permettant de comprendre la nature et la fonction de l'image ;
    - Un mécanisme permet à l'utilisateur de remplacer l'image embarquée par une image possédant une alternative permettant de comprendre la nature et la fonction de l'image.
- Test 1.4.7 : Chaque image embarquée (balise embedavec l'attribut type="image/…") utilisée comme CAPTCHA ou comme image-test, qui utilise une propriété aria-label, aria-labelledbyou un attribut title, vérifie-t-elle ces conditions ?
    - S'il est présent, le contenu de l'attribut titleest identique au contenu de l'attribut aria-label ;
    - S'il est présent, le contenu de l'attribut titleest identique au passage de texte lié par la propriété aria-labelledby.
- Test 1.4.8 : Chaque image vectorielle (balise svg) utilisée comme CAPTCHA ou comme image-test, en l'absence d'alternative, vérifie-t-elle ces conditions ?
    - La balise svgpossède un role="img";
    - La balise svgpossède une propriété aria-labeldont le contenu permet de comprendre la nature et la fonction de l'image et identique à l'attribut titles'il est présent ;
    - La balise svgpossède une balise descdont le contenu permet de comprendre la nature et la fonction de l'image et identique à la propriété aria-labelet à l'attribut title de la balise svgs'il est présent ;
    - Un lien adjacent permet d'accéder à une alternative dont le contenu permet de comprendre la nature et la fonction de l'image et identique à la propriété aria- labelet à l'attribut titlede la balise svgs'il est présent.
- Test 1.4.9 : Pour chaque image vectorielle (balise svg) utilisée comme CAPTCHA ou comme image-test, possédant une alternative, cette alternative est-elle correctement restituée par les technologies d'assistance ?
- Test 1.4.10 Chaque image bitmap (balise canvas) utilisée comme CAPTCHA ou comme image-test vérifie-t-elle une de ces conditions ?
    - Le contenu de l'alternative (contenu entre <canvas> et </canvas>) permet de comprendre la nature et la fonction de l'image ;
    - L'image bitmap est immédiatement suivie d'un lien adjacent permettant d'afficher une page ou un passage de texte contenant une alternative permettant de comprendre la nature et la fonction de l'image ;
    - Un mécanisme permet à l'utilisateur de remplacer l'image bitmap par un texte alternatif permettant de comprendre la nature et la fonction de l'image ;
    - Un mécanisme permet à l'utilisateur de remplacer l'image bitmap par une image possédant une alternative permettant de comprendre la nature et la fonction de l'image.
- Test 1.4.11 : Chaque image bitmap (balise canvas) utilisée comme CAPTCHA ou comme

image-test, qui utilise une propriété aria-label, aria-labelledbyou un attribut title, vérifie-t-elle ces conditions ?

- S'il est présent, le contenu de l'attribut titleest identique au contenu de l'attribut aria-label;
- S'il est présent, le contenu de l'attribut titleest identique au passage de texte lié par la propriété aria-labelledby.

- Test 1.4.12 : Pour chaque image bitmap (balise canvas) utilisée comme CAPTCHA ou comme image-test, ayant une alternative textuelle, l'alternative textuelle est-elle correctement restituée par les technologies d'assistance ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.1.1

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G143 - G100

Critère 1.5 [A] Pour chaque image utilisée comme CAPTCHA, une solution d'accès alternatif au contenu ou à la fonction du CAPTCHA est-elle présente ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 1.5.1 : Chaque image (balises img, area, object, embed, svg, canvas) utilisée comme CAPTCHA vérifie-t-elle une de ces conditions ?
  - Il existe une autre forme de CAPTCHA non graphique, au moins ;
  - Il existe une autre solution d'accès à la fonctionnalité sécurisée par le CAPTCHA.
- Test 1.5.2 : Chaque bouton associé à une image (balise inputavec l'attribut type="image") utilisée comme CAPTCHA vérifie-t-il une de ces conditions ?
  - Il existe une autre forme de CAPTCHA non graphique, au moins ;
  - Il existe une autre solution d'accès à la fonctionnalité sécurisée par le CAPTCHA.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.1.1

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G144

Critère 1.6 [A] Chaque image porteuse d'information a-t-elle, si nécessaire, une description détaillée ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 1.6.1 : Chaque image (balise img) porteuse d'information, qui nécessite une description

détaillée, vérifie-t-elle une de ces conditions ?

- Il existe un attribut longdescqui donne l'adresse (url) d'une page contenant la description détaillée ;
- Il existe un attribut altcontenant la référence à une description détaillée adjacente à l'image ;
- Il existe un lien adjacent (*via* une url ou une ancre) permettant d'accéder au contenu de la description détaillée.

- Test 1.6.2 : Chaque image objet (balise objectavec l'attribut type="image/…") porteuse d'information, qui nécessite une description détaillée, vérifie-t-elle une de ces conditions ?
  - Il existe un lien adjacent (*via* une url ou une ancre) permettant d'accéder au contenu de la description détaillée ;
  - Il existe une description détaillée clairement identifiable adjacente à l'image objet.
- Test 1.6.3 : Chaque image embarquée (balise embed) porteuse d'information, qui nécessite une description détaillée, vérifie-t-elle une de ces conditions ?
  - Il existe un lien adjacent (*via* une url ou une ancre) permettant d'accéder au contenu de la description détaillée ;
  - Il existe une description détaillée clairement identifiable adjacente à l'image embarquée.
- Test 1.6.4 : Chaque bouton de type image (balise inputavec l'attribut type="image") porteur d'information, qui nécessite une description détaillée, vérifie-t-il une de ces conditions ?
  - Il existe un attribut altcontenant la référence à une description détaillée adjacente à l'image ;
  - Il existe un lien adjacent (*via* une url ou une ancre) permettant d'accéder au contenu de la description détaillée ;
  - Il existe une propriété aria-describedbyréférençant un passage de texte faisant office de description détaillée.
- Test 1.6.5 : Chaque bouton de type image (balise inputavec l'attribut type="image") porteur d'information, qui implémente une référence à une description détaillée adjacente *via* une propriété aria-describedby, vérifie-t-il ces conditions ?
  - Le passage de texte est identifié *via* un attribut id;
  - La valeur de l'attribut idest unique ;
  - La valeur de la propriété ARIA aria-describedbyest égale à la valeur de l'attribut id.
- Test 1.6.6 : Chaque image vectorielle (balise svg) porteuse d'information, qui nécessite une description détaillée, vérifie-t-elle une de ces conditions ?
  - Il existe une propriété aria-label contenant une référence à une description détaillée adjacente à l'image vectorielle ;

- Il existe une balise desccontenant une référence à une description détaillée adjacente à l'image vectorielle ;
- Il existe une balise desccontenant la description détaillée ;
- Il existe un lien adjacent (*via* une url ou une ancre) permettant d'accéder au contenu de la description détaillée.

- Test 1.6.7 : Pour chaque image vectorielle (balise svg) porteuse d'information, qui implémente une référence à une description détaillée adjacente *via* une propriété aria- label ou une balise desc, cette référence est-elle correctement restituée par les technologies d'assistance ?
- Test 1.6.8 : Chaque image bitmap (balise canvas), qui nécessite une description détaillée, vérifie-t-elle une de ces conditions ?
  - Il existe un passage de texte entre <canvas> et </canvas> contenant une référence à une description détaillée adjacente à l'image bitmap ;
  - Il existe un contenu textuel entre <canvas>et </canvas>faisant office de description détaillée ;
  - Il existe un lien adjacent (*via* une url ou une ancre) permettant d'accéder au contenu de la description détaillée.
- Test 1.6.9 : Pour chaque image bitmap (balise canvas) porteuse d'information, qui implémente une référence à une description détaillée adjacente, cette référence est-elle correctement restituée par les technologies d'assistance ?
- Test 1.6.10 : Pour chaque image (balise img, area, object, embed, svg, canvas) porteuse d'information, qui implémente une description détaillée et qui utilise une propriété aria-describedby, la propriété aria-describedbyréférence-t-elle la description détaillée ?

Note technique : Consulter la note technique au sujet des images vectorielles et de l'utilisation de la propriété aria-describedby.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.1.1

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G92 - G74 - G73 - H45 - ARIA6

Critère 1.7 [A] Pour chaque image porteuse d'information ayant une description détaillée, cette description est-elle pertinente ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 1.7.1 : Chaque image (balise img) porteuse d'information, ayant une description détaillée, vérifie-t-elle une de ces conditions ?
  - La description détaillée *via* l'adresse référencée dans l'attribut longdescest

pertinente ;
    - La description détaillée dans la page et signalée dans l'attribut altest pertinente ;
    - La description détaillée *via* un lien adjacent est pertinente.
- Test 1.7.2 : Chaque bouton de type image (balise inputavec l'attribut type="image") porteur d'information, ayant une description détaillée, vérifie-t-il une de ces conditions ?
    - La description détaillée *via* l'adresse référencée dans l'attribut longdescest pertinente ;
    - La description détaillée dans la page et signalée dans l'attribut altest pertinente ;
    - La description détaillée *via* un lien adjacent est pertinente ;
    - Le passage de texte référencé *via* la propriété aria-describedbyest pertinent.
- Test 1.7.3 : Chaque image objet (balise objectavec l'attribut type="image/…") porteuse d'information, ayant une description détaillée, vérifie-t-elle une de ces conditions ?
    - La description détaillée adjacente à l'image objet est pertinente ;
    - La description détaillée *via* un lien adjacent est pertinente.
- Test 1.7.4 : Chaque image embarquée (balise embedavec l'attribut type="image/…") porteuse d'information, ayant une description détaillée, vérifie-t-elle une de ces conditions ?
    - La description détaillée adjacente à l'image embarquée est pertinente ;
    - La description détaillée *via* un lien adjacent est pertinente.
- Test 1.7.5 : Chaque image vectorielle (balise svg) porteuse d'information, ayant une description détaillée, vérifie-t-elle une de ces conditions ?
    - La description détaillée adjacente à l'image vectorielle est pertinente ;
    - La description détaillée contenue dans la balise descest pertinente ;
    - La description détaillée *via* un lien adjacent est pertinente.
- Test 1.7.6 : Pour chaque image vectorielle (balise svg) porteuse d'information, ayant une description détaillée implémentée *via* la balise desc, cette description détaillée est-elle correctement restituée par les technologies d'assistance ?
- Test 1.7.7 : Chaque image bitmap (balise canvas) porteuse d'information, ayant une description détaillée, vérifie-t-elle une de ces conditions ?
    - La description détaillée adjacente à l'image bitmap est pertinente ;
    - La description détaillée contenue entre <canvas>et </canvas>est pertinente ;
    - La description détaillée *via* un lien adjacent est pertinente.
- Test 1.7.8 : Pour chaque image bitmap (balise canvas) porteuse d'information, ayant une description détaillée entre <canvas> et </canvas>, cette description détaillée est-elle correctement restituée par les technologies d'assistance ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.1.1

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G92 - F67

Critère 1.8 [AA] Chaque image texte porteuse d'information, en l'absence d'un mécanisme de remplacement, doit si possible être remplacée par du texte stylé. Cette règle est-elle respectée (hors cas particuliers) ?

Principe WCAG : Perceptible

Niveau RGAA PF : AA

- Test 1.8.1 : Chaque image texte (balise img) porteuse d'information, en l'absence d'un mécanisme de remplacement, doit si possible être remplacé par du texte stylé. Cette règle est-elle respectée (hors cas particuliers) ?
- Test 1.8.2 : Pour chaque bouton "image texte" (balise inputavec l'attribut type="image") porteur d'information, en l'absence d'un mécanisme de remplacement, doit si possible être remplacé par du texte stylé. Cette règle est-elle respectée (hors cas particuliers) ?
- Test 1.8.3 : Chaque image texte objet (balise objectavec l'attribut type="image/…") porteuse d'information, en l'absence d'un mécanisme de remplacement, doit si possible être remplacée par du texte stylé. Cette règle est-elle respectée (hors cas particuliers) ?
- Test 1.8.4 : Chaque image texte embarquée (balise embedavec l'attribut type="image/…") porteuse d'information, en l'absence d'un mécanisme de remplacement, doit si possible être remplacée par du texte stylé. Cette règle est-elle respectée (hors cas particuliers) ?
- Test 1.8.5 : Chaque image texte bitmap (balise canvas) porteuse d'information, en l'absence d'un mécanisme de remplacement, doit si possible être remplacée par du texte stylé. Cette règle est-elle respectée (hors cas particuliers) ?

Note technique : Consulter la note technique au sujet des images vectorielles de type texte.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.4.5

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G136 - G140 - C22 - C30

Critère 1.9 [AAA] Chaque image texte porteuse d'information, doit si possible être remplacée par du texte stylé. Cette règle est-elle respectée (hors cas particuliers) ?

Principe WCAG : Perceptible

Niveau RGAA PF : AAA

- Test 1.9.1 : Chaque image texte (balise img) porteuse d'information doit si possible être remplacée par du texte stylé. Cette règle est-elle respectée (hors cas particuliers) ?
- Test 1.9.2 : Chaque bouton "image texte" (balise inputavec l'attribut type="image") porteur d'information doit si possible être remplacé par du texte stylé. Cette règle est-elle

respectée (hors cas particuliers) ?

- Test 1.9.3 : Chaque image texte objet (balise objectavec l'attribut type="image/…") porteuse d'information doit si possible être remplacée par du texte stylé. Cette règle est-elle respectée (hors cas particuliers) ?
- Test 1.9.4 : Chaque image texte embarquée (balise embedavec l'attribut type="image/…") porteuse d'information doit si possible être remplacée par du texte stylé. Cette règle est-elle respectée (hors cas particuliers) ?
- Test 1.9.5 : Chaque image texte bitmap (balise canvas) porteuse d'information doit si possible être remplacée par du texte stylé. Cette règle est-elle respectée (hors cas particuliers) ?

Note technique : Consulter la note technique au sujet des images vectorielles de type texte.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.4.9

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G140 - C22 - C30

Critère 1.10 [A] Chaque légende d'image est-elle, si nécessaire, correctement reliée à l'image correspondante ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 1.10.1 : Chaque image légendée (balise imgou inputavec l'attribut type="image"associée à une légende adjacente) vérifie-t-elle, si nécessaire, ces conditions ?
    - L'image (balise img) et sa légende sont contenues dans une balise figure;
    - La balise figurepossède un attribut role="group";
    - Le contenu de l'attribut altde l'image contient une référence à la légende adjacente.
- Test 1.10.2 : Chaque image objet légendée (balise objectavec l'attribut type="image/…"associée à une légende adjacente) vérifie-t-elle, si nécessaire, ces conditions ?
    - L'image objet (balise object) et sa légende sont contenues dans une balise figure;
    - La balise figurepossède un attribut role="group".
- Test 1.10.3 : Chaque image embarquée légendée (balise embedassociée à une légende adjacente) vérifie-t-elle, si nécessaire, ces conditions ?
    - L'image embarquée (balise embed) et sa légende sont contenues dans une balise figure;
    - La balise figurepossède un attribut role="group";
    - L'alternative contient une référence à la légende adjacente.

- Test 1.10.4 : Chaque image vectorielle légendée (balise svgassociée à une légende adjacente) vérifie-t-elle, si nécessaire, ces conditions ?
    - L'image vectorielle (balise svg) et sa légende sont contenues dans une balise figure;
    - La balise figurepossède un role="group";
    - Le contenu de la propriété aria-label ou de la balise desc de l'image vectorielle contient une référence à la légende adjacente.
- Test 1.10.5 : Chaque image bitmap légendée (balise canvasassociée à une légende adjacente) vérifie-t-elle, si nécessaire, ces conditions ?
    - L'image bitmap (balise canvas) et sa légende sont contenues dans une balise figure;
    - La balise figurepossède un attribut role="group";
    - Le contenu entre <canvas> et </canvas> de l'image bitmap contient une référence à la légende adjacente.

Note technique : Consulter la note technique au sujet des légendes d'images.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.1.1 - 4.1.2

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G140 - ARIA4 - ARIA6

2. Cadres

Principe WCAG : Robuste

Recommandation :

Donner à chaque cadre en ligne un titre pertinent.

Critère 2.1 [A] Chaque cadre en ligne a-t-il un titre de cadre ?

Principe WCAG : Robuste

Niveau RGAA PF : A

- Test 2.1.1 : Chaque cadre en ligne (balise iframe) a-t-il un attribut title?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 4.1.2

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : H64

Critère 2.2 [A] Pour chaque cadre en ligne ayant un titre de cadre, ce titre de cadre est-il pertinent ?

Principe WCAG : Robuste

Niveau RGAA PF : A

- Test 2.2.1 : Pour chaque cadre en ligne (balise iframe) ayant un attribut title, le contenu de cet attribut est-il pertinent ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 4.1.2

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : H64

3. Couleurs

Principe WCAG : Perceptible

Recommandation :

Ne pas donner l'information uniquement par la couleur et utiliser des contrastes de couleurs suffisamment élevés.

Critère 3.1 [A] Dans chaque page Web, l'information ne doit pas être donnée uniquement par la couleur. Cette règle est-elle respectée ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 3.1.1 : Pour chaque mot ou ensemble de mots dont la mise en couleur est porteuse d'information, l'information ne doit pas être donnée uniquement par la couleur. Cette règle est-elle respectée ?
- Test 3.1.2 : Pour chaque indication de couleur donnée par un texte, l'information ne doit pas être donnée uniquement par la couleur. Cette règle est-elle respectée ?
- Test 3.1.3 : Pour chaque image véhiculant une information, l'information ne doit pas être donnée uniquement par la couleur. Cette règle est-elle respectée ?
- Test 3.1.4 : Pour chaque propriété CSS déterminant une couleur et véhiculant une information, l'information ne doit pas être donnée uniquement par la couleur. Cette règle est-elle respectée ?
- Test 3.1.5 : Pour chaque média temporel véhiculant une information, l'information ne doit pas être donnée uniquement par la couleur. Cette règle est-elle respectée ?
- Test 3.1.6 : Pour chaque média non temporel véhiculant une information, l'information ne doit pas être donnée uniquement par la couleur. Cette règle est-elle respectée ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.4.1 - 1.3.1

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G14 - G182 - G111 - G117 - G138 - G205

Critère 3.2 [A] Dans chaque page Web, l'information ne doit pas être donnée uniquement par la couleur. Cette règle est-elle implémentée de façon pertinente ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 3.2.1 : Pour chaque mot ou ensemble de mots dont la mise en couleur est porteuse d'information, l'information ne doit pas être donnée uniquement par la couleur. Cette règle est-elle implémentée de façon pertinente ?
- Test 3.2.2 : Pour chaque indication de couleur donnée par un texte, l'information ne doit pas être donnée uniquement par la couleur. Cette règle est-elle implémentée de façon pertinente ?
- Test 3.2.3 : Pour chaque image véhiculant une information, l'information ne doit pas être donnée uniquement par la couleur. Cette règle est-elle implémentée de façon pertinente ?
- Test 3.2.4 : Pour chaque propriété CSS déterminant une couleur et véhiculant une information, l'information ne doit pas être donnée uniquement par la couleur. Cette règle est-elle implémentée de façon pertinente ?
- Test 3.2.5 : Pour chaque média temporel véhiculant une information, l'information ne doit pas être donnée uniquement par la couleur. Cette règle est-elle implémentée de façon pertinente ?
- Test 3.2.6 : Pour chaque média non temporel véhiculant une information, l'information ne doit pas être donnée uniquement par la couleur. Cette règle est-elle implémentée de façon pertinente ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.4.1

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G138 - F13

Critère 3.3 [AA] Dans chaque page Web, le contraste entre la couleur du texte et la couleur de son arrière-plan est-il suffisamment élevé (hors cas particuliers) ?

Principe WCAG : Perceptible

Niveau RGAA PF : AA

- Test 3.3.1 : Dans chaque page Web, jusqu'à 150% de la taille de police par défaut (ou 1.5em), le texte et le texte en image sans effet de graisse vérifient-ils une de ces conditions (hors cas particuliers) ?
    - Le rapport de contraste entre le texte et son arrière-plan est de 4.5:1, au moins ;
    - Un mécanisme permet à l'utilisateur d'afficher le texte avec un rapport de contraste de 4.5:1, au moins.

- Test 3.3.2 : Dans chaque page Web, jusqu'à 120% de la taille de police par défaut (ou 1.2em), le texte et le texte en image en gras vérifient-ils une de ces conditions (hors cas particuliers) ?
    - Le rapport de contraste entre le texte et son arrière-plan est de 4.5:1, au moins ;
    - Un mécanisme permet à l'utilisateur d'afficher le texte avec un rapport de contraste de 4.5:1, au moins.
- Test 3.3.3 : Dans chaque page Web, à partir de 150% de la taille de police par défaut (ou 1.5em), le texte et le texte en image sans effet de graisse vérifient-ils une de ces conditions (hors cas particuliers) ?
    - Le rapport de contraste entre le texte et son arrière-plan est de 3:1, au moins ;
    - Un mécanisme permet à l'utilisateur d'afficher le texte avec un rapport de contraste de 3:1, au moins.
- Test 3.3.4 : Dans chaque page Web, à partir de 120% de la taille de police par défaut (ou 1.2em), le texte et le texte en image en gras vérifient-ils une de ces conditions (hors cas particuliers) ?
    - Le rapport de contraste entre le texte et son arrière-plan est de 3:1, au moins ;
    - Un mécanisme permet à l'utilisateur d'afficher le texte avec un rapport de contraste de 3:1, au moins.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.4.3

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G18 - G136 - G148 - G174 - G145 - C29

Critère 3.4 [AAA] Dans chaque page Web, le contraste entre la couleur du texte et la couleur de son arrière-plan est-il amélioré (hors cas particuliers) ?

Principe WCAG : Perceptible

Niveau RGAA PF : AAA

- Test 3.4.1 : Dans chaque page Web, jusqu'à 150% de la taille de police par défaut (ou 1.5em), le texte et le texte en image sans effet de graisse vérifient-ils une de ces conditions (hors cas particuliers) ?
    - Le rapport de contraste entre le texte et son arrière-plan est de 7:1, au moins ;
    - Un mécanisme permet à l'utilisateur d'afficher le texte avec un rapport de contraste de 7:1, au moins.
- Test 3.4.2 : Dans chaque page Web, jusqu'à 120% de la taille de police par défaut (ou 1.2em), le texte et le texte en image en gras vérifient-ils une de ces conditions (hors cas particuliers) ?
    - Le rapport de contraste entre le texte et son arrière-plan est de 7:1, au moins ;
    - Un mécanisme permet à l'utilisateur d'afficher le texte avec un rapport de contraste

de 7:1, au moins.

- Test 3.4.3 : Dans chaque page Web, à partir de 150% de la taille de police par défaut (ou 1.5em), le texte et le texte en image sans effet de graisse vérifient-ils une de ces conditions (hors cas particuliers) ?
    - Le rapport de contraste entre le texte et son arrière-plan est de 4.5:1, au moins ;
    - Un mécanisme permet à l'utilisateur d'afficher le texte avec un rapport de contraste de 4.5:1, au moins.
- Test 3.4.4 : Dans chaque page Web, à partir de 120% de la taille de police par défaut (ou 1.2em), le texte et le texte en image en gras vérifient-ils une de ces conditions (hors cas particuliers) ?
    - Le rapport de contraste entre le texte et son arrière-plan est de 4.5:1, au moins ;
    - Un mécanisme permet à l'utilisateur d'afficher le texte avec un rapport de contraste de 4.5:1, au moins.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.4.6

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G148 - G17 - G18 - G174 - F83

4. Multimédia

Principe WCAG : Perceptible

Recommandation :

Donner si nécessaire à chaque média temporel une transcription textuelle, des sous-titres synchronisés et une audio-description synchronisée pertinents. Donner à chaque média non temporel une alternative textuelle pertinente. Rendre possible le contrôle de la consultation de chaque média temporel et non-temporel au clavier et s'assurer de leur compatibilité avec les technologies d'assistance.

Critère 4.1 [A] Chaque média temporel pré-enregistré a-t-il, si nécessaire, une transcription textuelle ou une audio-description (hors cas particuliers) ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 4.1.1 : Chaque média temporel pré-enregistré seulement audio, vérifie-t-il, si nécessaire, l'une de ces conditions (hors cas particuliers) ?
    - Il existe une transcription textuelle accessible *via* un lien adjacent (une url ou une ancre) ;
    - Il existe une transcription textuelle adjacente clairement identifiable.
- Test 4.1.2 : Chaque média temporel pré-enregistré seulement vidéo vérifie-t-il, si nécessaire,

l'une de ces conditions (hors cas particuliers) ?

- Il existe une version alternative « audio seulement » accessible *via* un lien adjacent (une url ou une ancre) ;
- Il existe une transcription textuelle accessible *via* un lien adjacent (une url ou une ancre) ;
- Il existe une transcription textuelle adjacente clairement identifiable ;
- Il existe une audio-description synchronisée ;
- Il existe une version alternative avec une audio-description synchronisée accessible *via* un lien adjacent (une url ou une ancre).

- Test 4.1.3 : Chaque média temporel synchronisé pré-enregistré vérifie-t-il, si nécessaire, une de ces conditions (hors cas particuliers) ?
  - Il existe une transcription textuelle accessible *via* un lien adjacent (une url ou une ancre) ;
  - Il existe une transcription textuelle adjacente clairement identifiable ;
  - Il existe une audio-description synchronisée ;
  - Il existe une version alternative avec une audio-description synchronisée accessible *via* un lien adjacent (une url ou une ancre).

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.2.1 - 1.2.3

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G58 - G69 - G78 - G158 - G159 - G173 - G8 - G166 - H96 - SM6 - SM7

Critère 4.2 [A] Pour chaque média temporel pré-enregistré ayant une transcription textuelle ou une audio-description synchronisée, celles-ci sont-elles pertinentes (hors cas particuliers) ?

Principe WCAG : Utilisable

Niveau RGAA PF : A

- Test 4.2.1 : Pour chaque média temporel pré-enregistré seulement audio, ayant une transcription textuelle, celle-ci est-elle pertinente (hors cas particuliers) ?
- Test 4.2.2 : Chaque média temporel pré-enregistré seulement vidéo vérifie-t-il une de ces conditions (hors cas particuliers) ?
  - La transcription textuelle est pertinente ;
  - L'audio-description synchronisée est pertinente ;
  - L'audio-description synchronisée de la version alternative est pertinente ;
  - La version alternative audio seulement est pertinente.
- Test 4.2.3 : Chaque média temporel synchronisé pré-enregistré vérifie-t-il une de ces conditions (hors cas particuliers) ?
  - La transcription textuelle est pertinente ;

- L'audio-description synchronisée est pertinente ;
- L'audio-description synchronisée de la version alternative est pertinente.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.2.1 - 1.2.3

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : F30 - F67 - SM6 - SM7

Critère 4.3 [A] Chaque média temporel synchronisé pré-enregistré a-t-il, si nécessaire, des sous-titres synchronisés (hors cas particuliers) ?

Principe WCAG : Utilisable

Niveau RGAA PF : A

- Test 4.3.1 : Chaque média temporel synchronisé pré-enregistré vérifie-t-il, si nécessaire, l'une de ces conditions (hors cas particuliers) ?
  - Le média temporel synchronisé possède des sous-titres synchronisés ;
  - Il existe une version alternative possédant des sous-titres synchronisés accessible *via* un lien adjacent (une url ou une ancre).
- Test 4.3.2 : Pour chaque média temporel synchronisé pré-enregistré possédant des sous-titres synchronisés diffusés *via* une balise track, la balise track possède-t-elle un attribut kind="captions"

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.2.2

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G58 - G93 - G87 - H95 - SM11 - SM12 - F74 - F75

Critère 4.4 [A] Pour chaque média temporel synchronisé pré-enregistré ayant des sous-titres synchronisés, ces sous-titres sont-ils pertinents ?

Principe WCAG : Utilisable

Niveau RGAA PF : A

- Test 4.4.1 : Pour chaque média temporel synchronisé pré-enregistré ayant des sous-titres synchronisés, ces sous-titres sont-ils pertinents ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.2.2

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G87 - G93 - F8 - F74 - F75 - SM11 - SM12

Critère 4.5 [AA] Chaque média temporel en direct a-t-il, si nécessaire, des sous-titres synchronisés ou une transcription textuelle (hors cas particuliers) ?

Principe WCAG : Utilisable

Niveau RGAA PF : AA

- Test 4.5.1 : Chaque média temporel seulement audio en direct vérifie-t-il, si nécessaire, une de ces conditions (hors cas particuliers) ?
    - Il existe des sous-titres synchronisés ;
    - Il existe une version ayant des sous-titres synchronisés accessible *via* un lien adjacent (une url ou une ancre) ;
    - Il existe une transcription textuelle accessible *via* un lien adjacent (une url ou une ancre) ;
    - Il existe une transcription textuelle adjacente clairement identifiable.
- Test 4.5.2 : Chaque média temporel synchronisé en direct vérifie-t-il, si nécessaire, une de ces conditions (hors cas particuliers) ?
    - Il existe des sous-titres synchronisés ;
    - Il existe une version ayant des sous-titres synchronisés accessible *via* un lien adjacent (une url ou une ancre) ;
    - Il existe une transcription textuelle accessible *via* un lien adjacent (une url ou une ancre) ;
    - Il existe une transcription textuelle adjacente clairement identifiable.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.2.4 - 1.2.9

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G9 - G150 - G151 - G157 - H95 - SM11 - SM12

Critère 4.6 [AA] Pour chaque média temporel en direct ayant des sous-titres synchronisés ou une transcription textuelle, ceux-ci sont-ils pertinents ?

Principe WCAG : Utilisable

Niveau RGAA PF : AA

- Test 4.6.1 : Chaque média temporel seulement audio en direct vérifie-t-il une de ces conditions ?
    - Les sous-titres synchronisés sont pertinents ;
    - Les sous-titres synchronisés de la version alternative sont pertinents ;
    - La transcription textuelle est pertinente.
- Test 4.6.2 : Chaque média temporel synchronisé en direct vérifie-t-il une de ces conditions ?

- Les sous-titres synchronisés sont pertinents ;
- Les sous-titres synchronisés de la version alternative sont pertinents ;
- La transcription textuelle est pertinente.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.2.4 - 1.2.9 Technique(s)

suffisante(s) et/ou échec(s) WCAG 2.0 : F8

Critère 4.7 [AA] Chaque média temporel pré-enregistré a-t-il, si nécessaire, une audio-description synchronisée (hors cas particuliers) ?

Principe WCAG : Utilisable

Niveau RGAA PF : AA

- Test 4.7.1 : Chaque média temporel pré-enregistré seulement vidéo vérifie-t-il, si nécessaire, une de ces conditions (hors cas particuliers) ?
  - Il existe une audio-description synchronisée ;
  - Il existe une version alternative avec une audio-description synchronisée.
- Test 4.7.2 : Chaque média temporel synchronisé pré-enregistré vérifie-t-il, si nécessaire, une de ces conditions (hors cas particuliers) ?
  - Il existe une audio-description synchronisée ;
  - Il existe une version alternative avec une audio-description synchronisée.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.2.5

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G58 - G8 - G78 - G173 - H96 - SM1 - SM2 - SM6 - SM7

Critère 4.8 [AA] Pour chaque média temporel pré-enregistré ayant une audio-description synchronisée, celle-ci est-elle pertinente ?

Principe WCAG : Utilisable

Niveau RGAA PF : AA

- Test 4.8.1 : Pour chaque média temporel pré-enregistré seulement vidéo ayant une audio-description synchronisée, celle-ci est-elle pertinente ?
- Test 4.8.2 : Pour chaque média temporel synchronisé ayant une audio-description synchronisée, celle-ci est-elle pertinente ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.2.5

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : SM1 - SM2 - SM6 - SM7

Critère 4.9 [AAA] Chaque média temporel pré-enregistré a-t-il, si nécessaire, une interprétation en langue des signes (hors cas particuliers) ?

Principe WCAG : Utilisable

Niveau RGAA PF : AAA

- Test 4.9.1 : Chaque média temporel pré-enregistré seulement audio a-t-il, si nécessaire, une interprétation en langue des signes adaptée à la langue du média (hors cas particuliers) ?
- Test 4.9.2 : Chaque média temporel synchronisé pré-enregistré a-t-il, si nécessaire, une interprétation en langue des signes adaptée à la langue du média (hors cas particuliers) ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.2.6

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G54 - G81 - SM13 - SM14

Critère 4.10 [AAA] Pour chaque média temporel pré-enregistré ayant une interprétation en langue des signes, celle-ci est-elle pertinente ?

Principe WCAG : Utilisable

Niveau RGAA PF : AAA

- Test 4.10.1 : Pour chaque média temporel pré-enregistré seulement audio ayant une interprétation en langue des signes, celle-ci est-elle pertinente ?
- Test 4.10.2 : Pour chaque média temporel synchronisé pré-enregistré ayant une interprétation en langue des signes, celle-ci est-elle pertinente ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.2.6

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G54 - G81 - SM13 - SM14

Critère 4.11 [AAA] Chaque média temporel pré-enregistré a-t-il, si nécessaire, une audio-description étendue synchronisée (hors cas particuliers) ?

Principe WCAG : Utilisable

Niveau RGAA PF : AAA

- Test 4.11.1 : Chaque média temporel synchronisé pré-enregistré vérifie-t-il, si nécessaire, une de ces conditions (hors cas particuliers) ?
    - Il existe une audio-description étendue synchronisée ;

    - Il existe une version alternative avec une audio-description étendue synchronisée.
- Test 4.11.2 : Chaque média temporel pré-enregistré seulement vidéo vérifie-t-il, si nécessaire, une de ces conditions (hors cas particuliers) ?
    - Il existe une audio-description étendue synchronisée ;
    - Il existe une version alternative avec une audio-description étendue synchronisée.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.2.7

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G58 - G8 - H96 - SM1 - SM2

Critère 4.12 [AAA] Pour chaque média temporel pré-enregistré ayant une audio-description étendue synchronisée, celle-ci est-elle pertinente ?

Principe WCAG : Utilisable

Niveau RGAA PF : AAA

- Test 4.12.1 : Pour chaque média temporel synchronisé pré-enregistré ayant une audio-description étendue synchronisée, celle-ci est-elle pertinente ?
- Test 4.12.2 : Pour chaque média temporel pré-enregistré seulement vidéo ayant une audio-description étendue synchronisée, celle-ci est-elle pertinente ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.2.7

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G8 - SM1 - SM2

Critère 4.13 [AAA] Chaque média temporel synchronisé ou seulement vidéo a-t-il, si nécessaire, une transcription textuelle (hors cas particuliers) ?

Principe WCAG : Utilisable

Niveau RGAA PF : AAA

- Test 4.13.1 : Chaque média temporel synchronisé vérifie-t-il si nécessaire une de ces conditions (hors cas particuliers) ?
    - Il existe une transcription textuelle accessible *via* un lien adjacent (une url ou une ancre) ;
    - Il existe une transcription textuelle adjacente clairement identifiable.
- Test 4.13.2 : Chaque média temporel seulement vidéo vérifie-t-il si nécessaire une de ces conditions (hors cas particuliers) ?
    - Il existe une transcription textuelle accessible *via* un lien adjacent (une url ou une ancre) ;

- Il existe une transcription textuelle adjacente clairement identifiable.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.2.8

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G58 - G69 - G159

Critère 4.14 [AAA] Pour chaque média temporel synchronisé ou seulement vidéo, ayant une transcription textuelle, celle-ci est-elle pertinente ?

Principe WCAG : Utilisable

Niveau RGAA PF : AAA

- Test 4.14.1 : Pour chaque média temporel seulement vidéo ayant une transcription textuelle, celle-ci est-elle pertinente ?
- Test 4.14.2 : Chaque média temporel synchronisé ayant une transcription textuelle, celle-ci est-elle pertinente ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.2.8

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : F74

Critère 4.15 [A] Chaque média temporel est-il clairement identifiable (hors cas particuliers) ?

Principe WCAG : Utilisable

Niveau RGAA PF : A

- Test 4.15.1 : Pour chaque média temporel seulement son, seulement vidéo ou synchronisé, le contenu textuel adjacent permet-il d'identifier clairement le média temporel (hors cas particuliers) ?
- Test 4.15.2 : Pour chaque média temporel seulement son en direct, seulement vidéo en direct ou synchronisé en direct, le contenu textuel adjacent permet-il d'identifier clairement le média temporel (hors cas particuliers) ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.1.1

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G68 - G100

Critère 4.16 [A] Chaque média non temporel a-t-il, si nécessaire, une alternative (hors cas particuliers) ?

Principe WCAG : Utilisable

Niveau RGAA PF : A

- Test 4.16.1 : Chaque média non temporel vérifie-t-il, si nécessaire, une de ces conditions (hors cas particuliers) ?
    - Un lien adjacent, clairement identifiable, contient l'adresse (url) d'une page contenant une alternative ;
    - Un lien adjacent, clairement identifiable, permet d'accéder à une alternative dans la page.
- Test 4.16.2 : Chaque média non temporel associé à une alternative vérifie-t-il une de ces conditions (hors cas particuliers) ?
    - La page référencée par le lien adjacent est accessible ;
    - L'alternative dans la page, référencée par le lien adjacent, est accessible.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.1.1

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : H35 - H46

Critère 4.17 [A] Pour chaque média non temporel ayant une alternative, cette alternative est-elle pertinente ?

Principe WCAG : Utilisable

Niveau RGAA PF : A

- Test 4.17.1 : Pour chaque média non temporel ayant une alternative, cette alternative permet-elle d'accéder au même contenu et à des fonctionnalités similaires ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.1.1

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : H46 - F30

Critère 4.18 [A] Chaque son déclenché automatiquement est-il contrôlable par l'utilisateur ?

Principe WCAG : Utilisable

Niveau RGAA PF : A

- Test 4.18.1 : Chaque séquence sonore déclenchée automatiquement *via* une balise object, video, audio, embed, bgsoundou un code JavaScript vérifie-t-elle une de ces conditions ?
    - La séquence sonore a une durée inférieure ou égale à 3 secondes ;
    - La séquence sonore peut être stoppée sur action de l'utilisateur ;
    - Le volume de la séquence sonore peut être contrôlé par l'utilisateur indépendamment du contrôle de volume du système.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.4.2

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G60 - G170 - G171 - F23 - F93

Critère 4.19 [AAA] Pour chaque média temporel seulement audio pré- enregistré, les dialogues sont-ils suffisamment audibles (hors cas particuliers) ?

Principe WCAG : Utilisable

Niveau RGAA PF : AAA

- Test 4.19.1 : Chaque média temporel audio pré-enregistré et diffusé *via* une balise object, video, audio, embed, bgsound, ou proposé en téléchargement, vérifie-t-il une de ces conditions (hors cas particuliers) ?
    - L'arrière-plan sonore peut être désactivé ;
    - La ou les pistes de dialogue sont 20 décibels plus élevées que l'arrière-plan sonore ;
    - Il existe une version alternative pour laquelle l'arrière-plan sonore peut être désactivé ;
    - Il existe une version alternative pour laquelle la ou les pistes de dialogue sont 20 décibels plus élevées que l'arrière-plan sonore.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.4.7

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G56

Critère 4.20 [A] La consultation de chaque média temporel est-elle, si nécessaire, contrôlable par le clavier et la souris ?

Principe WCAG : Utilisable

Niveau RGAA PF : A

- Test 4.20.1 : Chaque média temporel a-t-il, si nécessaire, les fonctionnalités de contrôle de sa consultation ?
- Test 4.20.2 : Pour chaque média temporel, chaque fonctionnalité vérifie-t-elle une de ces conditions ?
    - La fonctionnalité est accessible par le clavier et la souris ;
    - Une fonctionnalité accessible par le clavier et la souris permettant de réaliser la même action est présente dans la page.
- Test 4.20.3 : Pour chaque média temporel, chaque fonctionnalité vérifie-t-elle une de ces conditions ?
    - La fonctionnalité est activable par le clavier et la souris ;
    - Une fonctionnalité activable par le clavier et la souris permettant de réaliser la même

action est présente dans la page.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 2.1.1 - 2.1.2

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G90 - G4 G202

Critère 4.21 [A] La consultation de chaque média non temporel est-elle contrôlable par le clavier et la souris ?

Principe WCAG : Utilisable

Niveau RGAA PF : A

- Test 4.21.1 : Pour chaque média non temporel, chaque fonctionnalité vérifie-t-elle une de ces conditions ?
    - La fonctionnalité est accessible par le clavier et la souris ;
    - Une fonctionnalité accessible par le clavier et la souris permettant de réaliser la même action est présente dans la page.
- Test 4.21.2 : Pour chaque média non temporel, chaque fonctionnalité vérifie-t-elle une de ces conditions ?
    - La fonctionnalité est activable par le clavier et la souris ;
    - Une fonctionnalité activable par le clavier et la souris permettant de réaliser la même action est présente dans la page.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 2.1.1 - 2.1.2

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G90 - G4

Critère 4.22 [A] Chaque média temporel et non temporel est-il compatible avec les technologies d'assistance (hors cas particuliers) ?

Principe WCAG : Utilisable

Niveau RGAA PF : A

- Test 4.22.1 : Chaque média temporel et non temporel inséré *via* une balise objectou embedvérifie-t-il une de ces conditions (hors cas particuliers) ?
    - Le nom, le rôle, la valeur, le paramétrage et les changements d'états des composants d'interfaces sont accessibles aux technologies d'assistance *via* une API d'accessibilité ;
    - Une alternative compatible avec une API d'accessibilité permet d'accéder aux mêmes fonctionnalités.
- Test 4.22.2 : Chaque média temporel et non temporel inséré *via* une balise objectou

embed, qui possède une alternative compatible avec les technologies d'assistance, vérifie-t-il une de ces conditions ?

- L'alternative est adjacente au média temporel ou non temporel ;
- L'alternative est accessible *via* un lien adjacent (une url ou une ancre) ;
- Un mécanisme permet de remplacer le média temporel ou non temporel par son alternative.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 4.1.2

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G10 - G135 - F15 - F54

5. Tableaux

Principe WCAG : Perceptible

Recommandation :

Donner à chaque tableau de données complexe, un résumé et un titre pertinent, identifier clairement les cellules d'en-tête, utiliser un mécanisme pertinent pour lier les cellules de données aux cellules d'en-tête. Pour chaque tableau de mise en forme, veiller à sa bonne linéarisation.

Critère 5.1 [A] Chaque tableau de données complexe a-t-il un résumé ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 5.1.1 : Pour chaque tableau de données complexe (balise table) un résumé est-il disponible dans la balise caption?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.3.1

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : H73

Critère 5.2 [A] Pour chaque tableau de données complexe ayant un résumé, celui-ci est-il pertinent ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 5.2.1 : Pour chaque tableau de donnée complexes (balise table) ayant un résumé, celui-ci est-il pertinent ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.3.1

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : H73

Critère 5.3 [A] Pour chaque tableau de mise en forme, le contenu linéarisé reste-t-il compréhensible (hors cas particuliers) ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 5.3.1 : Chaque tableau de mise en forme vérifie-t-il ces conditions (hors cas particuliers) ?
    - Le contenu linéarisé reste compréhensible ;
    - La balise tablepossède un attribut role="presentation".

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.3.2 - 4.1.2

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : F49 - ARIA4

Critère 5.4 [A] Chaque tableau de données a-t-il un titre ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 5.4.1 : Chaque tableau de données (balise table) a-t-il une balise caption?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.3.1

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : H39

Critère 5.5 [A] Pour chaque tableau de données ayant un titre, celui-ci est-il pertinent ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 5.5.1 : Pour chaque tableau de données (balise table) ayant une balise caption, le contenu de cette balise donne-t-il le titre du tableau ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.3.1

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : H39

Critère 5.6 [A] Pour chaque tableau de données, chaque en-tête de colonnes et chaque en-tête de lignes sont-ils correctement déclarés ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 5.6.1 : Pour chaque tableau de données (balise table), chaque en-tête de colonnes a-t-il une balise th?
- Test 5.6.2 : Pour chaque tableau de données (balise table), chaque en-tête de lignes a-t-il une balise th?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.3.1

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : H51 - F91

Critère 5.7 [A] Pour chaque tableau de données, la technique appropriée permettant d'associer chaque cellule avec ses en-têtes est-elle utilisée ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 5.7.1 : Chaque en-tête (balise th) s'appliquant à la totalité de la ligne ou de la colonne possède-t-il un attribut idunique ou un attribut scope?
- Test 5.7.2 : Chaque en-tête (balise th) s'appliquant à la totalité de la ligne ou de la colonne et possédant un attribut scopevérifie-t-il une de ces conditions ?
    - L'en-tête possède un attribut scopeavec la valeur "row"pour les en-tête de lignes ;
    - L'en-tête possède un attribut scope avec la valeur "col" pour les en-tête de colonnes.
- Test 5.7.3 : Chaque en-tête (balise th) ne s'appliquant pas à la totalité de la ligne ou de la colonne vérifie-t-il ces conditions ?
    - L'en-tête ne possède pas d'attribut scope;
    - L'en-tête possède un attribut idunique.
- Test 5.7.4 : Chaque cellule (balise tdou th) associée à un ou plusieurs en-têtes possédant un attribut idvérifie-t-elle ces conditions ?
    - La cellule possède un attribut headers;
    - L'attribut headerspossède la liste des valeurs des en-têtes associés à la cellule.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.3.1

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : H63 - H43 - F90

Critère 5.8 [A] Chaque tableau de mise en forme ne doit pas utiliser d'éléments propres aux tableaux de données. Cette règle est-elle respectée ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 5.8.1 : Chaque tableau de mise en forme (balise table) vérifie-t-il ces conditions ?
    - Le tableau de mise en forme (balise table) ne possède pas de balises caption, th, thead, tfoot;
    - Les cellules du tableau de mise en forme (balise td) ne possèdent pas d'attributs scope, headers, colgroup, axis.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.3.1

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : F46

6. Liens

Principe WCAG : Perceptible

Recommandation :

Donner des intitulés de lien explicites, grâce à des informations de contexte notamment, et utiliser le titre de lien le moins possible.

Critère 6.1 [A] Chaque lien est-il explicite (hors cas particuliers) ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 6.1.1 : Chaque lien texte vérifie-t-il une de ces conditions (hors cas particuliers) ?
    - L'intitulé de lien seul permet d'en comprendre la fonction et la destination ;
    - Le contexte du lien permet d'en comprendre la fonction et la destination.
- Test 6.1.2 : Chaque lien image vérifie-t-il une de ces conditions (hors cas particuliers) ?
    - L'intitulé de lien seul permet d'en comprendre la fonction et la destination ;
    - Le contexte du lien permet d'en comprendre la fonction et la destination.
- Test 6.1.3 : Chaque lien composite vérifie-t-il une de ces conditions (hors cas particuliers) ?
    - L'intitulé de lien seul permet d'en comprendre la fonction et la destination ;
    - Le contexte du lien permet d'en comprendre la fonction et la destination.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.1.1 - 2.4.4 - 2.4.9

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : H79 - H78 - H79 - H80 - H81 - H30 - F89 - G91 - G53 - ARIA7 - ARIA8 - F63

Critère 6.2 [A] Pour chaque lien ayant un titre de lien, celui-ci est-il pertinent ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 6.2.1 : Pour chaque lien texte ayant un titre de lien (attribut title), le contenu de cet attribut est-il pertinent ?
- Test 6.2.2 : Pour chaque lien image ayant un titre de lien (attribut title), le contenu de cet attribut est-il pertinent ?
- Test 6.2.3 : Pour chaque lien composite ayant un titre de lien (attribut title), le contenu de cet attribut est-il pertinent ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 2.4.4

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : H33

Critère 6.3 [AAA] Chaque intitulé de lien seul est-il explicite hors contexte (hors cas particuliers) ?

Principe WCAG : Perceptible

Niveau RGAA PF : AAA

- Test 6.3.1 : Chaque lien texte vérifie-t-il une de ces conditions (hors cas particuliers) ?
  - L'intitulé du lien est explicite hors contexte ;
  - Un mécanisme permet à l'utilisateur d'obtenir un intitulé de lien explicite hors contexte ;
  - Le contenu du titre de lien (attribut title) est explicite hors contexte.
- Test 6.3.2 : Chaque intitulé de lien image est-il explicite hors contexte (hors cas particuliers) ?
- Test 6.3.3 : Chaque lien composite (contenu texte et de l'attribut alt) est-il explicite hors contexte (hors cas particuliers) ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 2.4.9

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G91 - G189 - H33 - SCR30 - F84

Critère 6.4 [A] Pour chaque page Web, chaque lien identique a-t-il les mêmes fonction et destination ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 6.4.1 : Pour chaque page Web, chaque lien identique de type texte a-t-il les mêmes fonction et destination ?
- Test 6.4.2 : Pour chaque page Web, chaque lien identique de type image a-t-il les mêmes fonction et destination ?
- Test 6.4.3 : Pour chaque page Web, chaque lien identique de type composite a-t-il les mêmes fonction et destination ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 2.4.4 - 3.2.4

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : H79 - H78 - H79 - H80 - G91 - G197 - H30 - H33 - ARIA7 - ARIA8

Critère 6.5 [A] Dans chaque page Web, chaque lien, à l'exception des ancres, a-t-il un intitulé ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 6.5.1 : Dans chaque page Web, chaque lien (balise aavec un attribut href), à l'exception des ancres, a-t-il un intitulé entre <a>et ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.1.1 - 2.4.4 - 2.4.9

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G91 - H30 - F89

7. Scripts

Principe WCAG : Perceptible

Recommandation :

Donner si nécessaire à chaque script une alternative pertinente. Rendre possible le contrôle de chaque code script au moins par le clavier et la souris et s'assurer de leur compatibilité avec les technologies d'assistance.

Critère 7.1 [A] Chaque script est-il, si nécessaire, compatible avec les technologies d'assistance ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 7.1.1 : Chaque script qui génère ou contrôle un composant d'interface vérifie-t-il, si nécessaire, une de ces conditions ?
    - Le nom, le rôle, la valeur, le paramétrage et les changements d'états sont accessibles aux technologies d'assistance *via* une API d'accessibilité ;
    - Un composant d'interface accessible permettant d'accéder aux mêmes fonctionnalités est présent dans la page ;
    - Une alternative accessible permet d'accéder aux mêmes fonctionnalités.
- Test 7.1.2 : Chaque fonctionnalité d'insertion de contenu contrôlée par un script utilise-t-elle des propriétés et méthodes conformes à la spécification DOM (Document Object Model) ?
- Test 7.1.3 : Chaque script qui génère, met à jour ou contrôle un composant d'interface qui comporte des rôles des états ou des propriétés correspondant à un motif de conception défini par l'API ARIA vérifie-t-il une de ces conditions ?
    - Le composant d'interface est conforme au motif de conception défini par l'API ARIA ;
    - Un composant d'interface présent sur la page, permettant d'accéder aux mêmes fonctionnalités, est conforme au motif de conception défini par l'API ARIA ;
    - Le composant d'interface adapte un motif de conception défini par l'API ARIA ;
    - Une alternative accessible permet d'accéder aux mêmes fonctionnalités.
- Test 7.1.4 : Chaque modification du rôle natif d'un élément HTML respecte-t-elle les règles et préconisations indiquées dans la spécification HTML5 et les notes techniques associées ?
- Test 7.1.5 : Chaque script qui génère ou contrôle un composant d'interface *via* des rôles, des états ou des propriétés définis par l'API ARIA respecte-t-il une de ces conditions ?
    - Le composant d'interface est correctement restitué par les technologies d'assistance ;
    - Une alternative accessible permet d'accéder aux mêmes fonctionnalités.
- Test 7.1.6 : Chaque composant d'interface qui utilise un rôle ARIA application respecte-t-il une de ces conditions ?
    - Le composant d'interface est correctement restitué par les technologies d'assistance ;
    - Une alternative accessible permet d'accéder aux mêmes fonctionnalités.

Note technique : Consulter la note technique au sujet des alternatives à JavaScript.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 4.1.2

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G10 - G135 - G136 - ARIA4 - ARIA5 - ARIA18 - ARIA19 - SCR21 - F15 - F19 - F42 - F59 - F79 - F20

Critère 7.2 [A] Pour chaque script ayant une alternative, cette alternative est-elle pertinente ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 7.2.1 : Chaque script débutant par la balise scriptet ayant une alternative vérifie-t-il une de ces conditions ?
    - L'alternative entre <noscript>et </noscript>permet d'accéder à des contenus et des fonctionnalités similaires ;
    - La page affichée, lorsque JavaScript est désactivé, permet d'accéder à des contenus et des fonctionnalités similaires ;
    - La page alternative permet d'accéder à des contenus et des fonctionnalités similaires ;
    - Le langage de script côté serveur permet d'accéder à des contenus et des fonctionnalités similaires ;
    - L'alternative présente dans la page permet d'accéder à des contenus et des fonctionnalités similaires.
- Test 7.2.2 : Chaque élément non textuel mis à jour par un script (dans la page, ou un cadre en ligne) et ayant une alternative vérifie-t-il ces conditions ?
    - L'alternative de l'élément non textuel est mise à jour ;
    - L'alternative mise à jour est pertinente.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 4.1.2 - 1.1.1

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G136 - F19 - F20.

Critère 7.3 [A] Chaque script est-il contrôlable par le clavier et la souris (hors cas particuliers) ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 7.3.1 : Chaque élément possédant un gestionnaire d'événement contrôlé par un script vérifie-t-il une de ces conditions (hors cas particuliers) ?
    - L'élément est accessible par le clavier et la souris ;
    - Un élément accessible par le clavier et la souris permettant de réaliser la même action est présent dans la page.
- Test 7.3.2 : Un script ne doit pas supprimer le focus d'un élément qui le reçoit. Cette règle est-elle respectée (hors cas particuliers) ?
- Test 7.3.3 : Chaque composant d'interface implémenté *via* un rôle défini par l'API ARIA et correspondant à un motif de conception respecte-t-il une de ces conditions ?
    - Les interactions au clavier sont conformes au comportement défini par le motif de conception pour les touches Echap, Barre d'espace, Tabulationet Flèches de directionau moins ;

- Un composant d'interface présent sur la page, permettant de réaliser la même action, possède des interactions au clavier conformes au comportement défini par le motif de conception, pour les touches Échap, Barre d'espace, Tabulationet Flèches de direction au moins ;
- Une alternative permettant d'accéder aux mêmes fonctionnalités est contrôlable par le clavier et la souris.

Note technique : Consulter la note technique au sujet des interactions au clavier *via* l'API ARIA.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.3.1 - 2.1.1 - 2.4.7

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G202 - SCR2 - SCR20 - SCR29 - SCR35 - G90 - F42 - F54 - F55

Critère 7.4 [A] Pour chaque script qui initie un changement de contexte, l'utilisateur est-il averti ou en a-t-il le contrôle ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 7.4.1 : Chaque script qui initie un changement de contexte vérifie-t-il une de ces conditions ?
  - L'utilisateur est averti par un texte de l'action du script et du type de changement avant son déclenchement ;
  - Le changement de contexte est initié par un bouton (inputde type submit, buttonou imageou balise button) explicite ;
  - Le changement de contexte est initié par un lien explicite.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 3.2.1 - 3.2.2 - 3.2.5

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : F9 - F22 - F36 - F37 - F41 - G13 - G76 - G80 - G107 - H32 - H84 - SCR19

Critère 7.5 [AAA] Chaque script qui provoque une alerte non sollicitée est-il contrôlable par l'utilisateur (hors cas particuliers) ?

Principe WCAG : Perceptible

Niveau RGAA PF : AAA

- Test 7.5.1 : Chaque script qui provoque une alerte non sollicitée est-il contrôlable par l'utilisateur (hors cas particuliers) ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 2.2.4

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : SCR14

8. Éléments Obligatoires

Principe WCAG : Perceptible

Recommandation :

Vérifier que chaque page Web a un code source valide selon le type de document, un titre pertinent et une indication de langue par défaut. Vérifier que les balises ne sont pas utilisées uniquement à des fins de présentation, que les changements de langues et de direction de sens de lecture sont indiqués.

Critère 8.1 [A] Chaque page Web est-elle définie par un type de document ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 8.1.1 : Pour chaque page Web, le type de document (balise doctype) est-il présent ?
- Test 8.1.2 : Pour chaque page Web, le type de document (balise doctype) est-il valide ?
- Test 8.1.3 : Pour chaque page Web possédant une déclaration de type de document, celle-ci est-elle située avant la balise htmldans le code source ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 4.1.1

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G134 - G192

Critère 8.2 [A] Pour chaque page Web, le code source est-il valide selon le type de document spécifié (hors cas particuliers) ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 8.2.1 : Pour chaque déclaration de type de document, le code source de la page vérifie-t-il ces conditions (hors cas particuliers) ?
    - Les balises respectent les règles d'écriture ;
    - L'imbrication des balises est conforme ;
    - L'ouverture et la fermeture des balises sont conformes ;
    - Les attributs respectent les règles d'écriture ;
    - Les valeurs des attributs respectent les règles d'écriture.
- Test 8.2.2 : Pour chaque déclaration de type de document, le code source de la page ne doit

pas utiliser d'éléments obsolètes. Cette règle est-elle respectée (hors cas particuliers) ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 4.1.1 - 4.1.2

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G134 - G192 - H74 - H75 - H88 - H93 - H94 - F70 - F77 - F62

Critère 8.3 [A] Dans chaque page Web, la langue par défaut est-elle présente ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 8.3.1 : Pour chaque page Web, l'indication de langue par défaut vérifie-t-elle une de ces conditions ?
    - L'indication de la langue de la page (attribut langet/ou xml:lang) est donnée pour l'élément html;
    - L'indication de la langue de la page (attribut langet/ou xml:lang) est donnée sur chaque élément de texte ou sur l'un des éléments parents.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 3.1.1

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : H57

Critère 8.4 [A] Pour chaque page Web ayant une langue par défaut, le code de langue est-il pertinent ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 8.4.1 : Pour chaque page Web ayant une langue par défaut, le code de langue vérifie-t-il ces conditions ?
    - Le code de langue est valide ;
    - Le code de langue est pertinent.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 3.1.1

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : H57

Critère 8.5 [A] Chaque page Web a-t-elle un titre de page ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 8.5.1 : Chaque page Web a-t-elle un titre de page (balise title) ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 2.4.2

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G88 - G127 - H25

Critère 8.6 [A] Pour chaque page Web ayant un titre de page, ce titre est-il pertinent ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 8.6.1 : Pour chaque page Web ayant un titre de page (balise title), le contenu de cette balise est-il pertinent ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 2.4.2

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G88 - G127 - F25

Critère 8.7 [AA] Dans chaque page Web, chaque changement de langue est-il indiqué dans le code source (hors cas particuliers) ?

Principe WCAG : Perceptible

Niveau RGAA PF : AA

- Test 8.7.1 : Dans chaque page Web, chaque texte écrit dans une langue différente de la langue par défaut vérifie-t-il une de ces conditions (hors cas particuliers) ?
    - L'indication de langue est donnée sur l'élément contenant le texte ;
    - L'indication de langue est donnée sur un des éléments parents.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 3.1.2

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : H58

Critère 8.8 [AA] Dans chaque page Web, chaque changement de langue est-il pertinent ?

Principe WCAG : Perceptible

Niveau RGAA PF : AA

- Test 8.8.1 : Dans chaque page Web, chaque changement de langue (attribut langet/ou

xml:lang) est-il valide ?

- Test 8.8.2 : Dans chaque page Web, chaque changement de langue (attribut langet/ou xml:lang) est-il pertinent ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 3.1.2

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : H58

Critère 8.9 [A] Dans chaque page Web, les balises ne doivent pas être utilisées uniquement à des fins de présentation. Cette règle est- elle respectée ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 8.9.1 : Dans chaque page Web les balises (à l'exception de div, spanet table) ne doivent pas être utilisées uniquement à des fins de présentation. Cette règle est-elle respectée ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.3.1

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G115 - H88 - F43 - F92

Critère 8.10 [A] Dans chaque page Web, les changements du sens de lecture sont-ils signalés ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 8.10.1 : Dans chaque page Web, chaque texte dont le sens de lecture est différent du sens de lecture par défaut vérifie-t-il ces conditions ?
    - Le texte est contenu dans une balise possédant un attribut dir;
    - La valeur de l'attribut direst conforme (rtlou ltr) ;
    - La valeur de l'attribut direst pertinente.
- Test 8.10.2 : Dans chaque page Web, chaque changement du sens de lecture (attribut dir) vérifie-t-il ces conditions ?
    - La valeur de l'attribut direst conforme (rtlou ltr) ;
    - La valeur de l'attribut direst pertinente.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.3.2

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : H56

9. Structuration de l'information

Principe WCAG : Perceptible

Recommandation :

Utiliser des titres, des listes, des abréviations et des citations pour structurer l'information. S'assurer que la structure du document est cohérente.

Critère 9.1 [A] Dans chaque page Web, l'information est-elle structurée par l'utilisation appropriée de titres ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 9.1.1 : Dans chaque page Web, y a-t-il un titre de niveau 1 (balise h1ou balise possédant un rôle ARIA "heading"associé à une propriété aria-level="1") ?
- Test 9.1.2 : Dans chaque page Web, la hiérarchie entre les titres (balise hou balise possédant un rôle ARIA "heading"associé à une propriété aria-level) est-elle pertinente ?
- Test 9.1.3 : Dans chaque page Web, chaque titre (balise hou balise possédant un rôle ARIA "heading"associé à une propriété aria-level) nécessaire à la structure de l'information est-il présent ?
- Test 9.1.4 : Dans chaque page Web, chaque titre (balise hou balise possédant un rôle ARIA "heading"associé à une propriété aria-level) est-il pertinent ?

Note technique : Consulter la note technique au sujet du rôle ARIA headinget l'utilisation des titres h1.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.3.1 - 2.4.1 - 2.4.6 - 2.4.10 - 4.1.2

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : H69 - G115 - G130 - H42 - G141 - ARIA4 - ARIA12

Critère 9.2 [A] Dans chaque page Web, la structure du document est-elle cohérente ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 9.2.1 : Dans chaque page Web, la structure du document vérifie-t-elle ces conditions ?
  - La zone d'en-tête de la page est structurée *via* une balise header;
  - Les zones de navigation principales et secondaires sont structurées *via* une balise

nav;
    - La balise navest réservée à la structuration des zones de navigation principales et secondaires ;
    - La zone de contenu principal est structurée *via* une balise main;
    - La structure du document utilise une balise mainunique ;
    - La zone de pied de page est structurée *via* une balise footer.
- Test 9.2.2 : Dans chaque page Web, l'arborescence du document est-elle cohérente ?

Note technique : Consulter la note technique au sujet de la structure du document et de l'outline.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.3.1

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G115 - ARIA11

Critère 9.3 [A] Dans chaque page Web, chaque liste est-elle correctement structurée ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 9.3.1 : Dans chaque page Web, les informations regroupées sous forme de listes non ordonnées vérifient-elles une de ces conditions ?
    - La liste utilise les balises HTML ulet li;
    - La liste utilise les rôles ARIA listet listitem;
- Test 9.3.2 : Dans chaque page Web, les informations regroupées sous forme de listes ordonnées vérifient-elles une de ces conditions ?
    - La liste utilise les balises HTML olet li;
    - La liste utilise les rôles ARIA listet listitem.
- Test 9.3.3 : Dans chaque page Web, les informations regroupées sous forme de listes de définitions utilisent-elles les balises dlet dt/dd?

Note technique : Consulter la note technique au sujet des rôles listet listitem.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.3.1

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G153 - G115 - H40 - H48 - H97 - F2

Critère 9.4 [AAA] Dans chaque page Web, la première occurrence de chaque abréviation permet-elle d'en connaître la signification ?

Principe WCAG : Perceptible

Niveau RGAA PF : AAA

- Test 9.4.1 : Dans chaque page Web, la première occurrence de chaque abréviation vérifie-t-elle une de ces conditions ?
    - L'abréviation est accompagnée de sa signification sous forme d'un texte adjacent ;
    - L'abréviation est implémentée *via* un lien référençant une page ou un emplacement dans la page qui permet d'en connaître la signification ;
    - L'abréviation fait partie d'un lien possédant un attribut titlequi permet d'en connaître la signification ;
    - La signification de l'abréviation est présente dans un glossaire présent sur le site ;
    - L'abréviation est implémentée *via* une balise abbrpossédant un attribut titlequi permet d'en connaître la signification.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 3.1.4

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G55 - G70 - G97 - G102 - H28

Critère 9.5 [AAA] Dans chaque page Web, la signification de chaque abréviation est-elle pertinente ?

Principe WCAG : Perceptible

Niveau RGAA PF : AAA

- Test 9.5.1 : Dans chaque page Web, la signification de chaque abréviation est-elle pertinente ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 3.1.4

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G55 - G70 - G97 - G102 - H28

Critère 9.6 [A] Dans chaque page Web, chaque citation est-elle correctement indiquée ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 9.6.1 : Dans chaque page Web, chaque citation courte utilise-t-elle une balise q?
- Test 9.6.2 : Dans chaque page Web, chaque bloc de citation utilise-t-il une balise blockquote?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.3.1

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G115 - H49 - F2

10. Présentation de l'information

Principe WCAG : Perceptible

Recommandation :

Utiliser des feuilles de styles pour contrôler la présentation de l'information. Vérifier l'effet de l'agrandissement des taille des caractères sur la lisibilité. S'assurer que les liens sont correctement identifiables, que la prise de focus est signalée, que l'interlignage est suffisant et donner la possibilité à l'utilisateur de contrôler la justification des textes. S'assurer que les textes cachés sont correctement restitués et que l'information n'est pas donnée uniquement par la forme ou la position d'un élément.

Critère 10.1 [A] Dans le site Web, des feuilles de styles sont-elles utilisées pour contrôler la présentation de l'information ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 10.1.1 : Dans chaque page Web, les balises servant à la présentation de l'information ne doivent pas être présentes dans le code source des pages. Cette règle est-elle respectée ?
- Test 10.1.2 : Dans chaque page Web, les attributs servant à la présentation de l'information ne doivent pas être présents dans le code source des pages. Cette règle est-elle respectée ?
- Test 10.1.3 : Dans chaque page Web, l'utilisation des espaces vérifie-t-elle ces conditions ?
    - Les espaces ne sont pas utilisés pour séparer les lettres d'un mot ;
    - Les espaces ne sont pas utilisés pour simuler des tableaux ;
    - Les espaces ne sont pas utilisés pour simuler des colonnes de texte.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.3.1 - 1.3.2

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G140 - F32 - F33 - F34 - C6 - C8 - C18 - C22 - F48

Critère 10.2 [A] Dans chaque page Web, le contenu visible reste-t-il présent lorsque les feuilles de styles sont désactivées ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 10.2.1 : Dans chaque page Web, l'information reste-t-elle présente lorsque les feuilles de styles sont désactivées ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.1.1 - 1.3.1

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G140 - F3 - F87

Critère 10.3 [A] Dans chaque page Web, l'information reste-t-elle compréhensible lorsque les feuilles de styles sont désactivées ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 10.3.1 : Dans chaque page Web, l'information reste-t-elle compréhensible lorsque les feuilles de styles sont désactivées ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.3.2 - 2.4.3

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : F1 - G59 - G140

Critère 10.4 [AA] Dans chaque page Web, le texte reste-t-il lisible lorsque la taille des caractères est augmentée jusqu'à 200%, au moins ?

Principe WCAG : Perceptible

Niveau RGAA PF : AA

- Test 10.4.1 : Dans les feuilles de styles du site Web, les unités non relatives (pt, pc, mm, cm, in) ne doivent pas être utilisées pour les types de média screen, tv, handheld, projection. Cette règle est-elle respectée ?
- Test 10.4.2 : Dans les feuilles de styles du site Web, pour les types de média screen, tv, handheld, projection, les tailles de caractères utilisent-elles uniquement des unités relatives ?
- Test 10.4.3 : Dans chaque page Web, l'augmentation de la taille des caractères jusqu'à 200%, au moins, ne doit pas provoquer de perte d'information. Cette règle est-elle respectée ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.4.4

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G146 - F80 - F69 - C14 - C12 - C13 - C17 - C28 - G179 - SCR34

Critère 10.5 [AA] Dans chaque page Web, les déclarations CSS de couleurs de fond d'élément et de police sont-elles correctement utilisées?

Principe WCAG : Perceptible

Niveau RGAA PF : AA

- Test 10.5.1 : Dans chaque page Web, chaque déclaration CSS de couleurs de police (color), d'un élément susceptible de contenir du texte, est-elle accompagnée d'une déclaration de couleur de fond (background, background-color), au moins, héritée d'un parent ?
- Test 10.5.2 : Dans chaque page Web, chaque déclaration de couleur de fond (background, background-color), d'un élément susceptible de contenir du texte, est-elle accompagnée d'une déclaration de couleur de police (color) au moins, héritée d'un parent ?
- Test 10.5.3 : Dans chaque page Web, chaque utilisation d'une image pour créer une couleur de fond d'un élément susceptible de contenir du texte, *via* CSS (background, background-image), est-elle accompagnée d'une déclaration de couleur de fond (background, background-color), au moins, héritée d'un parent ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.4.3 - 1.4.6 - 1.4.8

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : F24

Critère 10.6 [A] Dans chaque page Web, chaque lien dont la nature n'est pas évidente est-il visible par rapport au texte environnant ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 10.6.1 : Dans chaque page Web, chaque lien texte signalé uniquement par la couleur, et dont la nature n'est pas évidente, a-t-il un rapport de contraste supérieur ou égal à 3:1 par rapport au texte environnant ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.4.1

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G183 - F73

Critère 10.7 [A] Dans chaque page Web, pour chaque élément recevant le focus, la prise de focus est-elle visible ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 10.7.1 : Pour chaque élément recevant le focus, l'indication visuelle du navigateur ne doit pas être supprimée (propriété CSS outline, outline-color, outline-width, outline-style). Cette règle est-elle respectée ?
- Test 10.7.2 : Pour chaque élément recevant le focus, l'indication visuelle du navigateur ne doit pas être dégradée (propriété CSS outline-color). Cette règle est-elle respectée ?
- Test 10.7.3 : Chaque lien dans un texte signalé par la couleur uniquement vérifie-t-il ces conditions ?
    - Une indication visuelle autre que la couleur permet de signaler la prise de focus au clavier ;
    - Une indication visuelle autre que la couleur permet de signaler le survol du lien à la souris.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.4.1 - 2.4.7

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G149 - G183 - F73 - F78 - G165 - C15 - G195 - SCR31

Critère 10.8 [AAA] Dans chaque page Web, le choix de la couleur de fond et de police du texte est-il contrôlable par l'utilisateur ?

Principe WCAG : Perceptible

Niveau RGAA PF : AAA

- Test 10.8.1 : Pour chaque bloc de texte contenu dans une balise HTML, la couleur de fond est-elle contrôlable par l'utilisateur ?
- Test 10.8.2 : Pour chaque bloc de texte contenu dans une balise HTML, la couleur de police est-elle contrôlable par l'utilisateur ?
- Test 10.8.3 : Pour chaque bloc de texte contenu dans une balise object, embed, svgou canvas, la couleur de fond est-elle contrôlable par l'utilisateur ?
- Test 10.8.4 : Pour chaque bloc de texte contenu dans une balise object, embed, svgou canvas, la couleur de police est-elle contrôlable par l'utilisateur ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.4.8

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G156 - G175

Critère 10.9 [AAA] Pour chaque page Web, le texte ne doit pas être justifié. Cette règle est-elle respectée ?

Principe WCAG : Perceptible

Niveau RGAA PF : AAA

- Test 10.9.1 : Chaque page Web vérifie-t-elle une de ces conditions ?
    - Le texte n'est pas justifié ;
    - Un mécanisme permet à l'utilisateur de supprimer la justification du texte.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.4.8

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : F88 - G166 - G172

Critère 10.10 [AAA] Pour chaque page Web, en affichage plein écran et avec une taille de police à 200%, chaque bloc de texte reste-t-il lisible sans l'utilisation de la barre de défilement horizontal ?

Principe WCAG : Perceptible

Niveau RGAA PF : AAA

- Test 10.10.1 : Dans chaque page Web, l'augmentation de la taille des caractères à 200% vérifie-t-elle une de ces conditions ?
    - En affichage plein écran, pour lire un bloc de texte, l'utilisation de la barre de défilement horizontal n'est pas nécessaire ;
    - Un mécanisme permet de rendre inutile l'utilisation de la barre de défilement horizontal pour lire un bloc de texte en affichage plein écran.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.4.8

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G146 - G206 - C19 - C24 - C28

Critère 10.11 [AAA] Pour chaque page Web, les blocs de texte ont-ils une largeur inférieure ou égale à 80 caractères (hors cas particuliers) ?

Principe WCAG : Perceptible

Niveau RGAA PF : AAA

- Test 10.11.1 : Pour chaque page Web, chaque bloc de texte vérifie-t-il une de ces conditions (hors cas particuliers) ?
    - Chaque bloc de texte a une largeur inférieure ou égale à 80 caractères ;
    - L'utilisateur peut réduire la largeur de chaque bloc de texte à 80 caractères en redimensionnant la fenêtre de son navigateur.

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G204 - C20

Critère 10.12 [AAA] Pour chaque page Web, l'espace entre les lignes et les paragraphes est-il suffisant ?

Principe WCAG : Perceptible

Niveau RGAA PF : AAA

- Test 10.12.1 : Pour chaque page Web, chaque bloc de texte vérifie-t-il une de ces conditions ?
    - La valeur de l'interligne est égale à 1,5 fois la taille du texte, au moins ;
    - Un mécanisme permet d'augmenter la valeur de l'interligne à 1,5 fois la taille du texte, au moins.
- Test 10.12.2 : Pour chaque page Web, chaque bloc de texte vérifie-t-il une de ces conditions ?
    - La valeur de l'espacement entre deux paragraphes est égale à 1,5 fois la valeur de l'interligne, au moins ;
    - Un mécanisme permet d'augmenter la valeur de l'espacement entre deux paragraphes à 1,5 fois la valeur de l'interligne, au moins.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.4.8

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G188 - C21

Critère 10.13 [A] Pour chaque page Web, les textes cachés sont-ils correctement affichés pour être restitués par les technologies d'assistance ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 10.13.1 : Dans chaque page Web, chaque texte caché vérifie-t-il une de ces conditions ?
    - Le texte n'a pas vocation à être restitué par les technologies d'assistance ;
    - Le texte est rendu visible sur action de l'utilisateur sur l'élément lui-même ou un élément précédant le texte caché ;
    - Le texte caché fait partie d'un motif de conception défini par l'API ARIA, prenant en charge l'état affiché ou masqué du contenu.

Note technique : Consulter la note technique au sujet de la propriété aria-hiddenet de l'attribut hidden.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 4.1.2 - 1.3.2

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G57

Critère 10.14 [A] Dans chaque page Web, l'information ne doit pas être donnée uniquement par la forme, taille ou position. Cette règle est-elle respectée ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 10.14.1 : Dans chaque page Web, pour chaque texte ou ensemble de textes, l'information ne doit pas être donnée uniquement par la forme, taille ou position. Cette règle est-elle respectée ?
- Test 10.14.2 : Dans chaque page Web, pour chaque image ou ensemble d'images, l'information ne doit pas être donnée uniquement par la forme, taille ou position. Cette règle est-elle respectée ?
- Test 10.14.3 : Dans chaque page Web, pour chaque média temporel, l'information ne doit pas être donnée uniquement par la forme, taille ou position. Cette règle est-elle respectée ?
- Test 10.14.4 : Dans chaque page Web, pour chaque média non temporel, l'information ne doit pas être donnée uniquement par la forme, taille ou position. Cette règle est-elle respectée ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.4.1 - 1.3.3

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G96 - G111 - G140 - F14 - F26

Critère 10.15 [A] Dans chaque page Web, l'information ne doit pas être donnée par la forme, taille ou position uniquement. Cette règle est-elle implémentée de façon pertinente ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 10.15.1 : Dans chaque page Web, pour chaque texte ou ensemble de textes, l'information ne doit pas être donnée uniquement par la forme, taille ou position. Cette règle est-elle implémentée de façon pertinente ?
- Test 10.15.2 : Dans chaque page Web, pour chaque image ou ensemble d'images, l'information ne doit pas être donnée par la forme, taille ou position uniquement. Cette règle est-elle implémentée de façon pertinente ?
- Test 10.15.3 : Dans chaque page Web, pour chaque média temporel, l'information ne doit pas être donnée par la forme, taille ou position uniquement. Cette règle est-elle implémentée de façon pertinente ?
- Test 10.15.4 : Dans chaque page Web, pour chaque média non temporel, l'information ne doit pas être donnée par la forme, taille ou position uniquement. Cette règle est-elle

implémentée de façon pertinente ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.4.1 - 1.3.3

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G96 - G111 - G140 - F14 - F26

11. Formulaires

Principe WCAG : Perceptible

Recommandation :

Associer pour chaque formulaire chacun de ses champs à son étiquette, grouper les champs dans des blocs d'informations de même nature, structurer les listes de choix de manière pertinente, donner à chaque bouton un intitulé explicite. Vérifier la présence d'aide à la saisie, s'assurer que le contrôle de saisie est accessible et que l'utilisateur peut contrôler les données à caractère financier, juridique ou personnel.

Critère 11.1 [A] Chaque champ de formulaire a-t-il une étiquette ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 11.1.1 : Chaque champ de formulaire vérifie-t-il une de ces conditions ?
  - Le champ de formulaire possède un attribut title;
  - Une étiquette (balise label) est associée au champ de formulaire ;
  - Le champ de formulaire possède une propriété aria-label ;
  - Le champ de formulaire possède une propriété aria-labelledbyréférençant un passage de texte identifié.
- Test 11.1.2 : Chaque champ de formulaire, associé à une étiquette (balise label), vérifie-t-il ces conditions ?
  - Le champ de formulaire possède un attribut id ;
  - La valeur de l'attribut idest unique ;
  - La balise labelpossède un attribut for ;
  - La valeur de l'attribut forest égale à la valeur de l'attribut iddu champ de formulaire associé.
- Test 11.1.3 : Chaque champ de formulaire associé à une étiquette *via* la propriété ARIA aria-labelledby, vérifie-t-il ces conditions ?
  - L'étiquettepossède un attribut id ;
  - La valeur de l'attribut idest unique ;
  - Les valeurs de la propriété ARIA aria-labelledbysont égales à la valeur des attributs iddes passages de textes utilisés pour créer l'étiquette ;

        - L'étiquetteliée par la propriété ARIA aria-labelledbyest visible à la prise de focus au moins.
- Test 11.1.4 : Chaque champ de formulaire qui utilise une propriété ARIA aria-labeldoit être accompagné d'un passage de texte visible et accolé au champ permettant de comprendre la nature de la saisie attendue. Cette règle est-elle respectée ?
- Test 11.1.5 : Chaque champ de formulaire qui utilise un attribut titlecomme étiquette, vérifie-t-il une de ces conditions ?
    - L'attribut placeholderest absent ;
    - L'attribut placeholderest identique à l'attribut title.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.3.1 - 2.4.6 - 3.3.2 - 4.1.2

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : H44 - H65 - G82 - G131 - ARIA6 - ARIA9 - ARIA16 - ARIA14 - F82 - F86

Critère 11.2 [A] Chaque étiquette associée à un champ de formulaire est-elle pertinente ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 11.2.1 : Chaque étiquette (balise label) permet-elle de connaître la fonction exacte du champ de formulaire auquel elle est associée ?
- Test 11.2.2 : Chaque attribut titlepermet-il de connaître la fonction exacte du champ de formulaire auquel il est associé ?
- Test 11.2.3 : Chaque étiquette implémentée *via* la propriété ARIA aria-labelpermet-elle de connaître la fonction exacte du champ de formulaire auquel elle est associée ?
- Test 11.2.4 : Chaque étiquette implémentée *via* la propriété ARIA aria-labelledby permet-elle de connaître la fonction exacte du champ de formulaire auquel elle est associée ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 2.4.6 - 3.3.2

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : H44 - H65 - G182 - G131 - ARIA6 - ARIA9 - ARIA16 - ARIA14

Critère 11.3 [AA] Dans chaque formulaire, chaque étiquette associée à un champ de formulaire ayant la même fonction et répété plusieurs fois dans une même page ou dans un ensemble de pages est-elle cohérente ?

Principe WCAG : Perceptible

Niveau RGAA PF : AA

- Test 11.3.1 : Chaque étiquette associée à un champ de formulaire ayant la même fonction et répétée plusieurs fois dans une même page est-elle cohérente ?
- Test 11.3.2 : Chaque étiquette associée à un champ de formulaire ayant la même fonction et répétée dans un ensemble de pages est-elle cohérente ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 3.2.4

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : F31

Critère 11.4 [A] Dans chaque formulaire, chaque étiquette de champ et son champ associé sont-ils accolés ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 11.4.1 : Dans chaque formulaire, chaque étiquette de champ et son champ associé sont-ils accolés ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 3.3.2

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G162

Critère 11.5 [A] Dans chaque formulaire, les informations de même nature sont-elles regroupées, si nécessaire ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 11.5.1 : Dans chaque formulaire, les informations de même nature sont-elles regroupées *via* une balise fieldset, si nécessaire ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.3.1 - 3.3.2 Technique(s)

suffisante(s) et/ou échec(s) WCAG 2.0 : H71

Critère 11.6 [A] Dans chaque formulaire, chaque regroupement de champs de formulaire a-t-il une légende ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 11.6.1 : Chaque regroupement de champs de formulaire (balise fieldset) est-il suivi dans le code source par une légende (balise legend) ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.3.1 - 3.3.2 Technique(s)

suffisante(s) et/ou échec(s) WCAG 2.0 : H71

Critère 11.7 [A] Dans chaque formulaire, chaque légende associée à un groupement de champs de formulaire est-elle pertinente ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 11.7.1 : Dans chaque formulaire, chaque légende (balise legend) associée à un groupement de champs de formulaire (balise fieldset) est-elle pertinente ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 3.3.2

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : H71

Critère 11.8 [A] Dans chaque formulaire, chaque liste de choix est-elle structurée de manière pertinente ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 11.8.1 : Dans chaque formulaire, pour chaque liste de choix (balise select), les items sont-ils regroupés avec une balise optgroup, si nécessaire ?
- Test 11.8.2 : Dans chaque liste de choix (balise select), chaque regroupement d'items de liste (balise optgroup) possède-t-il un attribut label?
- Test 11.8.3 : Pour chaque regroupement d'items de liste (balise optgroup) ayant un attribut label, le contenu de l'attribut labelest-il pertinent ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.3.1

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : H85

Critère 11.9 [A] Dans chaque formulaire, l'intitulé de chaque bouton est- il pertinent ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 11.9.1 : Dans chaque formulaire, l'intitulé de chaque bouton vérifie-t-il une de ces conditions ?
    - Le contenu de l'attribut valuedes boutons de formulaire de type submit, reset ou buttonest pertinent ;
    - Le contenu de la balise <button>est pertinent ;
    - Le contenu de l'attribut titleest pertinent ;
    - Le contenu de la propriété ARIA aria-labelest pertinent ;
    - Un passage de texte est lié au bouton *via* une propriété aria-labelledby.
- Test 11.9.2 : Dans chaque formulaire, l'intitulé de chaque bouton implémenté *via* une propriété ARIA aria-labelledbyvérifie-t-il ces conditions ?
    - Le passage de texte servant d'intitulé possède un attribut id ;
    - La valeur de l'attribut idest unique ;
    - Les valeurs de la propriété ARIA aria-labelledbysont égales aux valeurs des attributs iddes passages de texte utilisés pour créer l'étiquette ;
    - Le passage de texte est pertinent.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 4.1.2

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : H36 - H91 - ARIA6 - ARIA9 - ARIA16 - ARIA14

Critère 11.10 [A] Dans chaque formulaire, le contrôle de saisie est-il utilisé de manière pertinente ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 11.10.1 : Pour chaque formulaire, les indications de champs obligatoires vérifient-elles une de ces conditions ?
    - L'indication de champ obligatoire est donnée par un passage de texte situé avant le champ de formulaire ;
    - L'indication de champ obligatoire est donnée *via* un attribut required ;
    - L'indication de champ obligatoire est donnée *via* la propriété ARIA aria-required;
    - L'indication de champ obligatoire est donnée dans l'étiquette (balise label, attribut title, propriété ARIA aria-label, passage de texte lié *via* la propriété ARIA aria-labelledby) du champ de formulaire ;
    - L'indication de champ obligatoire est donnée par un passage de texte lié par la propriété ARIA aria-describedby.
- Test 11.10.2 : Chaque indication de champ obligatoire qui utilise les propriétés ARIA

aria-label, aria-requiredou l'attribut requireddoit être accompagnée d'une indication visuelle explicite dans l'étiquette (balise label) ou dans un passage de texte lié au champ par la propriété ARIA aria-describedbyou aria-labelledby, cette règle est-elle respectée ?

- Test 11.10.3 : Chaque indication de champ obligatoire qui utilise un passage de texte lié par la propriété ARIA aria-describedbyou aria-labelledbyvérifie-t-elle ces conditions ?
    - Le passage de texte est identifié *via* un attribut id ;
    - La valeur de l'attribut idest unique ;
    - Les valeurs de la propriété ARIA aria-describedbyou aria-labelledby sont égales aux valeurs des attributs id.
- Test 11.10.4 : Pour chaque formulaire, les erreurs de saisie vérifient-elles une de ces conditions ?
    - L'erreur de saisie est indiquée dans l'étiquette (balise label, attribut title, propriété ARIA aria-label, passage de texte lié *via* la propriété ARIA aria- labelledby) du champ de formulaire ;
    - L'erreur de saisie est indiquée par un passage de texte avant le champ de formulaire ;
    - Le champ de formulaire possède un typequi produit de manière automatique un message d'erreur de saisie ;
    - L'erreur de saisie est indiquée par un passage de texte lié par la propriété ARIA aria-describedby ;
    - L'erreur de saisie est indiquée *via* la propriété ARIA aria-invalid.
- Test 11.10.5 : Chaque indication d'erreur de saisie réalisée grâce à la propriété ARIA aria- label ou aria-invaliddoit être accompagnée d'une indication visuelle explicite dans l'étiquette : balise label, texte visible à proximité ou passage de texte lié au champ par la propriété ARIA aria-describedbyou aria-labelledby. Cette règle est-elle respectée ?
- Test 11.10.6 : Chaque erreur de saisie qui utilise un passage de texte lié par la propriété ARIA aria-describedbyou aria-labelledbyvérifie-t-elle ces conditions ?
    - Le passage de texte est identifié *via* un attribut id ;
    - La valeur de l'attribut idest unique ;
    - Les valeurs de la propriété ARIA aria-describedbyou aria-labelledby sont égales aux valeurs des attributs iddes passages de texte utilisés pour créer l'étiquette.
- Test 11.10.7 : Pour chaque formulaire, chaque champ obligatoire vérifie-t-il une de ces conditions ?
    - Le type de données et/ou de format est indiqué, si nécessaire, dans l'étiquette (balise label, attribut title, propriété ARIA aria-label, texte lié *via* la propriété

ARIA aria-labelledby) du champ ;
    - Le type de données et/ou de format est indiqué, si nécessaire, par un passage de texte avant le champ de formulaire ;
    - Le type de données et/ou de format est indiqué, si nécessaire, par un texte lié par la propriété ARIA aria-describedby.
- Test 11.10.8 : Chaque indication du type de données et/ou de format réalisée grâce à la propriété ARIA aria-labeldoit être accompagnée d'une indication visuelle explicite dans l'étiquette (balise label) ou dans un passage de texte lié au champ par la propriété ARIA aria-describedbyou aria-labelledby, cette règle est-elle respectée ?
- Test 11.10.9 : Chaque indication de type de données et/ou de format qui utilise un passage de texte lié par la propriété ARIA aria-describedby ou aria-labelledby vérifie- t-elle ces conditions ?
    - Le passage de texte est identifié *via* un attribut id ;
    - La valeur de l'attribut idest unique ;
    - Les valeurs de la propriété ARIA aria-describedbyou aria-labelledby sont égales aux valeurs des attributs id.
- Test 11.10.10 : Chaque champ de formulaire qui utilise un attribut titlecomme aide à la saisie, vérifie-t-il une de ces conditions ?
    - L'attribut placeholderest absent ;
    - L'attribut placeholderest identique à l'attribut title.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 3.3.1 - 3.3.2

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G83 - G84 - G85 - G89 - G184 - H44 - H89 - H90 - F81 - SCR18 - SCR32 - ARIA1 - ARIA2 - ARIA6 - ARIA9 - ARIA16 - ARIA21

Critère 11.11 [AA] Dans chaque formulaire, le contrôle de saisie est-il accompagné, si nécessaire, de suggestions facilitant la correction des erreurs de saisie ?

Principe WCAG : Perceptible

Niveau RGAA PF : AA

- Test 11.11.1 : Pour chaque formulaire, pour chaque erreur de saisie, les types et les formats de données sont-ils suggérés, si nécessaire ?
- Test 11.11.2 : Pour chaque formulaire, pour chaque erreur de saisie, des exemples de valeurs attendues sont-ils suggérés, si nécessaire ?

Note technique : Consulter la note technique au sujet des contrôles automatiques de format HTML5.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 3.3.3

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G84 - G85 - G89 - G177 - H89

Critère 11.12 [AA] Pour chaque formulaire, les données à caractère financier, juridique ou personnel peuvent-elles être modifiées, mises à jour ou récupérées par l'utilisateur ?

Principe WCAG : Perceptible

Niveau RGAA PF : AA

- Test 11.12.1 : Pour chaque formulaire, la saisie des données à caractère financier, juridique ou personnelle vérifie-t-elle une de ces conditions ?
    - L'utilisateur peut modifier ou annuler les données et les actions effectuées sur ces données après leur saisie ;
    - L'utilisateur peut vérifier et corriger les données avant la validation du formulaire ;
    - Un mécanisme de confirmation explicite, *via* un champ de formulaire ou une étape supplémentaire, est présent.
- Test 11.12.2 : Pour chaque formulaire, la suppression des données à caractère financier, juridique ou personnelle vérifie-t-elle une de ces conditions ?
    - Un mécanisme permet de récupérer les données supprimées par l'utilisateur ;
    - Un mécanisme de confirmation explicite de la suppression, *via* un champ de formulaire ou une étape supplémentaire, est présent.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 3.3.4

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G98 - G99 - G155 - G164 - G168

Critère 11.13 [AAA] Pour chaque formulaire, toutes les données peuvent-elles être modifiées, mises à jour ou récupérées par l'utilisateur ?

Principe WCAG : Perceptible

Niveau RGAA PF : AAA

- Test 11.13.1 : Pour chaque formulaire, la saisie des données vérifie-t-elle une de ces conditions ?
    - L'utilisateur peut modifier ou annuler les données et les actions effectuées sur ces données après leur saisie ;
    - L'utilisateur peut vérifier et corriger les données avant la validation du formulaire ;
    - Un mécanisme de confirmation explicite, *via* un champ de formulaire ou une étape supplémentaire, est présent.

- Test 11.13.2 : Pour chaque formulaire, la suppression des données vérifie-t-elle une de ces conditions ?
    - Un mécanisme permet de récupérer les données supprimées par l'utilisateur ;
    - Un mécanisme de confirmation explicite de la suppression, *via* un champ de formulaire ou une étape supplémentaire, est présent.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 3.3.6

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G98 - G99 - G155 - G164 - G168

Critère 11.14 [AAA] Pour chaque formulaire, des aides à la saisie sont-elles présentes ?

Principe WCAG : Perceptible

Niveau RGAA PF : AAA

- Test 11.14.1 : Chaque formulaire vérifie-t-il une de ces conditions ?
    - Il existe un lien vers une page d'aide ;
    - Il existe des indications avant le formulaire ;
    - Il existe des indications avant les champs de formulaire ;
    - Il existe des indications dans l'étiquette (balise label, attribut title, propriété aria-label, passage de texte lié *via* la propriété aria-labelledby) du champ de formulaire ;
    - Il existe des indications dans un passage de texte lié par la propriété ARIA aria-describedby;
    - Un assistant est disponible.
- Test 11.14.2 : Chaque indication qui utilise la propriété ARIA aria-label doit être accompagnée d'une indication visuelle équivalente explicite, cette règle est-elle respectée ?
- Test 11.14.3 : Chaque indication qui utilise un passage de texte lié par la propriété ARIA aria-describedbyvérifie-t-elle ces conditions ?
    - Le passage de texte est identifié *via* un attribut id ;
    - La valeur de l'attribut idest unique ;
    - La valeur de la propriété ARIA aria-describedbyest égale à la valeur de l'attribut id.
- Test 11.14.4 : Chaque champ de type texte vérifie-t-il, si nécessaire, l'une de ces conditions ?
    - Un correcteur orthographique est disponible ;
    - Des suggestions de saisie sont disponibles avant le champ du formulaire ;
    - Des suggestions de saisie sont disponibles dans l'étiquette (balise label, attribut title, propriété aria-label, passage de texte lié *via* la propriété aria-

labelledby) du champ de formulaire ;
    - Des suggestions de saisie sont disponibles dans un passage de texte lié par la propriété ARIA aria-describedby.
- Test 11.14.5 : Chaque suggestion qui utilise la propriété ARIA aria-labeldoit être accompagnée d'une suggestion visuelle équivalente explicite, cette règle est-elle respectée ?
- Test 11.14.6 : Chaque suggestion qui utilise un passage de texte lié par la propriété ARIA aria-describedbyvérifie-t-elle ces conditions ?
    - Le passage de texte est identifié *via* un attribut id ;
    - La valeur de l'attribut idest unique ;
    - La valeur de la propriété ARIA aria-describedbyest égale à la valeur de l'attribut id.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 3.3.5 - 3.3.2

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G71 - G193 - G194 - G184 - G89 - ARIA1 - ARIA6 - ARIA9 - ARIA16 - F81

Critère 11.15 [AAA] Pour chaque formulaire, chaque aide à la saisie est-elle pertinente ?

Principe WCAG : Perceptible

Niveau RGAA PF : AAA

- Test 11.15.1 : Pour chaque formulaire, chaque aide à la saisie est-elle pertinente ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 3.3.5 - 3.3.2

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G71 - G193 - G194 - G184 - G89 - ARIA1 - ARIA9 - ARIA16 - F81

12. Navigation

Principe WCAG : Utilisable

Recommandation :

Faciliter la navigation dans un ensemble de pages par au moins deux systèmes de navigation différents (menu de navigation, plan du site ou moteur de recherche), un fil d'Ariane et l'indication de la page active dans le menu de navigation. Identifier les groupes de liens importants et la zone de contenu et donner la possibilité de les éviter par des liens de navigation interne. S'assurer que l'ordre de tabulation est cohérent et que la page ne comporte pas de piège au clavier.

Critère 12.1 [AA] Chaque ensemble de pages dispose-t-il de deux systèmes de navigation différents, au moins (hors cas particuliers) ?

Principe WCAG : Utilisable

Niveau RGAA PF : AA

- Test 12.1.1 : Chaque ensemble de pages vérifie-t-il une de ces conditions (hors cas particuliers) ?
    - Un menu de navigation et un plan du site sont présents ;
    - Un menu de navigation et un moteur de recherche sont présents ;
    - Un moteur de recherche et un plan du site sont présents.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 2.4.5 - 2.4.8

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G63 - G64 - G161

Critère 12.2 [AA] Dans chaque ensemble de pages, le menu et les barres de navigation sont-ils toujours à la même place (hors cas particuliers) ?

Principe WCAG : Utilisable

Niveau RGAA PF : AA

- Test 12.2.1 : Dans chaque ensemble de pages, chaque page ayant un menu de navigation vérifie-t-elle ces conditions (hors cas particuliers) ?
    - Le menu de navigation est toujours à la même place dans la présentation ;
    - Le menu de navigation se présente toujours dans le même ordre relatif dans le code source.
- Test 12.2.2 : Chaque barre de navigation répétée dans un ensemble de pages vérifie-t-elle ces conditions (hors cas particuliers) ?
    - La barre de navigation est toujours à la même place dans la présentation ;
    - La barre de navigation se présente toujours dans le même ordre relatif dans le code source.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 3.2.3

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G61 - F66

Critère 12.3 [AA] Dans chaque ensemble de pages, le menu et les barres de navigation ont-ils une présentation cohérente (hors cas particuliers) ?

Principe WCAG : Utilisable

Niveau RGAA PF : AA

- Test 12.3.1 : Dans chaque ensemble de pages, le menu de navigation principal a-t-il une présentation cohérente (hors cas particuliers) ?
- Test 12.3.2 : Dans chaque ensemble de pages, les barres de navigation répétées ont-elles une présentation cohérente (hors cas particuliers) ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 3.2.3

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G61

Critère 12.4 [AA] La page "plan du site" est-elle pertinente ?

Principe WCAG : Utilisable

Niveau RGAA PF : AA

- Test 12.4.1 : La page "plan du site" est-elle représentative de l'architecture générale du site ?
- Test 12.4.2 : Les liens du plan du site sont-ils fonctionnels ?
- Test 12.4.3 : Les liens du plan du site renvoient-ils bien vers les pages indiquées par l'intitulé ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 2.4.5 - 2.4.8 Technique(s)

suffisante(s) et/ou échec(s) WCAG 2.0 : G63

Critère 12.5 [AA] Dans chaque ensemble de pages, la page "plan du site" est-elle atteignable de manière identique ?

Principe WCAG : Utilisable

Niveau RGAA PF : AA

- Test 12.5.1 : Dans chaque ensemble de pages, la page "plan du site" est-elle accessible à partir d'une fonctionnalité identique ?
- Test 12.5.2 : Dans chaque ensemble de pages, la fonctionnalité vers la page "plan du site" est-elle située à la même place dans la présentation ?
- Test 12.5.3 : Dans chaque ensemble de pages, la fonctionnalité vers la page "plan du site" se présente-t-elle toujours dans le même ordre relatif dans le code source ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 2.4.5 - 2.4.8 - 3.2.3 Technique(s)

suffisante(s) et/ou échec(s) WCAG 2.0 : G61 - G63

Critère 12.6 [AA] Dans chaque ensemble de pages, le moteur de recherche est-il atteignable de manière identique ?

Principe WCAG : Utilisable

Niveau RGAA PF : AA

- Test 12.6.1 : Dans chaque ensemble de pages, le moteur de recherche est-il accessible à partir d'une fonctionnalité identique ?
- Test 12.6.2 : Dans chaque ensemble de pages, la fonctionnalité vers le moteur de recherche est-elle située à la même place dans la présentation ?
- Test 12.6.3 : Dans chaque ensemble de pages, la fonctionnalité vers le moteur de recherche se présente-t-elle toujours dans le même ordre relatif dans le code source ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 3.2.3

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G61 - F66

Critère 12.7 [AA] Dans chaque page d'une collection de pages, des liens facilitant la navigation sont-ils présents ?

Principe WCAG : Utilisable

Niveau RGAA PF : AA

- Test 12.7.1 : Chaque page d'une collection de pages, vérifie-t-elle ces conditions ?
  - Un lien permet d'accéder à la page suivante ;
  - Un lien permet d'accéder à la page précédente ;
  - Des liens permettent d'accéder à chaque page de la collection de pages.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 2.4.5 - 2.4.8

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G125 - G126 - G127 - G185

Critère 12.8 [AAA] Dans chaque page Web, un fil d'Ariane est-il présent (hors cas particuliers) ?

Principe WCAG : Utilisable

Niveau RGAA PF : AAA

- Test 12.8.1 : Dans chaque page Web, un fil d'Ariane est-il présent (hors cas particuliers) ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 2.4.8

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G65

Critère 12.9 [AAA] Dans chaque page Web, le fil d'Ariane est-il pertinent?

Principe WCAG : Utilisable

Niveau RGAA PF : AAA

- Test 12.9.1 : Dans chaque page Web, le fil d'Ariane est-il représentatif de la position de la page dans l'arborescence du site ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 2.4.8

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G65

Critère 12.10 [A] Dans chaque page Web, les groupes de liens importants (menu, barre de navigation…) et la zone de contenu sont-ils identifiés ?

Principe WCAG : Utilisable

Niveau RGAA PF : A

- Test 12.10.1 : Dans chaque page Web, chaque groupe de liens importants est-il implémenté dans une balise commune ?
- Test 12.10.2 : Dans chaque page Web, chaque groupe de liens importants vérifie-t-il une de ces conditions ?
    - La balise structurant le groupe de liens importants possède un attribut id ;
    - La balise structurant le groupe de liens importants est immédiatement précédée, dans le code source, d'une ancre ;
    - Le premier lien du groupe de liens est immédiatement précédé, dans le code source, d'une ancre.
- Test 12.10.3 : Dans chaque page Web, la zone de contenu vérifie-t-elle une de ces conditions ?
    - La zone de contenu possède un attribut id;
    - La zone de contenu est immédiatement précédée, dans le code source, d'une ancre ;
    - Le premier élément de la zone de contenu est immédiatement précédé, dans le code source, d'une ancre.
- Test 12.10.4 : Dans chaque page Web, la structure du document vérifie-t-elle ces conditions ?
    - La zone d'en-tête de la page possède un rôle ARIA banner;

- Le menu de navigation principal possède un rôle ARIA navigation ;
- La zone de contenu principal possède un rôle ARIA main ;
- La zone de pied de page possède un rôle ARIA contentinfo ;
- Le moteur de recherche sur le site possède un rôle ARIA search ;
- Les rôles ARIA banner, main, contentinfoet searchsont uniques dans la page ;
- Le rôle ARIA navigationest réservé aux zones de navigations principales et secondaires.

Note technique : Consulter la note technique au sujet des rôles landmarket des liens d'évitement.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.3.1 - 2.4.1 - 4.1.2

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G115 - ARIA4 - ARIA11

Critère 12.11 [A] Dans chaque page Web, des liens d'évitement ou d'accès rapide aux groupes de liens importants et à la zone de contenu sont-ils présents (hors cas particuliers) ?

Principe WCAG : Utilisable

Niveau RGAA PF : A

- Test 12.11.1 : Dans chaque page Web, un lien permet-il d'éviter chaque groupe de liens importants identifié ou d'y accéder (hors cas particuliers) ?
- Test 12.11.2 : Dans chaque page Web, un lien permet-il d'éviter la zone de contenu identifiée ou d'y accéder (hors cas particuliers) ?
- Test 12.11.3 : Dans chaque page Web, chaque lien d'évitement ou d'accès rapide est-il fonctionnel (hors cas particuliers) ?
- Test 12.11.4 : Dans chaque ensemble de pages, les liens d'évitement ou d'accès rapide vérifient-ils ces conditions (hors cas particuliers) ?
    - Chaque lien est situé à la même place dans la présentation ;
    - Chaque lien se présente toujours dans le même ordre relatif dans le code source ;
    - Chaque lien est visible à la prise de focus de tabulation au moins.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 2.4.1 - 2.4.3 - 3.2.3

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G1 - G59 - G123 - G124 - SCR28 - F66

Critère 12.12 [AAA] Dans chaque page Web, la page en cours de consultation est-elle indiquée dans le menu de navigation ?

Principe WCAG : Utilisable

Niveau RGAA PF : AAA

- Test 12.12.1 : Dans chaque page Web, la page en cours de consultation est-elle indiquée dans le menu de navigation ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 2.4.8

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G128

Critère 12.13 [A] Dans chaque page Web, l'ordre de tabulation est-il cohérent ?

Principe WCAG : Utilisable

Niveau RGAA PF : A

- Test 12.13.1 : Dans chaque page Web, l'ordre de tabulation dans le contenu est-il cohérent ?
- Test 12.13.2 : Pour chaque script qui met à jour ou insère un contenu, l'ordre de tabulation reste-t-il cohérent ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 2.4.3

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G59 - H4 - F44 - SCR26 - SCR27 - SCR37 - C27 - F85

Critère 12.14 [A] Dans chaque page Web, la navigation ne doit pas contenir de piège au clavier. Cette règle est-elle respectée ?

Principe WCAG : Utilisable

Niveau RGAA PF : A

- Test 12.14.1 : Dans chaque page Web, chaque élément recevant le focus vérifie-t-il une de ces conditions ?
    - Il est possible d'atteindre l'élément suivant ou précédent pouvant recevoir le focus avec la touche de tabulation ;
    - L'utilisateur est informé d'un mécanisme fonctionnel permettant d'atteindre au clavier l'élément suivant ou précédent pouvant recevoir le focus.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 2.1.1 - 2.1.2

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : H91 - G21 - F10

13. Consultation

Principe WCAG : Perceptible

Recommandation :

Vérifier que l'utilisateur a le contrôle des procédés de rafraîchissement, des changements brusques de luminosité, des ouvertures de nouvelles fenêtres et des contenus en mouvement ou clignotants. Indiquer lorsqu'un contenu s'ouvre dans une nouvelle fenêtre et donner des informations relatives à la consultation des fichiers en téléchargement. Ne pas faire dépendre l'accomplissement d'une tâche d'une limite de temps sauf si elle est essentielle et s'assurer que les données saisies sont récupérées après une interruption de session authentifiée. S'assurer que les expressions inhabituelles et le jargon sont explicités. Proposer des versions accessibles ou rendre accessibles les documents en téléchargement.

Critère 13.1 [A] Pour chaque page Web, l'utilisateur a-t-il le contrôle de chaque limite de temps modifiant le contenu (hors cas particuliers) ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 13.1.1 : Pour chaque page Web, chaque procédé de rafraîchissement (balise object, balise embed, balise svg, balise canvas, balise meta) vérifie-t-il une de ces conditions (hors cas particuliers) ?
    - L'utilisateur peut arrêter ou relancer le rafraîchissement ;
    - L'utilisateur peut augmenter la limite de temps entre deux rafraîchissements de dix fois, au moins ;
    - L'utilisateur est averti de l'imminence du rafraîchissement et dispose de vingt secondes, au moins, pour augmenter la limite de temps avant le prochain rafraîchissement ;
    - La limite de temps entre deux rafraîchissements est de vingt heures, au moins.
- Test 13.1.2 : Pour chaque page Web, chaque procédé de redirection effectué *via* une balise metaest-il immédiat (hors cas particuliers) ?
- Test 13.1.3 : Pour chaque page Web, chaque procédé de redirection effectué *via* un script vérifie-t-il une de ces conditions (hors cas particuliers) ?
    - L'utilisateur peut arrêter ou relancer la redirection ;
    - L'utilisateur peut augmenter la limite de temps avant la redirection de dix fois, au moins ;
    - L'utilisateur est averti de l'imminence de la redirection et dispose de vingt secondes, au moins, pour augmenter la limite de temps avant la prochaine redirection ;

    - La limite de temps avant la redirection est de vingt heures, au moins.
- Test 13.1.4 : Pour chaque page Web, chaque procédé limitant le temps d'une session vérifie-t-il une de ces conditions (hors cas particuliers) ?
    - L'utilisateur peut supprimer la limite de temps ;
    - L'utilisateur peut augmenter la limite de temps ;
    - La limite de temps avant la fin de la session est de vingt heures au moins.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 2.2.1 - 2.2.2 - 2.2.4 - 3.2.5

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : F40 - F41 - F61 - F58 - G76 - G186 - G198 - H76 - SVR1 - SCR1 - SCR36 - G133 - G180 - G75 - G110 - SCR16

Critère 13.2 [A] Dans chaque page Web, pour chaque ouverture de nouvelle fenêtre, l'utilisateur est-il averti ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 13.2.1 : Dans chaque page Web, pour chaque ouverture d'une nouvelle fenêtre effectuée *via* un lien (attribut target) ou une commande JavaScript, l'utilisateur est-il averti ?
- Test 13.2.2 : Dans chaque page Web, pour chaque ouverture d'une nouvelle fenêtre effectuée *via* une balise object, ou embed, l'utilisateur est-il averti ?
- Test 13.2.3 : Dans chaque page Web, pour chaque ouverture d'une nouvelle fenêtre effectuée *via* un contrôle de formulaire, l'utilisateur est-il averti ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 2.4.4 - 3.2.5

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G201 - H33 - H83 - F22 - SCR24

Critère 13.3 [A] Dans chaque page Web, l'ouverture d'une nouvelle fenêtre ne doit pas être déclenchée sans action de l'utilisateur. Cette règle est-elle respectée ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 13.3.1 : Dans chaque page Web, l'ouverture d'une nouvelle fenêtre ne doit pas être déclenchée sans action de l'utilisateur. Cette règle est-elle respectée ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 3.2.1 - 3.2.5

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G107 - F22 - F52 - F55 - F60

Critère 13.4 [AAA] Dans chaque page Web, une tâche ne doit pas requérir de limite de temps pour être réalisée, sauf si elle se déroule en temps réel ou si cette limite de temps est essentielle. Cette règle est-elle respectée ?

Principe WCAG : Perceptible

Niveau RGAA PF : AAA

- Test 13.4.1 : Dans chaque page Web, chaque tâche limitée dans le temps vérifie-t-elle une de ces conditions ?
    - La tâche se déroule en temps réel ;
    - La tâche requiert une limite de temps essentielle à son bon déroulement.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 2.2.3

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G5

Critère 13.5 [AAA] Dans chaque page Web, lors d'une interruption de session authentifiée, les données saisies par l'utilisateur sont- elles récupérées après ré-authentification ?

Principe WCAG : Perceptible

Niveau RGAA PF : AAA

- Test 13.5.1 : Dans chaque page Web, lors d'une interruption de session authentifiée, les données saisies par l'utilisateur sont-elles récupérées après ré-authentification ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 2.2.5

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G105 - G181 - F12

Critère 13.6 [A] Dans chaque page Web, pour chaque fichier en téléchargement, des informations relatives à sa consultation sont- elles présentes (hors cas particuliers) ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 13.6.1 : Dans chaque page Web, chaque fichier en téléchargement *via* un lien ou un formulaire a-t-il des informations relatives à son format (hors cas particuliers) ?
- Test 13.6.2 : Dans chaque page Web, chaque fichier en téléchargement *via* un lien ou un formulaire a-t-il des informations relatives à son poids (hors cas particuliers) ?

- Test 13.6.3 : Dans chaque page Web, chaque fichier en téléchargement *via* un lien ou un formulaire a-t-il, si nécessaire, des informations relatives à sa langue (hors cas particuliers) ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 2.4.4

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : H33

Critère 13.7 [A] Dans chaque page Web, chaque document bureautique en téléchargement possède-t-il, si nécessaire, une version accessible ?

Principe WCAG : Perceptible Niveau

RGAA PF : A

- Test 13.7.1 : Dans chaque page Web, chaque fonctionnalité de téléchargement d'un document bureautique vérifie-t-elle une de ces conditions ?
    - Le document en téléchargement est compatible avec l'accessibilité ;
    - Il existe une version alternative du document en téléchargement compatible avec l'accessibilité ;
    - Il existe une version alternative au format HTML du document en téléchargement.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.1.1 - 1.3.2 - 1.3.1 - 2.4.1 - 2.4.3 - 3.1.1 - 4.1.2

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G10 - G135 - F15

Critère 13.8 [A] Pour chaque document bureautique ayant une version accessible, cette version offre-t-elle la même information ?

Principe WCAG : Perceptible Niveau

RGAA PF : A

- Test 13.8.1 : Chaque document bureautique ayant une version accessible vérifie-t-il une de ces conditions ?
    - La version compatible avec l'accessibilité offre la même information ;
    - La version alternative au format HTML est pertinente et offre la même information.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.1.1 - 1.3.2 - 1.3.1 - 2.4.1 - 2.4.3 - 3.1.1 - 4.1.2

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G10 - G135 - F15

Critère 13.9 [AAA] Dans chaque page Web, les expressions inhabituelles, les expressions idiomatiques ou le jargon sont-ils explicités ?

Principe WCAG : Perceptible

Niveau RGAA PF : AAA

- Test 13.9.1 : Dans chaque page Web, chaque expression inhabituelle ou limitée, chaque expression idiomatique ou le jargon vérifie-t-il une des conditions suivantes ?
    - Il existe une définition dans le contexte adjacent de l'expression indiquée par la balise dfn;
    - Il existe une définition *via* une liste de définition ;
    - Il existe une définition dans la page ;
    - L'expression est contenue dans un lien permettant d'accéder à la définition.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 3.1.3

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G55 - G101 - G112 - G160 - G153 - H54

Critère 13.10 [AAA] Dans chaque page Web, pour chaque expression inhabituelle ou limitée, idiomatique ou de jargon ayant une définition, cette définition est-elle pertinente ?

Principe WCAG : Perceptible

Niveau RGAA PF : AAA

- Test 13.10.1 : Dans chaque page Web, pour chaque expression inhabituelle ou limitée, idiomatique ou de jargon ayant une définition, cette définition vérifie-t-elle l'une de ces conditions ?
    - Le contenu de la définition associée est pertinent ;
    - Le contenu de la balise ddde la liste de définition est pertinent ;
    - La définition donnée par le contexte adjacent est pertinente.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 3.1.3

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G55 - G101 - G112 - H54

Critère 13.11 [A] Dans chaque page Web, chaque contenu cryptique (art ASCII, émoticon, syntaxe cryptique) a-t-il une alternative ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 13.11.1 : Dans chaque page Web, chaque contenu cryptique (art ASCII, émoticon, syntaxe cryptique) vérifie-t-il une de ces conditions ?
    - Un attribut titleest disponible ;
    - Une définition est donnée par le contexte adjacent.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.1.1

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G160 - G153 - H86 - F71 - F72

Critère 13.12 [A] Dans chaque page Web, pour chaque contenu cryptique (art ASCII, émoticon, syntaxe cryptique) ayant une alternative, cette alternative est-elle pertinente ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 13.12.1 : Dans chaque page Web, chaque contenu cryptique (art ASCII, émoticon, syntaxe cryptique) vérifie-t-il une de ces conditions ?
    - Le contenu de l'attribut titleest pertinent ;
    - La définition donnée par le contexte adjacent est pertinente.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.1.1

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : H86 - F71 - F72

Critère 13.13 [AAA] Dans chaque page Web, pour chaque mot dont le sens ne peut être compris sans en connaître la prononciation, celle-ci est-elle indiquée ?

Principe WCAG : Perceptible

Niveau RGAA PF : AAA

- Test 13.13.1 : Dans chaque page Web, chaque mot dont le sens ne peut être compris sans en connaître la prononciation, vérifie-t-il une de ces conditions ?
    - L'indication de la prononciation phonétique est présente de manière adjacente ;
    - L'indication de la prononciation phonétique est accessible *via* un lien.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 3.1.6

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G62 - G120 - G121 - G160 - G153

Critère 13.14 [AAA] Dans chaque page Web, chaque texte qui nécessite un niveau de lecture plus avancé que le premier cycle de l'enseignement secondaire a-t-il une version alternative ?

Principe WCAG : Perceptible

Niveau RGAA PF : AAA

- Test 13.14.1 : Dans chaque page Web, chaque texte qui nécessite un niveau de lecture plus avancé que le premier cycle de l'enseignement secondaire (hors noms propres et titre) vérifie-t-il une de ces conditions ?
    - Une illustration ou des symboles graphiques adaptés au niveau de lecture du premier cycle de l'enseignement secondaire sont présents ;
    - Une version en Langue des Signes Française est présente ;
    - Une version vocalisée du texte est présente ;
    - Un résumé adapté au niveau de lecture du premier cycle de l'enseignement secondaire est présent.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 2.1.3 - 3.1.5

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G79 - G86 - G103 - G160 - G153

Critère 13.15 [A] Dans chaque page Web, les changements brusques de luminosité ou les effets de flash sont-ils correctement utilisés ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 13.15.1 : Dans chaque page Web, chaque image (balise img, balise svg, balise canvas, balise embedou balise object) qui provoque un changement brusque de luminosité ou un effet de flash vérifie-t-elle une de ces conditions ?
    - La fréquence de l'effet est inférieure à 3 par seconde ;
    - La surface totale cumulée des effets est inférieure ou égale à 21 824 pixels.
- Test 13.15.2 : Dans chaque page Web, chaque script qui provoque un changement brusque de luminosité ou un effet de flash vérifie-t-il une de ces conditions ?
    - La fréquence de l'effet est inférieure à 3 par seconde ;
    - La surface totale cumulée des effets est inférieure ou égale à 21 824 pixels.
- Test 13.15.3 : Dans chaque page Web, chaque mise en forme CSS qui provoque un changement brusque de luminosité ou un effet de flash vérifie-t-elle une de ces conditions ?
    - La fréquence de l'effet est inférieure à 3 par seconde ;
    - La surface totale cumulée des effets est inférieure ou égale à 21 824 pixels.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 2.3.1

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G15 - G19 - G176

Critère 13.16 [AAA] Dans chaque page Web, les changements brusques de luminosité ou les effets de flash ont-ils une fréquence inférieure ou égale à 3 par seconde ?

Principe WCAG : Perceptible

Niveau RGAA PF : AAA

- Test 13.16.1 : Dans chaque page Web, chaque changement brusque de luminosité ou effet de flash provoqué par une image animée (balise img, balise svg, balise embed, balise canvasou balise object) a-t-il une fréquence inférieure ou égale à 3 par seconde ?
- Test 13.16.2 : Dans chaque page Web chaque changement brusque de luminosité ou effet de flash provoqué par un script a-t-il une fréquence inférieure ou égale à 3 par seconde ?
- Test 13.16.3 : Dans chaque page Web, chaque changement brusque de luminosité ou effet de flash provoqué par une mise en forme CSS a-t-il une fréquence inférieure ou égale à 3 par seconde ?

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 2.3.2

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G19

Critère 13.17 [A] Dans chaque page Web, chaque contenu en mouvement ou clignotant est-il contrôlable par l'utilisateur ?

Principe WCAG : Perceptible

Niveau RGAA PF : A

- Test 13.17.1 : Dans chaque page Web, chaque contenu en mouvement, déclenché automatiquement, vérifie-t-il une de ces conditions ?
    - La durée du mouvement est inférieure ou égale à 5 secondes ;
    - L'utilisateur peut arrêter et relancer le mouvement ;
    - L'utilisateur peut afficher et masquer le contenu en mouvement ;
    - L'utilisateur peut afficher la totalité de l'information sans le mouvement.
- Test 13.17.2 : Dans chaque page Web, chaque contenu clignotant, déclenché automatiquement, vérifie-t-il une de ces conditions ?
    - La durée du clignotement est inférieure ou égale à 5 secondes ;
    - L'utilisateur peut arrêter et relancer le clignotement ;
    - L'utilisateur peut afficher et masquer le contenu clignotant ;
    - L'utilisateur peut afficher la totalité de l'information sans le clignotement.

Correspondances WCAG 2.0

Critère(s) de succès WCAG 2.0 : 1.2.4 - 1.2.9 - 2.2.1 - 2.2.2

Technique(s) suffisante(s) et/ou échec(s) WCAG 2.0 : G4 - G11 - G152 - G186 - G187 - G191 - SM11 - SM12 - F47 - F50 - F4 - F7 - F16 - SCR22 - SCR33 - SCR36

Licence

Le référentiel technique (liste des critères, glossaire, cas particuliers, notes techniques, base de référence) est une copie adaptée du référentiel AccessiWeb HTML5/ARIA - Version de travail du 19/12/2013 - Édité par l'association BrailleNet.

ANNEXE 6 Quater

Référentiel Général d'Accessibilité pour les Administrations de la Polynésie française

RGAA PF

Glossaire

Historique des versions		
Date	**Version**	**Évolution du document**
	1.0	Publication de la première version du Référentiel Général d'Accessibilité pour les Administrations de la Polynésie française

RGAA PF – Glossaire

A

Accéder à chaque page de la collection de pages

Dans le cas où la collection de pages comporte un grand nombre de pages, il est habituel de présenter ces liens d'accès aux pages par groupes de liens, par séquences de 10 liens, par exemple. Cette pratique valide le test.

Accessible et activable par le clavier et la souris

- Un composant d'interface (lien, bouton, élément cliquable dans Flash…) est accessible au clavier et à la souris lorsque l'utilisateur peut prendre, indifféremment, le focus par le pointeur de la souris ou la touche tabulation.
- Un composant d'interface (lien, bouton, élément cliquable dans Flash…) est activable au clavier et à la souris lorsque l'utilisateur peut enclencher, indifféremment, l'action prévue par le composant d'interface par le clic de la souris ou la touche entrée du clavier.
- **Attention** : pour certains composants d'interface comme les sliders (bouton coulissant ou rotatif…), il n'est pas possible de contrôler le composant par la seule touche d'entrée. Dans cette situation, d'autres touches (comme les touches de direction) peuvent être utilisées.

Dans le référentiel, l'expression "contrôlable par le clavier et la souris" se rapporte également à la présente définition.

Note importante : le recours à certaines technologies peut rendre la gestion du focus trop complexe ou trop instable pour ne reposer que sur la tabulation, les touches de direction et la touche entrée.

Dans ce cas, la mise à disposition de raccourcis clavier peut être la seule solution pour rendre le composant utilisable.

Le critère peut être considéré comme conforme à la condition que les raccourcis clavier utilisés soient correctement documentés et qu'ils soient fonctionnels quelle que soit la position du focus dans l'interface.

Vous pouvez consulter, à ce sujet, la technique SL15: Providing Keyboard Shortcuts that Work Across the Entire Silverlight Application pour l'environnement Silverlight par exemple.

Adapter un motif de conception ARIA

L'API ARIA définit des motifs de conception, par exemple pour un système d'onglet ou une fenêtre modale, destinés à assurer un comportement homogène de référence des composants d'interface. Le respect de ces motifs de conception est exigé par le référentiel RGAA PF.

Néanmoins il est possible d'adapter ces motifs de conception en remplaçant une propriété mal supportée par une propriété équivalente ou en enrichissant le composant de propriétés améliorant

l’expérience utilisateur ou sécurisant son comportement.

Il appartient à l’auditeur de vérifier que ces adaptations sont cohérentes avec le motif de conception, ne modifient pas le comportement, en termes d’expérience utilisateur, du composant et que le composant adapté est correctement restitué par les technologies d’assistance.

Si ces exigences sont respectées, le composant peut-être déclaré "conforme" au motif de conception.

Alerte

Message d’alerte interrompant la navigation ou l’utilisation de la page, notamment en demandant de cliquer sur un bouton ou un lien pour continuer la navigation ou l’utilisation du contenu. Par exemple, une boîte de dialogue générée par JavaScript *via* la fonction alert. Par extension, une fenêtre modale (contenu présenté sous forme de "fenêtre" insérée ou affichée dans le DOM) qui nécessite d’être fermée pour continuer la navigation ou l’utilisation du contenu est considérée comme une alerte. Note : la désactivation des alertes concernées peut être proposée avant le déclenchement de l’alerte, par exemple, *via* un paramètre utilisateur ou lors de l’affichage de la première alerte, par exemple *via* une case à cocher "ne plus afficher cette alerte".

Alternative (à script)

Texte ou procédé associé au script *via* une technique appropriée et permettant de mettre à disposition une fonction ou un contenu similaire à celui proposé par script.

Note : lorsqu’une alternative à un procédé ou une fonctionnalité JavaScript est proposée, le moyen d’y accéder doit être fourni par le site lui-même. Il peut s’agir d’un lien ou d’un bouton permettant d’accéder à une page alternative fonctionnant sans JavaScript ou permettant de remplacer le(s) composant(s) par un composant alternatif fonctionnant sans JavaScript par exemple.

Alternative à une image SVG

Sont considérés comme des alternatives possibles à une image SVG :

- Un mécanisme de remplacement
- Un lien adjacent qui permet d’accéder à une alternative dont le contenu est pertinent, et identique à la propriété aria-labelet à l’attribut titlede la balise <svg>, s’il est présent.

Alternative courte et concise

Les conditions de restitution d’une alternative textuelle *via* des technologies d’assistance (par exemple une loupe d’écran) nécessitent qu’elle soit la plus courte possible. Une longueur maximale de 80 caractères est fortement recommandée ; elle limitera le nombre de manipulations nécessaires pour lire l’alternative par les utilisateurs de plages braille ou de loupes d’écran notamment.

Alternative textuelle (image)

Texte associé à une image *via* une technique appropriée et décrivant l’information véhiculée par

l'image (par rapport au contexte du contenu Web dans lequel elle se trouve). RGAA PF considère quatre types d'alternatives liées à la nature de l'image :

- **pour une image porteuse d'information**, l'alternative apporte l'information nécessaire à la compréhension du contenu auquel l'image est associée ;
- **pour une image de décoration**, l'alternative doit être vide (alt="") ;
- **pour une image-lien**, l'alternative doit permettre de comprendre la fonction et la destination du lien ;
- **pour une image CAPTCHA ou une image-test**, l'alternative ne peut pas apporter l'information véhiculée par l'image sans rendre la fonction associée inopérante. Dans ce cas de figure, l'alternative doit se contenter de permettre d'identifier la nature et la fonction de l'image.

Note 1 : pour une image CAPTCHA l'alternative peut être, par exemple : "Code de sécurité anti- spam" ou "code pour vérifier que vous êtes un humain" ou toute autre alternative permettant à l'utilisateur de comprendre la nature et la fonction de l'image.

Note 2 : pour un groupe d'images, par exemple un système de vote constitué de plusieurs images d'étoiles, il est fortement conseillé d'utiliser la première image du groupe pour donner une alternative plus cohérente au groupe d'image. Dans ce cas, les autres images du groupe sont considérées comme des images de décoration. Vous pouvez consulter, à ce sujet, la note suivante : A group of images that form a single larger picture with no links.

Ambigu pour tout le monde

L'intention ne peut être déterminée à partir du lien et de toute l'information de la page Web présentée à l'utilisateur en même temps que ce lien. (c'est-à-dire qu'un lecteur sans limitation fonctionnelle ne connaîtrait pas la fonction d'un lien avant de l'activer). **Exemple** : le mot "goyave" dans la phrase suivante utilisé comme lien : « L'une des exportations importantes est la goyave ».
Ce lien pourrait conduire à une définition de la goyave, à un graphe présentant une liste des quantités de goyaves exportées ou à une photo de personnes récoltant la goyave. Jusqu'à ce que le lien soit activé, tout utilisateur est dans l'incertitude et une personne handicapée n'est donc pas désavantagée.

Ancre

En HTML, une ancre (appelée aussi signet) est constituée d'une balise <a>avec l'attribut idet dépourvue de href, par exemple. Une ancre sert de cible à un lien de la forme Intitulé: Contenu par exemple.

Arborescence du document

Le test 9.2.2 demande de vérifier que la structure des éléments sectionnant (nav, section, articlepar exemple) est cohérente, c'est-à-dire représentative de l'architecture du document.

Cette structure est complémentaire à la structure des titres h(x)qui en sont un élément.

L'utilisation innapropriée de ces éléments sectionnants peut générer une arborescence de document incohérente, par exemple par l'utilisation abusive d'éléments sectionou article.

Note 1 : Pour accompagner la prise en charge progressive de l'arborescence du document et compte tenu du fait que le référentiel exige de disposer, en tout état de cause, d'une structure de contenu (balises h(x)) robuste et cohérente, **il est acceptable de considérer le test 9.2.2 comme non applicable** lorsqu'il n'est pas possible de s'assurer que l'arborescence du document est parfaitement cohérente. Vous pouvez consulter, à ce sujet la note technique : Note technique au sujet de l'arborescence du document.

Note 2 : vous pouvez consulter, à ce sujet, l'exemple donné par la spécification HTML5 : 4.3.10.2 Sample outlines.

Attribut target

L'attribut targetouvre une nouvelle fenêtre ou un nouvel onglet du navigateur selon sa valeur. Les valeurs suivantes de targetn'ouvrent pas de nouvelles fenêtres :

- _self;
- _top;
- _parent.

Pour toutes les autres valeurs de target, l'élément sur lequel il est positionné ouvrira une nouvelle fenêtre ou un nouvel onglet. C'est le cas de la valeur _blankpar exemple, mais également de toute autre valeur (numérique ou alphabétique) non définie par la spécification. Il est à noter d'ailleurs que ces valeurs ne provoquent pas d'erreur lors de la validation du code source en HTML5.

Audio-description étendue

Audio-description ajoutée à une présentation audiovisuelle en mettant en pause la vidéo de manière à avoir le temps d'ajouter des descriptions supplémentaires. **Note** : cette technique est à utiliser seulement si le sens de la vidéo est perdu sans audio-description supplémentaire et que les pauses entre les dialogues ou la narration sont trop courtes.

Audio-description synchronisée (média temporel)

Narration ajoutée (*via* un fichier son) à une piste sonore pour décrire les détails visuels importants qui ne peuvent être compris à partir de la piste sonore principale seulement. L'audio-description doit être synchronisée avec le média temporel grâce à l'utilisation de format spécialisés comme le format SRT par exemple.

- **Note 1** : l'audio-description d'une vidéo fournit de l'information à propos des actions, des personnages, des changements de scènes, du texte apparaissant à l'écran et d'autres contenus visuels.

- **Note 2** : dans une audio-description standard, la narration est ajoutée durant les pauses qui existent dans le dialogue. (Voir aussi audio-description étendue.)
- **Note 3** : lorsque toute l'information de la vidéo est déjà donnée dans la piste audio, aucune audio-description supplémentaire n'est requise.

B

Barre de navigation

Liste de liens permettant une navigation spécifique dans le site, dans une rubrique ou dans une collection de pages. Les principales barres de navigation sont :

- Le menu de navigation principal ;
- Un fil d'Ariane ;
- Une liste de navigation d'une liste de résultats ;
- Un menu de sous-rubrique.

Bloc d'informations de même nature

Dans un formulaire, ensemble des champs pouvant être regroupés par la nature des informations attendues. Le regroupement vise à identifier les champs devant être traités comme un ensemble.

Quelques exemples :

- Trois champs successifs pour saisir une date (jour/mois/année) ;
- Champs successifs pour un numéro de téléphone ;
- Un bloc destiné à saisir l'identité et l'adresse de l'utilisateur, lorsque le formulaire contient plusieurs blocs de contact ;
- Un ensemble de boutons radio ou de cases à cocher qui se rapportent à une question.

Ces champs doivent être regroupés par une balise fieldsetaccompagnée d'une balise legend pertinente. Dans le cas de boutons radio, la légende est généralement l'intitulé de la question.

Note : lorsque le formulaire est uniquement constitué d'un seul bloc d'informations de même nature (l'identité et l'adresse de l'utilisateur, par exemple) ou d'un champ unique (un moteur de recherche, par exemple), la présence de l'élément fieldsetn'est pas obligatoire.

Bouton (formulaire)

Élément d'un formulaire qui permet d'effectuer une action prédéfinie. Par exemple, le bouton de soumission d'un formulaire permet l'envoi au serveur des informations collectées pour leur traitement. L'intitulé d'un bouton doit décrire l'action qui résulte de son activation (par exemple : "Lancer votre recherche", "Envoyer votre message").

En HTML, il y a trois types de boutons de formulaire :

- Balise input de type submit, resetou button;
- Balise input de type image;

- Balise button.

L’intitulé du bouton peut être de quatre types :

- Le contenu de l’attribut valuedes boutons de type submit, resetou button;
- Le contenu de l’attribut altd’un bouton de type image;
- Le contenu de l’attribut titlelorsqu’il est présent ;
- Le contenu de la balise button.

C

Cadre en ligne

Élément HTML (balise iframe) permettant d’afficher un contenu dans la page Web dans laquelle il est implémenté.

CAPTCHA

Un CAPTCHA est un test utilisé pour distinguer un utilisateur humain d’un ordinateur. Le test utilise souvent des images contenant du texte déformé, mélangé avec d’autres formes ou utilisant des jeux de couleur altérées, que l’utilisateur est invité à retaper. D’autres formes de CAPTCHA peuvent être basées sur des questions logiques ou des extraits sonores.

Champ de saisie de formulaire

Objet d’un formulaire permettant à l’utilisateur :

- De saisir des données textuelles ou préformatées :
    - input type="text";
    - input type="password";
    - input type="search";
    - input type="tel";
    - input type="email";
    - input type="number";
    - input type="tel"
    - input type="url";
    - textarea;
- De sélectionner des valeurs prédéfinies :
    - input type="checkbox";
    - input type="radio";
    - input type="date";
    - input type="range";
    - input type="color";
    - input type="time";

    - select;
    - datalist;
    - optgroup;
    - option;
    - keygen;
- De télécharger des fichiers :
    - input type="file";
- Ou d'afficher des résultats :
    - output;
    - progress;
    - meter.

Les objets de formulaires suivants ne sont pas considérés comme des champs de formulaires :

- input type="submit";
- input type="reset";
- input type="hidden";
- input type="image";
- input type="button";
- button.

Changement brusque de luminosité ou effet de flash

Alternance de luminosité relative qui peut causer des crises chez certaines personnes si leur taille est suffisamment importante dans une gamme de fréquences spécifiques.

Changement de contexte

Changements majeurs dans le contenu d'une page Web qui, s'ils sont faits sans que l'utilisateur n'en soit conscient, peuvent désorienter l'utilisateur qui ne peut voir l'ensemble de la page en même temps. Les changements de contexte comprennent les changements :

1. D'agent utilisateur ;
2. D'espace de restitution ;
3. De focus ;
4. De contenu qui modifie la signification de la page Web ;

Note : Un changement de contenu n'est pas toujours un changement de contexte. Un changement dans le contenu comme le déploiement d'une arborescence, un menu dynamique ou un déplacement de tabulation ne change pas nécessairement le contexte à moins qu'il ne change aussi l'un des éléments énumérés ci-dessus (le focus, par exemple).

Exemple : l'ouverture d'une nouvelle fenêtre, le déplacement du focus sur un composant différent, le déplacement vers une nouvelle page (y compris tout ce qui, pour l'utilisateur, aurait l'air d'un déplacement vers une autre page) ou la réorganisation significative du contenu d'une page sont

autant d'exemples d'un changement de contexte.

Changement de langue

L'indication des changements de langue est nécessaire pour indiquer aux technologies d'assistance de modifier la restitution vocale d'un élément. Les changement de langue concernent tous les contenus, y compris les valeurs de certains attributs comme title.

Note : il n'est pas possible d'indiquer des changements de langue dans une valeur d'attribut elle- même, dans ce cas le changement de langue est indiqué sur l'élément qui contient l'attribut. Par exemple un lien affecté d'un titleen anglais devra comporter un attribut lang="en". Lorsque l'attribut contient plusieurs passage de texte dans des langues différentes, le critère est non applicable.

Code de langue

Code de 2 caractères (ISO 639-1) ou 3 caractères (ISO 639-2 et suivants) permettant d'indiquer la langue d'un document ou d'un passage de texte. L'indication du code de langue est constituée de deux parties séparées par un tiret sur le modèle lang="[code]-[option]".

- [code] représente un code de langue valide sur 2 ou 3 caractères ;
- [option] est une indication laissée à l'appréciation de l'auteur.

Lorsqu'un code de pays est utilisé comme option, il peut servir à indiquer une régionalisation de la langue, l'indication "en-us" indique la langue américaine, par exemple. L'indication du code de langue ne concerne que la partie [code] avant le tiret.

Code valide

- Cas d'une page HTML : code dans lequel l'implémentation des balises et des attributs respecte les spécifications du type de document déclaré.
    - **Note 1** : Sauf indication contraire, les attributs non répertoriés par les spécifications sont non applicables.
    - **Note 2** : Sauf indication contraire, les balises non répertoriées par les spécifications sont non applicables.
    - **Note 3** : La règle C3 de la spécification XHTML ("Minimisation d'élément et contenu d'élément vide", en anglais) stipule que l'utilisation d'éléments minimisés (<elm />) pour des éléments vides (par exemple à la place de) est déconseillée. Cette pratique constitue une non-conformité dans le cadre de RGAA PF.
- Cas d'une page implémentant WAI-ARIA : code dans lequel l'implémentation des balises et des attributs respecte les spécifications du type de document déclaré et dans lequel l'implémentation WAI ARIA est conforme à la spécification WAI-ARIA.

Collection de pages

Pages reliées les unes aux autres par des liens et ayant un thème ou une nature commune. Par

exemple, les pages de résultats d'un moteur de recherche ou les pages d'un catalogue (pour une même recherche) sont des collections de pages.

Compatible avec les technologies d'assistance

Un contenu ou une fonctionnalité doit être compatible avec les technologies d'assistance des utilisateurs ainsi qu'avec les fonctions d'accessibilité des navigateurs et des autres agents utilisateurs *via* une API d'accessibilité.

Cela concerne, à la fois, la technologie, ses fonctionnalités et ses usages :

- La façon dont la technologie Web est utilisée doit être compatible avec les technologies d'assistance des utilisateurs. Cela signifie que la façon dont la technologie est utilisée a été testée dans une perspective d'interopérabilité avec des utilisateurs des technologies d'assistance dans la ou les langues du contenu ;
- La technologie fonctionne de façon native dans des agents utilisateurs largement distribués qui sont, eux-mêmes, compatibles avec l'accessibilité (comme HTML et CSS) ou avec un module d'extension largement distribué qui est, lui-même, compatible avec l'accessibilité.

La vérification de la compatibilité avec les technologies d'assistance nécessite de réaliser un certain nombre de tests spécifiques à la technologie utilisée, par exemple :

- Vérifier le nom, le rôle, le paramétrage et les changement d'états des composants d'interface ;
- Vérifier que la restitution d'un composant d'interface est correcte pour la ou les technologies d'assistance utilisées.

Compréhensible (ordre de lecture)

Un contenu compréhensible est lisible (l'ordre des éléments est logique) et cohérent (l'enchaînement de la lecture est cohérent).

Contenu visible

Pour le test 10.2.1 : "Contenu présent" signifie que le contenu visible reste présent lorsque CSS est désactivé. Par exemple, une image porteuse d'information en propriété de fond CSS invalide ce test car l'information n'est plus "présente" lorsque CSS est désactivé. En revanche, une image porteuse d'information en propriété de fond CSS mais accompagnée d'un texte caché valide ce test car l'information est bien "présente" lorsque CSS est désactivé.

Note : la pratique qui consiste à gérer des images en propriété de fond d'éléments *via* CSS est formellement déconseillée, même si elle est accompagnée d'un texte caché.

Contexte du lien

Le contexte du lien représente les informations supplémentaires (on parle d'informations de contexte) qui peuvent être mises en relation par un programme informatique avec l'intitulé du lien. Les informations de contexte qui permettent de rendre un lien explicite sont les suivantes :

- Le contenu de la phrase dans laquelle le lien texte est présent ;
- Le contenu du paragraphe (balise p) dans lequel le lien texte est présent ;
- Le contenu de l'item de liste (balise li) ou le contenu d'un item de liste parent (balise li) dans lequel le lien texte est présent ;
- Le contenu du titre (balise h) précédent le lien texte ;
- Le contenu de la ou les cellule(s) d'en-tête de tableau (balise(s) th) associée(s) à la cellule de donnée (balise td) dans laquelle le lien texte est présent ;
- Le contenu de la cellule de donnée (balise td) dans laquelle le lien texte est présent ;
- Le contenu du titre de lien (attribut title) ;
- Le contenu de la propriété aria-label;
- Le contenu du passage de texte lié par la propriété aria-labelledby;

Note 1 : l'un des 9 contextes de lien doit permettre à lui seul d'expliciter le lien.

Note 2 : RGAA PF 3 considère que des liens particuliers comme des liens de type mailto (qui génère un lien sous la forme d'une adresse email cliquable) sont suffisamment explicites et ne requiert pas de signaler, *via* un title, que l'action consiste à envoyer un email. L'attention des auteurs est appelée sur le fait que cette règle générale peut être adaptée au contexte, par exemple si la page contient plusieurs adresses email cliquables affectées de comportements différents (envoyer un email *via* le client de messagerie pour l'une, accéder à un formulaire pour l'autre) il peut être nécessaire de donner des informations complémentaire sur l'action du lien afin de différencier leurs comportements.

Contraste

Opposition marquée entre la luminosité d'une couleur de premier plan et d'une couleur d'arrière- plan. Le rapport de contraste est basé sur la différence de luminosité relative entre l'arrière-plan et le premier plan selon la règle : (L1 + 0,05) / (L2 + 0,05) où L1 est la luminosité relative la plus claire et L2 la luminosité relative la plus sombre. La luminosité est calculée selon la formule suivante : L = 0,2126 * R + 0,7152 * G + 0,0722 * B. Où R, G et B sont définis par :

- Si RsRGB >= 0,03928 alors R = RsRGB/12,92 sinon R = ((RsRGB+0,055)/1,055) ^ 2,4 ;
- Si GsRGB >= 0,03928 alors G = GsRGB/12,92 sinon G = ((GsRGB+0,055)/1,055) ^ 2,4 ;
- Si BsRGB >= 0,03928 alors B = BsRGB/12.92 sinon B = ((BsRGB+0,055)/1,055) ^ 2,4 ;

et RsRGB, GsRGB et BsRGB sont définis par :

- RsRGB = R8bit/255 ;
- GsRGB = G8bit/255 ;
- BsRGB = B8bit/255.

Le caractère "^" est l'opérateur exponentiel.

Note : la mesure de contraste concerne le texte, le texte en image, le texte et le texte en image dans les animations, le texte de sous-titrage et le texte incrusté dans les vidéos. Pour le texte et le texte en

image dans les animations, le texte de sous-titrage et le texte incrusté dans les vidéos, la taille de la police doit être mesurée par rapport à la taille d'affichage par défaut (telle qu'affichée). Les textes présents dans les éléments d'une image ou d'une vidéo (par exemple un écriteau, une affiche etc.) ne sont pas concernés.

Source : Procédure de calcul de contraste des WCAG (en anglais).

Contrôle (contenu en mouvement ou clignotant)

Possibilité pour l'utilisateur de contrôler l'affichage ou la lecture d'un contenu en mouvement ou clignotant par le clavier et la souris, au moins.

Tous les contenus en mouvement, à l'exception des média temporels pris en charge par la thématique multimédia, sont concernés : les images animés (par exemple un gif animé), les contenus en mouvement proposés *via* une balise object, du code JavaScriptou des effets CSSpar exemple.

Note 1 : lorsque c'est approprié, la méthode de contrôle devrait être disponible comme premier élément de la page.

Note 2 : la méthode de contrôle du contenu en mouvement ou clignotant doit permettre à l'utilisateur d'interagir avec le reste de la page. En conséquence, l'arrêt ou la mise en pause *via* un événement déclenché uniquement sur la prise de focus ne permet pas de valider le critère.

Note 2 : Dans certains cas, le mouvement fait partie intégrante du composant et il n'est pas possible d'en donner le contrôle à l'utilsateur, par exemple une barre de progression dont la fonction est d'indiquer par un mouvement la progression d'un évènement comme un téléchargement. Dans ce cas le critère est Non Applicable.

Contrôle (son déclenché automatiquement)

Possibilité pour l'utilisateur d'arrêter ou de relancer un son déclenché automatiquement.

Note : la méthode de contrôle du son devrait être disponible comme premier élément de la page.

Contrôle de la consultation (d'un média temporel)

Possibilité pour l'utilisateur de contrôler la consultation d'un média temporel par le clavier et la souris, au moins. Les points suivants doivent être respectés :

- Liste des fonctionnalités obligatoires de contrôle de la consultation :
    - L'objet multimédia doit toujours avoir les fonctionnalités suivantes, au minimum : lecture, pause ou stop ;
    - Si l'objet multimédia a du son, il doit avoir une fonctionnalité de contrôle du volume ;
    - Si l'objet multimédia a des sous-titres, il doit avoir une fonctionnalité de contrôle de l'apparition/disparition des sous-titres ;
    - Si l'objet multimédia a une audio-description, il doit avoir une fonctionnalité de

contrôle de l'apparition/disparition de l'audio-description.

- Chaque fonctionnalité doit être accessible par le clavier, *via* la touche de tabulation, et par la souris au moins ;
- Chaque fonctionnalité doit être activable par le clavier et par la souris, au moins.

Note : s'il n'y a pas de son à un média temporel, il n'est pas utile de mettre une fonctionnalité de contrôle du volume.

Contrôle de saisie (formulaire)

Ensemble des processus qui permettent de prévenir l'utilisateur des champs obligatoires, des indications de type ou de format attendus et des erreurs de saisie dans un formulaire. Ces contrôles de saisie peuvent être implémentés par l'auteur des contenus ou s'appuyer sur des attributs (comme requiredou pattern), des propriétés WAI-ARIA (comme aria-required) ou des types de champ qui produisent de manière automatique des indications de saisie ou d'erreurs (comme les types url, email, date, timepar exemple.

Note importante : lorsqu'une page est renvoyée avec des erreurs de saisie le titre de la page doit comporter la mention **"erreur sur le formulaire"**.

D

Description détaillée (image)

Contenu associé à une image en complément de son alternative textuelle afin de décrire en totalité l'information véhiculée par l'image. La description détaillée peut être insérée *via* :

- Un attribut longdesc qui contient l'adresse d'une page ou d'un emplacement dans la page contenant la description détaillée ;
- Une référence, dans l'attribut alt, à une description détaillée adjacente à l'image ;
- Un lien adjacent à l'image qui contient l'adresse d'une page ou d'un emplacement dans la page contenant la description détaillée.

E

Ensemble de pages

Pages Web liées les unes aux autres par des liens et constituant un ensemble cohérent à l'intérieur d'un site Web. Par exemple, les pages d'un processus de paiement électronique, les pages d'une rubrique spécifique, les pages d'un blog, les pages d'administration d'un compte client sont autant d'ensembles de page.

Note : la page d'accueil d'un site Web peut constituer, à elle seule, un "ensemble de pages" du fait de son unicité.

En-tête de colonne ou de ligne

Contenu d'une cellule dans un tableau de données (la première cellule d'une colonne ou d'une

ligne, généralement) qui sert d'intitulé pour la totalité ou une partie des cellules de la colonne ou de la ligne. Une colonne ou une ligne peut contenir plusieurs en-têtes (en-tête intermédiaire). Les en-têtes doivent utiliser une balise th.

Environnement maîtrisé

Tout environnement dans lequel l'accès à l'information, les technologies, les conditions d'utilisation et le profil des utilisateurs peuvent être connus et maîtrisés. Les principaux éléments dont la maîtrise est essentielle sont :

- Le type et la version des navigateurs ;
- Les technologies supportées, leur version et leur activation (JavaScript, WAI-ARIA, Flash, Silverlight…) ;
- Les technologies d'assistance et tout dispositif utilisé de manière spécifique par les utilisateurs handicapés ;
- Les systèmes d'exploitation et les APIs d'accessibilité supportées ;
- La formation des utilisateurs de technologies d'assistance à l'utilisation de tout dispositif particulier (interface, application en ligne…).

Les auteurs et les administrateurs doivent garantir la compatibilité des technologies utilisées et de leurs usages par les utilisateurs et leurs technologies (y compris les technologies d'assistance). Les services d'information ou les sites Web, quel que soit leur statut, qui offrent un accès public ne peuvent pas être considérés comme des environnements maîtrisés.

Étiquette de champ de formulaire

Texte à proximité du champ de formulaire permettant d'en connaître la nature, le type ou le format des informations attendues. L'étiquette peut être associée au champ de formulaire de plusieurs manières :

- Par l'utilisation d'une balise label;
- Par l'utilisation de la propriété WAI-ARIA aria-label;
- Par l'utilisation d'une liaison entre le texte et le champ par la propriété WAI-ARIA aria-labelledby;
- Par l'utilisation de l'attribut title.

Note importante : lorsque plusieurs de ces techniques sont présentes sur un même champ, le calcul du « nom accessible », c'est-à-dire ce qui sera restitué, obéit à un ordre strict :

1. aria-labelledby;
2. Sinon aria-label;
3. Sinon label;
4. Sinon title.

Cet ordre doit être utilisé pour l'évaluation de la pertinence de l'étiquette (critère 11.2). Par

exemple, même dans le cas de la présence d'un label, c'est le passage de texte référencé par aria-labelledby qui doit être pris en compte. Référence :

Accessible name and description calculation.

Note importante au sujet de l'utilisation de placeholder: lorsque l'attribut placeholder est présent, il est susceptible d'être restitué à la place de l'attribut title. Par conséquent, lorsque ces deux attributs title et placeholdersont présents, ils doivent être identiques.

Étiquettes cohérentes

Les étiquettes de champs de formulaire présentes dans une même page ou dans un ensemble de pages et réclamant la saisie d'une même information doivent être formulées sans ambiguïté pour que l'utilisateur sache que l'information qu'il doit communiquer est la même.

F

Feuille de style

Le langage CSS destiné à la mise en forme des éléments du contenu (exemples : couleur du fond de la page, taille/police/couleur des caractères, positionnement de l'information dans la page Web…). Les styles CSS peuvent être externes (fichier CSS), embarqués (déclarés dans l'en-tête de la page) ou en ligne (déclarés *via* l'attribut styled'une balise).

Fonctionnalités de contrôle (média temporel)

Il s'agit des fonctionnalités de contrôle de la consultation (objet multimédia) suivantes :

- L'objet multimédia doit toujours avoir les fonctionnalités suivantes, au minimum : lecture, pause, stop ;
- Si l'objet multimédia a du son, il doit avoir une fonctionnalité permettant d'activer ou de désactiver le son et d'en contrôler le niveau sonore ;
- Si l'objet multimédia a des sous-titres, il doit avoir une fonctionnalité de contrôle de l'apparition/disparition des sous-titres ;
- Si l'objet multimédia a une audio-description, il doit avoir une fonctionnalité de contrôle de l'apparition/disparition de l'audio-description.

Note : s'il n'y a pas de son à un objet multimédia, il n'est pas utile de mettre une fonctionnalité de contrôle du volume. Si cette fonctionnalité est cependant présente et qu'elle nécessite une alternative textuelle pour être comprise par certains utilisateurs (exemple : bouton "volume" dans une vidéo en Flash), il faut alors lui en donner une puisque l'utilisateur est susceptible d'y accéder et de vouloir l'activer.

I

Image de décoration

Image n'ayant aucune fonction et ne véhiculant aucune information particulière par rapport au contenu auquel elle est associée. Exemples :

- Une image servant à caler la mise en page ;
- Une image de coin arrondie pour habiller un bloc d'information ;
- Une image d'illustration n'apportant aucune information nécessaire à la compréhension du texte auquel elle est associée.

Image objet

Image incorporée ou générée par une balise object.

Image porteuse d'information

Image qui véhicule une information nécessaire à la compréhension du contenu auquel elle est associée.

Image réactive

1. **Image réactive** côté client (attribut usemap) : image divisée en zones cliquables ou neutres (attribut nohref).
2. **Image réactive côté serveur** (attribut ismap) : image pour laquelle le navigateur transmet au serveur les coordonnées du pointeur, chaque jeu de coordonnées correspondant à une ressource (page Web). L'image réactive côté serveur est extrêmement rare.

Note : en HTML5, l'attribut ismapest obsolète non conforme pour les boutons de type image (input type="image").

Image-test

Image servant dans un test, Captcha ou une image servant de test dans un quiz ou un jeu. Exemple : une série d'images présente un détail issu de tableaux célèbres; il faut reconnaître le titre et le peintre de chaque tableau. Dans cette situation, il n'est pas possible de donner une alternative pertinente (par exemple le nom du tableau et/ou du peintre) sans rendre le test inutilisable.
L'alternative doit alors se contenter de donner la possibilité d'identifier l'image, par exemple "image 1 du test".

Image texte

Image affichant du texte.

Note : il n'est pas recommandé d'utiliser des images textes. Lorsqu'il est possible de reproduire les mêmes effets en CSS, le critère 1.8 [AA] impose que le texte soit reproduit en texte CSS, ou qu'un mécanisme de remplacement permette à l'utilisateur de remplacer ces images par du texte stylé en CSS.

Image texte objet

Image générée par la balise objectet affichant du texte.

Image véhiculant une information (donnée par la couleur)

Image dont tout ou partie du contenu transmet visuellement une information par l'intermédiaire d'une couleur uniquement.

Indication donnée par la forme, la taille ou la position

Il peut s'agir, par exemple :

- De la présence d'un marqueur visuel, pour indiquer la page active dans un menu de navigation, (indication donnée par la position) ;
- D'une mise en avant-plan pour indiquer un onglet actif (indication donnée par la forme) ;
- D'une modification de la taille de police dans un nuage de tags (indication donnée par la taille).

Ou tout autre effet graphique similaire.

Information (donnée par la couleur)

Information transmise visuellement par l'intermédiaire d'une couleur. L'indication que les champs en rouge sont obligatoires dans un formulaire, un changement de couleur de fond pour indiquer la page active dans un menu de navigation, le changement de couleur d'un nom d'article pour indiquer son indisponibilité dans une liste d'article sont autant d'exemples d'indication donnée par la couleur.

L'indication donnée uniquement par la couleur doit être accompagnée d'une autre méthode à destination des utilisateurs qui ne voient pas ou perçoivent mal les couleurs ou leurs associations.

L'autre moyen de récupérer une information par la couleur peut être très divers, lorsqu'il s'agit d'un moyen faisant intervenir du graphisme (utilisation de CSS ou d'élément graphique) l'indication visuelle pourrait devoir être accompagnée d'une indication textuelle. Par exemple, un effet de bordure, de gras, de changement typographique ou autre dispositif similaire sera jugé insuffisant car ces indications ne seront pas accessibles aux personnes aveugles, notamment.

Intitulé de lien

Information textuelle comprise entre et d'un lien, complété si nécessaire d'informations de contexte.

Les 4 différents types de liens sont :

- Lien texte : il s'agit du texte compris entre et , complété si nécessaire d'informations de contexte ;
- Lien image : il s'agit du contenu de l'alternative textuelle de l'image comprise entre et , complété si nécessaire d'informations de contexte ;

- Lien composite : il s'agit de l'ensemble du texte et du contenu de l'alternative textuelle de la ou des images compris entre et , complété si nécessaire d'informations de contexte ;
- Lien vectoriel : il s'agit du contenu de l'alternative textuelle de l'image vectorielle (balise svg) comprise entre et complété si nécessaire d'informations de contexte. L'intitulé de lien pour un lien vectoriel est le contenu de l'alternative textuelle de l'image vectorielle.

Note 1 : voir la définition de lien image pour plus de précisions.

Note 2 : un lien image pour lequel l'attribut altest absent est considéré comme non applicable pour le critère 6.5.

J

Jusqu'à ou à partir de 150% (1.5em) de la taille de police par défaut sans effet de graisse. Jusqu'à ou à partir de 120% (1.2em) de la taille de police par défaut en gras

Jusqu'à ou à partir de 120% (1.2em) de la taille de police par défaut en gras

Ces deux mesures déterminent la taille relative des caractères correspondant à une taille de caractères équivalent à 14 points gras ou 18 points sans effet de graisse en considérant que la police de corps (body) est à 100%.

Note : jusqu'à 150% et jusqu'à 120% signifie que la taille des caractères est strictement inférieure à 150 ou 120%. À partir de 150% et à partir de 120% signifie que la taille des caractères est égale ou supérieure à 150 ou 120%.

La taille de police par défaut est la taille définie par l'auteur pour le document ou, en son absence, la taille par défaut utilisée par l'agent utilisateur (ie le navigateur).

L

Langue par défaut

Indication de la langue de traitement principale du document qui peut être présente sur l'élément racine htmlou sur chaque élément de la page concerné *via* les attributs langet/ou xml:lang selon le schéma suivant :

- Pour HTML jusqu'à la version 4.01 : attribut langobligatoire, attribut xml:langnon supporté
- Pour XHTML 1.0 servi en "text/html": attribut langet xml:langobligatoires
- Pour XHTML 1.0 servi en "application/xhtml+xml": attribut xml:lang obligatoire, attribut langrecommandé
- Pour XHTML 1.1 : attribut xml:langobligatoire, attribut langnon supporté

- Pour HTML5 : attribut langobligatoire

Le nom, le rôle, la valeur, le paramétrage et les changements d'états Un composant doit avoir un rôle et un nom appropriés, ses valeurs, états et paramètres éventuels doivent également être accessibles et correctement transmis aux APIs d'accessibilité notamment.

Un composant peut s'appuyer sur un élément interactif HTML ou sur un élément non interactif surchargé par l'API ARIA *via* un rôle adh'oc. **Important** : les boutons (balises button ou input type="button") lorsqu'ils sont contrôlés *via* JavaScript sont à évaluer avec le **critère 7.1**.

Le nom peut être l'intitulé du composant comme l'intitulé d'un bouton par exemple.

La valeur est, par exemple, l'élément sélectionné d'une liste déroulante ou la valeur actuelle d'un curseur (slider).

Le rôle correspond au type d'élément défini par la spécification HTML ou l'API WAI-ARIA (comme la balise buttonou le rôle ARIA role="button").

Le paramétrage correspond aux informations particulières d'un composant, généralement mis à disposition par l'API WAI-ARIA. Par exemple aria-controlsest un paramètre qui transmet aux APIs l'information que le composant contrôle tel ou tel contenu (référencé par son identifiant - attribut id).

Les changements d'états sont également mis à disposition par l'API WAI-ARIA. Par exemple aria-expandedest un état permettant de signaler aux APIs que le composant est "ouvert" ou "fermé". **Note :** un état peut également être transmis *via* le nom, lorsque l'intitulé est changé dynamiquement pour correspondre à l'état de la zone contrôlée notamment.

Ces paramètres ne sont pas obligatoires mais peuvent être requis s'ils sont indispensables pour rendre le composant accessible. C'est à l'auditeur de considérer les cas où ces paramètres sont indispensables en fonction du contexte lié à l'utilisation du composant.

L'auditeur doit également vérifier que, lorsqu'il sont présents, ces paramètres sont correctement utilisés.

Note : les rôles, propriétés et états ARIA s'implémentent *via* des attributs, par exemple role="banner", aria-hidden="true".

Légende d'image

Lorsqu'un texte, adjacent à une image, contient des informations sur l'image (par exemple un copyright, une date, un auteur…) ou est destiné à compléter les informations apportées par l'image (par exemple un texte associé à une image dans une galerie d'images), on parle de légende d'image.

Lorsqu'une image est légendée il est nécessaire d'associer la légende de l'image à l'image par une relation de structure, de telle sorte que les technologies d'assistance puissent traiter l'image et sa légende comme un ensemble unique.

HTML5 propose d'associer une légende à une image *via* les éléments figure(l'ensemble de l'image et la légende) et figcaption(la légende).

Une image sans légende peut définir :

- Une image qui n'est pas insérée dans un élément figure;
- Une image insérée dans un élément figuresans élément figcaption.

Note : lorsque le texte adjacent à l'image peut faire office de texte de remplacement, il n'est pas obligatoire de recourir à l'ensemble figure, figcaption, l'image pouvant être simplement traitée comme une image de décoration.

Vous pouvez consulter, à ce sujet, la note Requirements for providing text to act as an alternative for images du W3C.

Lien

Élément HTML (balise a) activable par l'utilisateur (par la souris, le clavier…) et déclenchant une action (affichage d'une page Web, téléchargement d'un fichier…) ou un événement généré par un script. Un lien possède au minimum :

- Une référence de ressource (attribut href) ;
- Un intitulé de lien compris entre et .

Lien adjacent

Lien présenté de manière adjacente dans la représentation graphique (CSS activé) et dans le code HTML. Dans le code HTML, le lien doit se situer juste avant ou juste après l'objet avec lequel il est adjacent.

Lien composite

Lien dont le contenu entre et est constitué de 2 éléments de type différent, au moins ; par exemple, du texte et une ou plusieurs images. L'intitulé de lien pour un lien composite est l'ensemble du texte et du contenu de l'alternative textuelle de ou des images compris entre et .

Note importante: il est rappelé que l'utilisation de deux liens adjacents (lien image et lien texte) et identiques constitue une gêne importante pour l'utilisateur. Même si cela ne constitue pas une non-conformité, cet usage devrait être évité. Une manière de traiter ce type de liens est d'inclure l'image dans le lien texte de façon à constituer un lien composite, ce qui évitera la redondance.

Vous pouvez consulter à ce sujet la technique H2 : Combining adjacent image and text links for the same resource.

Lien dont la nature n'est pas évidente

Lien qui peut être confondu avec un texte normal lorsqu'il est signalé uniquement par la couleur par certains types d'utilisateurs ne percevant pas ou mal les couleurs. Par exemple, dans ce texte

"Nouvelle grève à la SNCF", si le mot "grève" est un lien signalé uniquement par la couleur, sa nature peut être ignorée par les utilisateurs ne percevant pas la couleur et accédant au contenu CSS activées. En revanche, dans ce texte " Nouvelle grève à la SNCF, lire la suite" si "lire la suite" est un lien, un utilisateur ne percevant pas les couleurs n'aura pas de problème pour en comprendre la nature.

Note : "signalés uniquement par la couleur" signifie que le lien n'est accompagné d'aucun marqueur visuel (icône, soulignement, bordure…). En conséquence un lien de la même couleur que le texte environnant est concerné par ce critère.

Lien explicite hors contexte

Un lien est explicite hors contexte lorsque l'intitulé du lien seul (contenu entre la balise et) permet de connaître et de comprendre la fonction et la destination du lien.

Lien image

Lien dont le contenu entre et est uniquement constitué d'une image. L'intitulé de lien pour un lien image est le contenu de l'alternative textuelle de l'image.

Un lien image peut être constitué :

- D'une image (balise img), l'alternative est le contenu de l'attribut alt;
- D'une zone cliquable (balise area) possédant un attribut href, l'alternative est le contenu de l'attribut alt;
- D'une image objet (balise object), l'alternative est contenue entre <object>et </object>;
- D'une image bitmap (balise canvas), l'alternative est contenue entre <canvas>et </canvas>;
- D'une image embarquée (balise embed), l'alternative est contenue entre <embed>et </embed>;
- D'une image vectorielle (balise svg), l'alternative est contenue dans les attributs title, aria-label ou la balise <desc>.

Note au sujet de embed: en HTML5, la balise embeda été modifiée. C'est une balise autofermante qui ne peut pas embarquer de contenu alternatif. Les propriétés ARIA, comme aria- labelqui permettrait d'embarquer une alternative, n'étant pas supportées de manière uniforme, il n'est pas possible d'utiliser une image embarquée, porteuse d'information, *via* l'élément embed HTML5.

Lien texte

Lien dont le contenu entre et est uniquement constitué de texte (il s'agit de son intitulé de lien).

Liens d’évitement ou d’accès rapide

Liens dont la fonction est de permettre de naviguer à l’intérieur du contenu (lien d’évitement, lien d’accès au formulaire de recherche ou au menu..).

Liens identiques

Deux liens sont dits identiques quand le lien x (intitulé du lien seul, contenu de l’attribut titleou contexte du lien) est égal au lien y. Cette définition s’applique à tous les types de liens : lien texte, lien image (les liens ont alors la même image) et lien composite.

Attention : des liens avec des intitulés identiques mais des titres de liens différents ou des contextes de liens différents ne sont pas identiques (exemple : cliquer ici et cliquer ici).

Liste de choix

Champ de formulaire affichant une série d’items à sélectionner sous forme d’une liste déroulante (balise selectavec des balises option).

Listes

Suite d’éléments pouvant être regroupés sous la forme d’une liste structurée ordonnée, non ordonnée ou de définition. Par exemple la suite des liens d’un menu de navigation est une liste de liens non ordonnée, les différentes étapes d’une procédure est une liste d’éléments ordonnés, le couple terme/définition d’un glossaire est une liste de définition. En HTML, les listes utilisent les balises suivantes :

- Liste ordonnée : balises olet li(chaque élément de la liste est affecté d’un marqueur indéxé) ;
- Liste non ordonnée : balises ulet li(chaque élément de la liste est affecté d’un marqueur non-indéxé ;
- Liste de définition : balises dl, dt(terme à définir) et dd(définition).

M

Mécanisme de remplacement

Mécanisme généralement basé sur CSS, permettant à l’utilisateur de remplacer du texte par du texte en image et inversement sur le principe du style switcher. Le mécanisme peut utiliser un langage de script côté serveur ou un langage de script côté client.

Média non temporel

Contenu qui ne se déroule pas dans le temps, consultable *via* un plugin (Flash, Java, Silverlight…) ou *via* les éléments svget canvas; par exemple, une carte interactive en Flash, une application

Flash ou Java, un diaporama sont des médias non temporels. Un média non temporel peut contenir des médias temporels (un lecteur Flash qui propose une liste de vidéos à consulter, par exemple).

Note : l'utilisation du paramètre wmodepour un objet Flash avec les valeurs "transparent"et "opaque" invalide de fait le critère 4.21 (La consultation de chaque média non temporel est-elle contrôlable par le clavier et la souris ?). En effet, l'utilisation de ces valeurs a pour conséquence que l'animation Flash vue du côté des utilisateurs de lecteur d'écran est invisible.

Média temporel (type son, vidéo et synchronisé)

- Média temporel seulement audio : contenu sonore (Wave, Mp3…) ;
- Média temporel seulement vidéo : images ou photos en mouvement ou en séquence ;
- Média temporel synchronisé : flux audio ou vidéo synchronisé avec un autre format pour présenter de l'information et/ou comportant des composants temporels interactifs. Un média temporel peut être consulté de 2 manières différentes :
    - Fichier à télécharger consultable avec un logiciel externe à la page Web ;
    - Contenu embarqué dans la page Web et consultable dans la page Web *via* :
        - Un plugin (par exemple une vidéo diffusée par un lecteur Flash) ;
        - L'élément video(par exemple une vidéo) ;
        - L'élément audio(par exemple un podcast) ;
        - L'élément svg(par exemple un dessin animé vectoriel) ;
        - L'élément canvas(par exemple un dessin animé en image bitmap).
        - L'élément bgsoundpour diffuser un arrière-plan sonore à la page Web.

Un média temporel peut être diffusé en temps réel ou être proposé en lecture de manière asynchrone (média pré-enregistré).

Note 1 : l'utilisation du paramètre wmodepour un objet Flash avec les valeurs "transparent" et "opaque" invalide de fait le critère 4.20 (La consultation de chaque média temporel est-elle contrôlable par le clavier et la souris ?). En effet, l'utilisation de ces valeurs a pour conséquence que l'animation Flash vue du côté des utilisateurs de lecteur d'écran est invisible.

Note 2 : les gif animés, les animations d'images réalisées par JavaScript ou CSS ne sont pas considérés comme étant des médias temporels.

Note 3 : l'élément bgsoundest spécifique à Internet Explorer et ne devrait pas être utilisé.

Menu de navigation

Zone contenant des liens qui permettent de naviguer dans les rubriques principales du site. Il s'agit généralement du menu principal et des menus contextuels.

Note : Les liens de pied de page renvoyant vers les mentions légales, plan du site et autres informations concernant le site ne sont pas considérés comme un menu de navigation principal.

Voir la définition technique de zone d'en-tête fournie par l'API ARIA navigation (role).

Modification du rôle natif d'un élément HTML

La spécification WAI-ARIA permet de modifier le rôle natif d'un élément, par exemple modifier un élément a href=""en élément button.

Ces modifications ne peuvent être réalisées que sous certaines conditions décrites dans le document : Notes on Using WAI-ARIA in HTML qui définit un certain nombre de restrictions notamment.

Pour qu'une modification du rôle natif d'un élément HTML *via* WAI-ARIA soit compatible, il faut que les restrictions soient respectées.

Moteur de recherche (interne à un site Web)

Zone contenant le moteur de recherche permettant d'effectuer des recherches sur les contenus de l'ensemble du site

Note : Attention à ne pas confondre cette zone de recherche, unique dans le site, avec tout autre moteur de recherche permettant par exemple de faire des recherches sur une partie restreinte du site : un catalogue, les offres sur une section marchés publics…

Voir la définition technique de zone d'en-tête fournie par l'API ARIA search (role).

Motif de conception

Un motif de conception (Design Pattern) est un modèle défini par l'API WAI-ARIA qui décrit la structure, les rôles et propriétés et le comportement que doit respecter un composant JavaScript (widget).

Les motifs de conception sont décrits dans le document : WAI-ARIA 1.0 Authoring Practices.

Un composant développé avec JavaScript doit respecter le motif de conception correspondant au rôle WAI-ARIA utilisé.

Note 1: compte tenu du manque de support de certaines propriétés et de certains rôles WAI-ARIA et de la grande variabilité des situations dans lesquelles un composant JavaScript peut être proposé, il est possible d'adapter des motifs de conception à des contextes ou des utilisations particulières.
Dans ce cas, le motif de conception adapté doit :

- Respecter la structure générale, par exemple un ensemble de panneaux (rôle tabpanel) d'un système d'onglets est forcément lié à un ensemble d'onglets (rôle tablist) ;
- Utiliser en remplacement d'un role ou d'une propriété WAI-ARIA mal supporté, un rôle ou une propriété WAI-ARIA équivalent, offrant un comportement et une restitution similaire.

Note 2: Cela ne concerne pas le fait d'enrichir un motif de conception de rôles ou propriétés WAI-ARIA supplémentaires dont la compatibilité avec l'accessibilité est contrôlée par le test de restitution sur la base de référence. Par exemple l'ajout de la propriété aria-hiddensur les panneaux (rôle tabpanel) d'un système d'onglets ne définit pas un motif de conception adapté.

O

Ordre de tabulation

Ordre dans lequel le focus se déplace (vers un élément suivant ou vers un élément précédent). L'ordre naturel est celui qui est implémenté *via* le code source. Lorsqu'il est modifié par l'utilisation de l'attribut tabindexou par l'utilisation d'une commande JavaScript, c'est l'ordre modifié qui fait référence.

Attention : lorsqu'un élément initie un changement dans la page (changement de contexte, gestion de zones cachées, ajout de contenu, gestion de champs de formulaire…) il est nécessaire d'activer l'élément qui initie le changement pour tester la cohérence de l'ordre de tabulation.

P

Page "plan du site"

Page dédiée présentant l'arborescence d'un site Web, généralement sous forme de listes de liens organisées en rubriques et sous-rubriques donnant accès à l'ensemble des pages du site.

Note 1 : les liens du plan du site peuvent être constitués de balises aou de balises area.

Note 2 : il n'est pas nécessaire que le plan du site contienne les liens vers toutes les pages du site, en revanche il est nécessaire qu'à partir du plan du site, l'utilisateur puisse atteindre l'ensemble des pages du site.

Pertinence (information autrement que par la couleur)

Le moyen pour récupérer une information autrement que par la couleur doit être accessible à tous. Par exemple, dans le cas d'une liste d'articles dont les articles en jaune sont en promotion, l'utilisation de texte caché *via* CSS est un moyen de récupérer l'information "en promotion", mais il n'est pas pertinent car cette information restera cachée à l'utilisateur qui visualise la page CSS activée.

Note : l'utilisation d'une balise d'emphase (strongou em) comme autre moyen pour récupérer une information donnée par la couleur permet de valider le critère même si ces éléments ne sont généralement pas supportés par les technologies d'assistance, particulièrement les lecteurs d'écrans.

Présentation de l'information

Restitution visuelle des contenus *via* un navigateur en mode graphique. La présentation concerne le style, la position et les dimensions des éléments HTML et de leur contenu. La présentation de l'information doit être réalisée *via* CSS. Les éléments (basefont, blink, center, font, marquee, s, strike, tt, u, binget small) et les attributs (align, alink, background, bgcolor, border, cellpading, cellspacing, char, charoff, clear, compact, color, frameborder,hspace, link, marginheight, marginwidth, text, valign, vlink, vspace, size) sont interdits.

Note : Les attributs widthet heightutilisés sur d'autres éléments que les balises img, object, embed, canvaset svg, sont également interdits.

Prise de focus

La prise de focus est l'état renvoyé par un élément qui reçoit l'attention suite à une action de l'utilisateur. Il y a trois moyens en HTML de donner le focus à un élément :

- En activant l'élément par un dispositif de pointage (souris) ;
- En activant l'élément par la touche tabulation ;
- En activant l'élément par un raccourci clavier (accesskey).

Certains éléments reçoivent naturellement le focus, par exemple : a, area, button, input, object, select, label, legend, optgroup, optionet textarea. Le comportement de l'élément, lors de la prise de focus, dépend de sa nature ; un lien, par exemple, devra être activé après la prise de focus (sauf utilisation de script). En revanche, un élément de formulaire, comme textarea, devra autoriser la saisie suite à la prise de focus. Les éléments labelet legendne reçoivent la prise de focus que *via* le pointeur souris. Pour l'élément label, le comportement attendu est de transférer la prise de focus sur l'élément qui lui est associé.

Note 1 : la spécification WAI-ARIA étend le rôle attribué à l'attribut tabindexen définissant que tout élément html peut acquérir la possibilité de recevoir le focus en lui attribuant la valeur tabindex="0". En revanche, aucun comportement n'est attribué *via* la seule présence de tabindex. De même, la valeur tabindex="-1"retire l'élément qui en est affecté du plan de tabulation en inhibant sa capacité à signaler la "prise de focus". L'utilisation de tabindex, conformément à la spécification WAI-ARIA, peut valider certains tests relatifs à la gestion du focus de tabulation, notamment.

Note 2 : l'indication visuelle du focus ne doit pas être dégradée, c'est à dire amoindrie au moyen de valeurs qui en dégrade le style par rapport à son style par défaut.

Procédé de rafraîchissement

Technique visant à modifier le contenu d'un ou de plusieurs éléments de la page Web. Le procédé de rafraîchissement peut s'effectuer par rechargement automatique de la page ou de manière dynamique sans rechargement de la page (*via* AJAX, par exemple). L'utilisateur doit pouvoir contrôler chaque procédé de rafraîchissement de manière indépendante.

Propriété CSS déterminant une couleur

Cela concerne les propriétés suivantes : color, background-color, background, border-color, border, outline-color, outline.

Note : l'utilisation d'une image de fond pour insérer une couleur (propriété background:url…) est également concernée.

Propriétés et méthodes conformes à la spécification DOM

Les méthodes d'insertion de contenu conformes à la spécification DOM permettent de créer, insérer et manipuler des éléments *via* le DOM (par exemple document.createElementet element.appendChild) par opposition à la méthode document.writequi peut poser des problèmes dans certains contextes (voir : https://www.w3.org/TR/html5/webappapis.html#dom- document-write).

R

Redirection

Procédé qui consiste pour l'affichage d'une page sur le poste client à rediriger l'utilisateur vers une autre page, sur le même domaine ou sur un domaine différent.

Correctement restitué (par les technologies d'assistance)

Lorsqu'un critère, un test ou une condition de test demande de vérifier la restitution d'un dispositif, il faut s'assurer que ladite restitution est compatible avec l'accessibilité.

Le test consiste à vérifier que la restitution est pertinente pour au moins une des combinaisons de la base de référence utilisée pour déclarer qu'un élément, un dispositif ou une alternative est "compatible avec l'accessibilité".

Par exemple : le test 1.3.7 demande de vérifier que l'alternative d'une image porteuse d'information vectorielle est correctement restituée.

On procède alors à un test avec NVDA (dernière version) et Firefox, JAWS (version précédente) et IE9+, et Voice Over (dernière version) et Safari.

Si on constate que l'alternative est correctement restituée, le test est validé.

Résumé (de tableau)

Un résumé est un passage de texte associé à un tableau de données complexe. Il permet de donner des informations sur la nature et la structure du tableau afin d'en faciliter l'utilisation par les utilisateurs de technologies d'assistance par exemple.

Note : l'attribut summaryest obsolète non conforme en HTML5 et ne doit plus être utilisé.

Parmi les 5 techniques proposées par HTML5, la seule technique utilisable actuellement est celle qui consiste à insérer le résumé directement dans le titre (balise caption) en masquant le résumé *via* CSS si nécessaire.

Consulter la note technique au sujet du résumé de tableau.

S

Script

Code généralement écrit sous forme d'une liste de commandes (par exemple JavaScript). Les langages interprétés côté client nécessitent un navigateur compatible sur lequel l'exécution du langage est active. Les commandes d'un langage de script côté client peuvent être embarquées ou contenues dans un fichier externe. Dans les deux cas, l'insertion se fait *via* la balise <script>.

Sens de lecture

Indique le sens de lecture du document ou d'un passage de texte *via* l'attribut dir, dir="ltr", par exemple. Les deux valeurs reconnues sont :

- ltr(left to right) indique un sens de lecture de gauche à droite ;
- rtl(right to left) indique un sens de lecture de droite à gauche.

Note : en l'absence d'indication de sens de lecture *via* l'attribut dirsur l'élément html, body, ou un des parents du texte analysé, le sens de lecture par défaut est de gauche à droite (valeur ltr).

Site Web : ensemble de toutes les pages Web

- Reliées par des liens Web ;
- Appartenant au même nom de domaine (ex : references.modernisation.gouv.fr) ;
- Qui constituent un ensemble cohérent du point de vue de l'utilisateur.

Cas particulier des pages Web d'un sous-domaine ; un sous-domaine peut :

- Soit appartenir au site Web attaché au nom de domaine, si l'utilisateur en a une perception cohérente avec les autres pages du site Web (par exemple : même structure, même navigation…) ;
- Soit ne pas appartenir au site Web attaché au nom de domaine (par exemple : différents blogs en sous-domaine d'un nom de domaine et sans relation les uns avec les autres).

Sous-titres synchronisés (objet multimédia)

Texte des informations audio (paroles d'un personnage, bruit important pour comprendre l'action…) présentes dans un média temporel et affiché de manière synchrone avec le flux de l'objet multimédia.

Note 1 : pour différencier les sources sonores (différents personnages, voix off…), il est recommandé d'utiliser un mécanisme approprié (mise entre crochets, mise en italique, annonce explicite du type "voix off : …").

Note 2 : il ne faut pas confondre le sous-titrage pour la traduction (kind="subtitles"en HTML5 par exemple) et le sous-titrage pour sourds et malentendants (kind="captions"en HTML5 par exemple). Ces deux types de sous-titrage poursuivent des buts différents. Seule la présence et la pertinence d'un sous-titrage pour sourds et malentendants permet d'être conforme.

Système de navigation

Tout procédé permettant une navigation dans le site ou dans une page, les systèmes de navigation retenus sont :

- Menu de navigation principal ;
- Table de contenu ;
- Plan du site ;
- Moteur de recherche.

T

Tableau de données

Élément HTML (balise table) permettant de structurer des informations en lignes et en colonnes *via* des cellules de données (balise td) et des cellules d'en-têtes (balise th).

Tableau de données complexe

Lorsqu'un tableau de données contient des en-têtes qui ne sont pas répartis uniquement sur la première ligne et/ou la première colonne de la grille ou dont la portée n'est pas valable pour l'ensemble de la colonne ou de la ligne, on parle de tableau de données complexe. Il est alors nécessaire de fournir un "résumé" permettant d'en expliquer sa nature et sa structure afin d'en faciliter la consultation pour des utilisateurs de technologies d'assistance par exemple.

Tableau de mise en forme

Technique qui utilise un élément HTML (balise table) pour contrôler l'affichage d'informations *via* des cellules (balise td).

Taille des caractères

Valeur attribuée aux polices de caractères présentes sur une page Web. Pour les contenus Web, les tailles de caractères doivent être définies avec des unités relatives (%, em, rem, vw, vh, vminou vmax) ou des mots clés (xx-small, x-small, small, medium, large, x-large, xx- large, xsmaller, larger).

Note : l'utilisation du pixel (px) est proscrite.

Texte caché

Les technologies d'assistance (notamment les lecteurs d'écran) ne restituent pas le texte masqué *via* les propriétés :

- displayavec la valeur none (display:none)
- visibilityavec la valeur hidden (visibility :hidden)
- widthet heightavec les valeurs 0 (width:0;height:0)
- font-sizeavec la valeur 0 (font-size:0)

- Attribut HTML5 hidden
- Propriété aria-hidden="true"

Tous les contenus texte utilisant une ou plusieurs de ces propriétés sont applicables pour le critère 10.13.

Texte stylé

Texte dont la mise en forme est contrôlée par une feuille de styles.

Titre

Élément HTML (balise h) à 6 niveaux de hiérarchie (de h1pour le titre le plus important à h6pour le moins important) permettant de structurer l'information d'un contenu Web. La hiérarchie entre les titres doit être respectée dans une page Web et les degrés de titre ne peuvent pas être sautés (un titre h3ne peut pas venir directement après un titre h1, par exemple). Dans chaque page Web, il doit y avoir un titre h1, au moins.

Note : les titres cachés *via* CSS sont considérés comme présents et valident le critère 9.1.

Titre d'un tableau (de données)

Contenu d'un élément HTML (balise caption) qui permet d'identifier le contenu d'un tableau de données de manière claire et concise.

Titre de cadre

Contenu de l'attribut titlede la balise iframepermettant de connaitre la nature du contenu diffusé *via* le cadre en ligne lorsque l'utilisateur navigue de cadre en cadre ou affiche la liste des cadres de la page par exemple.

Note 1 : Certains cadres en ligne servent uniquement à des opérations techniques tels que des traitements applicatifs destinés à préparer ou piloter des contenus affichés dans la page comme les cadres en ligne utilisés par certains réseaux sociaux comme Facebook par exemple.

Si ces cadres sont dépourvus de titre de cadre fournis par le service distant, ou si les titres de cadres sont jugés non pertinents, des mentions génériques peuvent être utilisées, par exemple title="contenus techniques Facebook".

Note 2 : Si cela ne gêne pas le fonctionnement de ce type de cadre, il est possible de les rendre indisponibles aux technologies d'assistance en utilisant une propriété ARIA aria- hidden="true"par exemple.

Titre de lien

Contenu de l'attribut titled'un lien. Ce contenu ne doit être présent que s'il est nécessaire pour identifier la destination du lien de manière explicite. Un titre de lien doit reprendre l'intitulé de lien en y ajoutant des informations. Un titre de lien sera considéré comme non-pertinent dans les cas suivants :

- Le titre de lien est vide ;
- Le titre de lien est identique à l'intitulé du lien (Cf. note 1) ;
- Le titre de lien ne reprend pas l'intitulé du lien.

Note 1 : Par exception, un titre de lien identique à l'intitulé est accepté dans le seul cas d'un lien image (lien ne contenant que des images), une icône par exemple.

Note 2 : Il est rappelé que l'attribut titlepeut poser de vrais problèmes de restitution, par exemple au clavier, sur les surfaces tactiles, lorsqu'une technologie d'assistance est paramétrée pour ne pas les restituer et ne devrait être utilisé qu'en dernier recours.

Titre de page

Contenu de la balise titled'une page Web permettant d'identifier de manière claire, concise et unique les contenus/la nature de la page ("Plan du site www.nomdusite.fr" pour une page présentant le plan du site Web, par exemple).

Transcription textuelle (média temporel)

Contenu textuel associé à un média temporel par la technique appropriée (texte codé en HTML ou dans un fichier texte qui se trouve dans la même page ou consultable suivant un lien). Ce contenu donne accès à l'utilisateur (de manière indépendante de la consultation de l'objet multimédia) à :

- La totalité de ce qui y est exprimé oralement ;
- Toutes les informations descriptives nécessaires à une compréhension équivalente de l'action.

Ces informations textuelles doivent être présentées dans l'ordre chronologique de leur apparition dans le média temporel.

Note : la transcription textuelle doit se situer à l'extérieur de la balise object.

Type de document

Ensemble de données de référence qui permet aux agents utilisateurs de connaître les caractéristiques techniques des langages utilisés sur la page Web (balise doctype).

Type et format de données

Indication concernant le type et le format des données attendus lors de la saisie d'un champ de formulaire. Par exemple :

- Date (jj/mm/aaa) ;
- Montant en euros ;
- Code postal (5 chiffres : ex. 75001).

Note importante : lorsque le type de champ de formulaire propose un masque de saisie, comme par exemple les champs dateou time, l'indication de format n'est pas nécessaire.

U

Uniquement à des fins de présentation

Uniquement à des fins de présentation : utilisation de balises HTML pour une finalité différente de celle prévue dans les spécifications (au regard du type de document déclaré). Exemples : utilisation des balises hà seule fin de créer un effet typographique ; utilisation de la balise blockquoteà seule fin de mettre un paragraphe en retrait, etc.

Note 1 : l'utilisation d'éléments divou spanpour créer des paragraphes est considérée comme non conforme et invalide le critère.

Note 2 : WAI-ARIA propose un rôle presentationpermettant de supprimer la sémantique d'un élément, par exemple <h1 role="presentation"> Titre</h1>. Dans ce cas, le texte sera correctement restitué mais le titre lui ne le sera plus (l'élément restitué sera un élément indéterminé du type <>Titre</>. L'utilisation du rôle presentationpeut être requise lorsque l'on utilise un motif de conception ARIA.

L'utilisation du rôle presentationpeut être également utilisé pour supprimer la sémantique d'un élément lorsque ce dernier est utilisé uniquement à des fins de présentation, par exemple <blokquote role="presentation">aura le même effet qu'une absence d'élément blockquote.

Même si cette utilisation est fortement déconseillée (dans le cas de technologie d'assistance qui n'implémenteraient pas ARIA par exemple) elle peut être considérée comme conforme à WCAG. En revanche l'utilisation d'un rôle presentationsur un élément dont la nature (par exemple la sémantique) est essentielle à la compréhension du contenu est une violation des règles WCAG (particulièrement de l'échec F92) et invalide le critère.

Url

Adresse permettant d'accéder aux ressources du World Wide Web : document HTML, pages Web, image, son…

Note : dans le référentiel RGAA PF, la notion d'url est utilisée à la place de uri (chaîne de caractères compacte identifiant une ressource).

V

Version accessible (pour un document en téléchargement)

Les documents en téléchargement dont les types de format sont reconnus compatibles avec l'accessibilité doivent être rendus accessibles soit directement soit par l'intermédiaire d'une version accessible ou d'une version en HTML. Les formats de document dont la compatibilité est reconnue sont :

- Microsoft Office (Word 2003, OOXML) ;

- Open Office Org (ODF) ;
- Adobe PDF ;
- Epub/Daisy.

Les contenus doivent être conformes à la liste des critères Documents Bureautiques en téléchargement (format ODT, 74 kilo-octets).

Note : le format txt ne peut pas être utilisé pour produire une version accessible pour un document en téléchargement.

Version alternative "audio seulement"

Une version "audio seulement" est une version sonore, sous la forme d'un simple fichier au format MP3 par exemple, utilisée comme alternative à une vidéo seulement (vidéo sans information sonore). Les seuls utilisateurs impactés par l'accessibilité étant les personnes aveugles, qui ne peuvent pas voir la vidéo, WCAG considère comme acceptable de proposer en alternative une version sonore.

La version "audio seulement" doit contenir toutes les informations visuelles importantes de la vidéo.

Généralement il est plus simple de produire une version sonore qu'une version textuelle lorsque la vidéo est très descriptive (la transcription textuelle nécessitant souvent un travail rédactionnel important). Il est rappelé, néanmoins, que seule la transcription textuelle assure un accès universel aux informations diffusées par la vidéo, dans le cas où un utilisateur ne serait pas en capacité de lancer la vidéo par exemple.

Z

Zone (d'une image réactive)

Zone cliquable ou zone non cliquable d'une image réactive côté client ou zone cliquable d'une image réactive côté serveur.

Zone cliquable

Région d'une image réactive à laquelle une action a été associée ; par exemple, le déclenchement d'un événement en cliquant sur un lien (pour une zone cliquable côté client : balise areaavec l'attribut href). Les balises areasont contenues dans la balise map.

Pour les images réactives côté serveur, les coordonnées sont détenues sur le serveur.

Zone d'en-tête

Zone située en haut du document et contenant généralement le titre du document, un logo, un slogan…

Note : Attention à ne pas confondre cette zone d'en-tête, unique dans le site, avec tout contenu pouvant être balisé en HTML5 avec l'élément header.

Voir la définition technique fournie par l'API ARIA : Banner (role).

Zone de contenu principal

Zone contenant les principaux contenus de la page, là où se trouvent les informations et fonctionnalités de fond (donc en dehors des menus, de la recherche ou des zones secondaires de publicités, actualités connexes…).

Note : Cette zone est unique dans la page. Elle peut être difficile à déterminer sur certaines pages particulières, comme la page d'accueil.

Voir la définition technique fournie par l'API ARIA : Main (role).

Zone de pied de page

Il s'agit des informations concernant le fonctionnement du site ou les informations légales. On y trouve par exemple les mentions légales, les crédits, les conditions d'utilisation, le plan du site et éventuellement la page accessibilité.

Note : Attention à ne pas confondre cette zone de pied de page, unique dans le site, avec tout contenu pouvant être balisé en HTML5 avec l'élément footer.

Voir la définition technique fournie par l'API ARIA : Contentinfo (role)

Zone non cliquable

Région d'une image réactive à laquelle aucune action n'est associée. Une zone cliquable côté client est contenue dans une balise area:

- Avec l'attribut nohreflorsque le code HTML de la page n'est pas du HTML5 ;
- Sans attribut hrefen HTML5.

Les balises areasont contenues dans la balise map.

RGAA PF – Cas particuliers

Plusieurs critères RGAA PF font référence à des cas particuliers nécessaires à leur compréhension et application. Ce document liste l'ensemble des cas particuliers pour lesquels le critère concerné est non applicable.

Images

Critère 1.3

Il existe une gestion de cas particuliers lorsque l'image est utilisée comme CAPTCHA ou comme image-test. Dans cette situation, où il n'est pas possible de donner une alternative pertinente sans détruire l'objet du CAPTCHA ou du test, le critère est non applicable.

Note : le cas des CAPTCHA et des images-test est traité de manière spécifique par le critère 1.4.

Critère 1.8

Pour ce critère, il existe une gestion de cas particulier lorsque le texte fait partie d'un logo ou d'un élément associé à l'identité graphique d'un organisme ou d'une société (un slogan, par exemple). Dans ces situations, le critère est non applicable pour ces éléments.

Critère 1.9

Pour ce critère, il existe une gestion de cas particulier lorsque le texte fait partie d'un logo ou d'un élément associé à l'identité graphique d'un organisme ou d'une société (un slogan, par exemple). Dans ces situations, le critère est non applicable pour ces éléments.

Note 1 : les changements de couleurs consécutifs à la prise de focus ne sont pas concernés par l'application du critère, sauf si le contenu change également lors de la prise de focus.

Note 2 : les indications des états de liens (visités ou actifs) ne sont pas concernées par l'application du critère.

Couleurs

Critères 3.3 - 3.4

Pour ces critères, il existe une gestion de cas particulier lorsque le texte fait partie d'un logo ou d'un élément associé à l'identité graphique d'un organisme ou d'une société. Dans ces situations, les critères sont non applicables pour ces éléments.

Note 1 : Les cas particuliers concernant des textes associés à l'identité graphique d'un organisme ou d'une société devraient être limités à des éléments particuliers comme un slogan par exemple. Dans le cas où c'est l'intégralité d'une charte graphique, particulièrement lorsque la charte graphique est imposée, qui est en cause, comme un choix de couleur de police par exemple, la solution consiste à avoir recours à une version alternative, à fort contraste.

Note 2 : Les changements de couleurs consécutifs à la prise de focus ne sont pas concernés par

l'application du critère, sauf si le contenu change également lors de la prise de focus.

Note 3 : les indications des états de liens (visités ou actifs) ne sont pas concernées par l'application du critère.

Pour ces critères, il existe une gestion de cas particuliers lorsque le texte en image est utilisé comme CAPTCHA ou comme image-test. Dans cette situation, les critères sont non applicables.

Multimédia

Critères 4.1 - 4.2 - 4.3 - 4.5 - 4.7 - 4.9 - 4.11 - 4.13

Il existe une gestion de cas particulier lorsque :

- Le média temporel est utilisé à des fins décoratives (i.e. il n'apporte aucune information) ;
- Le média temporel est lui-même une alternative à un contenu de la page (une vidéo en langue des signes ou la vocalisation d'un texte, par exemple) ;
- Le média temporel est utilisé pour accéder à une version agrandie ;
- Le média temporel est utilisé comme un CAPTCHA ;
- Le média temporel fait partie d'un test qui deviendrait inutile si la transcription textuelle, les sous-titres synchronisés ou l'audio-description étaient communiqués.

Dans ces situations, le critère est non applicable.

Critère 4.15

Il existe une gestion de cas particulier lorsque le média temporel est utilisé à des fins décoratives (i.e. il n'apporte aucune information). Dans cette situation, le critère est non applicable.

Critère 4.16

Il existe une gestion de cas particulier lorsque :

- Le média non temporel est utilisé à des fins décoratives (i.e. il n'apporte aucune information) ;
- Le média non temporel est diffusé dans un environnement maîtrisé ;
- Le média non temporel est inséré *via* JavaScript en vérifiant la présence et la version du plug-in, en remplacement d'un contenu alternatif déjà présent.

Dans ces situations, le critère est non applicable.

Critère 4.19

Il existe une gestion de cas particulier lorsque le média temporel est utilisé comme CAPTCHA ou fait partie d'un test qui deviendrait inutile si l'arrière-plan sonore pouvait être désactivé, ou si la ou les pistes de dialogue étaient 20 décibels plus élevées que l'arrière-plan sonore.

Dans ces situations, le critère est non applicable.

Critère 4.22

Il existe une gestion de cas particulier lorsque : le média temporel ou non temporel est utilisé à des fins décoratives (i.e. il n'apporte aucune information). Dans ces situations, le critère est non applicable.

Tableaux

Critère 5.3

L'API ARIA propose un mécanisme permettant de surcharger le rôle natif d'un élément HTML pour proposer des composants. Ainsi, il est possible d'utiliser des tableaux de mise en forme pour construire des listes :

```
<table role="list">
    <tr role="listitem">
    <td role="presentation"><img src="puce.png" alt=""/></td>
    <td role="presentation">lorem ipsum</td>
    </tr>
…
</table>
```

Si cet usage est fortement déconseillé, il est néanmoins conforme. Le tableau n'étant pas restitué comme un tableau mais comme une liste, il n'est pas utile de signaler qu'il s'agit d'un tableau de mise en forme. Dans ce cas, le critère est non applicable.

Liens

Critères 6.1 et 6.3

Il existe une gestion de cas particulier lorsque le lien est ambigu pour tout le monde. Dans cette situation, où il n'est pas possible de rendre le lien explicite dans son contexte, le critère est non applicable.

Scripts

Critère 7.3

Il existe une gestion de cas particulier lorsque la fonctionnalité dépend de l'utilisation d'un gestionnaire d'événement sans équivalent universel, par exemple, une application de dessin à main levée ne pourra pas être rendue contrôlable au clavier. Dans ces situations, le critère est non applicable.

Critère 7.5

Il existe une gestion de cas particulier lorsque l'alerte non sollicitée concerne un cas d'urgence, un événement ou une situation soudaine et imprévue qui exige une action immédiate afin de préserver la santé, la sécurité ou la propriété. Dans ces situations, le critère est non applicable.

Éléments Obligatoires

Critère 8.2

Il y a une gestion de cas particulier sur la conformité du code HTML.

Pour accompagner la prise en charge progressive de HTML5 par les navigateurs, les APIs d'accessibilité et les technologies d'assistance, certains critères peuvent exiger la présence d'attributs ou de balises déclarés "obsolètes" en HTML5. Dans ce cas le test 8.2.2 est non applicable.

Critère 8.7

Il y a une gestion de cas particulier sur le changement de langue pour les cas suivants :

- Nom propre, le critère est **non applicable** ;
- Nom commun de langue étrangère présent dans le dictionnaire officiel de la langue par défaut de la page Web, le critère est **non applicable** (**Note :** le dictionnaire officiel est celui recommandé par l'académie en charge de la langue en question). Pour la France, par exemple, le lien vers le dictionnaire officiel se trouve sur le site de l'Académie française à l'adresse suivante : http://www.academie-francaise.fr/le-dictionnaire/la-9e-edition. Pour toute demande auprès du service du dictionnaire de l'Académie française, utiliser le formulaire de contact du service du dictionnaire ;
- Le terme de langue étrangère soumis, *via* un champ de formulaire et réaffiché dans la page (par exemple comme indication du terme recherché dans le cas d'un moteur de recherche), le critère est **non applicable** ;
- Passage de texte dont la langue ne peut pas être déterminée : le critère est **non applicable** ;
- Terme ou passage de texte issus d'une langue morte ou imaginaire pour laquelle il n'existe pas d'interprétation vocale : le critère est **non applicable**.

Note : pour les noms communs de langue étrangère, absents dans le dictionnaire officiel de la langue par défaut de la page Web, et qui sont passés dans le langage commun (exemple : newsletter) : le critère est **applicable**, uniquement lorsque l'absence d'indication de langue peut provoquer une incompréhension pour la restitution.

Présentation de l'information

Critère 10.11

Il existe une gestion de cas particulier pour les langues chinoises, japonaises et coréennes. Dans ces situations, le nombre de caractères de référence est de 40.

Navigation

Critère 12.1

Il existe une gestion de cas particulier lorsque le site Web est constitué d'une seule page ou d'un

nombre très limité de pages (cf. note) pour lesquels la fonction de recherche du navigateur dans le contenu est considérée comme équivalente à un moteur de recherche. Dans ce cas-là, le critère est non applicable.

Note : l'appréciation d'un nombre très limité de pages devrait réserver ce cas particulier à un site de 2 ou 3 pages, par exemple, avec un volume de contenu peu important.

Critères 12.2 - 12.3

Il existe une gestion de cas particulier lorsque :

- Les pages d'un ensemble de pages sont le résultat ou une partie d'un processus (un processus de paiement ou de prise de commande, par exemple) ;
- La page est la page d'accueil ;
- Le site Web est constitué d'une seule page.

Dans ces situations, le critère est non applicable.

Critère 12.8

Il existe une gestion de cas particulier lorsque la page est la page d'accueil ou lorsque le site Web est constitué d'une seule page. Dans ce cas, le critère est non applicable.

Critères 12.11

Il existe une gestion de cas particulier lorsque le site Web est constitué d'une seule page.

Dans ce cas de figure, l'obligation de la présence d'un lien d'accès rapide est liée au contexte de la page : présence ou absence de navigation ou de contenus additionnels par exemple. Le critère peut être considéré comme non applicable lorsqu'il est avéré qu'un lien d'accès rapide est inutile.

Consultation

Critère 13.1

Il existe une gestion de cas particulier lorsque la limite de temps est essentielle, notamment lorsqu'elle ne pourrait pas être supprimée sans changer fondamentalement le contenu ou les fonctionnalités liées au contenu.

Dans ces situations, le critère est non applicable. Par exemple, le rafraîchissement d'un flux RSS dans une page n'est pas une limite de temps essentielle ; le critère est applicable. En revanche, une redirection automatique qui amène vers la nouvelle version d'une page à partir d'une url obsolète est essentielle ; le critère est non applicable.

Critère 13.6

Il existe une gestion de cas particulier lorsque le document est produit de manière dynamique (par exemple une facture). Dans cette situation, l'indication de poids est facultative, les autres indications (type de fichier et langue) restent exigibles.

RGAA PF – Notes techniques

Les notes techniques ci-dessous donnent des explications pour la prise en charge de certains éléments HTML5 dont le support peut être variable et la manière dont le référentiel propose de les prendre en charge.

Images

Critère 1.2 [A]

Lorsqu'une image est associée à une légende, la note technique WCAG recommande de renseigner systématiquement l'alternative de l'image (cf. critère 1.10). Dans ce cas le critère 1.2 est non applicable.

Un attribut WAI-ARIA role="presentation"ne peut pas être utilisé pour déclarer une image de décoration conformément aux indications données par la spécification sur les restrictions de l'utilisation des rôles WAI-ARIA.

Critère 1.3 [A] : attribut title

La note WCAG interdit l'utilisation de l'attribut titleen remplacement de l'attribut alt, néanmoins il est souvent utile d'utiliser l'attribut titlepour faire apparaître une infobulle (tooltip) sur les images particulièrement obscures. Si l'attribut titleest utilisé de cette manière, le contenu de l'attribut titledoit être strictement identique à celui de l'alternative.

Critère 1.3 [A] : balise <title>dans les éléments SVG

Le manque de support de l'élément <title>par les technologies d'assistance crée une difficulté dans le cas de l'utilisation de l'élément <desc>pour implémenter l'alternative courte de l'image si l'image nécessite une description détaillée. Dans ce cas il est recommandé d'utiliser un texte adjacent ou un lien adjacent pour créer la description détaillée.

Les tests 1.3.9 et 1.3.12 sont utilisés pour vérifier que l'implémentation de l'alternative est compatible avec l'accessibilité (par exemple avec la base de référence considérée).

Critère 1.6 [A]

Le manque de support de l'élément <title>par les technologies d'assistance crée une difficulté dans le cas de l'utilisation de l'élément <desc>pour implémenter l'alternative courte de l'image si l'image nécessite une description détaillée. Dans ce cas il est recommandé d'utiliser un texte adjacent ou un lien adjacent pour créer la description détaillée.

Si l'élément <desc>est utilisé pour implémenter la description détaillée, il est recommandé d'utiliser un attribut aria-labelpour implémenter l'alternative courte de l'image.

L'utilisation de l'attribut aria-describedbyn'est pas possible pour lier une image à sa description détaillée par manque de support des technologies d'assistance.

La description détaillée adjacente peut être implémentée *via* une balise <figcaption>, dans ce cas le critère 1.10 doit être vérifié (utilisation de <figure>et du rôle group, notamment).

Critère 1.8 [AA] et 1.9 [AAA]

Le texte dans les images vectorielles étant du texte réel, il n'est pas concerné par ce critère.

Critère 1.10 [A]

L'implémentation d'un role="group"sur l'élément parent figureest destiné à pallier le manque de support actuel des éléments figurepar les technologies d'assistance. Bien que recommandée, l'utilisation d'un élément figcaptiondans un élément figureest optionnelle. En revanche l'utilisation d'un élément figcaptionpour associer une légende à une image impose l'utilisation d'un élément parent figure. La référence à la légende adjacente peut être une expression du type "image 1" ou équivalent lorsque cette expression est reprise dans la légende.

Bien que recommandé par HTML5, la note WCAG stipule que le titlene peut pas être utilisé pour "labelliser" l'image.

Les attributs aria-labelledbyet aria-describedbyne peuvent pas être utilisés actuellement par manque de support par les technologies d'assistance.

Note : les images légendées doivent par ailleurs respecter le critère 1.3 relatif aux images porteuses d'information.

Tableaux

Critère 5.1 [A]

La spécification propose plusieurs méthodes pour lier un résumé à un tableau (tableau lié à un passage de texte avec aria-describedby, tableau groupé *via* figureavec le résumé en texte adjacent, tableau groupé avec figureavec le résumé dans un élément figcaption, résumé dans un élément detailsdans l'élément caption).

Ces méthodes n'ont pas un support suffisant pour être utilisées actuellement.

Scripts

Critère 7.1 [A]

Le critère 7.1 implémente la notion de "compatible avec les technologies d'assistance" tel que définie par les WCAG, ainsi que le recours à l'API WAI-ARIA pour rendre un composant ou une fonctionnalité accessible. Le bon usage de l'API WAI-ARIA est vérifié *via* les tests 7.1.3, 7.1.4, 7.1.5 et 7.1.6.

Note importante : dans un environnement HTML5, beaucoup de composants peuvent nécessiter JavaScript pour fonctionner, en conséquence la fourniture d'une alternative à un composant JavaScript qui ne pourrait pas être rendu accessible devra bénéficier d'une méthode spécifique au

composant en cause, permettant de le remplacer par une alternative accessible (et de le réactiver).

Cela signifie que la désactivation de JavaScript pour l'ensemble de la page ne sera pas acceptée comme une méthode valable, à moins qu'elle ne remette pas en cause l'utilisation des autres composants.

Critère 7.3 [A]

ARIA définit pour un certain nombre de rôles, dédiés au développement de composants d'interface, un ensemble d'interactions au clavier basées sur les touches Échap, Barre d'espace, Tabulationet touches de directionauxquelles peuvent se rajouter d'autres interactions basées sur les touches de pagination, de débutou de finpar exemple. Afin d'accompagner la prise en charge progressive de ces interactions au clavier, le référentiel limite l'exigence aux touches d'interactions principales (Échap, barre d'espace, tabulation, flèches de direction) telles qu'elles sont définies par les motifs de conception.

Structuration de l'information

Critère 9.1 [A]

ARIA permet de définir des titres *via* le rôle headinget la propriété aria-level(indication du niveau de titre). Bien qu'il soit préférable d'utiliser l'élément de titre natif en HTML <hx>, l'utilisation du rôle WAI-ARIA headingest compatible avec l'accessibilité.

Bien que la spécification HTML5 autorise l'utilisation exclusive de titres de niveau 1 (h1), le manque de support des technologies d'assistance oblige à utiliser une hiérarchie de titres pertinente.

Critère 9.2 [A]

L'arborescence du document (outline) est générée par l'utilisation des balises sectionnantes <nav>, <article>, <section>, <aside>et les sections implicites générées par l'utilisation d'une balise <hx>(lorsque la balise <hx>n'est pas le premier enfant d'une section).

Une balise sectionnante permet de structurer ou de regrouper un contenu, les parties d'un contenu, ou un ensemble de contenus qui peuvent être considérés de manière indépendante du reste du document.

Une zone de navigation dans le site ou dans une rubrique, un sommaire ou la zone de navigation d'une collection de pages (<nav>), un contenu "complémentaire" au contenu principal (<aside>), le contenu principal ou le regroupement de plusieurs contenus comme des articles (<article>ou <section>) un ou des contenus secondaires comme un commentaire, un widget Twitter, un fil RSS (<article>ou <section>) sont autant d'exemples de contenus sectionnés.

Lorsqu'il s'agit de contenus, par opposition à des zones de navigation (<nav>) ou des zones de contenus complémentaires (<aside>), une section devrait posséder si c'est approprié une zone d'en-tête (<header>) et un pied de section (<footer>).

Le premier titre <hx> dans une section donne le "nom" de la section tel qu'il sera reporté dans l'arborescence du document. Les titres suivants (<hx>) créent des sections implicites qui seront présentées comme l'arborescence du contenu de la section.

Une section pouvant être considérée de manière indépendante du reste de la page, l'arborescence générée par les sections implicites (<hx>) est calculée à partir d'un niveau 1 affecté au premier titre de la section.

Lorsqu'elle est utilisée, l'arborescence du document peut donc être différente de l'arborescence du contenu représentée par l'ensemble des titres <hx>de la page, même si les deux structures restent similaires.

Cette arborescence doit donc être représentative de la structure du document et être cohérente avec la structuration du contenu générée par l'utilisation des balises <hx>. La structuration du contenu générée par les balises <hx> pouvant être, théoriquement, déduite de l'arborescence du document, la spécification HTML5 recommande d'utiliser uniquement des titres <h1>. Cet usage est proscrit et le critère 9.1 impose d'utiliser une hiérarchie de titres (<hx>) cohérente.

Si l'arborescence du document (à la condition qu'elle soit cohérente) peut permettre de proposer à l'utilisateur des fonctionnalités d'exploration et de navigation, sur certaines technologies d'assistance, elle influe sur la hiérarchie de titres générée par l'utilisation des balises <hx>en modifiant le niveau des titres restitués.

Pour accompagner la prise en charge progressive de l'arborescence du document et compte tenu du fait que le référentiel exige de disposer, en tout état de cause, d'une structure de contenu (balises <hx>) robuste et cohérente, **il est acceptable de considérer le test 9.2.2 comme non applicable** lorsqu'il n'est pas possible de s'assurer que l'arborescence du document est parfaitement cohérente. Dans ce cas, la non-conformité au test devrait être relevée sous la forme d'une simple alerte.

Critère 9.3 [A]

Les rôles WAI-ARIA listet listitempeuvent nécessiter l'utilisation des propriétés aria- setsizeet aria-posinsetdans le cas où l'ensemble de la liste n'est pas disponible *via* le DOM généré au moment de la consultation.

Bien que possédant un rôle definition, utilisé en combinaison avec la propriété aria- labelledby, WAI-ARIA ne propose pas de rôle équivalent à une liste de définition HTML. Le rôle definitionne peut donc pas être utilisée comme équivalent à une liste de définition HTML dl.

Les rôles tree, tablist, menu, comboboxet listboxne sont pas équivalents à une liste HTML ulou ol.

Références : The roles model - list

Présentation de l’information

Critère 10.13 [A]

WAI-ARIA propose une propriété aria-hidden(trueou false) qui permet d’inhiber la restitution d’un contenu en direction des technologies d’assistance, sans influencer sur sa visibilité en direction des agents utilisateurs : un contenu avec aria-hidden="true"ne sera donc plus vocalisable, mais restera visible.

Sauf si le contenu contrôlé par aria-hidden n’a pas vocation à être restitué par les technologies d’assistance, la valeur de l’attribut aria-hiddendoit être cohérente avec l’état affiché ou masqué du contenu à l’écran.

La spécification HTML5 propose un attribut hiddenqui permet de rendre indisponible (quand l’attribut hiddenest présent) un contenu dans le DOM généré (de manière similaire au type="hidden"sur un contrôle de formulaire).

Il est possible d’avoir des situations où un contenu contrôlé par hiddenou aria-hiddense trouve momentanément dans un état incohérent avec le statut affiché ou masqué du contenu, par exemple si l’on désire rendre disponible un élément, mais que son affichage à l’écran reste dépendant d’une action ultérieure. Dans ce cas, c’est l’état final du contenu qui doit être considéré.

Formulaires

Critère 11.11 [AA]

Certains types de formulaire HTML5 proposent des messages d’aide à la saisie automatique, par exemple les types urlet emailaffichent un message du type "veuillez saisir une adresse e-mail valide" dans le cas où l’adresse e-mail saisie ne correspond pas au format attendu. Ces messages sont personnalisables *via* l’API Constraint Validation qui peut permettre de personnaliser les messages d’erreur et valider le critère. Attention cependant, le support de cette API n’est pas encore stabilisé. Le type patternqui permet d’effectuer automatiquement des contrôles de format (*via* des expressions régulières) affiche également un message d’aide, mais ce dernier est personnalisable *via* l’attribut title, ce dispositif valide le critère.

Référence : WHATWG - 4.10.21.3 The constraint validation API.

Navigation

Critère 12.10 [A]

WAI-ARIA propose des rôles permettant d’indiquer les zones principales (régions) du document. Ces rôles sont très profitables aux utilisateurs de lecteurs d’écran notamment, mais également aux utilisateurs de la navigation au clavier qui peuvent ainsi bénéficier de fonctionnalités de navigation rapide dans la structure du document. Si la plupart des lecteurs d’écran mettent à disposition ces fonctionnalités, les navigateurs n’ont pas encore proposé de fonctionnalité de navigation dédiée

pour les utilisateurs qui ne peuvent pas utiliser la souris. La mise en place des liens d'évitement reste donc une exigence.

RGAA PF – Base de références

Plusieurs critères RGAA PF font référence à des tests de restitution à effectuer sur un ensemble de technologies d'assistance (TA), de navigateurs et de systèmes d'exploitation. Ce document décrit et explique les combinaisons qui ont été retenues pour constituer la base de référence.

Compatible avec les technologies d'assistance - Base de référence

La base de référence est constituée des configurations (technologie d'assistance, système d'exploitation, navigateur) qui permettent de déclarer qu'un dispositif HTML5/ARIA est "compatible avec l'accessibilité" tel que défini par WCAG.

Elle est établie par consensus à partir de la liste des technologies d'assistance dont l'usage est suffisamment répandu, ou, dans certains cas lorsqu'elle est fournie de manière native et constitue le moyen privilégié d'accès à l'information et aux fonctionnalités.

Base de référence

La base de référence permettant de couvrir la proportion la plus large des usages est constituée de combinaisons associant des technologies d'assistance d'usage suffisamment répandu, les deux systèmes d'exploitation Windows XP+ et OSX et les trois navigateurs IE9+, Firefox et Safari.

Pour qu'un dispositif HTML5/ARIA ou son alternative soit considéré comme compatible avec l'accessibilité il faut qu'il soit pleinement fonctionnel, en termes de restitution et de fonctionnalités, sur au moins une des combinaisons suivantes :

Base de référence - Combinaison 1

Technologie d'assistance (TA)	Version TA	Navigateur
NVDA	Dernière version	Firefox
JAWS	Version précédente	Firefox ou Internet Explore 9+
Voice Over	Dernière version	Safari

Base de référence - Combinaison 2

Technologie d'assistance (TA)	Version TA	Navigateur
JAWS	Version précédente	Firefox
NVDA	Dernière version	Firefox
Voice Over	Dernière version	Safari

Exigences complémentaires

Les règles suivantes doivent également être respectées :

1. L'ensemble des dispositifs HTML5/ARIA ou leurs alternatives doivent être pleinement fonctionnels, sur l'ensemble des pages du site, sans nécessiter de changement de technologie d'assistance en cours d'utilisation ;
2. Lorsque des alternatives à des dispositifs HTML5/ARIA sont proposées, elles ne doivent pas nécessiter la désactivation d'une technologie (par exemple JavaScript ou le plugin Flash) sauf s'il s'agit d'une fonctionnalité proposée par le site lui-même. Par exemple :
    - Le site met à disposition une version alternative conforme pleinement fonctionnelle sans le recours aux technologies dont l'usage est non compatible avec l'accessibilité ;
    - Le site met à disposition une fonctionnalité de remplacement des dispositifs HTML5/ARIA par des dispositifs alternatifs compatibles ;
3. Un moyen est mis à disposition des utilisateurs de technologies d'assistance pour signaler les problèmes rencontrés et obtenir, *via* un dispositif de compensation, les informations qui seraient rendues indisponibles ;
4. Si une déclaration de conformité est établie, elle doit comporter la liste des technologies d'assistance avec lesquelles les dispositifs HTML5/ARIA ont été testés et les résultats de ces tests (par exemple "supporté", "non supporté", "supporté partiellement") au moins.

Environnement maîtrisé

Lorsque le site Web est destiné à être diffusé et utilisé dans un environnement maîtrisé, la base de référence est constituée des configurations (technologie d'assistance, système d'exploitation, navigateur) effectivement utilisés dans l'environnement maîtrisé.

Par exemple, lorsque le site Web est exclusivement diffusé dans un environnement GNU/Linux, les tests devront être réalisés uniquement sur les navigateurs et les technologies d'assistance utilisés par les agents sur cette plateforme. Cette base de référence se substitue à la base de référence utilisée en environnement non maîtrisé.

RGAA PF – Références

Le RGAA PF a été établi en utilisant un certain nombre de références et de sources documentaires. Ce document liste les références qui ont été utilisées.

Documents de référence

- Traduction française agréée "Règles pour l'accessibilité des contenus Web (WCAG) 2.0" (http://www.w3.org/Translations/WCAG20-fr/) ;
- Techniques For WCAG 2 (http://www.w3.org/TR/WCAG20-TECHS/) ;
- HTML 4.01 Specification (http://www.w3.org/TR/html401/) ;
- HTML5 A vocabulary and associated APIs for HTML and XHTML (http://www.w3.org/TR/html5/) - référence à la date d'octobre 2014 ;
- HTML 5.1 Nightly A vocabulary and associated APIs for HTML and XHTML (http://www.w3.org/html/wg/drafts/html/master/) - référence à la date de juillet 2014 ;
- Using WAI-ARIA in HTML (http://w3c.github.io/aria-in-html/) - référence à la date de juin 2014 ;
- HTML5: Techniques for providing useful text alternatives (http://www.w3.org/TR/html-alt-techniques/) - référence à la date d'octobre 2012 ;
- Accessible Rich Internet Applications (WAI-ARIA) 1.0 (http://www.w3.org/TR/wai-aria/) - référence à la date de mars 2014 ;
- WAI-ARIA 1.0 Authoring Practices (http://www.w3.org/WAI/PF/aria-practices/) - référence à la date d'avril 2014.

Autres documents

- Web Content Accessibility Guidelines Working Group (Wiki) (http://www.w3.org/WAI/GL/wiki/Main_Page) ;
- HTML to Platform Accessibility APIs Implementation Guide (http://rawgit.com/w3c/html-api-map/master/index.html) - référence à la date de juillet 2014 ;
- User Agent Accessibility Guidelines (UAAG) 2.0 (http://www.w3.org/TR/UAAG20/) - référence à la date de novembre 2013 ;
- Authoring Tool Accessibility Guidelines (ATAG) 2.0 (http://www.w3.org/WAI/AU/ATAG20/) - référence à la date d'octobre 2013 ;
- WAI-ARIA 1.0 User Agent Implementation Guide (http://www.w3.org/TR/wai-aria-implementation/) - référence à la date de mars 2014 ;
- Accessible Rich Internet Applications (WAI-ARIA) 1.1 (http://rawgit.com/w3c/aria/master/spec/aria.html) - référence à la date de juillet 2014 ;
- Core Accessibility API Mappings 1.1 (http://www.w3.org/TR/core-aam-1.1/) - référence à la date de juin 2014.

Licence

Le référentiel technique (liste des critères, glossaire, cas particuliers, notes techniques, base de référence) est une copie adaptée du référentiel AccessiWeb HTML5/ARIA - Version de travail du 19/12/2013 - Édité par l'association BrailleNet.

ANNEXE 7

Référentiel Général d'Interopérabilité

Historique des versions		
Date	**Version**	**Évolution du document**
	1.0	Publication de la première version du référentiel général d'interopérabilité

1 Contexte, définitions et objectifs

1.1 Champ d'application du RGI

Le présent **Référentiel Général d'Interopérabilité** ou **RGI** permet l'usage sur des normes et standards retenus sur les questions d'interopérabilité critiques aux « frontières », et au-delà des « frontières » des systèmes de chaque ministère, service de l'administration polynésienne et les établissements publics placés sous sa responsabilité. Les problèmes d'interopérabilité interne aux systèmes informatiques de ces organisations doivent en premier lieu être traités dans leurs propres cadres de cohérence technique (CCT), tout en veillant à appliquer au mieux les recommandations du présent cadre.

Le RGI prend en compte la notion de **profil d'interopérabilité**. Un profil d'interopérabilité regroupe un ensemble de standards et de recommandations autour de cas d'usage définis. Il s'agit de faciliter l'appropriation de ce référentiel, en se focalisant sur quelques grands usages clés. Il s'agit également de limiter les choix de standards dans un contexte donné.

Cette première version est le fruit d'un travail interservice animé par la Direction générale de l'économie numérique (DGEN) et le Service informatique de la Polynésie française (SIPF).

1.2 Remarques préalables et documents de référence

Cette version s'inspire des meilleures pratiques dans une très grande variété de champs d'expertise présente sur le marché de la standardisation, de l'architecture technique, et plus globalement de l'urbanisation de système d'information (appelée aussi architecture d'entreprise). Elle ne souscrit donc à aucune méthode ni aucun outil propriétaire.

La démarche utilisée et les critères de sélections sont décrits ci-après.

Le présent RGI est un document technique qui s'adresse avant tout aux spécialistes en système d'information : chef de projet, architecte, urbaniste, concepteur, développeur, intégrateur. Il est donc fortement recommandé d'avoir une connaissance minimum des principes nationaux de l'interopérabilité.

Par ailleurs, le présent document est l'un des trois référentiels généraux qui s'appliquent réglementairement à l'ensemble des autorités administratives. Les deux autres sont :

- Le Référentiel Général de Sécurité de la Polynésie française (RGS)
- Le Référentiel Général d'Accessibilité pour l'Administration polynésienne (RGAAP)

1.3 Version

La présente version 1.0 du RGI résulte de l'arrêté relatif à la dématérialisation des actes des autorités administratives et aux téléservices portant approbation du référentiel général d'interopérabilité.

Le RGI de la Polynésie française est composé de deux documents.

Le présent document « Contexte, définitions et objectifs » est une copie adaptée de la version 2.0 du RGI de l'Etat.

Le référentiel technique est une reproduction de la version 2.0 du RGI de l'Etat.

Sa mise à jour est assurée par la Direction générale de l'économie numérique.

Le RGI ainsi que ses annexes sont disponibles en ligne sur le site Internet www.lexpol.pf

1.4 Cadre légal

Le présent référentiel est pris en application de l'arrêté relatif à la dématérialisation des actes des autorités administratives et aux téléservices portant approbation du référentiel général d'interopérabilité, lui-même pris en application des articles LP 46 et suivants de la loi du pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

1.5 Définitions

La Commission Européenne définit l'interopérabilité comme suit :

> « L'interopérabilité est l'aptitude d'organisations disparates et diverses à interagir en vue de la réalisation d'objectifs communs mutuellement avantageux, arrêtés d'un commun accord, impliquant le partage d'informations et de connaissances entre ces organisations à travers les processus métiers qu'elles prennent en charge, grâce à l'échange de données entre leurs systèmes de TIC respectifs. »

L'Association Francophone des Utilisateurs de Logiciels Libres (AFUL) et wikipedia s'accordent sur une version étendue de cette définition :

> « L'interopérabilité est la capacité que possède un produit ou un système, dont les interfaces sont intégralement connues, à fonctionner avec d'autres produits ou systèmes existants ou futurs et ce sans restriction d'accès ou de mise en œuvre. »

Nous retiendrons la définition de Wikipedia pour le RGI. La Commission Européenne définit également ce que doit être un cadre d'interopérabilité : un cadre de niveau Européen ou *European Interoperability Framework* (EIF), et un cadre national d'interopérabilité par États membres ou *National Interoperability Framework* (NIF) :

> « Un cadre d'interopérabilité est une approche concertée de l'interopérabilité pour les organisations qui souhaitent travailler ensemble à la délivrance conjointe de services publics. Au sein de son champ d'application, il spécifie un ensemble d'éléments communs tels que le vocabulaire, les concepts, les principes, les politiques, directives, recommandations, normes, spécifications et pratiques. »

Le RGI correspond au NIF Français.

Plusieurs éléments importants sont à retenir dans ces définitions :

- L'approche concertée entre les parties ;
- Le fait que les interfaces des systèmes par lesquelles les échanges sont réalisés soient intégralement connues et donc décrites d'un point de vue technique, sémantique, fonctionnel et opérationnel ;
- La capacité à fonctionner avec d'autres systèmes sans restriction ;
- Le fait que l'interopérabilité ne soit pas qu'une question technique, mais touche également aux questions de vocabulaire, de concepts métiers, de principes d'architecture et d'organisation, de réglementation, de droit, de politiques.

L'interopérabilité réelle suppose donc que :

- Les interfaces des systèmes reposent sur des standards ouverts,
- L'implémentation qui est faite de ce standard respecte le cas échéant un profil technique lorsque ceci est applicable,
- L'implémentation soit testée vis-à-vis d'une implémentation de référence lorsque celle-ci est

disponible,

- Les choix d'implémentation résultants soient dûment documentés ainsi que tous les écarts avec les points précédents.

Pour faciliter et alléger la lecture du document, et même si la langue française distingue les deux termes « standard » et « norme », le terme « standard » est utilisé par défaut dans l'ensemble du document en lieu et place de « norme et standard » (au singulier ou au pluriel).

1.6 Objectifs du RGI

Concevoir, mettre en place, opérer, et entretenir des organisations, des dispositifs, ou des systèmes qui soient interopérables, et cela à moindre coût, passe notamment par des choix communs de standards d'échange, des choix de sémantique commune. Mais un standard ne règle pas à lui seul les questions d'interopérabilité. De plus, parfois, la manière d'implémenter un standard peut également créer d'autres difficultés qui conduiront à réduire l'interopérabilité. Leurs spécifications ne peuvent pas prévoir tous les cas ou besoins d'implémentation, d'où l'absolue nécessité de retenir des standards qui ont fait leurs preuves, sans que cela obère l'évolution des systèmes concernés, la recherche et l'innovation.

Les choix d'assemblage de ces standards, les choix d'architecture mais aussi les choix de solutions (composants, logiciels, infrastructure) sont tout aussi importants. Le Référentiel Général d'Interopérabilité n'a pas l'objectif de définir les solutions à retenir. Il ne serait pas non plus efficace d'imposer une solution unique pour l'ensemble de l'écosystème public. Le RGI ne fait qu'identifier les standards incontournables, et les quelques assemblages clés, sous la forme de profils d'interopérabilité à retenir.

Le RGI est donc volontairement limitatif. L'objectif est bien de standardiser, c'est-à-dire principalement de faciliter les choix, et d'éviter la prolifération coûteuse de choix hétérogènes, sans imposer une solution unique, tout en appliquant le principe de subsidiarité. Le rôle de chaque autorité administrative est ainsi de s'aligner sur le RGI, avec un calendrier public, pour concevoir, mettre en place et entretenir des dispositifs interopérable.

<table>
<tr><td>

- **Protocoles (normalisés)**
- **Formats et structures de données (ouverts et normalisés)**
- **Sémantiques (normalisées ou référencées)**

</td><td rowspan="2">Cadres d'architecture</td><td>Principes, Normes & standards</td></tr>
<tr><td>

- **Profils : Assemblages de protocoles, formats, structures de données pour répondre à des cas d'usage / des fonctionnalités propres au gouvernement**
  - Partir du cas d'usage générique : vision fonctionnelle dynamique
  - Décliner l'architecture générique nécessaire
    - Principes & règles d'architecture
    - Constituants : composant logiciel, protocole, format et structure de données
    - Cinématique d'ensemble

</td><td>Assemblage & architecture</td></tr>
</table>

• **Solutions : composants disponibles** o Identifier / Référencer les solutions qui implémentent des assemblages identifiés o Référencer les solutions open source qui permettent, a minima, de vérifier les formats et les structures de données préconisées o Annuaire de services /composants		**Solutions au sein du gouvernement**

Le schéma ci-dessus illustre des 3 facettes à prendre en compte dans la conception, la mise en place et l'entretien de dispositifs interopérables.

1.7 Démarche et partis pris

L'approche adoptée pour l'élaboration du RGI repose sur les principes suivants :

- *Co-construit* : l'élaboration de ce document est le fruit d'un travail de concertation et de coopération entre les experts des différents ministères, opérateurs, et plus globalement des professionnels des systèmes d'information. Il a fait l'objet d'un appel public à commentaires.
- *Utile et facile à consulter* : Le document proposé à la lecture se veut utile et facile à consulter. Il est focalisé sur l'essentiel, le bon sens, et la simplification.
- *État de l'art du web* : Le document fait référence à des normes et standards reconnus dans le monde du web et plus généralement du numérique. Il s'appuie sur les travaux réalisés par les organismes de normalisation et de standardisation reconnus (ISO, IETF, UIT, W3C, OASIS, OIF...).
- *Méthode* : Le référencement des normes et standards s'appuie sur des critères d'adoption explicités dans le document. Ces critères reposent sur la méthode d'évaluation des normes et standards élaborée par la Commission Européenne : CAMSS (Common Assessment Method for Standards and Specifications) pour les technologies de l'information.
- *Uniquement l'interopérabilité* : Le périmètre du document est l'interopérabilité principalement technique et syntaxique ; le document n'est donc pas un cadre ou un manuel d'architecture des systèmes d'information, un référentiel d'analyse ou de développement, ni un recueil de solutions techniques.
- *Général* : Le RGI concerne l'ensemble des autorités administratives, c'est-à-dire pour mémoire : la Polynésie française, ses établissements publics, les autorités administratives indépendantes, les organismes de protection sociale et les autres organismes et personnes de droit public et de droit privé chargés d'une mission de service public administratif, ainsi que les administrations de l'État en Polynésie française et les communes polynésiennes, leurs groupements et leurs établissements publics.
- *Focalisé* : Même si une partie significative du document constitue une liste importante de standards, l'objectif est de rester focalisé sur l'essentiel en matière d'interopérabilité entre systèmes d'information, entre applications, entre le poste d'un utilisateur (usager, agent, partenaire, tiers...) et les systèmes d'information des administrations. La notion de **profil d'interopérabilité**, introduite dans cette nouvelle version, permet de choisir les standards en fonction des cas d'usage, ou des sphères d'emplois, les plus répandus.

1.8 Critères d'adoption retenus

Un standard sélectionné pour le RGI, répond aux critères suivants :

- *Ouvert :* La spécification fonctionnelle et technique du standard doit être complète, publique, sans restriction ni d'accès ni de mise en œuvre. La spécification est disponible à coût zéro, (voire à coût

faible ou marginal sans toutefois limiter la réutilisation notamment dans des logiciels libres). Il est maintenu par une organisation sans but lucratif (organisme de standardisation, forum, consortium...). Ses évolutions se font sur la base d'un processus de décision transparent, ouvert, et accessible à toutes les parties intéressées. Un calendrier d'évolutions est publié et les parties intéressées sont informées de la teneur des prochaines versions. Les droits du standard sont sous sur une base libre de droits et compatible avec les logiciels libres et les logiciels propriétaires.

- *Pertinent :* L'utilité, la nécessité et la simplicité de la mise en œuvre doit être clairement démontrées, reconnues et adoptées massivement par le marché.
- *Mature :* Le standard, en plus d'être bien établi et soutenu par les infrastructures technologiques, a démontré sa fiabilité suite à son application dans un contexte réel d'utilisation, sans empêcher les innovations. Son expérimentation ou mise en œuvre pilote ne revêt qu'un caractère démonstratif. Les éléments de preuve doivent être publics, reproductibles sans restriction d'accès aucune. Le standard présente la stabilité nécessaire et les nouvelles versions doivent prendre en compte au moins les problématiques de compatibilité ascendante.
- *Indépendant :* Le standard est indépendant de toute infrastructure technologique, logicielle ou bien matérielle d'un constructeur ou d'un éditeur. Son choix ne doit pas imposer des restrictions d'acquisition ou d'utilisation par l'organisme qui l'adopte. Par défaut, ils sont à même de supporter le multilinguisme.
- *Facile à déployer :* Le déploiement du standard ne doit pas être contraignant et engendrer des coûts de déploiement supplémentaire en dehors des coûts (humains, organisationnels, matériels...) nécessaires ou induits par la mise en conformité des systèmes telle que rappelée dans le chapitre 1.3, ou ceux inhérents aux défauts ou à l'hétérogénéité des architectures en place.
- *Soutenu par l'industrie :* Le standard doit être bien établi dans l'industrie pour son périmètre d'usage. Sa réputation dans le domaine auquel il se rattache doit être solide et démontrée. Les éléments de preuve, ouverts et non réfutables, doivent être disponibles. Des expertises, y compris scientifiques comme la recherche universitaire, autour de son implémentation et de sa maintenance sont proposées par de nombreux prestataires. Ce critère peut venir pondérer ou bien appuyer la maturité d'un standard.

Selon la maturité et l'écosystème du thème étudié, le poids des critères peut se révéler différent. Il faut également noter que la non satisfaction d'un critère n'est pas éliminatoire.

Ces critères imposent donc a minima que ces standards ouverts et interopérables soient implémentés dans des solutions logicielles libres, pour faciliter les tests, l'appropriation, et ne pas imposer de fait l'acquisition de solutions propriétaires coûteuses. Cela n'enlève en rien la liberté des autorités administratives de choisir des solutions éditeurs, mais ce n'est donc en aucune manière une contrainte.

1.9 Périmètre de l'interopérabilité

Le RGI traite des questions d'interopérabilité dans les différents cas illustrés dans le schéma ci-après. Le terme « Autorité Administrative » ou « AA » définit une organisation publique au sens large. Cela peut être la Polynésie française, ses établissements publics, les autorités administratives indépendantes, les organismes de protection sociale et les autres organismes et personnes de droit public et de droit privé chargés d'une mission de service public administratif, ainsi que les administrations de l'État en Polynésie française et des communes polynésiennes:

Trois principaux cas sont identifiés :

- Les échanges entre autorités administratives : A↔A ou encore symbolisé A2A.
- Les échanges entre une autorité administrative et une entreprise (au sens large, une unité légale,

que ce soit une entreprise, une personne physique, une association) : A↔B ou encore symbolisé A2B

- Les échanges entre une autorité administrative et un citoyen : A↔C ou encore symbolisé A2C

Pour leurs besoins internes, les autorités administratives restent libres du choix des normes, standards et pratiques à mettre en œuvre. Toutefois, il est souhaitable qu'elles suivent par défaut les recommandations du RGI.

Le référentiel d'interopérabilité polynésien doit également s'intégrer dans le contexte européen, défini par les travaux de l'EIF, dont le périmètre est présenté par le schéma ci-dessus.

L'objectif de l'EIF est de favoriser le développement de services en ligne européens (EPS pour European Public Services), en facilitant la coopération entre les administrations des différents États Membres. Le cadre européen propose des recommandations et bonnes pratiques aux niveaux organisationnel, sémantique et technique.

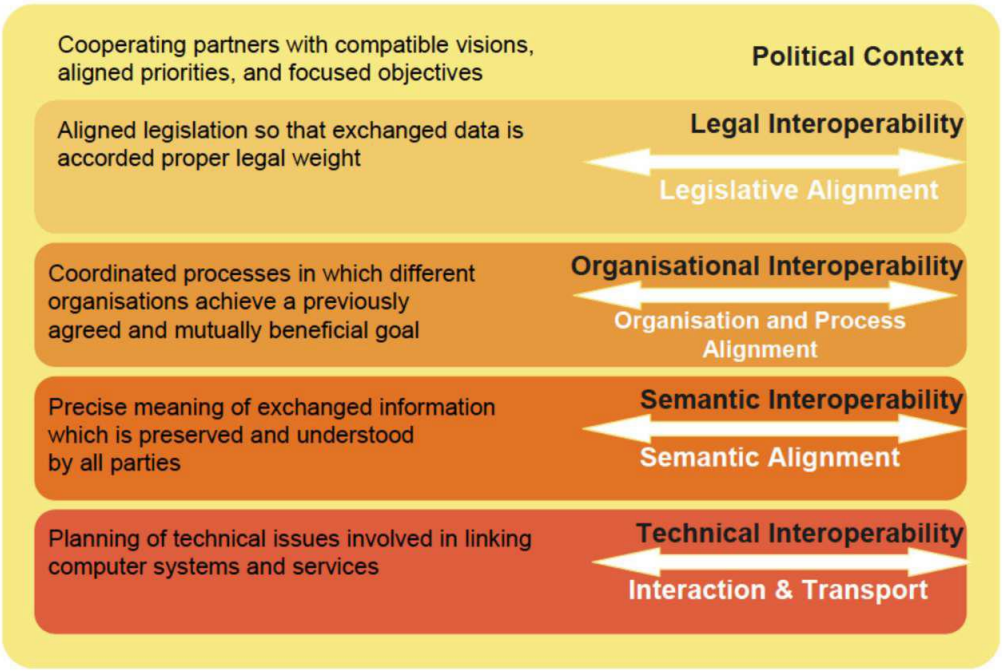
La Commission Européenne recommande à tous les États Membres d'aligner leur cadre d'interopérabilité respectif sur le cadre européen EIF. Un observatoire des cadres nationaux NIFO (National Interoperability Framework Observatory) a été mis en place afin, entre autres, de faciliter cet alignement. Un état des lieux actualisé est en cours par la commission.

1.10 Les différents niveaux d'interopérabilité

Un échange réussi entre parties prenantes nécessite la prise en compte de différentes problématiques qui peuvent se décomposer en « niveaux d'interopérabilité ».

Le schéma ci-après, repris du modèle proposé dans l'EIF, présente quatre niveaux d'interopérabilité. Un cinquième niveau dit syntaxique ou « *Syntaxic interoperability* » est également identifié et permet de découpler dans le niveau technique, les questions de protocoles d'échanges, des questions de formats d'échanges.

À chaque niveau correspondent des standards et des principes sur lesquels les parties doivent s'aligner pour concevoir et opérer des échanges efficacement.



European Interoperability Framework : Interoperability Level

Niveau politique

Des visions partagées, des orientations et des stratégies convergentes favorisent la coopération, la communication et plus particulièrement les échanges entre les différentes parties prenantes, chacun à leur niveau d'activité.

Niveau juridique

Les échanges doivent se conformer :

- Au cadre légal dont dépendent les parties prenantes (droit national et international, propriété intellectuelle, confidentialité, etc.) ;
- Aux accords contractuels établis entre parties prenantes (modalités de l'échange, niveaux de services, etc.).

Niveau organisationnel

L'interopérabilité organisationnelle est liée aux organisations et aux processus notamment mis en œuvre pour favoriser et opérer les échanges. Elle concerne aussi les compétences et les connaissances associées au fonctionnement de ces organisations.

En termes d'organisation, il s'agit par exemple de définir les rôles et les responsabilités des personnes qui prennent part à l'échange au sein de leur entité. En termes de processus il s'agit de définir qui envoie la donnée, à quel moment, suite à quel événement... mais aussi comment sont partagés les rôles et les responsabilités entre les différentes parties prenantes.

Niveau sémantique

La sémantique recouvre à la fois la signification des mots, le rapport entre le sens des mots (homonymie, synonymie, etc.), mais aussi le cycle de vie d'une information, ses règles d'agrégation ou de décomposition, etc. Le sens des mots varie selon les organisations, les métiers, les acteurs et les contextes, tant métiers que culturels. Toute collaboration entre entités demande une communication, au sens d'un échange d'informations. Pour cela, ces entités s'entendent sur la signification des données qu'elles

échangent et sur le contexte de cet échange. Il est question ici de concept métier (exemple : une entreprise, un chiffre d'affaires, un revenu fiscal de référence, etc.).

Niveau technique : protocole d'échange et syntaxique

Le niveau technique concerne les questions relatives aux protocoles d'échanges de données, et à leurs formats, mais aussi les conditions et formats de « stockage » de ces données. Il est d'usage de séparer ce niveau en deux parties. Une partie « protocole d'échanges » pour tout ce qui touche aux transports des données, et donc au « tuyau » dans lequel les données circulent. Et une autre partie «syntaxe » pour tout ce qui concerne les formats techniques qui permettent de véhiculer les données (leur structure, leur codification...), indépendamment de leur sens qui lui est traité au niveau sémantique.

1.11 Évolutions du RGI

Le Référentiel Général d'Interopérabilité doit pouvoir évoluer fréquemment, afin de s'adapter aux évolutions technologiques, aux évolutions des standards, aux besoins d'interopérabilité du système d'information de la Polynésie française, ou bien encore, aux exigences et recommandations de la commission européenne.

Cette présente version est disponible sur le site web suivant :

http://www.lexpol.pf/

L'adresse courriel ci-dessous gérée par la Direction générale de l'économie numérique est également accessible :

contact@dgen.gov.pf

Cette adresse courriel permet de collecter toutes les remarques, critiques, questions et propositions d'évolutions du RGI. Une synthèse des questions pertinentes (sous forme de FAQ) et propositions d'évolution à l'étude sera régulièrement mise en place sur le site web du RGI.

1.12 Conformité à la version du RGI

Les autorités administratives sont toutes tenues de suivre les recommandations de la présente version du RGI.

2 Organisation des exigences d'interopérabilité

2.1 Description des standards

Chaque standard identifié dans la présente version du RGI est présenté selon le modèle suivant :

Niveau	Catégorie	Sous catégorie
Statut	**Sigle**	Nom du standard
Le lien vers la page Wikipedia, en français (en anglais si c'est la seule version disponible) du standard. Suivi d'un très court texte descriptif : résumé extrait de Wikipedia au moment de la rédaction du présent document.		
Organisme de standardisation	Le nom et le lien vers les spécifications de référence du standard.	

Les standards ont été sélectionnés selon les critères du chapitre 1.8. Plutôt que de « réinventer » une description résumée et propre au RGI de chaque standard, avec tous les risques que cela comporte, il a été

choisi d'utiliser Wikipedia comme source documentaire pour la description synthétique du standard. Par construction, Wikipedia est totalement aligné sur la démarche d'élaboration du RGI, décrite au chapitre 1.7. Le contenu de Wikipedia va évoluer indépendamment du RGI, et donc le RGI sera, dans quelques cas, désynchronisé de Wikipedia. C'est en réalité une force pour l'utilisation des standards identifiés d'avoir des informations les plus « à l'état de l'art » possible. Et c'est la raison pour laquelle le lien vers la page Wikipedia a également été inséré en plus du résumé.

Le RGI ne contient volontairement pas d'aide ou de conseil à la mise en œuvre des standards retenus. Le lien vers Wikipedia et la description résumée provenant de Wikipedia ne remplacent évidemment pas les spécifications officielles de référence du standard produites et validées par les organismes de standardisation ou de normalisation. Le lien vers spécification de référence du standard est inclus également dans le cartouche de chaque standard.

De plus, les pages Wikipedia référencées contiennent la plupart du temps des aides précieuses pour la compréhension et l'application des standards. Le RGI étant un document applicable, le choix des pages en langue Française est naturel. Il faut toutefois souligner que les pages en anglais de Wikipedia sont dans la plupart des cas bien plus complètes, précises et évoluent plus rapidement.

Concernant le lien vers les spécifications de référence du standard. Le présent document n'a pas vocation à lister de manière exhaustive l'ensemble des documents de spécifications pour chaque standard. En effet, dans de nombreux cas, les spécifications se composent de plusieurs documents et d'annexes. Il existe toutefois toujours un document central ou chapeau. C'est l'url ou la référence de ce document qui est retenu pour chaque standard.

2.2 Statut et version

À chaque standard est associé un statut pour faciliter la prise en compte et la mise en conformité. Le statut permettra également de gérer la transition dans le temps d'une version du RGI à une autre, et d'une version de standard à une autre. Les statuts retenus sont les suivants :

Statut	Explication du statut
En observation	Il s'agit d'un standard en émergence, ou dont la maturité, la mise en œuvre et le soutien par la recherche et/ou l'industrie ne sont pas totalement acquis. Son application est à prendre avec précaution, et après une phase de tests et d'expérimentations qu'il conviendra de partager avec la communauté. Dans le cas où les expérimentations seraient probantes, il passerait dans une version suivante du RGI au statut « recommandé », dans le cas contraire il serait « retiré » du référentiel.
Recommandé	Il s'agit d'un standard qui répond à tous les critères de sélection, et qui est aligné avec la stratégie de transformation et de modernisation du système d'information et de communication de l'État. C'est un standard qui doit être respecté et appliqué par tous.
En fin de vie	Il s'agit d'un standard en fin de vie, dont le soutien se termine car d'autres standards de remplacement émergent. Son application est à prendre donc également avec précaution. Il est donc considéré « en sursis », mais si son retrait n'a pas encore été demandé dans tous les systèmes existants, il ne doit cependant pas être considéré comme « recommandé » pour tous les nouveaux projets.

Les standards sont dans de nombreux cas versionnés. La version ne sera généralement pas mentionnée, ou éventuellement une version a minima sera recommandée. Dans quelques cas où la version est jugée

discriminante, elle sera explicitement identifiée avec le standard. Par exemple pour le standard *Security assertion markup language* (SAML), la version 2 est une évolution majeure de la version 1, et présente des différences importantes pour les questions d'interopérabilité. Seule donc la version 2 (ou une version ultérieure) est recommandée.

Les standards qui ne sont pas listés dans le présent RGI ne peuvent pas être considéré comme « recommandé », ni même à « en observation ». Plus précisément, les standards reconnus utiles pour les questions d'interopérabilité, dans les conditions d'usages définis dans le présent document, sont ceux qui sont listés dans le RGI. Les autres standards, ceux qui ne sont pas cités, ne doivent donc pas être utilisés dans le cadre d'échanges (du périmètre couvert par le RGI).

Le présent RGI n'est donc pas un catalogue complet des standards informatiques sur lesquels un statut a été posé.

2.3 Les standards et la sécurité

Pour de nombreux standards, il existe une version équivalente sécurisée. Le présent RGI identifie parfois les deux versions, quand les deux versions présentent un intérêt pour l'interopérabilité. Le choix de la version, sécurisée ou non, dépend de l'analyse de sécurité. Quel que soit le type de projet ou d'évolution de tout ou partie d'un système d'information, il est rappelé que **les autorités compétentes doivent réaliser une analyse de sécurité**. Cette analyse dépend du contexte, du niveau de complexité, de criticité, du niveau de sensibilité des données. L'utilisation du RGS (cf.

Remarques préalables et documents de **référence**) est une aide précieuse pour cette analyse, en plus d'être un document applicable par tous les acteurs.

La mise en place et l'utilisation de protocoles sécurisés, nécessite bien souvent d'utiliser des algorithmes de chiffrement avec des longueurs de clefs déterminées. Ces choix sont également à faire en fonction de l'analyse de sécurité, en se basant encore une fois sur le RGS.

Au regard de l'analyse de sécurité, le choix de la version non sécurisée d'un standard peut s'accompagner de mesures de sécurité complémentaires.

2.4 Le profil d'interopérabilité

Un profil d'interopérabilité est un ensemble **limité** de standards à utiliser dans un contexte, un usage déterminé. L'objectif est de cadrer l'utilisation du RGI et d'éviter la prolifération de standards et de combinaison de standards pour un usage donné. La liste des standards du profil est volontairement limitative. Donc, dans le contexte d'usage du profil, aucun autre standard ne devra être utilisé. Et, en fonction des besoins, seule une partie des standards peut s'avérer nécessaire. Le chapitre Erreur : source de la référence non trouvée est consacré à ces profils.

Chaque profil est présenté selon le tableau ci-après.

Numéro	**Nom du Profil**	Numéro du profil prérequis
Statut	Liste des standards du profil	
Court texte descriptif du profil et de son contexte d'utilisation.		
Organisme référent pour le profil		

Les profils avec un statut de « recommandé » seront à privilégier sur les autres car ils sont alignés avec la stratégie « État plate-forme » et la nécessité de maîtriser la prolifération des choix technologiques, qui conduit à terme inexorablement à accroître la dette technique de l'État.

2.5 Organisation des standards

Les standards présentés sont organisés selon le découpage présenté dans le tableau ci-après pour l'interopérabilité technique et syntaxique. Ce découpage n'a pas la prétention d'être une classification parfaite des standards identifiés. C'est uniquement un moyen pratique d'organisation du document. Certains standards regroupent en réalité plusieurs des catégories ou sous-catégories. Ils sont positionnés dans ce cas dans la catégorie ou sous-catégorie principale.

Niveau	**Catégorie**	**Sous catégorie**
Technique	Réseau	
Technique	Transport	
Technique	Session	
Technique	Application	Transfert
Technique	Application	Exploitation
Technique	Application	Accès
Technique	Application	Multimédia
Technique	Application	Messagerie
Technique	Service	Identité & Authentification
Technique	Service	Service web
Technique	Service	Orchestration de services
Technique	Service	Géospatial
Syntaxique	Encodage	Caractère
Syntaxique	Encodage	Compression
Syntaxique	Document	
Syntaxique	Web	
Syntaxique	Structuration des données	
Syntaxique	Structuration des données	Description d'API
Syntaxique	Structuration des données	Identifiant
Syntaxique	Structuration des données	Géospatial
Syntaxique	Structuration des données	Carnet d'adresse
Syntaxique	Structuration des données	Calendrier
Syntaxique	Traitement de données structurées	
Syntaxique	Traitement de données structurées	Géospatial
Syntaxique	Multimedia	Conteneur vidéo
Syntaxique	Multimedia	Codec vidéo
Syntaxique	Multimedia	Conteneur audio
Syntaxique	Multimedia	Codec audio
Syntaxique	Multimedia	Image
Syntaxique	Signature	
Syntaxique	Message de sécurité	

2.6 Les organismes de standardisation

L'ensemble des standards retenus sont issus :

- D'organismes de standardisation ou de normalisation internationaux reconnus,
- ou bien encore d'organismes publics qui ont produit des cadres normatifs.

Dans quelques cas d'exception, il s'agit de standards de fait spécifiés par une organisation privée. Le tableau ci-après les liste, avec le lien de leur site web.

Sigle	**Nom et lien**
AFNOR	Agence Française de Normalisation
AFS	Archives Fédérales Suisse
BnF	Bibliothèque nationale de France
CEN	Comité Européen de Normalisation
DSS	Direction de la Sécurité Sociale
DISIC	Direction Interministérielle des Systèmes d'Information et de Communication
ECMA	European association for standardizing information and communication systems
ETSI	European Telecommunications Standards Institute
IEEE	Institute of Electrical and Electronics Engineers
IETF	The Internet Engineering Task Force
ISO	Organisation Internationale de Normalisation
OASIS	Organization for the Advancement of Structured Information Standards
OGC	Open Geospatial Consortium
OIF	OpenID Foundation
SIAF	Service Interministériel des Archives de France
UIT	Union internationale des télécommunications
W3C	World Wide Web Consortium
Xiph	Association à but non lucratif pour le développement de protocoles et logiciels libres

2.7 Actualisation des liens

L'ensemble des liens (URL) a été défini et accédé à la date de publication du présent document. Compte tenu de l'évolution permanente des contenus disponibles sur internet, leur disponibilité, leur complétude ou la qualité des informations mises à dispositions ne peuvent être garanties. Ces liens sont fournis à titre documentaire.

3 Interopérabilité technique

Synthèse des standards retenus pour le niveau technique

Les protocoles en fin de vie ou retirés ne sont pas présents dans cette synthèse. Seuls les protocoles recommandés ou en observation sont donc listés.

Niveau	Catégorie	Sous-Catégorie	Standards
Technique	Réseau		IPv6, IPSec
Technique	Transport		TCP, UDP, NTP, RTP, SRTP, RTCP, TLS
Technique	Session		SSH
Technique	Application	Transfert	HTTP, HTTPS, CORS, FTP, SFTP, R66, AMQP, AS2
Technique	Application	Exploitation	DNS, DNSSEC
Technique	Application	Accès	LDAP, LDAPS
Technique	Application	Multimédia	RTSP, H.323, SIP, MGCP
Technique	Application	Messagerie	SMTP, SMTPS, S/MIME, POP3, POP3S, IMAP4, IMAP4S, XMPP, XMPPS, WebRTC
Technique	Service	Identité & Authentification	OpenPGP, SAMLv2.0, Oauth 2.0, Open ID Connect
Technique	Service	Service web	SOAPv1.2, WSDL, UDDI, MTOM, XOP, WS-Security, WS-Addressing, InterOPS
Technique	Service	Orchestration de services	WS-BPEL, WS-CDL
Technique	Service	Géospatial	WMS, WFS, TJS, WMTS, CSW, WCS, WPS,

3.1 Listes des standards pour le niveau technique

3.1.1 Réseau

Technique	**Réseau**		
En fin de vie	**IPv4**	Internet Protocol version 4	
http://fr.wikipedia.org/wiki/IPv4 Internet Protocol est une famille de protocoles de communication de réseau informatique conçus pour être utilisés par Internet. Les protocoles IP sont au niveau 3 dans le modèle OSI. Les protocoles IP s'intègrent dans la suite des protocoles Internet et permettent un service d'adressage unique, codé sur 32 bits, pour l'ensemble des terminaux connectés.			
IETF	RFC 791, mise à jour par les RFC 1349, RFC 2474, RFC 6864		

Technique	**Réseau**		
Recommandé	**IPv6**	Internet Protocol version 6	

http://fr.wikipedia.org/wiki/IPv6 Cette nouvelle version du protocole IP est recommandée car elle apporte de nombreuses améliorations, notamment : • La simplification du routage et des en-têtes des messages / Paquets • L'adressage plus large : espace d'adresse sur 128 bits au lieu de 32 bits pour IPv4 ; • L'intégration de IPSec ; • L'amélioration de l'auto configuration des réseaux. Il est donc fortement recommandé de : • Retenir IPv6 qui est assez mature pour être déployé ; • Vérifier avant tout nouveau déploiement de solution, que le soutien IPv6 est assuré et que l'interopérabilité avec IPv4 est fonctionnelle ; • Envisager les scénarios de migration d'IPv4 vers IPv6.

IETF	RFC 2460

Technique	**Réseau**	**Sécurisation**	
Recommandé	**IPSec**	Internet Protocol Security	
http://fr.wikipedia.org/wiki/Internet_Protocol_Security IPsec est un cadre de standards ouverts pour assurer des communications privées et protégées sur des réseaux IP, par l'utilisation des services de sécurité cryptographiques. IPsec se différencie des standards de sécurité antérieurs en n'étant pas limité à une seule méthode d'authentification ou d'algorithme et c'est la raison pour laquelle il est considéré comme un cadre de standards ouverts. De plus, IPsec opère à la couche réseau (couche 3 du modèle OSI) contrairement aux standards antérieurs qui opéraient à la couche application (couche 7 du modèle OSI), ce qui le rend indépendant des applications, et veut dire que les utilisateurs n'ont pas besoin de configurer chaque application aux standards IPsec			
IETF	RFC 4301 - 4309		

3.1.2 Transport

Technique	**Transport**		
Recommandé	**TCP**	Transmission Control Protocol	
http://fr.wikipedia.org/wiki/Transmission_Control_Protocol Dans le modèle Internet, aussi appelé modèle TCP/IP, TCP est situé au-dessus de IP. Dans le modèle OSI, il correspond à la couche transport, intermédiaire de la couche réseau et de la couche session. Le protocole TCP reste le meilleur composant permettant de fiabiliser les flux de type HTTP, SMTP et FTP.			
IETF	RFC 793, et ses misesà jour.		

Technique	**Transport**		
Recommandé	**UDP**	User Datagram Protocol	

http://fr.wikipedia.org/wiki/User_Datagram_Protocol UDP fait partie de la couche transport de la pile de protocole TCP/IP : dans l'adaptation approximative de cette dernière au modèle OSI, il appartiendrait à la couche 4, comme TCP. Le rôle de ce protocole est de permettre la transmission de données de manière très simple entre deux entités, chacune étant définie par une adresse IP et un numéro de port. Contrairement au protocole TCP, il fonctionne sans négociation. La nature de UDP le rend utile pour transmettre rapidement de petites quantités de données, depuis un serveur vers de nombreux clients ou bien dans des cas où la perte d'un datagramme est moins gênante que l'attente de sa retransmission. Le DNS, la voix sur IP ou les jeux en ligne sont des utilisateurs typiques de ce protocole.	
IETF	RFC 768

Technique	**Transport**		
Recommandé	**NTP**	Network Time Protocol	
http://fr.wikipedia.org/wiki/Network_Time_Protocol Le Protocole d'Heure Réseau (Network Time Protocol ou NTP) est un protocole qui permet de synchroniser, par réseau informatique, l'horloge locale d'ordinateurs sur un serveur d'heure de référence.			
IETF	RFC 5905		

Technique	**Transport**		
Recommandé	**RTP**	Real-Time Transport Protocol	
http://fr.wikipedia.org/wiki/Real-time_Transport_Protocol Real-Time Transport Protocol (RTP) est un protocole de communication informatique permettant le transport de données soumises à des contraintes de temps réel, tels que des flux média audio ou vidéo. RTP est à l'heure actuelle principalement utilisé comme transport de média pour les services de la voix sur IP ou de vidéo conférence, voire de streaming. En mode unidirectionnel, il est toujours associé avec un autre protocole de signalisation qui gère l'établissement de session et permet l'échange du numéro de port utilisé par les deux extrémités. On peut citer : • Le protocole SIP pour les services de VoIP et de visioconférences ; • Le protocole H.323 pour les mêmes services (ancienne génération) ; • Le protocole RTSP pour le streaming bien que ce dernier possède un mode d'encapsulation TCP.			
IETF	RFC 3550		

Technique	**Transport**		
Recommandé	**SRTP**	Secure Real-time Transport Protocol	
http://fr.wikipedia.org/wiki/Secure_Real-time_Transport_Protocol Version sécurisée du protocole RTP.			
IETF	RFC 3711 et sa mise à jour RFC 6904		

Technique	**Transport**		
Recommandé	**RTCP**	Real-time Transport Control Protocol	

http://fr.wikipedia.org/wiki/Real-time_Transport_Control_Protocol RTCP est un protocole de contrôle des flux RTP, permettant de véhiculer des informations basiques sur les participants d'une session, et sur la qualité de service. Il repose sur des transmissions périodiques de paquets de contrôle par tous les participants dans la session. Le RTCP est un protocole couplé au RTP.	
IETF	RFC 3550

Technique	**Transport**	**Sécurisation**	
Recommandé	**TLS**	Transport Layer Security (TLS),	
http://fr.wikipedia.org/wiki/Transport_Layer_Security TLS et son prédécesseur SSL, sont des protocoles de sécurisation des échanges sur Internet. Le protocole SSL était développé à l'origine par Netscape. L'IETF, en a poursuivi le développement en le rebaptisant Transport Layer Security (TLS). On parle parfois de SSL/TLS pour désigner indifféremment SSL ou TLS. TLS (ou SSL) fonctionne suivant un mode client-serveur. Il permet de satisfaire aux objectifs de sécurité suivants : • L'authentification du serveur ; • La confidentialité des données échangées (ou session chiffrée) ; • L'intégrité des données échangées ; • De manière optionnelle, l'authentification du client (mais dans la réalité celle-ci est souvent assurée par le serveur). version 1.2 ou ultérieure doit être retenu pour ce standard. C'est la seule conforme au RGS.			
IETF	RFC 5246		

3.1.3 Session

Technique	**Session**		
Recommandé	**SSH**	Secure Shell	
http://fr.wikipedia.org/wiki/Secure_Shell SSH est à la fois un programme informatique et un protocole de communication sécurisé. Le protocole de connexion impose un échange de clés de chiffrement en début de connexion. Par la suite, tous les segments TCP sont authentifiés et chiffrés.			
IETF	RFC 4251, RFC 4252, RFC 4253, RFC 4254		

3.1.4 Application

Technique	**Application**	**Transfert**	
Recommandé	**HTTP**	Hypertext Transfer Protocol	
http://fr.wikipedia.org/wiki/Hypertext_Transfer_Protocol HTTP est un protocole de communication client-serveur développé pour le web. HTTP est un protocole de la couche application qui utilise le protocole TCP comme couche de transport. La version 1.1 actualisée en 2014 est recommandée. Il convient de noter que la version 2 de HTTP est en cours de mise en place. Des premières implémentations sont d'ores et déjà disponibles. Même si l''IETF précise que la version 2 est interopérable avec la version 1.1 pour faciliter son adoption, la version 2 n'est à ce stade pas recommandée. La version sécurisée HTTPS doit être privilégiée, en fonction des objectifs de sécurité.			

IETF	RFC 7230 à RFC 7237

Technique	**Application**	**Transfert**	
Recommandé	**HTTPS**	HyperText Transfer Protocol Secure	
http://fr.wikipedia.org/wiki/HyperText_Transfer_Protocol_Secure Version sécurisée du protocole HTTP sur le protocole TLS			
IETF	RFC 2818		

Technique	**Application**	**Transfert**	
Recommandé	**CORS**	Cross-origin resource sharing	
http://en.wikipedia.org/wiki/Cross-origin_resource_sharing CORS est une spécification W3C, qui autorise les requêtes Cross-Domain. Elle permet de gérer les accès à une ressource sur un serveur, lié à un domaine, par un script provenant d'un serveur lié à un autre domaine. Il est à noter que cette spécification CORS n'est pas supportée par certaines anciennes versions de navigateurs web.			
W3C	W3C CORS Recommandation		

Technique	**Application**	**Transfert**	
Recommandé	**FTP**	File Transfer Protocol	
http://fr.wikipedia.org/wiki/File_Transfer_Protocol FTP est un protocole de communication destiné à l'échange informatique de fichiers sur un réseau TCP/IP. Il permet, depuis un ordinateur, de copier des fichiers vers un autre ordinateur du réseau, ou encore de supprimer ou de modifier des fichiers sur cet ordinateur. Il faut noter que ce standard est à utiliser dans les cas où l'analyse de risque ne demande pas de sécurisation particulière.			
IETF	RFC 959, RFC 3659 et RFC 2640		

Technique	**Application**	**Transfert**	
Retiré	**FTPS**	File Transfer Protocol Secure	
http://fr.wikipedia.org/wiki/File_Transfer_Protocol_Secure Le FTPS est un protocole de communication destiné à l'échange informatique de fichiers sur un réseau TCP/IP, variante du FTP sécurisé avec les protocoles TLS/SSL. Il permet au visiteur de vérifier l'identité du serveur auquel il accède grâce à un certificat d'authentification. Il permet également de chiffrer la communication. L'utilisation de ce standard n'est pas recommandée et son retrait est demandé au profit du SFTP. En effet, le protocole FTPS ne chiffre que le flux de données et non les enveloppes du flux. Certaines informations passent donc en claire (comme par exemple, le nom des fichiers). Le protocole SFTP lui utilise le protocole FTP dans un tunnel sécurisé SSH, où tout est chiffré.			
IETF	RFC 4217, RFC 2228 et RFC 2818		

Technique	**Application**	**Transfert**	

Recommandé	**SFTP**	Secure File Transfer Protocol *ou* SSH File Transfer Protocol
http://fr.wikipedia.org/wiki/Secure_File_Transfer_Protocol http://en.wikipedia.org/wiki/SSH_File_Transfer_Protocol SFTP est une variante du protocole FTP qui « tunnelise » la session à travers une connexion Secure Shell (protocole SSH) pour la sécuriser. Il ne doit donc pas être confondu avec le FTPS qui utilise le protocole TLS. SFTP est exceptionnellement placé « Recommandé » malgré le fait que ses spécifications ne sont pas considérées comme validées au niveau de l'IETF. Elles n'ont toutefois pas évoluées depuis 2006 d'une part, et d'autre part, ce protocole est préférable au FTPS considéré comme moins sécurisé.		
IETF	Pas de RFC. SSH File Transfer Protocol, Draft 13, July 2006	

Technique	**Application**	**Transfert**	
En fin de vie	**PeSIT**	Protocole d'Echanges pour un Système Interbancaire de Télécompensation	
http://fr.wikipedia.org/wiki/PeSIT PeSIT est un protocole d'échange de fichiers entre systèmes informatiques reliés par une liaison de télécommunication, développé en France. Ce standard est positionné « en fin de vie », ou plus précisément, en sursis, car il n'est supporté que par une seule entreprise. Une alternative ouverte est actuellement en recherche. Son retrait n'est pas encore demandé, mais il n'est donc plus recommandé car propriétaire.			
PeSIT	http://www.pesit.com/		

Technique	**Application**	**Transfert**	
En fin de vie	**PRESTO 2.0**	Protocole d'échange standard et ouvert de l'Administration	
PRESTO est un protocole d'échange de fichiers défini par l'administration française pour ses besoins propres. Ce standard est positionné « en fin de vie », dans le sens ou une alternative ouverte et maintenue est actuellement en recherche. Son retrait n'est pas encore demandé, mais il n'est donc plus recommandé car non maintenu. Une évolution ouverte vers REST de ce standard permettrait de le repasser à « recommandé ». Les versions 1.0 et 1.1 doivent être considérées chacune comme « retirée » car s'appuyant sur des protocoles à proscrire d'un point de vue sécurité. Seule la version 2.0 (ou ultérieure) est recommandée.			
SGMAP	PRESTO 2.0		

Technique	**Application**	**Transfert**	
En observation	**R66**	R66	
http://fr.wikipedia.org/wiki/Waarp Le protocole R66 a été conçu pour permettre les fonctionnalités avancées d'un moniteur de transfert de fichiers dans un contexte de production sécurisée. Le protocole R66, et notamment son implémentation **waarp**, est une alternative ouverte à PeSIT. Mais sa maturité et son maintien ne sont pas jugés suffisants. Il est donc défini « en observation ».			
Waarp	R66 Protocol		

Technique	Application	Transfert	
En observation	**AMQP**	Advanced Message Queuing Protocol	
http://fr.wikipedia.org/wiki/Advanced_Message_Queuing_Protocol AMQP est un protocole ouvert pour les systèmes de messagerie orientés intergiciel. Il standardise les échanges entre serveurs de messages en se basant sur les principes suivants : orienté message, utilisation de files d'attente, routage (point à point et par diffusion/abonnement), fiabilité et sécurité.			
OASIS	OASIS AMQP v1.0		

Technique	Application	Transfert	
Recommandé	**AS2**	Applicability Statement 2	
https://fr.wikipedia.org/wiki/Applicability_Statement_2 AS2 est une spécification décrivant une méthode de transport de données électroniques sécurisée et fiable au travers d'Internet, basée sur le protocole HTTP et le standard S/MIME. Les données peuvent être en lien avec de l'EDI (Échange de données informatisé) mais peuvent très bien être de tout autre type. AS2 spécifie le mode de connexion, de livraison, de validation et d'acquittement des données. Ce mode de communication enveloppe le message qui est envoyé ensuite par Internet. La sécurité des communications est assurée par des certificats numériques et du chiffrement. L'implémentation d'AS2 nécessite deux machines, un client et un serveur, reliés tous deux à Internet. Le client peut lui-même être un serveur pour recevoir des données. Le client envoie des données au serveur (trading partner), puis à réception, l'application envoie un acquittement (ou MDN - Message Disposition Notification) à l'émetteur.			
IETF	RFC 4130		

Technique	Application	Exploitation	
Recommandé	**DNS**	Domain Name System	
http://fr.wikipedia.org/wiki/Domain_Name_System Le DNS est un service permettant de traduire un nom de domaine en informations de plusieurs types qui y sont associées, notamment en adresses IP de la machine portant ce nom.			
IETF	RFC 1034, RFC 1035, RFC 6895		

Technique	Application	Exploitation	
Recommandé	**DNSSEC**	Domain Name System Security Extensions	
http://fr.wikipedia.org/wiki/Domain_Name_System_Security_Extensions DNSSEC est un protocole permettant de résoudre certains problèmes de sécurité liés au protocole DNS. Il permet de sécuriser les données envoyées par le DNS. Contrairement à d'autres protocoles comme SSL, il ne sécurise pas juste un canal de communication mais il protège les données, les enregistrements DNS, de bout en bout. Ainsi, il est efficace même lorsqu'un serveur intermédiaire trahit.			
IETF	RFC 4033, RFC 4034 et RFC 4035		

Technique	Application	Accès	

Recommandé	**LDAP**	Lightweight Directory Access Protocol
http://fr.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol LDAP est à l'origine un protocole permettant l'interrogation et la modification des services d'annuaire. Ce protocole repose sur TCP/IP. Il a cependant évolué pour représenter une norme pour les systèmes d'annuaires, incluant un modèle de données, un modèle de nommage, un modèle fonctionnel basé sur le protocole LDAP, un modèle de sécurité et un modèle de réplication. C'est une structure arborescente dont chacun des nœuds est constitué d'attributs associés à leurs valeurs.		
IETF	RFC 4510 (la principale)	

Technique	**Application**	**Accès**	
Recommandé	**LDAPS**	LDAP over SSL, ou, Secure LDAP	
http://fr.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol LDAPS est un protocole permettant de sécuriser le LDAP par l'utilisation du protocole TLS (SSL).			
IETF	RFC 4513		

Technique	**Application**	**Multimédia**	
Recommandé	**RTSP**	Real Time Streaming Protocol	
http://fr.wikipedia.org/wiki/Real_Time_Streaming_Protocol RTSP est un protocole de communication de niveau applicatif (niveau 7 du modèle OSI) destiné aux systèmes de streaming média. Il permet de contrôler un serveur de média à distance, offrant des fonctionnalités typiques d'un lecteur vidéo telles que « lecture » et « pause », et permettant un accès en fonction de la position temporelle. RTSP ne transporte pas les données elles-mêmes et doit être associé à un protocole de transport comme RTP			
IETF	RFC 2326		

Technique	**Application**	**Multimédia**	
Retiré	**H.320**	H.320	
https://fr.wikipedia.org/wiki/H.320 H.320 est un protocole pour la visiophonie à bande étroite sur le réseau RNIS. Les principaux protocoles appartenant à cette suite sont H.221, H.230, H.242, les codecs audio comme G.711 et vidéo comme H.261 et H.263. Il spécifie les caractéristiques techniques des systèmes et équipements de terminaux visiophoniques à bande étroite typiquement pour des services de visioconférence et de visiophonie Ce protocol est clairement à retirer au profit éventuellement du H.323 ou plutot du SIP..			
UIT			

Technique	**Application**	**Multimédia**	
Recommandé	**H.323**	H.323	

http://fr.wikipedia.org/wiki/H.323 H.323 regroupe un ensemble de protocoles de communication de la voix, de l'image et de données sur IP. H.323 ressemble davantage à une association de plusieurs protocoles différents et qui peuvent être regroupés en trois catégories : la signalisation, la négociation de codec, et le transport de l'information. Le protocole SIP est recommandé.	
UIT	H.323 : Packet-based multimedia communications systems

Technique	**Application**	**Multimédia**	
Recommandé	**SIP**	Session Initiation Protocol	
http://fr.wikipedia.org/wiki/Session_Initiation_Protocol SIP est un protocole, de la couche applicative, de gestion de sessions souvent utilisé dans les télécommunications multimédia (son, image, etc.). SIP n'est pas seulement destiné à la VoIP mais aussi à de nombreuses autres applications telles que la visiophonie, la messagerie instantanée, la réalité virtuelle... Il se charge de l'authentification et de la localisation des multiples participants. Il se charge également de la négociation sur les types de média utilisables par les différents participants.			
IETF	RFC 3261, RFC 6665		

Technique	**Application**	**Multimédia**	
Recommandé	**MGCP**	Media Gateway Control Protocol	
http://fr.wikipedia.org/wiki/Media_Gateway_Control_Protocol MGCP est un protocole permettant de contrôler les passerelles multimédia (Media Gateways) qui assurent la conversion de la voix et de la vidéo entre les réseaux IP et le Réseau Téléphonique Commuté (RTC).			
IETF	RFC 3435		

Technique	**Application**	**Messagerie**	
Recommandé	**SMTP et SMTPS**	Simple Mail Transfer Protocol	
http://fr.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol SMTP, littéralement « protocole simple de transfert de courrier », est un protocole de communication utilisé pour transférer le courrier électronique (courriel) vers les serveurs de messagerie électronique. Le SMTPS n'est pas un standard en soi, mais une méthode pour sécuriser le protocole SMTP.			
IETF	RFC 5321		

Technique	**Application**	**Messagerie**	
Recommandé	**S/MIME**	*Secure / Multipurpose Internet Mail Extensions*	
http://fr.wikipedia.org/wiki/S/MIME S/MIME est une norme de cryptographie et de signature numérique de courriel encapsulés en format MIME. Elle assure l'intégrité, l'authentification, la non-répudiation et la confidentialité des données.			
IETF	RFC 5750		

Technique	**Application**	**Messagerie**	
Recommandé	**POP3**	Post Office Protocol	

http://fr.wikipedia.org/wiki/Post_Office_Protocol POP est un protocole qui permet de récupérer les courriers électroniques situés sur un serveur de messagerie électronique. En règle générale (configuration par défaut) POP se connecte sur le serveur, récupère le courrier, efface le courrier sur le serveur et se déconnecte. Ce protocole a été réalisé en plusieurs versions respectivement POP1, POP2 et POP3. C'est POP3, ou Post Office Protocol Version 3 qui est utilisé de façon standard.	
IETF	RFC 1939

Technique	**Application**	**Messagerie**	
Recommandé	**POP3S**	POP3 over SSL	
http://fr.wikipedia.org/wiki/Post_Office_Protocol Version sécurisée du standard POP3 qui utilise le standard TLS (SSL).			
IETF	RFC 2595		

Technique	**Application**	**Messagerie**	
Recommandé	**IMAP4**	Internet Message Access Protocol	
http://fr.wikipedia.org/wiki/Internet_Message_Access_Protocol IMAP est un protocole qui permet de récupérer les courriers électroniques déposés sur des serveurs de messagerie. Son but est donc similaire à POP3, l'autre principal protocole de relève du courrier. Mais contrairement à ce dernier, il a été conçu pour permettre de laisser les messages sur le serveur.			
IETF	RFC 3501		

Technique	**Application**	**Messagerie**	
Recommandé	**IMAP4S**	IMAP over SSL	
http://fr.wikipedia.org/wiki/Internet_Message_Access_Protocol Version sécurisée du standard IMAP qui utilise le standard TLS (SSL).			
IETF	RFC 2595		

Technique	**Application**	**Messagerie**	
Recommandé	**XMPP et XMPPS**	Extensible Messaging and Presence Protocol	
http://fr.wikipedia.org/wiki/Extensible_Messaging_and_Presence_Protocol XMPP est un ensemble de protocoles standards ouverts pour la messagerie instantanée, et plus généralement une architecture décentralisée d'échange de données. XMPP est également un système de collaboration en quasi-temps-réel et d'échange multimédia via le protocole Jingle, dont la voix sur réseau IP (téléphonie sur Internet), la visioconférence et l'échange de fichiers sont des exemples d'applications. Il existe une version sécurisée de ces protocoles, XMPPS.			
IETF	RFC 6120, RFC 6121, RFC 6122, RFC 3922, RFC 3923		

Technique	**Application**	**Messagerie**	
En observation	**WebRTC**	Web Real-Time Communication	

http://fr.wikipedia.org/wiki/WebRTC WebRTC est une API JavaScript actuellement au stade de brouillon (Draft) développée au sein du W3C et de l'IETF. C'est aussi un canevas logiciel avec des implémentations précoces dans différents navigateurs web pour permettre une communication en temps réel. Le but du WebRTC est de lier des applications comme la voix sur IP, le partage de fichiers en pair à pair en s'affranchissant des plugins propriétaires jusqu'alors nécessaires.

IETF W3C	Draft : http://tools.ietf.org/wg/rtcweb/ Draft : http://www.w3.org/2011/04/webrtc/

3.1.5 Service

Technique	**Service**	**Identité & Authentification**
Recommandé	**OpenPGP**	OpenPGP Message Format
https://fr.wikipedia.org/wiki/OpenPGP OpenPGP est un format de cryptographie. Ce standard décrit le format des messages, signatures ou certificats que peuvent s'envoyer des logiciels comme GNU Privacy Guard. Ce n'est donc pas un logiciel, mais un format pour l'échange sécurisé de données, qui doit son nom au programme historique Pretty Good Privacy (PGP).		
IETF	RFC 4880	

Technique	**Service**	**Identité & Authentification**
Recommandé	**SAMLv2.0**	Security assertion markup language version 2
http://fr.wikipedia.org/wiki/Security_assertion_markup_language SAML est un protocole pour échanger des informations d'authentification et d'autorisation entre des parties, en particulier entre un fournisseur d'identité et un fournisseur de service. Basé sur le langage XML. SAML propose l'authentification unique (en anglais single sign-on ou SSO) sur le web. De cette manière, un utilisateur peut naviguer sur plusieurs sites différents en ne s'authentifiant qu'une seule fois. Dans la pratique SAML est une suite de spécifications. Le SAMLConform notamment décrit les modes opérationnels à destinations des implémentations de SAML 2.0. Il précise les exigences techniques pour la conformité SAML v2.0. Il convient sur ce type de standard d'être explicite sur les modes opérationnels et options retenus.		
OASIS	SAML specification	

Technique	**Service**	**Identité & Authentification**
Recommandé	**Oauth 2.0**	Open standard to authorization
http://en.wikipedia.org/wiki/OAuth OAuth est un protocole ouvert. Il permet d'autoriser un site web à utiliser l'API sécurisée d'un autre site web pour le compte d'un utilisateur. OAuth n'est pas un protocole d'authentification. OAuth permet aux utilisateurs de donner, à un site « consommateur », l'accès à des informations personnelles provenant d'un site « fournisseur » de service ou de données, ceci tout en protégeant le pseudonyme et le mot de passe des utilisateurs. Le protocole Oauth peut permettre différentes orchestrations entre les parties prenantes. Il convient de préciser de manière explicite les choix et options retenus sous peine de non interopérabilité des réalisations.		

IETF	RFC 6749, RFC 6750

Technique	**Service**	**Identité & Authentification**
Recommandé	**Open ID Connect**	Open ID Connect protocol
http://en.wikipedia.org/wiki/OpenID_Connect OpenId Connect s'appuie sur le standard Oauth 2,0 auquel il ajoute une couche d'identification. Il permet à un site web client de récupérer l'identité d'un utilisateur (ainsi que d'autres données types) en se basant sur les mécanismes d'authentification d'un serveur tiers au travers d'appels REST.		
OpenID Foundation	Open ID Connect protocol specification	

Technique	**Service**	**Service web**	
Recommandé	**SOAPv1.2**	Simple Object Access Protocol	
http://fr.wikipedia.org/wiki/SOAP SOAP (ancien acronyme de Simple Object Access Protocol) est un protocole de RPC (protocole réseau permettant de faire des appels de procédures sur un ordinateur distant à l'aide d'un serveur d'applications) orienté objet bâti sur XML. Il permet la transmission de messages entre objets distants, ce qui veut dire qu'il autorise un objet à invoquer des méthodes d'objets physiquement situés sur un autre serveur. Le transfert se fait le plus souvent à l'aide du protocole HTTP, mais peut également se faire par un autre protocole, comme SMTP. La version 1.2 du protocole est recommandée.			
W3C	SOAP specification		

Technique	**Service**	**Service web**	
Recommandé	**WSDL**	Web Services Description Language	
http://fr.wikipedia.org/wiki/Web_Services_Description_Language WSDL est une grammaire XML permettant de décrire un service web. Le WSDL décrit une interface publique d'accès à un service web, notamment dans le cadre d'architectures de type SOA (Service Oriented Architecture). C'est une description fondée sur le XML qui indique « comment communiquer pour utiliser le service ».			
W3C	Web Services Description Language		

Technique	**Service**	**Service web**	
Recommandé	**UDDI**	Universal Description Discovery and Integration	
http://fr.wikipedia.org/wiki/Universal_Description_Discovery_and_Integration UDDI est un annuaire de services fondé sur XML et plus particulièrement destiné aux services Web. Un annuaire UDDI permet de localiser sur le réseau le service Web recherché.			
OAIS	http://uddi.xml.org/wiki		

Technique	**Service**	**Service web**	
Recommandé	**MTOM**	Message Transmission Optimization Mechanism	

http://fr.wikipedia.org/wiki/Message_Transmission_Optimization_Mechanism MTOM est une méthode d'envoi de données binaires par services Web. MTOM est habituellement utilisé avec XOP (XML-binary Optimized Packaging). Il est recommandé d'associer l'usage de MTOM au protocole SOAPv1.2.	
W3C	*Message Transmission Optimization Mechanism*

Technique	**Service**	**Service web**	
Recommandé	**XOP**	XML-binary Optimized Packaging	
http://en.wikipedia.org/wiki/XML-binary_Optimized_Packaging XOP est un mécanisme défini pour la sérialisation d'ensembles d'information XML (XML Information Sets) contenant des données binaires, ainsi que pour leur désérialisation en retour. Il est recommandé d'associer l'usage de XOP au protocole SOAPv1.2.			
W3C	XML-binary Optimized Packaging		

Technique	**Service**	**Service web**	
Recommandé	**WS-Security ou WSS**	Web Services Security	
http://fr.wikipedia.org/wiki/WS-Security WS-Security (Web Services Security) est un protocole de communications qui permet d'appliquer de la sécurité aux services web. Le protocole contient des spécifications sur la façon dont l'intégrité et la confidentialité peuvent être appliquées aux messages de services web. Le protocole WSS inclut des détails sur l'utilisation de SAML et Kerberos, et des formats de certificat comme X.509.			
OASIS	WSS technical specification		

Technique	**Service**	**Service web**	
Recommandé	**WS-Addressing**	Web Services Addressing	
http://en.wikipedia.org/wiki/WS-Addressing WS-Addressing est une spécification de mécanismes de transport neutre qui permet à des services Web de communiquer des informations d'adressage. Deux parties le composent essentiellement : une structure pour communiquer une référence à un service Web final, et un ensemble de propriétés d'adressage de messages qui associent des informations d'adressage à un message particulier.			
W3C	WS-Adressing working group		

Technique	**Service**	**Service web**	
Recommandé	**InterOPS**	Interopérabilité entre Organismes de la Protection Sociale	

http://fr.wikipedia.org/wiki/InterOPS
InterOPS est un standard informatique d'interopérabilité, interne à l'administration, qui permet l'établissement d'un espace de confiance entre des organismes de la sphère sociale française, au travers des 3 modèles d'échanges suivants :

- InterOPS-A (Application à application) : échanges, en protocole "Web Services", effectués soit dans un contexte applicatif sans identification d'un utilisateur, soit dans un contexte où un utilisateur d'un organisme client atteint les applications des organismes fournisseurs au travers d'une application locale,
- InterOPS-P (Portail à portail) : accès d'un utilisateur d'un organisme client à l'application ou au service d'un organisme fournisseur, via les portails web respectifs des 2 organismes.
- InterOPS-S (Sphère de confiance) : accès d'un utilisateur à une sphère de confiance composée d'organismes jouant le rôle d'opérateur d'authentification et/ou le rôle d'opérateur de service.

InterOPS est en réalité un assemblage de standards. Se référer au profil d'interopérabilité n°6.
La version 2.0 ou supérieure est recommandée.

DSS	Spécification du standard InterOPS

Technique	**Service**	**Orchestration de services**
Recommandé	**WS-BPEL**	Web Services Business Process Execution Language

http://fr.wikipedia.org/wiki/Business_Process_Execution_Language
BPEL est un langage de programmation destiné à l'exécution des procédures d'entreprise. Le BPEL est issu des langages WSFL (Web Services Flow Language) et XLANG, et est dérivé du XML. Le BPEL vise à rendre possible le *programming in the large*. Les concepts de *programming in the large* et *programming in the small* distinguent deux aspects de l'écriture de procédures asynchrones à long terme qu'on voit généralement dans les procédures d'entreprise.
La version 2.0 ou supérieure est recommandée.

OASIS	OASIS Web Services Business Process Execution Language Version 2.0

Technique	**Service**	**Orchestration de services**
En observation	**WS-CDL**	Web Service Choreography Description Language

http://fr.wikipedia.org/wiki/Chor%C3%A9graphie_des_services_web_WS-*
En informatique, la chorégraphie est une généralisation de l'approche par orchestration qui consiste à concevoir une coordination décentralisée des applications, dans laquelle il n'y a pas de machine privilégiée (serveur informatique) mais un réseau de machines interconnectées qui échangent des messages et effectuent des calculs.

W3C	Web Service Choreography Description Language

Technique	**Service**	**Géospatial**	
Recommandé	**WMS**	Web Map Service	

http://fr.wikipedia.org/wiki/Web_Map_Service
WMS est un protocole de communication standard qui permet d'obtenir des cartes de données géoréférencées à partir de différents serveurs de données. Cela permet de mettre en place un réseau de serveurs cartographiques à partir desquels des clients peuvent construire des cartes interactives.

OGC	http://www.opengeospatial.org/standards/wms

Technique	**Service**	**Géospatial**	
Recommandé	**WFS**	Web Feature Service	
http://fr.wikipedia.org/wiki/Web_Feature_Service WFS permet, au moyen d'une URL formatée, d'interroger des serveurs cartographiques afin de manipuler des objets géographiques (lignes, points, polygones...). Il complète le WMS qui permet la production de cartes géoréférencées à partir de serveurs géographiques.			
OGC	http://www.opengeospatial.org/standards/wfs		

Technique	**Service**	**Géospatial**	
Recommandé	**TJS**	Table Joining Service	
TJS défini une manière simple de décrire et d'échanger des données tabulaires contenant des informations sur des objets géographiques.			
OGC	TJS Specification		

Technique	**Service**	**Géospatial**	
Recommandé	**WMTS**	Web Map Tile Service	
http://fr.wikipedia.org/wiki/Web_Map_Tile_Service WMTS est un service web standard qui permet d'obtenir des cartes géoréférencées tuilées à partir d'un serveur de données sur le réseau. Ce service est comparable au Web Map Service mais tandis que le WMS permet de faire des requêtes complexes (dont la reprojection ou la symbolisation de données vecteur) nécessitant une certaine puissance de calcul côté serveur, le WMTS met l'accent sur la performance et ne permet de requêter que des images précalculées (tuiles) appartenant à des dallages prédéfinis. Cela permet aux utilisateurs de construire des cartes interactives en ligne avec une bonne réactivité de l'IHM.			
OGC	http://www.opengeospatial.org/standards/wmts		

Technique	**Service**	**Géospatial**	
Recommandé	**CSW**	Catalog Service for the Web	
http://en.wikipedia.org/wiki/Catalog_Service_for_the_Web CSW (Catalog Service for the Web, parfois nommé Catalog Service - Web) est un standard de publication d'un catalogue d'enregistrements géospatiaux en XML sur Internet (via HTTP). Le catalogue est constitué d'enregistrements qui décrivent des données géospatiales (par ex. KML), des services géospatiaux (par ex. WMS), et des ressources liées. CSW est une partie (ou "profil") du service de catalogue OGC, qui définit des interfaces communes pour la découverte, la navigation et la requête de métadonnées sur des données, des services, et d'autres ressources potentielles.			
OGC	OGC CSW Specification		

Technique	**Service**	**Géospatial**	
En observation	**WCS**	Web Coverage Service	

http://fr.wikipedia.org/wiki/Web_Coverage_Service WCS est un standard fournissant une interface permettant d'effectuer des recherches internet sur des données cartographiées.	
OGC	http://www.opengeospatial.org/standards/wcs

Technique	**Service**	**Géospatial**	
En observation	**WPS**	Web Processing Service	
http://fr.wikipedia.org/wiki/Web_Process_Service WPS fournit des règles pour normaliser les appels de services de traitement des données géospatiales.			
OGC	http://www.opengeospatial.org/standards/wps		

4 Interopérabilité Syntaxique

Synthèse des standards retenus pour le niveau syntaxique

Les standards retirés ou en fin de vie ne sont pas présents dans cette synthèse.

Niveau	**Catégorie**	**Sous-Catégorie**	**Standards**
Syntaxique	Encodage	Caractère	UTF-8
Syntaxique	Encodage	Compression	Bzip2, gzip, ZIP, 7z, TAR
Syntaxique	Document		ODF, OOXML, DocBook, PDF, PDF/A, EPUB3
Syntaxique	Web		HTML, CSS, Internet media type, ATOM, APP, Javascript, CMIS
Syntaxique	Structuration des données		XML, EXI XSD, JSON, OData, LDIF, RDF, OWL2, SPARQL, KML, DOM, SIARD, XMI, OAIS, SEDA
Syntaxique	Structuration des données	Description d'API	YAML, RAML
Syntaxique	Structuration des données	Identifiant	URI, ARK, ISNI
Syntaxique	Structuration des données	Géospatial	Shapefile, GeoJSON, GeoSpatial-Metadata, GML
Syntaxique	Structuration des données	Carnet d'adresse	vCard
Syntaxique	Structuration des données	Calendrier	iCalendar
Syntaxique	Traitement de données structurées		XSLT, XPath, XLink, XQuery, XInclude, XPointer, XML Signature
Syntaxique	Traitement de données structurées	Géospatial	OpenLS, OWS Context, SLD
Syntaxique	Multimedia	Conteneur vidéo	MPEG-TS, MP4, MKV, WebM
Syntaxique	Multimedia	Codec vidéo	VP8, VP9, H.264, H.265
Syntaxique	Multimedia	Conteneur audio	OGG
Syntaxique	Multimedia	Codec audio	Opus, MP3, Vorbis, AAC, FLAC
Syntaxique	Multimedia	Image	GeoTIFF, PNG, JPEG, SVG
Syntaxique	Signature		PAdES, XAdES, CAdES, ASIC
Syntaxique	Message de sécurité		IDMEF, IODEF

4.1 Liste des standards retenus pour le niveau syntaxique

4.1.1 Encodage

Syntaxique	**Encodage**	**Caractère**	
Recommandé	**UTF-8**	Universal Character Set Transformation Format - 8 bits	
http://fr.wikipedia.org/wiki/UTF-8 UTF-8 est un codage de caractères informatiques conçu pour coder l'ensemble des caractères du « répertoire universel de caractères codés », initialement développé par l'ISO dans la norme internationale ISO/CEI 10646, ce codage est aujourd'hui totalement compatible avec le standard Unicode, en restant compatible avec la norme ASCII limitée à l'anglais « standard » (et quelques autres langues beaucoup moins fréquentes utilisant un jeu réduit de caractères. Les accents ne sont pas supportés par l'ASCII). Ce standard doit être utilisé pour tout échange de données structurées ou non. Le choix d'un encodage UTF-16 voire UTF-32 n'est interdit dans la mesure où ils sont bien UTF.			
IETF	RFC 3629 et ISO/CEI 10646		

Syntaxique	**Encodage**	**Compression**	
Recommandé	**Bzip2**	Bzip2	
http://fr.wikipedia.org/wiki/Bzip2 bzip2 est à la fois le nom d'un algorithme de compression de données et celui d'un logiciel libre			
Bzip	http://bzip.org/		

Syntaxique	**Encodage**	**Compression**	
Recommandé	**gzip**	GNU Zip	
http://fr.wikipedia.org/wiki/Gzip gzip est à la fois un format de compression et le logiciel libre de compression qui a été créé pour remplacer le programme compress d'Unix.			
IETF	Spécifications du format gzip :RFC 1950, RFC 1951 et RFC 1952		

Syntaxique	**Encodage**	**Compression**	
Recommandé	**ZIP**	ZIP	
http://fr.wikipedia.org/wiki/ZIP_(format_de_fichier) Le ZIP est un format conteneur de fichier permettant l'utilisation d'un seul fichier pour stocker plusieurs fichiers et la compression de données (diminution de l'espace occupé sur le support numérique) sans perte de qualité. On peut donc le comparer à la combinaison de tar (archivage) et gzip (compression) dans le cadre d'une archive compressée .tgz. Le format ZIP a un avantage sur les autres formats de compression qui le rend actuellement irremplaçable et le fait préférer dans certains cas : il intègre un index de son contenu permettant d'extraire à la demande un item de l'archive sans devoir décompresser toute l'archive au préalable (avec donc un gain de temps et d'espace utilisé). Le format ODF correspond en réalité à une archive ZIP.			
PKWARE	Spécifications du format zip sur le site de pkware		

Syntaxique	**Encodage**	**Compression**	
Recommandé	**7z**	Seven ZIP	
http://fr.wikipedia.org/wiki/7z 7z est un format conteneur ayant une architecture ouverte.			

7-zip	7z specification

Syntaxique	**Encodage**	**Compression**	
Recommandé	**TAR**	Tape Archiver	
http://fr.wikipedia.org/wiki/Tar_(informatique) TAR est à la fois un format et un logiciel permettant de contenir dans un seul fichier des fichiers standard des systèmes de type UNIX. Il a été créé dans les premières versions d'UNIX et standardisé par les normes POSIX.1-1988 puis POSIX.1-2001.			
IEEE	POSIX.1-2001		

4.1.2 Document

Syntaxique	**Document**		
En fin de vie	**TXT**	Text File	
http://fr.wikipedia.org/wiki/Fichier_texte En informatique, un fichier texte ou fichier texte brut ou fichier texte simple est un fichier dont le contenu représente uniquement une suite de caractères. Il utilise nécessairement une forme particulière de codage de caractère qui peut être une variante ou une extension du standard ASCII. Il n'existe aucune définition officielle, et les différentes interprétations de ce qu'est un fichier texte se partagent des propriétés essentielles. Ce format est retenu dans le RGI par exception. Il doit être évité car il n'est pas nécessairement interopérable d'une plate-forme à l'autre ; le codage, par exemple, des retours chariots peut-être problématique. Lorsqu'on utilisera le format TXT il est recommandé de préciser l'encodage UTF-8 et le retour chariot. Il peut être utile de suivre la syntaxe Markdown/CommonMark. Le site http://commonmark.org/ standardise une syntaxe intuitive utilisant Unicode (avec de préférence un codage UTF-8), utilisée sur de nombreux sites web majeurs comme GitHub. Pour tout nouveau projet, il est par contre recommandé d'utiliser le standard XML ou JSON.			
Aucun	Absence de spécification précise		

Syntaxique	**Document**		
Recommandé	**ODF**	Open Document Format for Office Applications	
http://fr.wikipedia.org/wiki/OpenDocument OpenDocument est un format ouvert de données pour les applications bureautiques : traitements de texte, tableurs, présentations, diagrammes, dessins et base de données bureautique. OpenDocument est la désignation d'usage d'une norme dont l'appellation officielle est OASIS Open Document Format for Office Applications, également abrégée par le sigle ODF			
OASIS ISO	Open Document Format for Office Applications Version 1.2 ISO/IEC 26300-1:2015, ISO/IEC 26300-2:2015, ISO/IEC 26300-3:2015		

Syntaxique	**Document**		
En observation	**OOXML**	Office Open XML strict	

http://fr.wikipedia.org/wiki/Office_Open_XML
Office Open XML est une norme ISO/CEI 29500 créée par Microsoft, destinée à répondre à la demande d'interopérabilité dans les environnements de bureautique. Ce format (dont les suffixes sont .docx, .xlsx, .pptx...) est utilisé à partir de Microsoft Office 2007, en remplacement des précédents formats Microsoft (reconnus à leurs suffixes tels que : .doc, .xls, .ppt), il est toutefois légèrement différent, pour ces versions d'office, de la norme ISO définitive, qui a tenu compte des remarques des membres de l'organisme normalisateur. Seule la suite Office à partir de la version 2013 est totalement compatible avec la norme (en lecture et en écriture).
Le standard est conservé dans le RGI au statut « en observation ». Sa complexité, son manque d'ouverture (notamment dans la gouvernance de la norme) et le strict respect tardif de la norme par Microsoft même n'ont pas permis de réviser son statut. La version « *transitionnal* » de la norme n'est quant à elle pas recommandée.
Pour des besoins d'échanges d'informations sous forme de tableaux qui notamment embarquerait du code, l'utilisation d'OOXML peut être une alternative. C'est toutefois une pratique à encadrer.

ISO ECMA	ISO/CEI 29500 :2008-2012 ECMA-376 4th Edition - décembre 2012

Syntaxique	**Document**		
Recommandé	**DocBook**	DocBook schema	

https://fr.wikipedia.org/wiki/DocBook
DocBook est un langage de balisage sémantique pour la documentation technique. À l'origine prévu pour écrire de la documentation technique portée sur le domaine informatique (matériel et logiciel), il peut être utilisé pour n'importe quel type de documentation.
En tant que langage sémantique DocBook permet à ses utilisateurs de créer du contenu sous une forme neutre vis-à-vis de la présentation qui ne fait que capturer la structure logique du contenu; contenu qui peut ensuite être publié dans une grande variété de formats, notamment HTML, XHTML, EPUB, PDF, pages de man, Web help et HTML Help, sans obliger les utilisateurs à faire des changements dans le contenu source. En d'autres mots, quand un document est écrit dans le format DocBook il devient facilement portable vers d'autres formats. Il résout ainsi le problème de reformatage en n'ayant à écrire qu'une seule fois à base de balises XML.
Avantages :

- Le format DocBook ne contient que des données et aucune information de mise en forme
- Le format DocBook est adapté aux traitements par lots
- Le format DocBook est lisible sans aucun outil spécifique
- Le format DocBook est extrêmement facile à exploiter
- De très nombreux outils savent exploiter le format DocBook (*LibreOffice*/*OpenOffice, etc.)*
- Le format DocBook est un format idéal pour l'archivage de par les points précédents

Pour toutes ces raisons DocBook s'est imposé comme le format standard pour la documentation logicielle (notamment dans la communauté Open Source) et commence à être utilisé dans l'industrie.

OASIS	DocBook V5

Syntaxique	**Document**		
Recommandé	**PDF**	Portable Document Format	

http://fr.wikipedia.org/wiki/Portable_Document_Format Le PDF est un langage de description de pages dont la spécificité est de préserver la mise en forme d'un fichier – polices d'écritures, images, objets graphiques, etc. – telle qu'elle a été définie par son auteur, et cela quels que soient le logiciel, le système d'exploitation et le matriel utilisés pour l'imprimer ou le visualiser. PDF faisant référence à une grande variété de formats, toutes leurs subtilités ne sont pas explicitées dans le présent document. La version 1.7 du standard est recommandé. Il faut noter que de nombreux logiciels produisent des PDF non strictement conformes à la norme et qui posent donc des problèmes d'interopérabilité. Par ailleurs, Les PDF incorporant des objets non-standard (animations swf par exemple), reposant sur des plugins, ou embarquant des contenus actifs, ou des scripts, ou encore du code exécutable, sont à proscrire.

ISO	ISO 32000-1:2008

Syntaxique	**Document**		
Recommandé	**PDF/A**	Portable Document Format pour l'Archivage	
http://fr.wikipedia.org/wiki/PDF/A-1 PDF/A-1 est une version standardisée du PDF. Son usage est très répandu pour conserver et échanger des documents numériques, sur le long terme. Le format PDF/A-1 est fidèle aux documents originaux : les polices, les images, les objets graphiques et la mise en forme du fichier source sont préservés, quelles que soient l'application et la plate-forme utilisées pour le créer. D'autres versions du PDF/A ont été publiées, notamment les PDF/A-2 et PDF/A-3. L'usage du PDF/A-3 est fortement déconseillé, car il peut encapsuler des formats binaires non maîtrisés.			
ISO	ISO 19005-1:2005, ISO 19005-2:2011		

Syntaxique	**Document**		
En observation	**EPUB3**	Electronic Publication	
http://fr.wikipedia.org/wiki/EPUB_%28format%29 EPUB est un format ouvert standardisé pour les livres numériques. EPUB est conçu pour faciliter la mise en page du contenu, le texte affiché étant ajusté pour le type d'appareil de lecture. Il est également conçu comme le seul format pouvant à la fois satisfaire les éditeurs pour leurs besoins internes et la distribution. Ce format englobe le standard Open eBook1. La dernière version standardisée, EPUB3, repose sur l'HTML5, ce qui ouvre la voie à de nombreuses extensions. Elle offre de nouvelles caractéristiques telles que la prise en charge de l'affichage de toutes les langues, un espace spécifique pour les métadonnées, un développement de l'interactivité permettant l'ajout de contenus enrichis (graphismes, typographies, multimédias).			
IDPF ISO	EPUB3 Specification En cours (ISO/IEC TS30135-1 à 7)		

4.1.3 Web

Syntaxique	**Web**		
Recommandé	**HTML**	Hypertext Markup Language	

http://fr.wikipedia.org/wiki/Hypertext_Markup_Language HTML est le format de données conçu pour représenter les pages web. C'est un langage de balisage permettant d'écrire de l'hypertexte, d'où son nom. HTML permet également de structurer sémantiquement et de mettre en forme le contenu des pages, d'inclure des ressources multimédias dont des images, des formulaires de saisie, et des programmes informatiques. Il permet de créer des documents interopérables avec des équipements très variés de manière conforme aux exigences de l'accessibilité du web. Il est souvent utilisé conjointement avec des langages de programmation (JavaScript) et des formats de présentation (feuilles de style en cascade CSS). **La version 5** de HTML est « recommandée ». La version 5.1 peut être considérée d'ores et déjà « en observation ».

W3C	Spécification HTML5

Principe	**Web**		
Recommandé	**Navigateur web**		
Cette recommandation ne concerne pas un standard de protocole d'échange ou de format, mais porte sur un principe de construction et de mise en œuvre de services numériques. Globalement, les principes de constructions des services numériques de la sphère publique se basent avant tout sur les standards du web. La capacité des navigateurs web, utilisés par les usagers (particulier, professionnel, entreprise, associations) et les agents sur tout type d'équipements mobiles ou fixes, à respecter ces standards devient un élément critique. Il est donc recommandé de s'assurer de la compatibilité des services numériques en lignes avec les navigateurs web suivants (quelque soit la plateforme) : • Chrome version 35 ou supérieure • Internet Explorer version 10 ou supérieure • Firefox version 31 ou supérieure • Safari version 7 ou supérieure			

Syntaxique	**Web**		
Retiré	**XHTML**	Extensible HyperText Markup Language	
http://fr.wikipedia.org/wiki/XHTML XHTML est un langage de balisage servant à écrire des pages pour le web. Conçu à l'origine comme le successeur de HTML, XHTML se fonde sur la syntaxe définie par XML. Le format HTML est recommandé en lieu et place du XHTML.			
W3C	Spécification XHTML		

Syntaxique	**Web**		
Recommandé	**CSS**	Cascading Style Sheets	
http://fr.wikipedia.org/wiki/Feuilles_de_style_en_cascade CSS est un langage informatique qui décrit la présentation des documents HTML et XML. La **version 2.1** ou supérieure est à privilégier.			
W3C	Cascading Style Sheets Specification		

Syntaxique	**Web**		
Recommandé	**Internet media type ou type MIME ou MIME ou Content-type**	Internet media type	
http://en.wikipedia.org/wiki/Internet_media_type Un Internet media type, à l'origine appelé type MIME ou juste MIME ou encore Content-type, est un identifiant de format de données sur internet. Les identifiants étaient à l'origine définis dans la RFC 2046 pour leur utilisation dans les courriels à travers du SMTP mais ils ont été étendus à d'autres protocoles comme le HTTP ou le SIP.			
IETF	RFC 6838, RFC 4855		

Syntaxique	**Web**		
Recommandé	**ATOM**	Atom Syndication format	
http://fr.wikipedia.org/wiki/Atom Le Format de Syndication Atom est un format ouvert de document basé sur XML conçu pour la syndication de contenu périodique, tel que les blogs ou les sites d'actualités			
IETF	RFC 4287		

Syntaxique	**Web**		
Recommandé	**APP ou AtomPub**	Atom Publishing Protocol	
http://fr.wikipedia.org/wiki/Atom_Publishing_Protocol APP ou AtomPub est un protocole informatique de création, modification et destruction de ressources Web , typiquement au format Atom. Il est surtout utilisé dans le contexte des blogs mais peut servir à d'autres usages. AtomPub est une implémentation technique se voulant respectueuse du style d'architecture REST.			
IETF	RFC 5023		

Syntaxique	**Web**		
Recommandé	**Javascript**	Javascript	
http://fr.wikipedia.org/wiki/JavaScript JavaScript est un langage de programmation de scripts principalement employé dans les pages web interactives mais aussi pour les serveurs. C'est un langage orienté objet à prototype, c'est-à-dire que les bases du langage et ses principales interfaces sont fournies par des objets qui ne sont pas des instances de classes, mais qui sont chacun équipés de constructeurs permettant de créer leurs propriétés, et notamment une propriété de prototypage qui permet d'en créer des objets héritiers personnalisés. En outre, les fonctions sont des objets de première classe.			
ECMA ISO	ECMA-262 SO/CEI 16262		

Syntaxique	**Web**		
Recommandé	**CMIS**	Content Management Interoperability Services	

http://en.wikipedia.org/wiki/Content_Management_Interoperability_Services CMIS est un protocole ouvert qui permet à différents gestionnaires de contenu (CMS) d'interopérer à travers internet. CMIS fournit un modèle de données commun couvrant les types de fichiers et répertoires avec des propriétés génériques pouvant être lues ou écrites. CMIS décrit aussi un système de gestion des droits d'accès, de contrôle de version et offre la possibilité de définir des relations génériques. Il dispose d'un ensemble de services pour modifier ou interroger le modèle de données et peut être utilisé par plusieurs protocoles comme SOAP et REST à l'aide de la convention Atom1. Le modèle est basé sur des architectures communes de systèmes de gestion de documents.

OASIS	CMIS OASIS Specification Version 1.1

4.1.4 Structuration de données

Syntaxique	**Structuration de données**		
Recommandé	**XML**	Extensible Markup Language	
http://fr.wikipedia.org/wiki/Extensible_Markup_Language XML ou « langage de balisage extensible » est un langage informatique de balisage générique. Cette syntaxe est dite « extensible » car elle permet de définir différents espaces de noms, c'est-à-dire des langages avec chacun leur vocabulaire et leur grammaire, comme XHTML, XSLT, RSS, SVG… Elle est reconnaissable par son usage des chevrons (< >) encadrant les balises. L'objectif initial est de faciliter l'échange automatisé de contenus complexes (arbres, texte riche…) entre systèmes informatiques hétérogènes (interopérabilité). Avec ses outils et langages associés, une application XML respecte généralement certains principes : • la structure d'un document XML est définie et peut-être validée par un schéma ; • un document XML est entièrement transformable dans un autre document XML.			
W3C	W3C Recommendation: Extensible Markup Language (XML) 1.0 (Fifth Edition)		

Syntaxique	**Structuration de données**		
En observation	**EXI**	Efficient XML Interchange	
http://en.wikipedia.org/wiki/Efficient_XML_Interchange EXI est un format XML binaire. Il permet de coder des documents XML dans un format de données binaire, au lieu de texte brut. L'utilisation d'un tel format XML binaire réduit généralement la verbosité de documents XML, et peut réduire ainsi le coût du parsing (par contre, la performance de l'écriture n'est généralement pas amélioré de façon similaire).			
W3C	EXI SpecificationEfficient XML Interchange (EXI) Format 1.0 (Second Edition)		

Syntaxique	**Structuration de données**	
Recommandé	**XSD**	XML Schema Definition
http://fr.wikipedia.org/wiki/XML_Schema XML Schema est un langage de description de format de document XML permettant de définir la structure et le type de contenu d'un document XML. Cette définition permet notamment de vérifier la validité de ce document.		

W3C	http://www.w3.org/XML/Schema

Syntaxique	**Structuration de données**	
Recommandé	**JSON**	JavaScript Object Notation
http://fr.wikipedia.org/wiki/JavaScript_Object_Notation JSON est un format de données textuelles dérivé de la notation des objets du langage JavaScript. Le principal avantage de JSON est qu'il est simple à mettre en œuvre par un développeur tout en étant complet. Il présente plusieurs avantages, tels que : • il est peu verbeux (XML simplifié), ce qui le rend lisible plus facilement que XMLaussi bien par un humain que par une machine ; • il reste facile à apprendre, car sa syntaxe est réduite et non extensible (bien que ne souffrant que de peu de limitations) ; • Ses types de données sont connus et simples à décrire.		
IETF	RFC 7159	

Syntaxique	**Structuration de données**	
Recommandé	**OData**	Open Data Protocol
http://en.wikipedia.org/wiki/Open_Data_Protocol OData est un protocol ouvert qui permet la création et la consommation d'API REST interopérable, de manière simple et standard. Odatat permet aux fournisseurs de données d'exposés sur le web de façon simple, sécurisée et interopérable toutes données (base de données relationnelles, systèmes de fichiers, CMS, sites webs traditionnels, sites collaboratifs...). Il fournit également un accès à l'information depuis un large éventail d'applications, des services, de magasins/stockages de données. Ce standard constitue une extension natuelle des technologies du web : HTTP, URI, Service RESTful, JSON... Il favorise le mashup de données et les applications composites.		
OASIS	OData version 4.0 protocol (part 1 à part 3)	

Syntaxique	**Structuration de données**	
Recommandé	**LDIF**	LDAP Data Interchange Format
http://fr.wikipedia.org/wiki/LDAP_Data_Interchange_Format LDIF est un format standardisé d'échange de données, qui permet la représentation des données contenues dans un annuaire LDAP. Il permet également la représentation d'opérations sur les données de l'annuaire (ajout, suppression, modification).		
IETF	RFC 2849	

Syntaxique	**Structuration de données**	
En fin de vie	**DSML**	Directory Service Markup Language
http://fr.wikipedia.org/wiki/LDAP_Data_Interchange_Format Le Directory Service Markup Language (DSML) est une représentation du contenu d'un annuaire LDAP, permettant l'interrogation et la modification des services d'annuaire dans un réseau informatique.		
OASIS		

Syntaxique	**Structuration de données**	
En fin de vie*	**CSV**	Comma-separated values
http://fr.wikipedia.org/wiki/Comma-separated_values CSV est un format informatique d'échange de données ouvert représentant des données tabulaires sous forme de valeurs séparées par des virgules. D'autres variantes de séparateur de champ peuvent être utilisées, notamment lorsque la virgule est un élément signifiant d'une donnée. L'utilisation des séparateurs de champs doit donc être utilisée avec circonspection et adaptée au contexte sous peine de rendre le fichier inexploitable. Ce format est retenu dans le RGI par exception. Il doit être évité car il n'est pas nécessairement interopérable d'une plateforme à l'autre, la spécification précisant uniquement le format des fins de ligne mais ne précisant pas l'encodage à utiliser pour le texte en lui-même et pour les séparateurs (la RFC mentionne uniquement un encodage US-ASCII). Note importante : Le standard CSV est au statut **recommandé uniquement** pour les échanges entre application et utilisateur. Pour tous les autres cas, il est considéré en « fin de vie ». Le standard XML est à privilégier pour les échanges entre applications ou systèmes, qui n'impliquent donc pas d'utilisateurs.		
IETF	RFC 4180	

Syntaxique	**Structuration de données**	
Recommandé	**RDF**	Resource Description Framework
http://fr.wikipedia.org/wiki/Resource_Description_Framework RDF est un modèle de graphe destiné à décrire de façon formelle les ressources Web et leurs métadonnées, de façon à permettre le traitement automatique de telles descriptions.		
W3C	Spécifications RDF	

Syntaxique	**Structuration de données**	
Recommandé	**OWL2**	Web Ontology Language
http://fr.wikipedia.org/wiki/Web_Ontology_Language OWL est un langage de représentation des connaissances construit sur le modèle de données de RDF. Il fournit les moyens pour définir des ontologies web structurées. En pratique, le langage OWL est conçu comme une extension de RDF. OWL est destiné à la description de classes au travers de caractéristiques des instances de cette classe et de types de propriétés. De ce fait, il est plus expressif que RDF, auxquels certains reprochent une insuffisance d'expressivité due à la seule définition des relations entre objets par des assertions. OWL apporte aussi une meilleure intégration, une évolution, un partage et une inférence plus facile des ontologies.		
W3C	OWL2 specification	

Syntaxique	**Structuration de données**	
En observation	**SPARQL**	SPARQL Protocol and RDF Query Language

SPARQL est un langage de requête et un protocole qui permet de rechercher, d'ajouter, de modifier ou de supprimer des données RDF disponibles à travers Internet. SPARQL est l'équivalent de SQL pour le web. Il permet d'accéder aux données du Web des données. Cela signifie qu'en théorie, on pourrait accéder à toutes les données du Web avec ce standard. L'ambition du W3C est d'offrir une interopérabilité non pas seulement aux niveaux des services, comme avec les services Web, mais aussi aux niveaux des données structurées ou non qui sont disponibles à travers l'Internet. La version 1.1 est à privilégier.

W3C	SPARQL version 1.1 specification

Syntaxique	**Structuration de données**	
En observation	**KML**	Keyhole Markup Language
http://fr.wikipedia.org/wiki/Keyhole_Markup_Language KML est une notation XML destinée à la visualisation et l'annotation de données géographiques pour des navigateurs de type map ou earth sur internet. La visualisation n'inclut pas seulement la présentation graphique de données en 2D ou 3D sur le globe, mais aussi le contrôle par l'utilisateur de la navigation (où il va ? Et où il regarde).		
OGC	KML Implementation specification	

Syntaxique	**Structuration de données**	
Recommandé	**DOM**	Document Object Model
http://fr.wikipedia.org/wiki/Document_Object_Model DOM est un standard du W3C qui décrit une interface indépendante de tout langage de programmation et de toute plate-forme, permettant à des programmes informatiques et à des scripts d'accéder ou de mettre à jour le contenu, la structure ou le style de documents XML et HTML. Le document peut ensuite être traité et les résultats de ces traitements peuvent être réincorporés dans le document tel qu'il sera présenté.		
W3C	DOM Level 3 specification	

Syntaxique	**Structuration de données**	
En observation	**SIARD**	Software Independent Archiving of Relational Databases
http://www.bar.admin.ch/dienstleistungen/00823/01911/index.html?lang=fr Le standard SIARD est un format de fichier ouvert pour l'archivage des contenus de bases de données relationnelles. Le SIARD est développé par les Archives Fédérales Suisses (AFS), et est actuellement utilisé par plus d'une cinquantaine d'États. Il s'agit d'une description normative d'un format de fichier servant à la conservation à long terme de bases de données relationnelles. Le format SIARD repose notamment sur les normes ISO Unicode et XML et les normes industrielles SQL1999 et ZIP. L'utilisation de normes reconnues internationalement a pour but de garantir la conservation à long terme et l'accès au modèle très répandu de bases de données relationnelles.		
AFS	SIARD Formatspezifikation	

Syntaxique	**Structuration de données**	
Recommandé	**XMI**	XML Metadata Interchange

http://fr.wikipedia.org/wiki/XML_Metadata_Interchange XML Metadata Interchange (XMI) est un standard pour l'échange d'informations de métadonnées UML basé sur XML. La version 2.0 ou supérieure est recommandée.	
OMG ISO	OMG XMI Specification ISO 19503

Syntaxique	**Structuration de données**	
Recommandé	**OAIS**	Open Archival Information System
http://fr.wikipedia.org/wiki/Open_Archival_Information_System L'Open Archival Information System ou OAIS (Système ouvert d'archivage d'information) est un modèle conceptuel destiné à la gestion, à l'archivage et à la préservation à long terme de documents et de données numériques. Le modèle OAIS constitue une référence décrivant dans les grandes lignes les fonctions, les responsabilités et l'organisation d'un système qui voudrait préserver de l'information, en particulier des données numériques, sur le long terme, pour en garantir l'accès à une communauté d'utilisateurs identifiés. Le long terme est défini comme suffisamment long pour être soumis à l'impact des évolutions technologiques.		
ISO AFNOR	ISO 14721:2012 NF Z 42-013	

Syntaxique	**Structuration de données**	
Recommandé	**SEDA**	Standard d'échange de données pour l'archivage
http://www.archivesdefrance.culture.gouv.fr/seda/ Le standard d'échange de données pour l'archivage modélise les différentes transactions (transfert, modification, élimination, communication et restitution) qui peuvent avoir lieu entre des acteurs (service d'archives, service producteur, service versant, autorité de contrôle, utilisateur) dans le cadre de l'archivage de données. Le SEDA a fait l'objet d'une normalisation à l'AFNOR qui a abouti à la norme NF Z 44022 Modélisation des échanges de données pour l'archivage.		
SIAF AFNOR	https://references.modernisation.gouv.fr/archivage-numerique NF Z 44022	

Syntaxique	**Structuration de données**	**Description d'API**
En observation	**YAML**	YAML Ain't Markup Language ou encore Yet Another Markup Language
http://fr.wikipedia.org/wiki/YAML YAML est un format de représentation de données par sérialisation Unicode. Il reprend des concepts d'autres langages comme XML, ou encore du format de message électronique tel que documenté par RFC 2822. L'idée de fond de YAML est que toute donnée peut être représentée par une combinaison de listes, tableaux (de hachage) et données scalaires. YAML décrit ces formes de données (les représentations YAML), ainsi qu'une syntaxe pour présenter ces données sous la forme d'un flux de caractères (le flux YAML). La syntaxe YAML se distingue de JSON par le fait qu'il se veut plus facilement lisible par une personne. Il se distingue du XML par le fait qu'il s'intéresse d'abord à la sérialisation de données, et moins à la documentation.		

YAML	YAML Version 1.2

Syntaxique	**Structuration de données**	**Description d'API**
En observation	**RAML**	RESTful API Modeling Language
http://en.wikipedia.org/wiki/RAML_%28software%29 RAML est un langage basé sur YAML pour décrire des API RESTful. Il fournit toutes les informations nécessaires pour décrire des API RESTful ou presque-RESTful. RAML est capable de décrire les API qui ne respectent pas toutes les contraintes de REST (d'où le qualificatif « presque-RESTful »). Il encourage la réutilisation, permet la découverte et le partage de modèle, et vise à l'émergence fondé sur le mérite des meilleures pratiques.		
RAML Workgroup	RAML Specification	

Syntaxique	**Structuration de données**	**Identifiant**
Recommandé	**URI (UDI)**	Uniform Resource Identifier
http://fr.wikipedia.org/wiki/Uniform_Resource_Identifier URI définit une syntaxe permettant de construire un identifiant d'une ressource sur un réseau (par exemple une ressource Web) physique ou abstraite, sous la forme d'une courte chaîne de caractères.		
IETF	RFC 3986	

Syntaxique	**Structuration de données**	**Identifiant**
En observation	**ARK**	Archival Resource Key
http://fr.wikipedia.org/wiki/Archival_Resource_Key ARK est un système d'identifiants basé sur la norme URI assurant opacité, extensibilité et indépendance, c'est-à-dire les critères nécessaires pour garantir l'identification d'une ressource sur le long terme. Les ARK peuvent désigner des objets de n'importe quel type : textuels, images, logiciels, sites web, aussi bien que des objets physiques, comme des livres, des statues, et même des concepts immatériels. Une identification pérenne est nécessaire car les protocoles d'accès aux objets (par exemple HTTP ou FTP), aussi bien que les sites d'hébergement, sont sujets à modification. Un ARK contient une partie imperméable aux changements, et une partie flexible, qui désigne une forme de l'objet, ou un mode d'accès à celui-ci. L'idée est de créer un nom suffisamment stable pour être associé de façon permanente à un objet spécifique, et permettre ainsi d'agir sur l'objet identifié.		
BnF CDL	ARK ARK Identifiers	

Syntaxique	**Structuration de données**	**Identifiant**
En observation	**ISNI**	International Standard Name Identifier

http://fr.wikipedia.org/wiki/International_Standard_Name_Identifier L'identifiant ISNI (International Standard Name Identifier) est un identifiant international, normalisé, qui permet d'identifier de façon unique et pérenne des personnes et des organismes. L'identification internationale, unique, pérenne et fiable que propose l'ISNI est indispensable à l'échange et à la diffusion des données entre différents secteurs. Elle permet le dialogue des différentes briques logicielles qui composent des systèmes d'information très hétérogènes. Gérés par une agence internationale, les identifiants ISNI (International Standard Name Identifier) présentent toutes les caractéristiques nécessaires : ils sont normalisés (ISO 27729), internationaux, uniques et pérennes. Le système s'est imposé rapidement à l'échelle internationale, avec actuellement près de 9 millions d'entités identifiées dans la base de données. La France participe activement à sa définition, sa gouvernance et sa diffusion, notamment par le biais de la BnF, agence d'enregistrement.

BnF ISO	ISNI ISO 27729

Syntaxique	**Structuration de données**		**Géospatial**
Recommandé	**Shapefile ou SHP**	*fichier de formes*	
http://fr.wikipedia.org/wiki/Shapefile Le shapefile (SHP) est un format de fichier issu du monde des Systèmes d'Informations Géographiques (ou SIG). Ce format est un standard de facto, largement utilisé par un grand nombre de logiciels libres comme propriétaires			
ESRI	Shapefile technical description		

Syntaxique	**Structuration de données**		**Géospatial**
Recommandé	**GeoJSON**	Geographic JSON	
http://fr.wikipedia.org/wiki/GeoJSON GeoJSON est un format ouvert d'encodage d'ensemble de données géospatiales simples utilisant la norme JSON (JavaScript Object Notation).			
Domaine public	GeoJSON Format Specification		

Syntaxique	**Structuration de données**		**Géospatial**
Recommandé	**GeoSpatial-Metadata**	Geographic Information - Metadata	
http://fr.wikipedia.org/wiki/ISO_19115 http://en.wikipedia.org/wiki/Geospatial_metadata Ensemble de standards de référence pour la gestion de métadonnées associées aux objets qui ont une extension géographique implicite ou explicite. Utilisés dans la gestion de catalogue de ressources.			
ISO	ISO 19115 norme chapeau ISO 19110, ISO 19119, ISO 19139		

Syntaxique	**Structuration de données**	

Recommandé	**GML**	Geography Markup Language
http://fr.wikipedia.org/wiki/Geography_Markup_Language GML est un langage dérivé du XML pour encoder, manipuler et échanger des données géographiques. Le GML consiste en un ensemble de schémas XML qui définissent un format ouvert pour l'échange de données géographiques et permettent de construire des modèles de données spécifiques pour des domaines spécialisés, comme l'urbanisme, l'hydrologie ou la géologie. Le GML est interopérable avec toutes les spécifications OpenGIS de l'OGC telles que Web Map Service (WMS) ou Web Feature Service (WFS).		
OGC	Schémas GML	

Syntaxique	**Structuration de données**	**Carnet d'adresses**
Recommandé	**vCard**	Visit Card
http://fr.wikipedia.org/wiki/VCard vCard est un format standard ouvert d'échange de données personnelles. Il est utilisé par la plupart des : logiciels de carnet d'adresses (y compris dans les appareils mobiles), de courriel, de messagerie instantanée.		
IETF	RFC6350 , RFC6868	

Syntaxique	**Structuration de données**	**Calendrier**
Recommandé	**iCalendar ou iCal**	Internet Calendaring and Scheduling
http://fr.wikipedia.org/wiki/ICalendar iCalendar est un standard pour les échanges de données de calendrier. Connu aussi sous le nom d'iCal, il définit la structuration des données dans un fichier de type événement de calendrier.		
IETF	RFC 5545, RFC6868	

4.1.5 Traitement de données structurées

Syntaxique	**Traitement de données structurées**	
Recommandé	**XSLT**	Extensible Stylesheet Language Transformations
http://fr.wikipedia.org/wiki/Extensible_Stylesheet_Language_Transformations XSLT est un langage de transformation XML de type fonctionnel. Il permet notamment de transformer un document XML dans un autre format, tel PDF ou encore HTML pour être affiché comme une page web.		
W3C	XSL Transformations	

Syntaxique	**Traitement de données structurées**	
Recommandé	**XPath**	Xpath
http://fr.wikipedia.org/wiki/XPath XPath est un langage (non XML) permettant de localiser une portion d'un document XML.		
W3C	XML Path Language	

Syntaxique	**Traitement de données structurées**	

Recommandé	**XLink**	XLink
http://fr.wikipedia.org/wiki/XLink XLink permet de créer des liens entre fichiers XML ou portions de fichiers XML (grâce à XPointer). Contrairement aux liens entre fichiers HTML, XLink permet de créer des liens liant plus de deux fichiers.		
W3C	XML Linking Language	

Syntaxique	**Traitement de données structurées**	
Recommandé	**XQuery**	XQuery
http://fr.wikipedia.org/wiki/XQuery XQuery est un langage de requête informatique permettant non seulement d'extraire des informations d'un document XML, ou d'une collection de documents XML, mais également d'effectuer des calculs complexes à partir des informations extraites et de reconstruire de nouveaux documents ou fragments XML.		
W3C	XML Query Language	

Syntaxique	**Traitement de données structurées**	
Recommandé	**XInclude**	XInclude
http://en.wikipedia.org/wiki/XInclude Xinclude est un langage permettant d'inclure des fragments de documents XML dans un document XML.		
W3C	XML Inclusions	

Syntaxique	**Traitement de données structurées**	
Recommandé	**XPointer**	XPointer
http://fr.wikipedia.org/wiki/XPointer XPointer permet de désigner un fragment de document XML en ligne, c'est-à-dire lui-même désigné par une URL. XPointer utilise la syntaxe XPath, enrichie d'options permettant de désigner des portions de document (range).		
W3C	Xpointer Framework	

Syntaxique	**Traitement de données structurées**	
Recommandé	**XML Signature ou XMLDsig ou XML-Dsig ou XML-Sig**	XML Signature
http://fr.wikipedia.org/wiki/XML_Signature XML Signature (aussi nommé XMLDsig, XML-DSig, XML-Sig) est une recommandation du W3C destinée à permettre l'utilisation de signatures numériques dans les documents XML. Tout comme les techniques générales de cryptographie à clé publique qu'elle met en œuvre, elle permet d'assurer l'authentification, l'intégrité et par voie de conséquence la non-répudiation des données signées, mais en tirant profit de la souplesse offerte par le langage XML.		
W3C	XML Signature Syntax and Processing	

Syntaxique	Traitement de données structurées	Geospatial
En observation	**OpenLS**	Open Location Service
http://www.opengeospatial.org/standards/ols OpenLS spécifie les interfaces dans les procédures de géocodage.		
OGC	Open Location Service specification	

Syntaxique	Traitement de données structurées	Geospatial
En observation	**OWS Context**	OGC Web Services Context Document
http://www.opengeospatial.org/standards/owc Cette norme décrit les cas d'utilisation, les exigences et le modèle conceptuel pour la norme de codage de contexte OWS. L'objectif de cette norme est de fournir un modèle de base, qui est étendu et codé comme défini dans les extensions à cette norme. Un « document de contexte » spécifie un ensemble de services entièrement configuré qui peut être échangé (avec une interprétation uniforme) entre les clients supportant la norme. Le OWS Context a été créé pour permettre l'échange d'un ensemble de ressources d'information configurées entre des applications, principalement comme un ensemble de services. OWS Context est développé aussi pour du contenu en ligne. L'objectif est de facliter des usages comme la distribution de résultats de recherche, l'échange d'un ensemble de ressources telles que l'OGC Web Feature Services (WFS), Web Map Service (WMS), Web Map Tile Service (WMTS), Web Covergae Service (WCS) et d'autres dans une « image commune des opérations ».		
OGC	OWS Context documents	

Syntaxique	Traitement de données structurées	Geospatial
Recommandé	**SLD**	Styled Layer Descriptor
http://fr.wikipedia.org/wiki/Descripteur_de_style_de_couche SLD est un schéma XML afin de décrire le style, l'apparence, des couches de carte. Il est capable de traiter des données vectorielles et Raster. Une utilisation typique des SLD est destinée aux Web Map Service(WMS) pour que ces derniers puissent interpréter efficacement une couche de données spécifique.		
OGC	OGC SLD implementation specification	

4.1.6 Multimédia – formats et codec audio et vidéo

Les premiers standards concernent les formats ou conteneur vidéo. Il s'agit de format de fichier pouvant contenir divers types de données : flux vidéo et/ou audio (compressés à l'aide de codec), des sous-titres, des éléments de chapitrage, ainsi que d'autres métadonnées. 4 formats conteneurs ont été identifiés. Les standards correspondant aux codecs retenus sont ensuite listés avec les restrictions de combinaison entre formats et codecs.

Syntaxique	Multimédia	Conteneur Vidéo	
Recommandé	**MPEG-TS**	Moving Picture Expert Group – Transport Stream MPEG-2 partie 1	

https://fr.wikipedia.org/wiki/MPEG_Transport_Stream Le protocole MPEG-TS définit les aspects de transport à travers des réseaux pour la télévision numérique. Son but premier est de permettre le multiplexage de vidéo et d'audio, afin de synchroniser le tout. Un flux MPEG-TS peut comprendre plusieurs programmes audio/vidéo, ainsi que des données de description de programmes et de service. MPEG-TS comprend des fonctionnalités de correction d'erreur pour le transport sur média non-sûr, et est largement utilisé pour la télévision numérique terrestre, par câble ou par satellite. Notamment, les standards de diffusion DVB et l'ATSC font appel à MPEG-TS. C'est un équivalent au Program Stream, protocole visant lui les médias dit sûrs, comme le DVD.

ISO	ISO/CEI 13818-1

Syntaxique	**Multimédia**	**Conteneur Vidéo**	
Recommandé	**MP4**	Moving Picture Expert Group – 4 part 14 (ainsi que part 1)	
https://fr.wikipedia.org/wiki/MPEG-4_Part_14 MP4 est une partie de la norme MPEG-4 spécifiant un format conteneur pour encapsuler des données de type multimédia (audio ou vidéo essentiellement). L'extension de nom de fichier généralement associée à ce format est « .mp4 ». La description du format MP4 a d'abord été spécifiée en s'inspirant du format de fichier QuickTime (tel qu'il était spécifié en 2001), et intégrée dans la mise à jour de la « Part 1 » de MPEG-4 publiée en 2001 (dont le nom précis est ISO/CEI 14496-1:2001). En 2003, une mise à jour des spécifications est intégrée dans la « Part 14 ». La part 14 est donc une évolution de la part 1.			
ISO	ISO/CEI 14496-14		

Syntaxique	**Multimédia**	**Conteneur Vidéo**	
Recommandé	**MKV**	*Matroska, Matriochka* ou poupée russe	
http://fr.wikipedia.org/wiki/Matroska MKV est un format de fichier multimédia, multiplate-forme et ouvert. Le format MKV est un conteneur vidéo, il peut regrouper au sein d'un même fichier plusieurs pistes vidéo et audio ainsi que des sous-titres et des chapitres. MKV n'est donc pas un codec mais un format conteneur pouvant contenir des flux encodés avec les codecs			
Matroska	http://www.matroska.org/		

Syntaxique	**Multimédia**	**Conteneur Vidéo**	
En observation	**WebM**	WebM	

http://fr.wikipedia.org/wiki/WebM WebM est un format multimédia ouvert principalement destiné à un usage sur le web. Il est basé sur un conteneur dérivé de Matroska, et regroupe des flux vidéos encodés en VP8 et des flux audios encodés en Vorbis1. Ce format fait partie des formats vidéos proposés pour la balise <video> de HTML5. Il est amené à remplacer le premier format ouvert proposé, Theora, et fait concurrence au format H.264. Depuis juillet 2013, le format WebM est capable d'embarquer les successeurs audio et vidéo respectifs de VP8 & Vorbis que sont VP9 et Opus. Ce format de conteneur doit être utilisé avec les combinaisons de codecs suivantes : • VP8 et Vorbis • VP9 et Opus, ou, VP9 et Vorbis

Format ouvert	WebM Container Guidelines

Syntaxique	**Multimédia**	**Codec Vidéo**	
Recommandé	**VP8**		
https://fr.wikipedia.org/wiki/VP9 VP8 était le dernier codec vidéo de On2 Technologies qui a remplacé VP7, son prédécesseur. Il a été annoncé le 13 septembre 2008. Réalisé à l'origine dans un format propriétaire, il a été racheté par Google qui en a fait un format ouvert le 19 mai 2010 dans le cadre du projet WebM.			
IETF Google	RFC 6386		

Syntaxique	**Multimédia**	**Codec Vidéo**	
En observation	**VP9**	Next Gen Open Video, ou, VP Next, ou VP9	
https://fr.wikipedia.org/wiki/VP9 VP9 est un codec vidéo ouvert et sans redevance développé par Google. Au début, au cours de son développement, VP9 a été successivement nommé Next Gen Open Video (NGOV) et VP-Next. VP9 est le successeur de VP8 (créé par On2 avant que Google ne rachète l'entreprise). Chromium, Chrome, Firefox, et Opera supportent le format vidéo VP9 dans l'élément HTML5 video.			
Google	VP9		

Syntaxique	**Multimédia**	**Codec Vidéo**	
Recommandé	**H.264 ou MPEG-4 AVC, ou encore AVC**	H.264, ou MPEG-4 AVC (Advanced Video Coding)	
http://fr.wikipedia.org/wiki/H.264 H.264, ou MPEG-4 AVC (Advanced Video Coding), ou MPEG-4 Part 10, est une norme de codage vidéo adapté aux différents besoins de l'industrie (vidéophonie, streaming, télévision, mobile).			
ISO UIT	ISO/CEI 14496-10 UIT-T H.264		

Syntaxique	**Multimédia**	**Codec Vidéo**	
En observation	**H.265 ou HEVC**	H.265, ou High Efficiency Video Coding	

http://fr.wikipedia.org/wiki/H.265/HEVC HEVC, ou H.265 est une norme de codage vidéo finalisée depuis janvier 2013, devant succéder au H.264/MPEG-4 AVC (Advanced Video Coding). Ses applications concernent aussi bien la compression des vidéos en très haute définition (2K, 4K, 8K...) que la diminution du débit de transmission sur réseau pour les vidéos en définition standard avec des applications pour la vidéo sur mobile et pour l'extension de l'éligibilité aux services audiovisuels (TV, VoD...) des abonnés aux réseaux fixes (ADSL...).	
ISO UIT	ISO/IEC 23008- 2 UIT-T H.265

Syntaxique	**Multimédia**	**Conteneur Audio**	
Recommandé	**OGG**	OGG	
http://fr.wikipedia.org/wiki/Ogg OGG est un format de fichier multimedia conteneur. Il peut contenir des pistes audio, vidéo et texte (sous-titres). Il peut y avoir plusieurs pistes de chaque type pour, par exemple, proposer des médias multilingues. Ce format de conteneur est tout particulièrement à utiliser avec le codec audio Vorbis.			
Xiph	http://www.xiph.org/		

Syntaxique	**Multimédia**	**Audio**	
En observation	**Opus**	Opus Interactive Audio Codec	
https://fr.wikipedia.org/wiki/Opus_Interactive_Audio_Codec Opus (à l'origine *Harmony*) est un format ouvert de compression audio avec pertes, libre de redevances, développé par l'IIETF dans le but d'être utilisé par des applications interactives sur Internet. Opus est la proposition, en format standard, acceptée dans la compétition codec de l'IETF pour un « nouvel Internet à large bande audio », actuellement en développement par le groupe de travail IETF codec. Il est basé sur deux propositions standards, initialement séparées, de la Fondation Xiph.org et Skype Technologies : respectivement le codec CELT, à faible temps de latence, et le codec SILK, orienté sur la communication à distance. Ce codec audio peut-être utilisé dans les conteneurs vidéo et audio suivant : MPEG-TS, MP4, OGG, MKV.			
IETF	RFC 6716		

Syntaxique	**Multimédia**	**Audio**	
Recommandé	**MP3**	MPEG-1/2 Audio Layer 3	

http://fr.wikipedia.org/wiki/MPEG-1/2_Audio_Layer_3 MP3 est la spécification sonore du standard MPEG-1/MPEG-2. MP3 est un format de compression audio capable de réduire significativement la quantité de données nécessaire pour restituer de l'audio, mais qui, pour l'auditeur, ressemble à une reproduction du son original non compressé : avec une bonne compression la différence de qualité devenant difficilement perceptible. Alors que la lecture du format MP3 est possible sans restriction, la génération de fichiers au format MP3 est soumise à des restrictions de mise en œuvre : L'algorithme « MPEG-1 Layer 3 » décrit dans les standards fran ISO/CEI IS 11172-3 et ISO/CEI IS 13818-3 est soumis à des redevances (droits commerciaux). Ce codec est à éviter dans les formats conteneurs MPEG-TS et MP4. Il à privilégier dans les fichiers audio standalone.

IETF	RFC 3003, RFC 5219

Syntaxique	**Multimédia**	**Audio**	
Recommandé	**Vorbis**	Vorbis	
http://fr.wikipedia.org/wiki/Vorbis Vorbis est un algorithme de compression et de décompression audio numérique plus performant sur le plan de la qualité et du taux de compression que le format MP3, mais moins populaire que ce dernier. Ce codec audio est recommandé avec les formats conteneurs VP8 ou VP9.			
Xiph	Vorbis		

Syntaxique	**Multimédia**	**Audio**	
Recommandé	**AAC**	Advanced Audio Coding	
https://fr.wikipedia.org/wiki/Advanced_Audio_Coding AAC est un codec audio avec perte de données ayant pour but d'offrir un meilleur rapport qualité sur débit binaire que le format plus ancien MPEG-1/2 Audio Layer 3 (plus connu sous le nom de MP3). Le AAC, est une extension du MPEG-2 (ISO/IEC 13818-7) et a été amélioré avec l'avènement du MPEG-4 Version 1, 2 et 3 (ISO/IEC 14496-3) ; Il fait donc partie des extensions MPEG-2 Partie 7 et MPEG-4 Partie 3. Le codec AAC est à privilégier avec le format conteneur MP4 (il est d'ailleurs bien souvent le codec par défaut pour ce conteneur).			
ISO	ISO/IEC 13818-7 et ISO/IEC 14496-3		

Syntaxique	**Multimédia**	**Audio**	
Recommandé	**FLAC**	Free Lossless Audio Codec	
http://fr.wikipedia.org/wiki/Free_Lossless_Audio_Codec FLAC est un codec libre de compression audio sans perte. À l'inverse de codecs tels que MP3 ou Vorbis, il n'enlève aucune information du flux audio. Cette qualité maximale a pour conséquence une quantité d'information plus élevée.			
Xiph	FLAC Specification		

4.1.7 Multimédia – Image

Syntaxique	**Multimédia**	**Image**	

Recommandé	**TIFF**	Tagged Image File Format
http://fr.wikipedia.org/wiki/Tagged_Image_File_Format TIFF est un format de fichier pour image numérique. Il s'agit d'un format de conteneur (ou encapsulation), à la manière de « avi » ou « zip », c'est-à-dire pouvant contenir des données de formats arbitraires.		
Domaine public	TIFF specification	

Syntaxique	**Multimédia**	**Image**	
Recommandé	**GeoTIFF**	Geographical Tagged Image File Format	
http://fr.wikipedia.org/wiki/GeoTIFF Le GeoTIFF est un standard du domaine public permettant d'ajouter des informations de géoréférencement à une image TIFF (projection, système de coordonnées, datation, ...). L'enregistrement des métadonnées de géoréférencement utilise la possibilité offerte par le format TIFF de pouvoir définir de l'information additionnelle sous forme de tags spécifiques. Le format TIFF définit nativement un certain nombre de tags (voir les Métadonnées TIFF). L'objectif des spécifications du GeoTIFF consiste à permettre de décrire toute information cartographique associée à une image TIFF provenant d'un système d'imagerie satellite, de photographie aérienne scannée, de cartes scannées, de modèle d'élévation digital, ou du résultat d'analyse géographique.			
Domaine public	GeoTIFF format specification		

Syntaxique	**Multimédia**	**Image**	
Recommandé	**PNG**	Portable Network Graphics	
http://fr.wikipedia.org/wiki/Portable_Network_Graphics PNG est un format ouvert d'images numériques, non destructeur spécialement adapté pour publier des images simples comprenant des aplats de couleurs.			
IETF	RFC 2083		

Syntaxique	**Multimédia**	**Image**	
Recommandé	**JPEG**	Joint Photographic Experts Group	
http://fr.wikipedia.org/wiki/JPEG JPEG est une norme qui définit le format d'enregistrement et l'algorithme de décodage pour une représentation numérique compressée d'une image fixe. JPEG normalise uniquement l'algorithme et le format de décodage. Le processus d'encodage quant à lui est laissé libre à la compétition des industriels et des universitaires. La seule contrainte est que l'image produite doit pouvoir être décodée par un décodeur respectant le standard.			
ISO ITU-T www.jpeg.org	ISO/CEI 10918-1 ITU-T Recommendation T.81 JPEG Specification		

Syntaxique	Multimédia	Image	
En fin de vie	**JPEG 2000**	Joint Photographic Experts Group 2000	
http://fr.wikipedia.org/wiki/JPEG_2000 JPEG 2000 est une norme de compression d'images. Elle est capable de travailler avec ou sans perte, utilisant une transformée en ondelettes (méthode d'analyse mathématique du signal). Les performances de JPEG 2000 en compression avec et sans perte sont supérieures à celle de la méthode de compression JPEG ISO/CEI 10918-1. On obtient donc des fichiers d'un poids inférieur pour une qualité d'image égale. De plus, les contours nets et contrastés sont mieux rendus. JPEG normalise uniquement l'algorithme et le format de décodage. La méthode d'encodage est laissée libre à la concurrence des industriels ou universitaires, du moment que l'image produite est décodable par un décodeur standard. Outre ses performances en compression, JPEG 2000 apporte une multitude de nouvelles caractéristiques telles la scalabilité, les régions d'intérêt, la résistance aux erreurs de transmission, le codage sans pertes, la polyvalence de l'organisation des données, ainsi que les diverses extensions visant une application (interactivité, sécurité, sans fil, etc.) qui font l'intérêt de cette norme. Par ses fonctionnalités avancées, sa capacité à gérer les images de grande taille, ainsi que d'excellentes performances à haut débit, JPEG 2000 s'adresse aux professionnels de l'image, mais n'a pour l'instant que peu d'applications grand public.			
ISO UIT-T www.jpeg.org	ISO/CEI 15444-1 ITU-T Recommendation T.800 JPEG 2000 Specification		

Syntaxique	Multimédia	Image	
En fin de vie	**GIF**	Graphics Interchange Format	
http://fr.wikipedia.org/wiki/Graphics_Interchange_Format GIF est un format d'image numérique.			
W3C	GIF Specification		

Syntaxique	Multimédia	Image	
Recommandé	**SVG**	Scalable Vector Graphics	
http://fr.wikipedia.org/wiki/Scalable_Vector_Graphics SVG est un format de données conçu pour décrire des ensembles de graphiques vectoriels et basé sur XML.			
W3C	Scalable Vector Graphics		

4.1.8 Signature

Syntaxique	Signature		
Recommandé	**PAdES**	PDF Advanced Electronic Signature	
http://fr.wikipedia.org/wiki/PAdES PAdES est un ensemble de restrictions et d'extensions au format PDF et ISO 32000-1 pour permettre la signature électronique de document PDF.			
ETSI	PADES Baseline Profile		

Syntaxique	**Signature**		
Recommandé	**XAdES**	XML Advanced Electronic Signatures	
http://en.wikipedia.org/wiki/XAdES XAdES est un ensemble d'extensions à la recommandation XML-DSig qui permet la signature électronique avancée de document XML. XAdES définit six profils différents : XAdES Basic, XAdES-T, XAdES-C, XAdES-X, XadES-X-L et XAdES-A. Le profil utilisé et attendu lors de la mise en place d'échange doit absolument être explicité par les différentes parties.			
ETSI	XAdES Baseline Profile		

Syntaxique	**Signature**		
Recommandé	**CAdES**	CMS Advanced Electronic Signatures	
http://en.wikipedia.org/wiki/CAdES_%28computing%29 CAdES est un ensemble d'extensions pour Cryptographic Message Syntax (CMS) pour la signature électronique avancée de données.			
ETSI	CadES Baseline Profile		

Syntaxique	**Signature**		
Recommandé	**ASIC**	Associated Signature Containers	
ASIC permet l'utilisation de structures de conteneurs pour associer des signatures CadES ou WadES détachées ou des jetons d'horodatage, avec un ou plusieurs objets signés à laquelle elles s'appliquent.			
ETSI	Associated Signature Containers		

4.1.9 Message de sécurité

Syntaxique	**Message de sécurité**		
Recommandé	**IDMEF**	Intrusion Detection Message Exchange Format	
https://fr.wikipedia.org/wiki/Intrusion_Detection_Message_Exchange_Format Utilisé dans le cadre de la sécurité informatique, IDMEF est un format de données qui sert à échanger des rapports d'incidents entre les logiciels de détection d'intrusion, de prévention d'intrusion et de collecte d'informations de sécurité et les logiciels qui doivent interagir avec eux. Les messages IDMEF sont conçus pour pouvoir être traités facilement automatiquement. La RFC décrit un format et des procédures d'échange entre des sondes de détection d'intrusion et des outils de management qui consolident et corrèlent ces informations. Ce type de format est indispensable pour pouvoir comparer des informations émanant de différents outils et différents éditeurs autour d'une structure commune. Un objet IDMEF contient des dates (création, détection, etc.), une description de la source (IP, process, service, etc.), une description de la cible, une classification... Environ une centaine de champs sont disponibles.			
IETF	RFC 4765, RFC 4766		

Syntaxique	**Message de sécurité**	

Recommandé	**IODEF**	
IODEF définit un format de partage d'information entre équipe de centres de sécurité. Un objet IODEF décrit fonctionnellement un incident de sécurité et peut inclure des objets IDMEF qui en décrivent l'aspect "technique".		
IETF	RFC 5070	

5 Interopérabilité sémantique

5.1 Définitions des concepts

Le présent chapitre donne la définition à retenir par tous pour les principaux concepts liés à l'interopérabilité.

Terme / Concept	Définition
Agent	Un agent désigne une personne agissant au nom ou pour le compte d'une autorité administrative.
Autorité Administrative	Sont considérées comme autorités administratives: la Polynésie française, ses établissements publics, les autorités administratives indépendantes, les organismes de protection sociale et les autres organismes et personnes de droit public et de droit privé chargés d'une mission de service public administratif, ainsi que les administrations de l'État en Polynésie française et les communes polynésiennes, leurs groupements et leurs établissements publics.
Donnée	Une donnée est une description élémentaire de nature numérique, représentée sous forme codée, d'une réalité (chose, événement, mesure, transaction, etc.) en vue d'être : • collectée, enregistrée, • traitée, manipulée, transformée, • conservée, archivée, • échangée, diffusée, communiquée. Il peut être question de donnée structurée, semi-structurée ou non-structurée.
Données de référence	Parmi les données collectées, traitées, manipulées, ou échangées au sein du système d'information des services publics, certaines ont des caractéristiques particulières, au nombre de cinq. Il est question alors de données de référence. Les cinq caractéristiques sont les suivantes : • 1) ces données sont utilisées fréquemment par un grand nombre d'acteurs internes ou externes (organisations, métiers, processus, applications…). • 2) la qualité de ces données est critique pour un grand nombre de processus. Elle conditionne directement l'efficacité et l'efficience de ces processus, et donc plus globalement impacte le pilotage de l'action publique. • 3) la sémantique de ces données, c'est-à-dire la formalisation du sens et de la signification de ces données, est partagée et relativement stable dans le temps. L'unicité et la richesse sémantique de ces données est recherchée pour simplifier les processus, optimiser leurs exécutions, et apporter plus de valeur aux bénéficiaires de ces processus. La portée de ces données, c'est-à-dire la couverture d'usage de ces données, est également un critère clé dans leurs utilisations, et des incompréhensions sur cette portée

Terme / Concept	Définition
	peuvent impacter également l'efficacité des processus. Il faut noter qu'une sémantique stable ne signifie pas qu'une donnée est stable. Certaines données de référence varient beaucoup et souvent dans le temps. • 4) Ces données ont une durée de vie qui va au-delà des processus opérationnels qui l'utilisent. De fait, les données de contextualisation qui leur sont associées, c'est-à-dire leurs métadonnées, sont critiques. • 5) La facilité d'accès, la disponibilité de ces données et la rigueur de leur administration sont critiques. Elles conditionnent l'efficacité et l'efficience globale des solutions mises en place pour utiliser ou exploiter ces données : depuis n'importe où, tout le temps, et quel que soit le dispositif technique qui en a besoin. L'identification des données de référence est un sujet particulièrement sensible et conditionne l'efficacité des échanges et de l'exploitation de ces données (identifiant unique et partagé). L'interopérabilité des dispositifs d'accès à ces données est une condition de succès.
Fournisseur d'identité Fournisseur d'authentification	Un fournisseur d'identité est une autorité administrative, ou encore une entreprise privée, qui à la capacité à fournir une identité vérifiée d'une personne ou d'une unité légale, avec un moyen d'authentification permettant de valider l'authenticité de la personne ou unité légale qui souhaite accéder à un service. Le mode d'authentification peut prendre différentes formes, dont le niveau de preuve de l'authenticité peut varier selon les besoins de sécurisation et de confiance. Les deux fonctionnalités peuvent être séparées : Fournisseur d'Identité simple et Fournisseur d'Authentification simple. Dans ce cas, le Fournisseur d'authentification assure uniquement l'authenticité de la personne qui se connecte, par rapport à une identité qui elle est fournie par un Fournisseur d'Identité simple.
Fournisseur de données	Un fournisseur de données est une autorité administrative, ou une entreprise privée, détenteur de données d'intérêt pour l'écosystème public, au titre de ses missions, et qu'il met à disposition sous la forme d'API. Par exemple : la DGFiP pour le revenu fiscal de référence.
Fournisseur de données contextualisées ou agrégateurs de données ou encore hub de données	Un fournisseur de données contextualisées joue un rôle « d'intermédiation » entre un ou plusieurs fournisseurs de données et un ou plusieurs fournisseurs de services publics, dans le but de ; • éviter la multiplicité des liens directs entre tous les fournisseurs potentiels de données, et tous les fournisseurs de services, • permettre aux fournisseurs de données d'exposer de manière relativement « standardisée » et « brute » les

Terme / Concept	Définition
	informations dont ils disposent sans être dépendants de tous les besoins potentiels des fournisseurs de services souvent conditionnés par une réglementation rigoureuse « du droit à en connaître », • consolider ou filtrer des informations de plusieurs sources, • favoriser l'émergence rapide de nouveaux usages/services numériques s'appuyant sur des données déjà mises à disposition, • faciliter le suivi par l'usager des informations diffusées ou échangées, quelles que soient les interactions « utilisées ». • À ce titre, il doit assumer « la délégation de confiance » du(es) fournisseur(s) de données d'origine quant à la bonne transmission des informations et au respect des conditions d'accès à cette information.
Fournisseur de service	Un fournisseur de service est une autorité administrative, ou une entreprise privée, apte à délivrer ou à opérer un service, avec une composante numérique, de manière directe ou indirecte au profit des usagers. Par exemple : une mairie, qui rend des services pour la petite enfance.
Personne	Une personne est un unique être humain titulaire de droits et d'obligations caractérisé par une identité civile. Le terme « individu » est également utilisé pour désigner une personne Note : Une personne n'est pas nécessairement une "personne physique" dans le sens « unité légale » exerçant une activité économique. *UN/CEFACT definition : An individual human being.*
Service	Un service est un ensemble de prestations mises à disposition par un acteur (une personne ou un groupe de personnes), appelé fournisseur, dans le but de produire un effet pour le bénéfice d'un autre acteur, appelé client, selon des conditions prédéfinies d'exercice des prestations. Un service se définit donc par un ou plusieurs : • Fournisseur du service ; • Contrat qui définit les conditions d'exercice du service par le fournisseur ; • Produit qui est le résultat des prestations réalisées par le fournisseur pour le client ; • Interface qui définit les moyens par lesquels le service est rendu.
Unité légale ou Entité légale ou encore Entreprise	Une unité légale est une organisation qui a une existence juridique légale, et dotée de droits et devoirs. Une unité légale peut être : • Une « personne morale », dont l'existence est reconnue par la loi indépendamment des personnes ou des institutions

Terme / Concept	Définition
	qui la possèdent ou qui en sont membres. Une personne morale peut désigner donc une entreprise de droit privé, mais aussi une association ou encore une organisation de droit public ; • Une « personne physique » appelée aussi « entreprise individuelle » qui en tant qu'indépendant exerce une activité économique.
Utilisateur	Un utilisateur désigne une personne qui utilise une ou plusieurs applications informatiques d'une ou plusieurs autorités administratives. Il peut être interne à l'autorité administrative, un agent, ou externe : un partenaire, un usager, un fournisseur, etc. Un utilisateur peut agir pour son propre compte ou pour le compte d'une unité légale ou bien encore d'une autre personne.
Usager	Un usager désigne une personne ou une unité légale utilisatrice et/ou bénéficiaire d'un ou plusieurs services publics. Dans la segmentation des usagers, il est souvent fait distinction entre Personne, Entreprise, et Association.

5.2 Modélisation

Deux standards sont identifiés concernant les travaux de modélisation (quelque soit le niveau de modélisation : organisation, métier, processus, fonctionnel, applicatif ou encore infrastructure...).

Sémantique	**Modélisation**		
Recommandé	**UML**	Unified Modeling Language	
http://fr.wikipedia.org/wiki/UML_%28informatique%29 UML est un langage de modélisation unifié, à base de notation graphique standardisée. Il est utilisé en développement logiciel, et en conception orientée objet. Ce n'est pas une méthode de modélisation. Il est recommandé d'utiliser la modélisation comme outil de conception et de partage : pour modéliser des processus, des activités, des données ou des échanges. Il est recommandé d'utiliser la version 2.4 ou supérieure de UML pour ces travaux de modélisation.			
OMG	OMG Unified Modeling Language specification		

Sémantique	**Modélisation**		
Recommandé	**BPMN**	Business Process Model and Notation	
http://fr.wikipedia.org/wiki/Business_Process_Model_and_Notation Le Business Process Model and Notation (BPMN) est une notation graphique standardisée pour modéliser des procédures d'entreprise ou des processus métier. La version 2.0 est recommandée.			
OMG	OMG BPMN specification		

5.3 Description des formats pivots

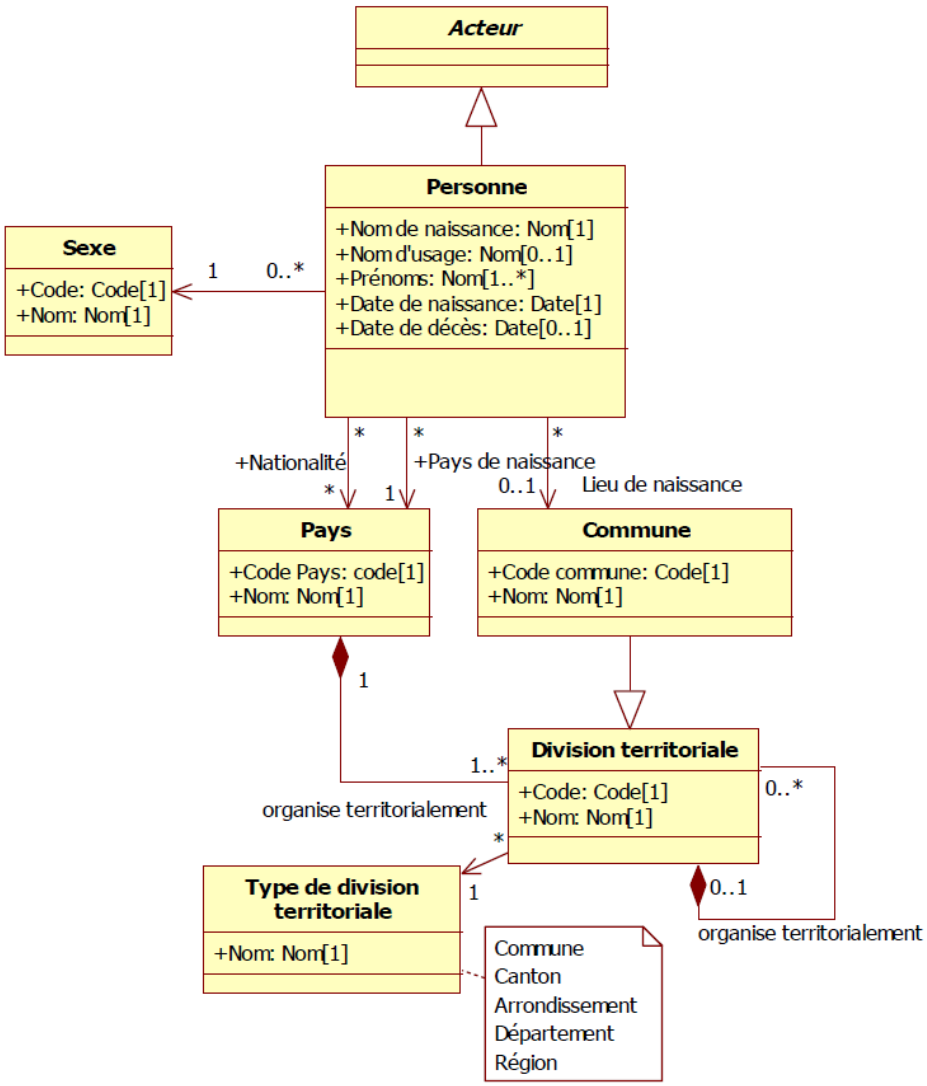
Il s'agit de décrire sous forme de format pivot (sémantique + syntaxe) les principaux objets métiers transverses échangés entre les autorités administratives et les usagers et entre les autorités administratives elles-mêmes.

Le présent paragraphe est un élément important pour l'interopérabilité mais son contenu est par nature évolutif dans les phases de mise en place, précis, dépendant éventuellement de nombreux autres standards. Il est donc difficile d'intégrer tous les éléments nécessaires dans un chapitre d'un document comme celui-ci. Il sera intégré au site web du RGI sous forme de ressources et de liens, notamment sous forme de schémas XML ou JSON réutilisables. Le présent document référence l'espace numérique où seront listés et décrits tous les formats pivots applicables dans tous les échanges. À titre d'illustration, le premier format pivot est intégré dans le présent document. Les travaux de l'*Association des développeurs et utilisateurs de logiciels libres pour les administrations et les collectivités* sur les formats pivots serviront de point de départ à l'enrichissement de ce chapitre. Les travaux ISA de la commission européenne *e-Government Core Vocabularies* est également une référence en la matière.

5.4 Identité pivot d'une personne

Sémantique	**Personne**		
Recommandé	**IdpPERS**	Identité Pivot d'une Personne	
L'identité pivot décrit la sémantique et le format à utiliser pour tous les échanges concernant les données d'identité qui caractérisent une personne et permettent de l'identifier			
DISIC	Le présent RGI		

La notion d'identité numérique est au cœur de la problématique d'interopérabilité des systèmes d'information de l'écosystème public. La présente version du RGI introduit la définition d'un point de vue sémantique et syntaxique, de l'identité pivot qui devrait être partagée par tous les fournisseurs (d'identité, de services ou de données). Il s'agit du minimum d'informations échangées (*minimum set of data*) concernant l'identité d'une personne.



Modèle UML de l'*Identité Pivot d'une Personne*

Le modèle UML ci-dessous présente les concepts concernés par l'identité d'une personne.

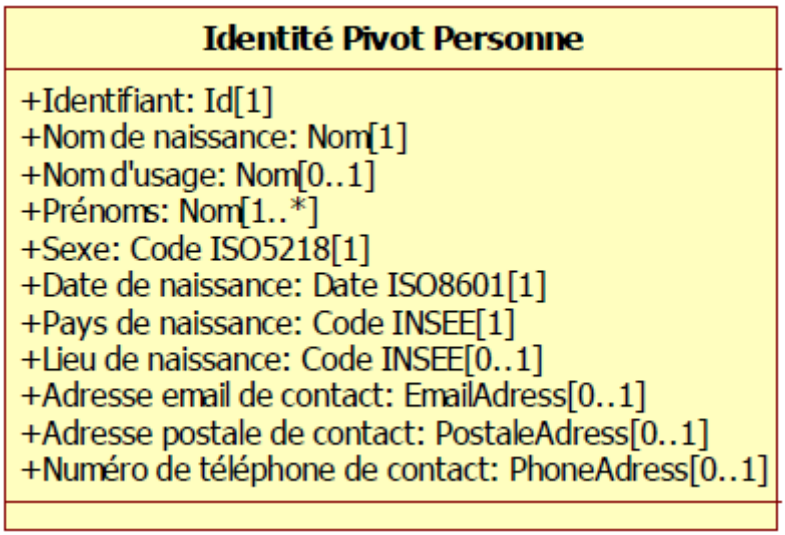
Définitions :

Objet	Définition
Personne	cf. 5.1 *En complément* : Une personne se caractérise par un ensemble d'informations qui caractérise son état civil : son sexe, sa localisation de naissance qui se compose principalement du pays de naissance, et pour les personnes nées en France, du département et de la commune (qui sont des éléments de division du territoire français).
Pays	Un pays désigne un territoire géographique habité, constituant une entité géographique et humaine. Il faut noter que les notions de Pays, de Nation et d'État peuvent sensiblement différer. Le Pays est une désignation géographique, une Nation désigne un peuple, alors qu'un État désigne les

Objet	Définition
	institutions fonctionnant sur un territoire. Le Code Géographique (COG) de l'INSEE identifie et codifie la liste des pays, reconnus par la France. Il faut également noter l'existence de la norme ISO 3166-2 qui codifie au niveau international l'ensemble des pays.
Division territoriale	Une division territoriale est un découpage du territoire d'un pays. Dans le cas de la France, les divisions territoriales peuvent jouter plusieurs rôles : circonscriptions administratives (lieux d'intervention de l'État à travers ses services déconcentrés), circonscription électorale (cadre dans lequel se tient un scrutin), collectivités territoriales (territoires dotés de la personnalité juridique et qui s'administrent librement). Si l'on prend le périmètre de la France métropolitaine, l'organisation territoriale du territoire est la suivante : Régions, départements, cantons, communes. Il existe également des regroupements de divisions territoriales : l'inter-région, ou les intercommunalités (métropole, communauté urbaine, communauté d'agglomérations, communauté de communes).
Sexe	Ensemble des caractéristiques anatomiques et des éléments fonctionnels distinguant le mâle de la femelle.

Format pivot d'échange :

Le schéma ci-après synthétise le format pivot retenu pour l'identité d'une personne.



Le tableau ci-dessous établit la correspondance avec les attributs du format pivot du règlement Européen eIDAS (Identification électronique et les services de confiance pour les transactions électronique au sein du marché intérieur) , le Minimum Data Set (MDS).

Nom du champ	Obligatoire	Format	Norme et nomenclature de référence

Nom du champ	Obligatoire	Format	Norme et nomenclature de référence
Identifiant de la personne eIDAS MDS Attributes : ***Unique Identifier***	Oui	Identifiant univoque de la personne dans le cadre eIDAS Identifiant unique de la personne dans le cadre de Fournisseur de service Français. String	UTF-8
Nom de naissance eIDAS MDS Attributes : ***Family Name at Birth***	Oui	String Au moins 1 lettre de l'alphabet. Constitué de : • Lettres de l'alphabet latin en majuscules ou minuscules ou accentuées, • Caractères spéciaux : espace, tiret, apostrophe. Type INSEE : *ChaineFrancaisOfficielType* [A-Za-zÀÂÄÇÉÈÊËÎÏÔÖÙÛÜŸàâäçéèêëîïôöùûüÿÆŒæœ\-']*	UTF-8
Prénoms eIDAS MDS Attributes : ***First Names at Birth***	Oui	String Au moins 1 lettre de l'alphabet. Constitué de : • Lettres de l'alphabet latin en majuscules ou minuscules ou accentuées, • Caractères spéciaux : tiret, apostrophe Les différents prénoms doivent être séparés par le caractère point virgule « ; ». Type INSEE : *ChaineFrancaisOfficielType* [A-Za-zÀÂÄÇÉÈÊËÎÏÔÖÙÛÜŸàâäçéèêëîïôöùûüÿÆŒæœ\-']*	UTF-8
Sexe eIDAS MDS Attributes : ***Gender***	Oui	Code Sexe international 0 = inconnu 1= homme 2 = femme 3 et 4 utilisés par l'INSEE pour les immatriculations en cours de personnes étrangères (\d{1}) Note : une correspondance avec le Code Sexe INSEE est possible avec masculin=M et féminin=F. Type INSEE : *SexeType* M|F	ISO 5218
Date de naissance eIDAS MDS	Oui	Date AAAA-MM-JJ Type INSEE : *DateType*	ISO 8601, format étendu

Nom du champ	Obligatoire	Format	Norme et nomenclature de référence
Attributes : ***Date of Birth***		(\d{4})-(\d{2})-(\d{2})	
Pays de naissance eIDAS MDS Attributes : ***Place of Birth***	Oui	Code du Pays de naissance ISO 3166-2 Type INSEE : *CodePaysIsoType* [A-Z]{2} Note : Une correspondance avec le Code du Pays du COG Type INSEE : *CodePaysouTerritoireEtrangerType* 99[0-9]{3}	ISO 3166-2 COG de l'INSEE
Lieu de naissance eIDAS MDS Attributes : ***Place of Birth***	Oui	Code de la Commune du COG Type INSEE : *CodeCommuneType* (([0-8][0-9AB])|(9[0-8AB]))[0-9]{3}	COG de l'INSEE
Nom d'usage eIDAS MDS Attributes : ***Current Family Name***	Non	String Au moins 1 lettre de l'alphabet. Constitué de : • Lettres de l'alphabet latin en majuscules ou minuscules ou accentuées, • Caractères spéciaux : espace, tiret, apostrophe. Type INSEE : *ChaineFrancaisOfficielType* [A-Za-zÀÂÄÇÉÈÊËÎÏÔÖÙÛÜŸàâäçéèêëîïôöùûüÿÆŒæœ\-']*	
Adresse courriel de contact	Non	Adresse courriel	RFC 3696
Adresse postale de contact eIDAS MDS Attributes : ***Current Address***	Non	Adresse postale Type INSEE : *AdressePostaleType*	
Adresse téléphonique de contact	Non	Numéro de téléphone Norme E.123 de l'ITU	E.123

6 Profil d'interopérabilité

6.1 Introduction

Un profil d'interopérabilité est un ensemble limité de standards, un groupe de spécification à utiliser dans un contexte opérationnel, un usage déterminé. L'objectif est d'aider aux choix de standard, cadrer l'utilisation des standards et éviter leur prolifération pour un usage donné. La liste des standards retenus pour un profil donné est donc volontairement limitative et correspond à un ensemble cohérent de fonctionnalités, de recommandations d'emploi à appliquer. **Ce chapitre constitue une première version d'identification et de définition des profils**. Il a vocation à être corrigé, complété et précisé dans le temps notamment sur les recommandations d'emplois des standards retenus : version, compatibilité entre standard, options à retenir, restrictions d'usage, points clés de mise en œuvre.

Dans le contexte d'usage du profil, le choix des standards doit s'effectuer parmi la liste proposée.

6.2 Synthèse des profils

Les profils retenus sont résumés dans le tableau ci-après.

n°	Pré-requis	Nom du Profil	Standards
P1	aucun	Fondations Polynésie Plateforme	IPv4/IPv6, TCP, HTTPS, CORS, TLS, URI, JSON, OData, Internet media type, SFTP, Javascript, HTML, ATOM, CSS, Oauth 2.0, Open ID Connect, CMIS, RDF, SPARQL, PDF, JPEG, WebM+VP9+Opus, RAML
P2	P1	Web service SOAP	SOAPv1.2, WSDL, MTOM, XOP, XML, XSD, UDDI, SAMLv2.0, WS-Security, WS-Addressing, XML Signature
P3	P1	Communication interpersonnelle et Bureautique	H.323, SIP, MGCP, XMPP, MKV, MP4, H.264, VP8, OGG, MP3, Vorbis, SVG, ZIP, 7z, SMTPS, POP3S, IMAP4S, iCal, vCard, PDF, ODF, EPUB3
P4	P1	Archivage	SEDA, OAIS, PDF/A, ODF, XML, SIARD, ZIP, TAR, FLAC, MIME
P5	P1	Géomatique	GML, KML, WFS, WMS, WCS, WPS, WMTS, CSW, GeoJSON, ATOM, Shapefile, GeoJSON, GeoSpatial-Metadata, OpenLS, OWS Context, GeoTIFF, JPEG 2000
P6	P2	Interopérabilité des Organismes de la Protection Sociale	InterOPS
P7	P1	Orchestration	WS-BPEL, WS-CDL
P8		Conception de système	UML, BPMN, XMI
P9	P1	Signature électronique	PAdES, XAdES, CAdES, ASIC

6.3 Description des profils

P1	**Fondations Polynésie Plateforme**	**aucun**
Recommandé	IPv4/IPv6, TCP, HTTPS, CORS, TLS, URI, JSON, OData, Internet media type, SFTP,	

P1	**Fondations Polynésie Plateforme**	**aucun**
	Javascript, HTML, ATOM, CSS, Oauth 2.0, Open ID Connect, CMIS, RDF, SPARQL, PDF, JPEG, WebM+VP9+Opus, RAML	

Le profil « Fondations Polynésie Plateforme » constitue le socle de base en matière d'interopérabilité pour tous les échanges de type A2C, A2B et A2A. Il concerne plus particulièrement les échanges entre : les usagers, les « fournisseurs de services », les « fournisseurs de données », et la brique mutualisée « FranceConnect » tels que définis dans la stratégie Etat Plateforme[1].

Le style d'architecture à retenir est REST - *Representational State Transfer. Ce n'est* ni un protocole ni un format, mais un ensemble de règles d'architecture. Ce style d'architecture doit respecter 6 contraintes suivantes :

- Client-serveur : les responsabilités sont séparées entre le client et le serveur. L'interface utilisateur est séparée de celle du stockage des données. Cela permet à ces deux interfaces d'évoluer indépendamment.
- Sans état : chaque requête d'un client vers un serveur doit contenir toute l'information nécessaire pour permettre au serveur de comprendre la requête, sans avoir à dépendre d'un contexte conservé sur le serveur. Cela libère de nombreuses interactions entre le client et le serveur, mais oblige le client à conserver localement toutes les données nécessaires au bon déroulement d'une requête sur un serveur.
- Mise en cache : le serveur envoie une réponse qui donne l'information sur la propension de cette réponse à être mise en cache, comme la fraîcheur, sa date de création, si elle doit être conservée dans le futur. Cela permet à des serveurs mandataires de décharger les contraintes sur le serveur et aux clients de ne pas faire de requêtes inutiles. Cela permet également d'améliorer l'extensibilité des serveurs.
- Une interface uniforme : cette contrainte agit selon 4 règles essentielles.
    - L'identification des ressources : chaque ressource est identifiée unitairement
    - La manipulation des ressources à travers des représentations : les ressources ont des représentations définies.
    - Un message auto-descriptif : les messages expliquent leur nature. Par exemple, si une représentation en HTML est codée en UTF-8, le message contient l'information nécessaire pour dire que c'est le cas.
    - Hypermédia comme moteur d'état de l'application : chaque accès aux états suivants de l'application est décrit dans le message courant.
- Un système hiérarchisé par couches : les états de l'application sont identifiés par des ressources individuelles. Toute l'information n'est pas envoyée dans une seule ressource unique. Les requêtes/réponses entre le client et le serveur augmentent et donc peuvent faire baisser la performance d'où l'importance de la mise en cache, etc. Le bénéfice est que cela rend beaucoup plus flexible l'évolution du système.
- Code-On-Demand (facultatif) : la possibilité pour les clients d'exécuter des scripts obtenus depuis le serveur. Cela permet d'éviter que le traitement ne se fasse que du côté serveur et permet donc de faire évoluer les fonctionnalités du client au cours du temps. En revanche cela réduit la visibilité de l'organisation des ressources. Un état devient dépendant du client et non plus du serveur ce qui contredit la règle 2. Il faut donc être prudent en utilisant cette contrainte.

Les termes REST et RESTful sont devenus des termes marketing pour rendre les services plus attractifs. Bien souvent, les services Web se réclamant de REST ne le sont pas. Tout au plus, ils appliquent le

[1]Se référer à la présentation de la stratégie Etat Plateforme disponible sur le site : http://references.modernisation.gouv.fr/strategie-du-si-de-letat

P1	Fondations Polynésie Plateforme	aucun
protocole HTTP de manière un peu plus conventionnelle. La communauté Web attachée aux principes de REST et la nature hypermedia des applications a décidé d'utiliser dorénavant le terme HATEOAS, qui est une abréviation pour Hypermedia as the Engine of Application State. La gestion des identités et des accès doit être mise en place par le protocole Open ID Connect (surcouche à Oauth 2.0). Ce profil n'a pas la prétention de couvrir tous les cas d'échanges. Les échanges entre systèmes nécessitant une gestion de type transactionnelle avec des structures de données complexe pourraient nécessiter des mécanismes complémentaires à ce profil (notamment le profil P2, ou dans la sphère de la « protection sociale » le profil P6).		

P2	Web service SOAP	P1
Recommandé	SOAPv1.2, WSDL, MTOM, XOP, XML, XSD, UDDI, SAMLv2.0, WS-Security, WS-Addressing, XML Signature, PRESTO 2.0	
Le profil « Web service SOAP » est un profil à la fois alternatif et complémentaire pour les mêmes types d'échanges que le profil Fondations Polynésie Plateforme. Le profil n°1 Fondations Polynésie Plateforme est recommandé, car plus simple dans sa mise en œuvre. Le profil n°2 ne peut être utilisé qu'en cas de difficultés technique à mettre en œuvre le profil n°1.		

P3	Communication interpersonnelle et Bureautique	P1
Recommandé	H.323, SIP, MGCP, XMPP, MKV, MP4, H.264, VP8, OGG, MP3, Vorbis, SVG, ZIP, 7z, SMTPS, POP3S, IMAP4S, iCal, vCard, PDF, ODF, EPUB3	
Ce profil regroupe tous les cas d'échange entre personnes (entre agents, entre usager et agent) de type messagerie, messagerie instantanée, audio ou visio conférence, etc. Ce profil porte également l'interopérabilité des échanges de documents entre personnes, ou entre systèmes et personnes. Les formats PDF et ODF doivent être considérés comme des formats pivots, le premier, PDF, pour les documents non modifiables, et le second, ODF, pour les documents modifiables. Ces choix n'imposent rien en termes de choix de logiciels de bureautique, mais uniquement sur les fonctions de conversion intégrées aux outils de travail collaboratif (fonction de conversion à la volée lors de l'insertion ou la récupération d'une pièce jointe dans un mail par exemple, ou à l'insertion d'un document dans un outil de partage, dans un réseau social d'entreprise, etc.).		

P4	Archivage	P1
Recommandé	SEDA, OAIS, PDF/A, ODF, XML, SIARD, ZIP, TAR, FLAC, MIME	

L'archivage numérique nécessite de prendre en compte les problématiques d'interopérabilité sur le moyen voire long terme et peut, dans certain cas, aller en contradiction avec les besoins de l'interopérabilité immédiate. Il repose sur une modélisation conceptuelle partagée au niveau internationale (OAIS).

D'un point de vue technique, cette interopérabilité repose sur la prise en compte des caractéristiques des supports physiques permettant la conservation des données, leur surveillance et leur migration sur d'autres supports ; elle concerne aussi la réplication des données/documents sur des sites distants.

D'un point de vue syntaxique, cette interopérabilité repose sur la prise en compte des caractéristiques de formats de documents/données et leur capacité à être prise en charge sur le moyen et le long terme.
On distingue trois catégories de formats dans le contexte de l'archivage numérique :

- Des formats de gestion et d'échange, pour les besoins d'interopérabilité immédiate avec des systèmes d'archivage : SEDA, ZIP, TAR, XML, JSON, CSV ;
- Des formats de diffusion/consultation, non pérennisables à long terme, mais utiles pour des besoins à court terme : JPEG, MP3 ;
- Des formats de conservation, considérés comme une garantie sur le moyen voire le long terme : MIME, TIFF, PDF/A, FLAC, ODF (pour conservation d'éléments dynamiques ou de calcul au-delà de la nature graphique du PDF, type tableur), SVG, CSV, JSON, XML, MP4. Les formats SIARD et JPEG 2000 sont en observation. Cette liste est non exhaustive et susceptible de modifications en fonction de l'état de l'art.

Pour les documents devant être conservés sur le long terme et enregistrés a posteriori dans un format de conservation, il est conseillé de conserver également une copie dans le format d'origine. Certains formats utilisés peuvent être des conteneurs qui acceptent des contenus avec différents codages. Sans pouvoir préciser tous ces codages, il est important d'en avoir conscience pour permettre d'effectuer des contrôles.

Ce profil précise plusieurs versions de format traduisant une grande variabilité cachée derrière les noms employés. Il est important de bien distinguer ces versions pour garantir un archivage pérenne.

P5	**Géomatique**	P1
Recommandé	GML, KML, WFS, WMS, WCS, WPS, WMTS, CSW, GeoJSON, ATOM, Shapefile, GeoJSON, GeoSpatial-Metadata, OpenLS, OWS Context, GeoTIFF, JPEG 2000, SLD	
L'information géographique présente une part importante des échanges entre les administrations. Le besoin de localiser des événements, des données, des activités, des objets est croissant pour une meilleure étude de l'impact des politiques publiques. Le présent profil identifie les principaux standards recommandés en la matière.		

P6	**InterOPS ou** **Interopérabilité des Organismes de la Protection Sociale**	P2
Recommandé	InterOPS	
Le profil InterOPS repose sur le standard InterOPS, qui s'appuie lui-même sur le profil « Web service SOAP » défini par la Direction de la Sécurité Sociale, et géré par le GIP MDS pour les échanges internes à la sphère Protection & Sécurité Sociale. Il est recommandé dans ce périmètre d'échange.		

P7	**Orchestration**	P2
Recommandé	WS-BPEL, WS-CDL	
Le profil Orchestration repose sur le profil « Fondations Etat Plateforme ». Il le complète avec les standards nécessaires à l'orchestration de l'exécution de services distribués.		

P8	**Conception de système**	P1
Recommandé	UML, BPMN, XMI	
La transformation du système d'information de l'Etat nécessite la coopération d'un grand nombre d'acteurs intervenant dans la définition, la conception, mais aussi la réalisation, l'intégration et l'exploitation de système. Le besoin d'échange entre ces acteurs d'éléments de conception est donc critique dans la réussite des projets de transformation. Il s'agit dans bien des cas d'éléments de modélisation (processus, données, échanges, architecture, etc.). Le profil « Conception de système » identifie les standards recommandés pour ces échanges.		

P9	**Signature électronique**	P1
Recommandé	PAdES, XAdES, CAdES, ASIC	
Ensemble des standards définissant les formats de signature électronique.		

7. ANNEXES

7 Tableaux de synthèses des standards

7.1 Technique

Niveau	Catégorie	Sous-Catégorie	Standards
Technique	Réseau		IPv6, IPSec
Technique	Transport		TCP, UDP, NTP, RTP, SRTP, RTCP, TLS (**Erreur ! Source du renvoi introuvable.**)
Technique	Session		SSH
Technique	Application	Transfert	HTTP, HTTPS, CORS, FTP, SFTP, R66, AMQP, AS2
Technique	Application	Exploitation	DNS, DNSSEC
Technique	Application	Accès	LDAP, LDAPS
Technique	Application	Multimédia	RTSP, H.323, SIP, MGCP
Technique	Application	Messagerie	SMTP, SMTPS, S/MIME, POP3, POP3S, IMAP4, IMAP4S, XMPP, XMPPS, WebRTC
Technique	Service	Identité & Authentification	OpenPGP, SAMLv2.0, Oauth 2.0, Open ID Connect
Technique	Service	Service web	SOAPv1.2, WSDL, UDDI, MTOM, XOP, WS-Security, WS-Addressing, InterOPS
Technique	Service	Orchestration de services	WS-BPEL, WS-CDL
Technique	Service	Géospatial	WMS, WFS, TJS, WMTS, CSW, WCS, WPS,

7.2 Syntaxique

Niveau	Catégorie	Sous-Catégorie	Standards
Syntaxique	Encodage	Caractère	UTF-8
Syntaxique	Encodage	Compression	Bzip2, gzip, ZIP, 7z, TAR
Syntaxique	Document		ODF, OOXML, DocBook, PDF, PDF/A, EPUB3
Syntaxique	Web		HTML, CSS, Internet media type, ATOM, APP, Javascript, CMIS
Syntaxique	Structuration des données		XML, EXI XSD, JSON, OData, LDIF, RDF, OWL2, SPARQL, KML, DOM, SIARD, XMI, OAIS, SEDA
Syntaxique	Structuration des données	Description d'API	YAML, RAML
Syntaxique	Structuration des données	Identifiant	URI, ARK, ISNI

Niveau	Catégorie	Sous-Catégorie	Standards
Syntaxique	Structuration des données	Géospatial	Shapefile, GeoJSON, GeoSpatial-Metadata, GML
Syntaxique	Structuration des données	Carnet d'adresse	vCard
Syntaxique	Structuration des données	Calendrier	iCalendar
Syntaxique	Traitement de données structurées		XSLT, XPath, XLink, XQuery, XInclude, XPointer, XML Signature
Syntaxique	Traitement de données structurées	Géospatial	OpenLS, OWS Context, SLD
Syntaxique	Multimedia	Conteneur vidéo	MPEG-TS, MP4, MKV, WebM
Syntaxique	Multimedia	Codec vidéo	VP8, VP9, H.264, H.265
Syntaxique	Multimedia	Conteneur audio	OGG
Syntaxique	Multimedia	Codec audio	Opus, MP3, Vorbis, AAC, FLAC
Syntaxique	Multimedia	Image	GeoTIFF, PNG, JPEG, SVG
Syntaxique	Signature		PAdES, XAdES, CAdES, ASIC
Syntaxique	Message de sécurité		IDMEF, IODEF

7.3 Profil

n°	Pré-requis	Nom du Profil	Standards
P1	aucun	Fondations Polynésie Plateforme	IPv4/IPv6, TCP, HTTPS, CORS, TLS, URI, JSON, OData, Internet media type, SFTP, Javascript, HTML, ATOM, CSS, Oauth 2.0, Open ID Connect, CMIS, RDF, SPARQL, PDF, JPEG, WebM+VP9+Opus, RAML
P2	P1	Web service SOAP	SOAPv1.2, WSDL, MTOM, XOP, XML, XSD, UDDI, SAMLv2.0, WS-Security, WS-Addressing, XML Signature
P3	P1	Communication interpersonnelle et Bureautique	H.323, SIP, MGCP, XMPP, MKV, MP4, H.264, VP8, OGG, MP3, Vorbis, SVG, ZIP, 7z, SMTPS, POP3S, IMAP4S, iCal, vCard, PDF, ODF, EPUB3
P4	P1	Archivage	SEDA, OAIS, PDF/A, ODF, XML, SIARD, ZIP, TAR, FLAC, MIME
P5	P1	Géomatique	GML, KML, WFS, WMS, WCS, WPS, WMTS, CSW, GeoJSON, ATOM, Shapefile, GeoJSON, GeoSpatial-Metadata, OpenLS, OWS Context, GeoTIFF, JPEG 2000

P6	P2	Interopérabilité des Organismes de la Protection Sociale	InterOPS
P7	P1	Orchestration	WS-BPEL, WS-CDL
P8		Conception de système	UML, BPMN, XMI
P9	P1	Signature électronique	PAdES, XAdES, CAdES, ASIC