ANNEXE 1

Référentiel général de sécurité

Historique des versions		
Date	**Version**	**Évolution du document**
18/10/2018	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 5
Chapitre 2. Description des étapes de la mise en conformité 6
2.1 Analyse des risques 6
2.2 Définition des objectifs de sécurité 6
2.3 Choix et mise en œuvre des mesures de sécurité adaptées 6
2.4 Homologation de sécurité du système d'information 7
2.5 Suivi opérationnel de la sécurité du système d'information 7
Chapitre 3. Règles relatives à la cryptographie et à la protection des échanges électroniques 8
3.1 Règles relatives à la cryptographie 8
3.2 Règles relatives à la protection des échanges électroniques 8
a. Règles relatives aux certificats électroniques 8
b. Règles relatives à l'horodatage électronique 10
Chapitre 4. Règles relatives aux accusés d'enregistrement et aux accusés de réception 11
Chapitre 5. Qualification des produits de sécurité et des prestataires de services de confiance 12
5.1 Qualification des produits de sécurité 12
5.2 Qualification des prestataires de services de confiance (PSCO) 12
Chapitre 6. Recommandations relatives à l'application du référentiel 13
6.1 Organiser la sécurité des systèmes d'information 13
a. Organiser les responsabilités liées à la sécurité des systèmes d'information 13
b. Mettre en place un système de management de la sécurité des systèmes d'information 13
c. Élaborer une politique de sécurité des systèmes d'information 13
6.2 Impliquer les instances décisionnelles 13
6.3 Adapter l'effort de protection des systèmes d'information aux enjeux de sécurité et prendre en compte la SSI dans les projets 13
6.4 Adopter une démarche globale 14
6.5 Informer et sensibiliser le personnel 14
6.6 Prendre en compte la sécurité dans les contrats et les achats 14
6.7 Prendre en compte la sécurité dans les projets d'externalisation et d'informatique en nuage 15
6.8 Mettre en place des mécanismes de défense des systèmes d'information 15
6.9 Utiliser les produits et prestataires labellisés pour leur sécurité 15
6.10 Élaborer des plans de traitement d'incidents ainsi que de continuité et de reprise d'activité 16
6.11 Procéder à des audits réguliers de la sécurité du système d'information 16
6.12 Réaliser une veille sur les menaces et les vulnérabilités 16
6.13 Favoriser l'interopérabilité 16
6.14 Appliquer des mesures respectueuses de la protection des données à caractère personnel 16
Chapitre 7. Liste des annexes du RGS 18
7.1 Documents applicables concernant l'utilisation de certificats électroniques 18
7.2 Documents applicables concernant l'utilisation de mécanismes cryptographiques 18
7.3 Référentiel d'exigences applicables aux prestataires d'audit de la SSI 18
7.4 Guide d'homologation 18
Chapitre 8. Références techniques 19

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.