



Premier ministre	
Agence nationale de la sécurité des systèmes d'information (ANSSI)	Secrétariat général pour la modernisation de l'action publique (SGMAP)

RÉFÉRENTIEL GÉNÉRAL DE SÉCURITÉ

version 2.0

HISTORIQUE DES VERSIONS		
DATE	VERSION	ÉVOLUTION DU DOCUMENT
06/05/2010	1.0	<i>Publication de la première version du Référentiel général de sécurité</i>
13/06/2014	2.0	<i>Publication de la deuxième version du Référentiel général de sécurité</i>

Les commentaires sur le présent document sont à adresser à :

<p>Agence nationale de la sécurité des systèmes d'information SGDSN/ANSSI Bureau de la maîtrise des risques et de la réglementation 51 boulevard de La Tour-Maubourg 75700 Paris 07 SP rgs [at] ssi.gouv.fr</p>

Le présent référentiel ainsi que les annexes sont disponibles en ligne sur les sites suivants :

- le site institutionnel de l'ANSSI (www.ssi.gouv.fr) ;
- le site institutionnel du SGMAP (www.referencesssi.gouv.fr).

Le présent référentiel est pris en application du décret n° 2010-112 du 2 février 2010, lui-même pris pour l'application des articles 9, 10 et 12 de 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. Il est publié par l'arrêté du 13 juin 2014 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques.

Ce référentiel remplace la première version du référentiel général de sécurité publiée par arrêté du Premier ministre le 6 mai 2010. Il complète les règles et les recommandations relatives aux certificats électroniques et contremarques de temps et permet la qualification des prestataires d'audit de la sécurité des systèmes d'information. Les mécanismes de transition entre la première et la deuxième version du référentiel sont décrits dans le chapitre 8 du présent document.

Il fait l'objet de recommandations de mise en œuvre décrites sur la page <http://www.ssi.gouv.fr/fr/reglementation-ssi/referentiel-general-de-securite/recommandations-relatives-a-la-mise-en-oeuvre-du-rgs.html>.

Les termes entre « [] » renvoient aux références documentaires décrites dans le chapitre 10 du présent document.

Référentiel général de sécurité			
Version du RGS	Date	Critère de diffusion	Page
2.0	13 juin 2014	PUBLIC	2/25

Sommaire

Chapitre 1.	Mise en conformité avec les exigences du « décret RGS ».....	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
Chapitre 4.	Règles relatives aux accusés d'enregistrement et aux accusés de réception	12
Chapitre 5.	Qualification des produits de sécurité et des prestataires de services de confiance .	13
5.1	Qualification des produits de sécurité.....	13
5.2	Qualification des prestataires de services de confiance (PSCO)	13
Chapitre 6.	Validation des certificats par l'État.....	15
6.1	Champ d'application.....	15
6.2	Règles de sécurité	15
6.3	Procédure de validation	16
6.4	Liste des informations relatives à la délivrance et à la validation	16

Référentiel général de sécurité			
Version du RGS	Date	Critère de diffusion	Page
2.0	13 juin 2014	PUBLIC	3/25

Chapitre 7. <i>Recommandations relatives à l'application du référentiel</i>	17
7.1 Organiser la sécurité des systèmes d'information _____	17
7.2 Impliquer les instances décisionnelles _____	17
7.3 Adapter l'effort de protection des systèmes d'information aux enjeux de sécurité et prendre en compte la SSI dans les projets _____	18
7.4 Adopter une démarche globale _____	18
7.5 Informer et sensibiliser le personnel _____	18
7.6 Prendre en compte la sécurité dans les contrats et les achats _____	18
7.7 Prendre en compte la sécurité dans les projets d'externalisation et d'informatique en nuage _____	19
7.8 Mettre en place des mécanismes de défense des systèmes d'information _____	19
7.9 Utiliser les produits et prestataires labellisés pour leur sécurité _____	20
7.10 Élaborer des plans de traitement d'incidents ainsi que de continuité et de reprise d'activité _____	20
7.11 Procéder à des audits réguliers de la sécurité du système d'information _____	20
7.12 Réaliser une veille sur les menaces et les vulnérabilités _____	21
7.13 Favoriser l'interopérabilité _____	21
Chapitre 8. <i>Transition entre la première et la deuxième version du RGS</i>	22
Chapitre 9. <i>Liste des annexes du RGS</i>	23
9.1 Documents applicables concernant l'utilisation de certificats électroniques _____	23
9.2 Documents applicables concernant l'utilisation de mécanismes cryptographiques _____	23
9.3 Référentiel d'exigences applicables aux prestataires d'audit de la SSI _____	23
Chapitre 10. <i>Références documentaires</i>	24
10.1 Références réglementaires _____	24
10.2 Références techniques _____	24

Référentiel général de sécurité			
Version du RGS	Date	Critère de diffusion	Page
2.0	13 juin 2014	PUBLIC	4/25

Chapitre 1. Mise en conformité avec les exigences du « décret RGS »

Le référentiel général de sécurité (RGS) vise à renforcer la confiance des usagers dans les services électroniques 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 le décret n° 2010-112 du 2 février 2010 (décret RGS) :

1. réalisation d'une analyse des risques (art. 3 al. 1) ;
2. définition des objectifs de sécurité (art. 3 al. 2) ;
3. choix et mise en œuvre des mesures appropriées de protection et de défense du SI (art. 3 al. 3) ;
4. homologation de sécurité du système d'information (art. 5) ;
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. décision d'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. 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 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 sur la documentation produits par l'ANSSI.

Référentiel général de sécurité			
Version du RGS	Date	Critère de diffusion	Page
2.0	13 juin 2014	PUBLIC	5/25

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 de la menace et des enjeux.

La démarche d'analyse de risques consiste à identifier les événements 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 menaces¹ 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) 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 2010, afin de formuler précisément ces objectifs de sécurité.

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. 3, al. 3 du décret RGS). 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).

¹ Une menace est considérée par le ISO/CEI Guide 73 : 2002 comme une « cause potentielle d'un incident indésirable, pouvant entraîner des dommages au sein d'un système et d'un organisme ».

Référentiel général de sécurité			
Version du RGS	Date	Critère de diffusion	Page
2.0	13 juin 2014	PUBLIC	6/25

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 l'ordonnance du 8 décembre 2005 doivent faire l'objet, avant leur mise en service opérationnelle, d'une décision d'homologation de sécurité.

Egalement dénommée « attestation formelle » (art. 5, al. 1 du décret RGS), elle est prononcée par une *autorité d'homologation*, désignée par la ou les autorités administratives chargées du système d'information².

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.

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 peuvent utiliser les recommandations décrites dans le guide publié par l'ANSSI [Guide homologation].

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 vite 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, à mener des audits réguliers, à appliquer des mesures correctives après un audit ou un incident, à mettre en œuvre une chaîne d'alerte en cas d'intrusion supposée ou avérée sur le système, à gérer les droits d'accès des utilisateurs, 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.

² Elle diffère de l'homologation prononcée sur le fondement de l'IGI 1300 pour les systèmes d'informations traitant des informations classifiées de défense.

Référentiel général de sécurité			
Version du RGS	Date	Critère de diffusion	Page
2.0	13 juin 2014	PUBLIC	7/25

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 et 7.

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, le Premier ministre recommande l'usage de produits qualifiés quand ils existent.

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]).

Référentiel général de sécurité			
Version du RGS	Date	Critère de diffusion	Page
2.0	13 juin 2014	PUBLIC	8/25

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

L'authentification³ a pour but de vérifier l'identité dont se réclame une personne ou une machine. 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 actes administratifs au sens de l'ordonnance du 8 décembre 2005 :

Conformément à l'article 8 de l'ordonnance du 8 décembre 2005, les autorités administratives doivent respecter les exigences du RGS lorsqu'elles mettent en œuvre, pour la signature de leurs actes administratifs, 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 administratifs qu'elle émet. Elle doit respecter les règles définies au présent chapitre.

Cas particulier de la signature « présumée fiable » au sens de l'article 1316-4 du Code civil :

Les exigences techniques définies en annexe de l'arrêté du 26 juillet 2004, et portant sur la délivrance de certificats électroniques dits « *qualifiés* » au sens du décret n° 2001-272 du 30 mars 2001, sont requises pour la génération de signatures électroniques « *présument fiables* » au sens de ce décret.

³ S'identifier consiste à communiquer une identité préalablement enregistrée, s'authentifier consiste à apporter la preuve de cette identité. L'authentification est généralement précédée d'une identification.

Référentiel général de sécurité			
Version du RGS	Date	Critère de diffusion	Page
2.0	13 juin 2014	PUBLIC	9/25

Ces exigences constituent un sous-ensemble de celles contenues dans le document [RGS_A2] pour le niveau de sécurité (***) de la fonction signature électronique, qui prévoit des exigences supplémentaires, essentiellement en matière de format et de variables de temps.

De ce fait, une signature électronique sécurisée au sens de l'article 1^{er} du décret n° 2001-272 du 30 mars 2001, établie avec un dispositif sécurisé de création de signature certifié conforme dans les conditions de l'article 3 et mettant en œuvre des certificats de signature électronique conformes au niveau de sécurité (***) de [RGS_A2], est *de facto* « présumée fiable » selon ce décret et donc au sens de l'article 1316-4 du code civil.

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.

Référentiel général de sécurité			
Version du RGS	Date	Critère de diffusion	Page
2.0	13 juin 2014	PUBLIC	10/25

Cas particulier de l'horodatage « présumé fiable », au sens des articles 1369-7 et 1369-8 du code civil

Le prestataire qui souhaite proposer un service d'horodatage bénéficiant de la présomption de fiabilité des articles 1369-7 et 1369-8 du code civil doit respecter les exigences techniques définies dans les articles 3 et 4 du décret n° 2011-434 du 20 avril 2011. Le prestataire peut utiliser un module d'horodatage qui doit avoir été certifié dans les conditions prévues dans le décret n° 2002-535 du 18 avril 2002 et peut avoir été qualifié selon les formes décrites dans l'arrêté du 20 avril 2011 relatif à la reconnaissance de la qualification des prestataires de services d'horodatage électronique et à l'accréditation des organismes qui procèdent à leur évaluation.

Les exigences du document [RGS_A5] constituent un sous-ensemble de celles contenues dans le décret 20 avril 2011, qui prévoit quelques exigences supplémentaires de certification des unités d'horodatage. De ce fait, un horodatage « présumé fiable » au sens de ce décret et des articles 1369-7 et 1369-8 du code civil est *de facto* conforme aux exigences du document [RGS_A5].

c Rattachement à l'infrastructure de gestion de la confiance de l'administration (IGC/A)

L'ANSSI offre, parallèlement au RGS, un service de certification électronique qui consiste à signer l'*autorité de certification* (AC) racine d'une autorité administrative par l'AC de l'infrastructure de gestion de la confiance de l'administration - IGC/A.

Les utilisateurs qui doivent se fier à des certificats délivrés par ou à cette autorité administrative ou à ses agents ont la garantie que ces certificats ont fait l'objet d'une vérification de la chaîne de certification jusqu'au certificat de AC « IGC/A »⁴.

L'ANSSI est l'autorité racine de l'IGC/A.

Les règles relatives à la mise en œuvre de l'IGC/A sont définies dans les politiques de certification de l'IGC/A [PC_IGC/A].

⁴ Les certificats racines de l'AC « IGC/A » ont fait l'objet d'un avis publié au Journal officiel. Lorsque ces certificats sont intégrés dans les logiciels installés sur les ordinateurs des utilisateurs, la vérification de la chaîne de certification est alors automatique (sous réserve de la bonne configuration du logiciel).

Référentiel général de sécurité			
Version du RGS	Date	Critère de diffusion	Page
2.0	13 juin 2014	PUBLIC	11/25

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

L'article 5 de l'ordonnance du 8 décembre 2005 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 5 de l'ordonnance du 8 décembre 2005 :

- 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].

Dans le cas particulier où les accusés sont émis en application des dispositions prévues à l'article 5.II de l'ordonnance du 8 décembre 2005, la date figurant sur les accusés doit faire foi, ce qui impose de garantir aux usagers un niveau de fiabilité supplémentaire. Les autorités administratives doivent en tenir compte dans leur besoin de sécurité et donc dans le choix des fonctions de sécurité et des niveaux de sécurité associés.

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.

Référentiel général de sécurité			
Version du RGS	Date	Critère de diffusion	Page
2.0	13 juin 2014	PUBLIC	12/25

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

Conformément à l'article 4 du décret RGS, les autorités administratives qui décident de recourir à des produits ou prestations de services visés par le RGS recourent à des produits de sécurité et à des prestataires de service de confiance qualifiés ou, à défaut, s'assurent de la conformité au RGS des produits de sécurité et services de confiance qu'elles choisissent.

Dans ce cas, elle attestent formellement de la conformité au RGS de ces produits de sécurité et services de confiance. Elles adressent ces attestations à l'ANSSI.

5.1 Qualification des produits de sécurité

La qualification de produits de sécurité prévoit trois niveaux de qualification :

- qualification *élémentaire* (décrite dans le document [QE]) ;
- qualification *standard* (décrite dans le document [QS]) ;
- qualification *renforcée* (décrite dans le document [QR]).

Un produit de sécurité est qualifié s'il a fait l'objet d'une attestation de qualification et d'un maintien de conditions de sécurité conforme aux procédures décrites dans les documents [QE], [QS] et [QR]. L'ANSSI instruit les demandes et délivre les attestations de qualification. La procédure de qualification repose sur une certification préalable, dans les formes prévues par le décret n° 2002-535 du 18 avril 2002 et par l'instruction n° 1414/ANSSI/SR du 30 mai 2011 relative à la *certification de sécurité de premier niveau des produits des technologies de l'information* (CSPN).

Le niveau *élémentaire* est accordé sur la base d'une CSPN. Les niveaux *standard* et *renforcé* le sont sur la base d'une certification « *Critères communs* ». Cependant, s'agissant d'un label spécifique pour l'administration, l'ANSSI procède à des contrôles complémentaires. Elle valide ainsi la cible de sécurité au regard des besoins de l'administration et réalise ou fait réaliser des tests relatifs à la cryptologie et son implémentation, sur la base des annexes B du RGS.

Pour garantir la cohérence des objectifs et des exigences de sécurité, il est recommandé que la cible de sécurité soit, autant que possible, conforme à un des profils de protection proposés par l'ANSSI (www.ssi.gouv.fr/fr/certification-qualification/cc/profils-de-protection/). L'ANSSI publie également le catalogue des produits de sécurité qualifiés : www.ssi.gouv.fr/fr/produits-et-prestataires/produits-qualifies/.

5.2 Qualification des prestataires de services de confiance (PSCO)

Les prestataires de services peuvent éventuellement appartenir à plusieurs catégories distinctes de PSCO. Ils doivent alors obtenir une qualification pour chaque type de prestation.

L'attestation de qualification est délivrée par un *organisme de qualification*, à l'issue d'une évaluation de la conformité du PSCO aux exigences du RGS qui lui sont applicables. Ces exigences sont présentées sous forme de référentiels annexés au RGS (annexes A et C). Les organismes de qualification sont, eux-mêmes, accrédités par le Comité français d'accréditation (COFRAC) et habilités par l'ANSSI, conformément à l'instruction n°1001/ANSSI/SR du 8 avril 2011

Lorsque le PSCO est une administration de l'État, l'ANSSI peut procéder elle-même à son évaluation et à sa qualification.

Dans tous les cas, la qualification est accordée pour une durée de trois ans.

La liste des organismes de qualification habilités et des PSCO qualifiés est publiée par l'ANSSI : www.ssi.gouv.fr/fr/produits-et-prestataires/prestataires-de-services-de-confiance-qualifies/

Référentiel général de sécurité			
Version du RGS	Date	Critère de diffusion	Page
2.0	13 juin 2014	PUBLIC	13/25

Les catégories de PSCO visées dans la présente version du RGS sont :

a Les prestataires de services de certification électronique

Les référentiels d'exigences applicables aux *prestataires de services de certification électronique* (PSCE) figurent en annexes A2 et A3, respectivement appelées « *politique de certification type – certificats électroniques de personnes* » et « *politique de certification type – certificats électroniques de services applicatifs* ».

Ces référentiels distinguent trois niveaux de sécurité, aux exigences croissantes : (*), (**) et (***). Ils visent distinctement les usages de chiffrement, d'authentification de personne, de signature électronique, d'authentification de machine et de cachet, ainsi que le double usage authentification et signature électronique.

Il est recommandé que les prestataires de services de certification électronique réalisent les démarches nécessaires à l'intégration de leurs certificats dans les principaux navigateurs. Les PSCE peuvent proposer des offres conformes aux différentes versions du RGS. Les qualifications relatives aux offres conformes à la première version du RGS seront caduques à l'issue de la période de 4 ans d'acceptation des certificats de ces offres prévue au chapitre 8 du présent document, relatif à la transition entre la première et la deuxième version du RGS.

b Les prestataires de services d'horodatage électronique

Le référentiel d'exigences applicable aux *prestataires de services d'horodatage électronique* (PSHE), qui prévoit un niveau de sécurité unique, figure en annexe A5, appelée « *politique d'horodatage type* ».

c Les prestataires d'audit de la sécurité des systèmes d'information

Le référentiel d'exigences applicables aux prestataires d'audit de la sécurité des systèmes d'information figure en annexe C du RGS. Il couvre les activités d'audit organisationnel, de code source, de configuration et d'architecture, ainsi que les tests d'intrusion.

Référentiel général de sécurité			
Version du RGS	Date	Critère de diffusion	Page
2.0	13 juin 2014	PUBLIC	14/25

Chapitre 6. Validation des certificats par l'État

6.1 Champ d'application

Les certificats électroniques délivrés aux autorités administratives et à leurs agents doivent être validés par l'État (art. 10 de l'ordonnance du 8 décembre 2005 et chapitre V du décret RGS), afin de garantir que leurs porteurs sont bien les autorités administratives ou les agents identifiés.

La procédure de validation est mise en œuvre par l'ANSSI (art. 21 du décret RGS). Elle consiste à vérifier que leur procédure de délivrance est conforme aux règles fixées au § 6.2⁵.

Elle concerne les certificats mis en œuvre dans le but d'assurer les fonctions de sécurité suivantes :

- authentification d'une personne et d'un serveur ;
- signature électronique et cachet ;
- confidentialité.

Conformément aux *politiques de certification types* (PC-Types) mentionnées au chapitre 3, la procédure de délivrance de certificats recouvre les aspects suivants :

- l'identification et la vérification de l'identité des agents à qui seront délivrés des certificats ;
- la fabrication technique des certificats ;
- la remise des certificats aux porteurs ;
- la publication (ou mise à disposition) des certificats, de leur statut et de la politique de certification ;
- la révocation et le renouvellement des certificats.

Lorsqu'elle met en place une procédure de délivrance de certificats, une autorité administrative s'appuie sur une *autorité de certification* (AC) interne ou externe, qui peut être publique ou privée. Une AC peut elle-même recourir à des prestataires externes pour la mise en œuvre de certaines des fonctions mentionnées. Dans tous les cas, l'autorité administrative reste seule responsable du processus global de délivrance.

6.2 Règles de sécurité

L'autorité de certification doit :

- rédiger une *politique de certification* (PC) par fonction de sécurité, usage (authentification, signature, chiffrement) et niveau de sécurité. Ces PC doivent être conformes aux modèles des PC-Types (annexes [RGS_A_2] à [RGS_A_3]) ;
- mettre en œuvre des clés cryptographiques d'AC spécifiquement restreintes et dédiées à la génération de certificats destinés aux autorités administratives (AA) ou à leurs agents et mentionner cette exigence dans la PC ;
- générer des certificats à destination exclusive des AA, ou de leurs agents, et mentionner explicitement cette exigence dans la PC ;
- lorsqu'elle recourt à des prestataires externes pour certaines fonctions, établir des procédures avec ces prestataires permettant de garantir le respect de la PC pour ce qui les concerne ;
- faire approuver cette PC par l'AA et en respecter les règles.

Lorsqu'elle recourt à une AC externe, l'autorité administrative doit établir des procédures qui lui permettent de s'assurer du respect, par cette AC, des règles du présent paragraphe.

⁵ La validation des certificats par l'Etat ne doit pas être confondue avec la validation du statut d'un certificat, qui consiste à vérifier notamment que celui-ci n'est pas révoqué ou expiré.

Référentiel général de sécurité			
Version du RGS	Date	Critère de diffusion	Page
2.0	13 juin 2014	PUBLIC	15/25

6.3 Procédure de validation

Les autorités administratives disposent d'un délai de trois ans à compter de la publication du présent référentiel pour obtenir la validation de leurs certificats (art. 23 du décret RGS). Pour les certificats délivrés après ce délai, la demande de validation devra être faite dans un délai de trois mois à compter de la délivrance des certificats.

À cet effet, l'autorité administrative adresse à l'ANSSI un dossier de demande de validation qui comporte les pièces suivantes :

- l'identification précise de l'AA et de l'AC concernées par la demande ;
- la PC de l'AC ainsi que, le cas échéant, une description de la chaîne de certification ;
- le cas échéant, les procédures mentionnées au § 6.2 établies entre l'AA et l'AC et entre l'AC et ses prestataires externes ;
- les résultats d'un audit de conformité de l'AC à sa PC, qui doit être réalisé par l'AC conformément aux règles des PC-Types ;
- le cas échéant, l'attestation de qualification de l'AC au sens du décret RGS ;
- le certificat de l'AC et, le cas échéant, une demande de publication de ce certificat sur le site internet de l'ANSSI.

À l'issue d'un délai de deux mois à compter de la réception du dossier complet, et sous réserve que l'ANSSI n'ait pas fait part à l'autorité administrative d'une non-conformité au regard des règles du § 6.2 du présent RGS, l'autorité administrative est réputée avoir obtenu la validation des certificats.

L'ANSSI peut, à tout moment, demander de vérifier sur place les conditions de délivrance des certificats afin de s'assurer que les procédures mises en place par l'AC sont conformes au présent référentiel (art. 22 du décret RGS). En cas de non-conformité signalée par l'ANSSI, l'autorité administrative dispose d'un délai de trois mois pour faire corriger les procédures de l'AC. À défaut, les certificats ne sont plus considérés comme conformes au décret RGS. L'ANSSI publie le nouveau statut de ce certificat sur son site.

L'AA doit faire une demande de renouvellement de la validation lors de chaque modification substantielle des conditions de délivrance des certificats, notamment lorsque le certificat de l'AC est expiré.

Dès que la validation a été obtenue, le certificat de l'AC est, sur demande de l'autorité administrative, mis à disposition du public par l'ANSSI sur son site Internet www.ssi.gouv.fr.

6.4 Liste des informations relatives à la délivrance et à la validation

Les autorités administratives mettent à disposition des usagers les informations relatives à la délivrance et à la validation des certificats électroniques (art. 22 du décret RGS) :

- la PC de l'AC ;
- le certificat de l'AC ;
- la mention de l'obtention de la validation des certificats au sens des présentes dispositions.

Référentiel général de sécurité			
Version du RGS	Date	Critère de diffusion	Page
2.0	13 juin 2014	PUBLIC	16/25

Chapitre 7. Recommandations relatives à l'application du référentiel

Au-delà de l'analyse de risques et de l'homologation, l'ANSSI recommande l'adoption de bonnes pratiques relatives à la méthodologie, aux procédures et à l'organisation.

7.1 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. Elle peut être mutualisée avec celle requise pour la protection des informations classifiées de défense, telle que définie dans l'*instruction générale interministérielle sur la protection du secret de la défense nationale* n° 1300/SGDSN/PSE/PSD.

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 échéant, 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), l'officier de la sécurité des systèmes d'information (OSSSI), le correspondants 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, 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.

7.2 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.

Référentiel général de sécurité			
Version du RGS	Date	Critère de diffusion	Page
2.0	13 juin 2014	PUBLIC	17/25

7.3 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). 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.

7.4 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.

7.5 Informé et sensibiliser le personnel

L'ensemble des agents d'une autorité administrative, et le cas échéant 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, l'ANSSI publie des bonnes pratiques pour l'application de principes de base en matière de sécurité des systèmes d'information : www.ssi.gouv.fr/fr/bonnes-pratiques/principes-generaux.

7.6 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.

Référentiel général de sécurité			
Version du RGS	Date	Critère de diffusion	Page
2.0	13 juin 2014	PUBLIC	18/25

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 ;
- préciser les clauses concernant les conditions de l'intervention et de l'accès physique et logique des sous-traitants ;
- préciser les clauses garantissant la qualité et la sécurité des prestations et produits fournis ;
- préciser les conditions de propriété des 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 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.

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

7.7 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.

7.8 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.) ;

Référentiel général de sécurité			
Version du RGS	Date	Critère de diffusion	Page
2.0	13 juin 2014	PUBLIC	19/25

- 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.

7.9 Utiliser les produits et prestataires labellisés pour leur sécurité

La qualification est un label, créé par l'ordonnance du 8 décembre 2005, qui permet d'attester de la confiance que l'on peut accorder à des produits de sécurité et à des prestataires de services de confiance (PSCO), ainsi que de leur conformité aux règles du RGS qui leurs sont applicables. D'autres labels existent pour attester de la compétence des professionnels, notamment en matière de SSI.

La nécessité de recourir à des produits de sécurité ou à des prestataires de services de confiance a été régulièrement rappelée par le Premier ministre ⁶, ainsi il est recommandé :

- d'utiliser chaque fois que possible des produits de sécurité qualifiés (cf. § 5.1) par l'ANSSI ;
- de recourir chaque fois que possible à des PSCO qualifiés (cf. § 5.2) ;
- 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.

7.10 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 test réguliers.

7.11 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.

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 le schéma décrit au chapitre 5.

⁶ Cf. communication relative à la protection des systèmes d'information lors du conseil des ministres du 25 mai 2011 (www.ssi.gouv.fr/IMG/pdf/2011-05-25_principales_mesures.pdf) et allocution sur la politique de cybersécurité de la France (www.ssi.gouv.fr/IMG/pdf/02-20_discours_de_jean-marc_ayrault_premier_ministre_-_inauguration_des_nouvelles_installations_de_lagence_nationale_de_la_securite_des_systemes_dinformation_anssi.pdf) du 20 février 2014.

Référentiel général de sécurité			
Version du RGS	Date	Critère de diffusion	Page
2.0	13 juin 2014	PUBLIC	20/25

7.12 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.

7.13 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*. Le processus de référencement est, quant à lui, décrit dans l'arrêté du 18 janvier 2012 relatif au référencement de produits de sécurité ou d'offres de prestataires de services de confiance.

Référentiel général de sécurité			
Version du RGS	Date	Critère de diffusion	Page
2.0	13 juin 2014	PUBLIC	21/25

Chapitre 8. Transition entre la première et la deuxième version du RGS

Conformément au I de l'article 14 de l'ordonnance du 8 décembre 2005, les autorités administratives avaient l'obligation de mettre leurs systèmes d'information existants en conformité avec la première version du RGS, dans un délai maximal de trois ans à compter de sa publication.

Aucune prestation de confiance, et notamment aucun certificat non conforme avec les exigences de cette première version du RGS, n'est donc susceptible d'être en circulation à l'issue de cette période de trois ans

Les autorités administratives doivent être en conformité avec les règles posées par la nouvelle version dès son entrée en vigueur.

Cependant, les mesures transitoires suivantes s'appliquent aux services de certification et d'horodatage électroniques :

- les certificats conformes aux annexes de la première version du RGS pourront encore être émis pendant l'année qui suit l'entrée en vigueur de la présente version. Les autorités administratives devront accepter ces certificats pendant leur durée de vie jusqu'à concurrence de trois (3) ans, soit au maximum pendant les quatre (4) années qui suivent l'entrée en vigueur de la présente version du référentiel général de sécurité ;
- les certificats conformes aux annexes de la présente version pourront être émis à compter de son entrée en vigueur. Les autorités administratives devront accepter ces certificats au plus tard un (1) an après cette date.

Référentiel général de sécurité			
Version du RGS	Date	Critère de diffusion	Page
2.0	13 juin 2014	PUBLIC	22/25

Chapitre 9. Liste des annexes du RGS

Les annexes contiennent les règles relatives aux mécanismes cryptographiques mis en œuvre dans les fonctions de sécurité traitées au chapitre 5 ainsi que celles, spécifiques à la deuxième version du RGS, applicables aux différentes catégories de prestataires de services de confiance. Ces documents sont consultables à l'adresse www.ssi.gouv.fr/rgs.

9.1 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 3.0
- [RGS_A2] Politique de Certification Type « certificats électroniques de personne », version 3.0
- [RGS_A3] Politique de Certification Type « services applicatifs », version 3.0
- [RGS_A4] Profils de certificats, CRL, OCSP et algorithmes cryptographiques, version 3.0
- [RGS_A5] Politique d'Horodatage Type, version 3.0

9.2 Documents applicables concernant l'utilisation de mécanismes cryptographiques

- [RGS_B1] Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03
- [RGS_B2] Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 2.00
- [RGS_B3] Règles et recommandations concernant les mécanismes d'authentification, version 1.0

9.3 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 1.1

Référentiel général de sécurité			
Version du RGS	Date	Critère de diffusion	Page
2.0	13 juin 2014	PUBLIC	23/25

Chapitre 10. Références documentaires

10.1 Références réglementaires

- [loi120400] Loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations.
- [DécretRGS] Décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005.
- [Décret2001-272] Décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique.
- [Décret2002-535] Décret n° 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.
- [Décret2011-434] Décret n° 2011-434 du 20 avril 2011 relatif à l'horodatage des courriers expédiés ou reçus par voie électronique pour la conclusion ou l'exécution d'un contrat.
- [Arrêté260704] Arrêté du 26 juillet 2004 relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation.
- [Arrêté200411] Arrêté du 20 avril 2011 relatif à la reconnaissance de la qualification des prestataires de services d'horodatage électronique et à l'accréditation des organismes qui procèdent à leur évaluation.
- [IGI1300] Instruction générale interministérielle n° 1300/SGDSN/PSE/PSD sur la protection du secret de la défense nationale, approuvée par arrêté du Premier Ministre du 30 novembre 2011.
- [I-CSPN] Instruction n° 1414/ANSSI/SR du 30 mai 2011 relative à la certification de sécurité de premier niveau des produits des technologies de l'information.
- [HabilitationOQ] Instruction n°1001/ANSSI/SR du 8 avril 2011 relative à la procédure d'habilitation des organismes qui procèdent à la qualification des prestataires de services de confiance, version 1.0.
- [Stratégie_France] Défense et sécurité des systèmes d'information - Stratégie de la France : www.ssi.gouv.fr/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf

10.2 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.

Référentiel général de sécurité			
Version du RGS	Date	Critère de diffusion	Page
2.0	13 juin 2014	PUBLIC	24/25

[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
[MaturitéSSI]	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 Externalisation]	Maîtriser les risques de l'infogérance – Externalisation des systèmes d'information. Disponible en ligne : www.ssi.gouv.fr/IMG/pdf/2010-12-03_Guide_externalisation.pdf
[Guide homologation]	L'homologation de sécurité en neuf étapes simples. Disponible en ligne : www.ssi.gouv.fr/IMG/pdf/guide_homologation_de_securite_en_9_etapes.pdf
[AvisCertsIGC/A]	Avis publié au Journal officiel de la République française du 6 avril 2012 - NOR : PRMD1208117V relatif aux certificats de l'IGC/A en cours de validité.
[GHI]	Guide d'hygiène informatique. Janvier 2013. Disponible sur : www.ssi.gouv.fr/IMG/pdf/guide_hygiene_informatique_anssi.pdf
[SI-industriels]	La cybersécurité des systèmes industriels. Juin 2012. Disponible en ligne : www.ssi.gouv.fr/IMG/pdf/guide_securite_industrielle_version_finale.pdf
[CC]	Common Criteria for Information Technology Security Evaluation.
[QE]	Processus de qualification d'un produit de sécurité – Niveau Élémentaire, version 1.0.
[QS]	Processus de qualification d'un produit de sécurité – Niveau Standard, version 1.2.
[QR]	Processus de qualification d'un produit de sécurité – Niveau Renforcé, version 1.0.
[PC_IGC/A]	Politiques de Certification de l'IGC/A, v2.0 (RSA2048 bits), v2.1 (RSA 4096 bits).

Référentiel général de sécurité			
Version du RGS	Date	Critère de diffusion	Page
2.0	13 juin 2014	PUBLIC	25/25