



Premier ministre

**Agence Nationale de la Sécurité des
Systèmes d'Information**



**Ministère du budget, des comptes
publics, de la fonction publique et
de la réforme de l'État**

**Direction Générale de la Modernisation
de l'État**

Référentiel Général de Sécurité

Version 0.99

Sommaire

1 - Introduction	4
1.1 - Forces et faiblesses du numérique	4
1.2 - Cadre juridique	5
1.3 - Elaboration, approbation et publication du RGS	6
1.4 - Autorités administratives concernées	6
1.5 - Objectif du RGS	6
1.6 - Documents constitutifs du RGS	6
1.6.1 - Le corps du RGS	6
1.6.2 - Les annexes du RGS	7
1.7 - A qui s'adresse le RGS ?	8
2 - Un cadre pour gérer la sécurité des systèmes d'information	10
2.1 - Introduction à la sécurité des systèmes d'information	10
2.2 - Six grands principes de gestion de la SSI	11
2.2.1 - Adopter une démarche globale	11
2.2.2 - Adapter la SSI selon les enjeux	11
2.2.3 - Gérer les risques SSI	12
2.2.4 - Élaborer une politique SSI	12
2.2.5 - Utiliser les produits et prestataires labellisés pour leur sécurité	12
2.2.6 - Viser une amélioration continue	13
2.3 - Intégration de la SSI dans le cycle de vie des systèmes d'information	13
2.3.1 - Des efforts proportionnés aux enjeux SSI	13
2.3.2 - Un engagement systématique : l'homologation de sécurité	13
2.3.3 - Des outils spécifiques pour différentes familles de téléservices	14
3 - Fonctions de sécurité	15
3.1 - Introduction	15
3.2 - Authentification	15
3.2.1 - Utilisation de mécanismes cryptographiques	16
3.2.2 - Authentification d'une personne par l'utilisation d'identifiants et de mots de passe statiques	16
3.2.3 - Authentification d'une personne par certificat électronique	16
3.2.4 - Authentification d'un serveur par certificat électronique	17
3.3 - Signature électronique	17
3.3.1 - Utilisation de mécanismes cryptographiques	18
3.3.2 - Signature d'une personne par certificat électronique	18
3.3.3 - Cachet d'un serveur par certificat électronique	19
3.4 - Confidentialité	19
3.4.1 - Utilisation de mécanismes cryptographiques	19
3.4.2 - Confidentialité par certificat électronique	19
3.5 - Horodatage	20
3.5.1 - Utilisation des mécanismes cryptographiques	20
3.5.2 - Horodatage par contremarques de temps	20
4 - Accusé d'enregistrement et accusé de réception	21
4.1 - Introduction	21
4.2 - Règles et recommandations de sécurité	21

Référentiel Général de Sécurité (RGS)		
Version	Date	Page
0.99	19/02/2010	2/33

5 -	Qualification	22
5.1 -	Qualification de produits de sécurité	22
5.2 -	Qualification des Prestataires de Services de Confiance (PSCO).....	23
6 -	Validation des certificats électroniques	25
6.1 -	Règles de sécurité.....	26
6.2 -	Procédure de validation.....	26
6.3 -	Liste des informations relatives à la délivrance et à la validation.....	27
6.4 -	Rôle de l'IGC/A	27
7 -	Liste des documents constitutifs du RGS.....	28
7.1 -	Documents applicables concernant l'utilisation de certificats électroniques dans les fonctions de sécurité.....	28
7.2 -	Documents applicables concernant l'utilisation de mécanismes cryptographiques dans les fonctions de sécurité.....	28
8 -	Liste des Profils de Protection	29
9 -	Glossaire.....	30
10 -	Références documentaires	32
10.1 -	Références réglementaires	32
10.2 -	Références techniques	32

Référentiel Général de Sécurité (RGS)		
Version	Date	Page
0.99	19/02/2010	3/33

1 - Introduction

1.1 - Forces et faiblesses du numérique

Les atouts

Les technologies numériques pénètrent chaque jour un peu plus notre société, dans chacune de ses activités, apportant autant de services nouveaux, de croissance, de simplification et d'efficacité. Ces possibilités nouvelles sont également mises à profit par l'État, notamment dans sa volonté de dématérialiser le plus grand nombre possible de ses processus et de ses échanges. Ainsi, le développement des téléservices est-il une préoccupation forte des autorités administratives pour simplifier et accélérer le traitement de l'ensemble des procédures au profit des autres autorités administratives et des usagers.

Cependant, cette évolution se traduit également par une dépendance et une vulnérabilité croissantes.

La dépendance

En effet, les données et les systèmes numériques deviennent désormais un patrimoine stratégique, parfois même vital pour l'organisme. L'interruption du service assuré par un système d'information, ou la destruction ou l'altération d'informations, peuvent conduire à une paralysie. Les informations présentent souvent un caractère de confidentialité élevé, dont l'enjeu peut être l'autonomie de décision politique, la protection de secrets comme ceux de l'instruction judiciaire ou des enquêtes de police, la préservation du patrimoine intellectuel ou technologique, ou encore l'égalité des chances des candidats aux marchés publics. Dans certains cas, pour les données personnelles par exemple, la divulgation à des personnes n'ayant pas à en connaître peut conduire à des sanctions pénales. Enfin, une perte de contrôle des processus internes, de plus en plus souvent assurés par des moyens informatiques, peut être dangereuse pour l'organisme, voire, quand ils concernent des industries ou des secteurs d'activité d'importance vitale, dramatique pour la nation ou pour la sécurité des populations.

La faiblesse des technologies de l'information

La sécurité des technologies de l'information n'a pas suivi l'extraordinaire développement de l'informatique et de ses usages. Le protocole Internet – l'IP –, les systèmes d'exploitation et les applications ont à l'origine été conçus pour être efficaces, dans des réseaux peu étendus, sans réelle prise en compte de la sécurité. Ceux qui sont aujourd'hui en service utilisent souvent des briques de base des premiers réseaux, alors que leur contexte d'emploi a radicalement changé, avec la multiplication des technologies de communication, notamment dans le domaine du « sans fil », avec la convergence des réseaux de téléphonie, de messagerie ou de transmissions de données vers l'IP, et avec l'interconnexion croissante de ces réseaux. Les logiciels, de plus en plus complexes, présentent souvent des failles de sécurité, qui obligent les éditeurs à les corriger en permanence, dès leur découverte. Les informations, les processus, hier confinés, sont devenus accessibles depuis presque n'importe quel point du globe, alors que dans le même temps, leur nombre et leur volume explosent avec l'augmentation des capacités de calcul et de mémoire.

Les risques et menaces

Dans ce contexte de dépendance croissante aux technologies numériques, les administrations et les entreprises sont soumises à des risques et des menaces de plus en plus importantes. Les pannes, les accidents, les catastrophes naturelles, y compris lointaines, ont des impacts bien plus graves que par le passé. Il en est de même des actes de malveillance, internes ou externes, sur les systèmes d'information. Dans le même temps, la cybercriminalité se développe au même rythme que l'exploitation du numérique, sous des formes très diverses et de plus en plus sophistiquées. La défiguration des sites Internet est devenue un mode de contestation politique ou sociale. La saturation des réseaux ou des terminaux de communication est une arme utilisée dans des conflits politiques ou sociaux, ou dans de simples luttes entre concurrents commerciaux. L'espionnage politique, commercial ou technologique se développe, avec des outils d'attaque permettant à distance d'avoir accès aux mémoires informatiques, de capter les frappes sur les claviers, de visualiser les pages affichées sur les écrans, ou encore de mettre en route le microphone dont

Référentiel Général de Sécurité (RGS)		
Version	Date	Page
0.99	19/02/2010	4/33

certaines ordinateurs sont dotés. L'usurpation d'identité est d'ores et déjà largement répandue sur l'Internet et se pratique par des méthodes telles que le « hameçonnage » (« phishing » en anglais) qui permet au fraudeur de récupérer des renseignements personnels sur la victime (exemple : faux sites marchands permettant de voler les données bancaires et de puiser dans les comptes de la victime). Cette cybercriminalité bénéficie de la relative simplicité des attaques sur des technologies numériques fragiles, de l'impunité que peut procurer la distance et d'une rentabilité élevée.

1.2 - Cadre juridique

Face à ces risques et à ces menaces, le gouvernement a estimé nécessaire de renforcer, par voie d'ordonnance, la sécurité des échanges électroniques.

Ainsi, la loi n° 2004-1343 du 9 décembre 2004 de simplification du droit, en son article 3, a autorisé le gouvernement à prendre par ordonnance les mesures nécessaires pour assurer la sécurité des informations échangées par voie électronique entre les usagers et les autorités administratives (appelées « AA » dans la suite du document), ainsi qu'entre les autorités administratives.

En application de cette loi, 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 (ci-après désignée [Ordonnance]) a été prise. Cette [Ordonnance] a été ratifiée par le parlement le 22 février 2006.

Elle s'inscrit dans la démarche globale du gouvernement en matière de réforme de l'État, plus précisément dans ses aspects de simplification des démarches des usagers et de facilitation de l'accès de ces derniers aux services publics, cette [Ordonnance] s'applique aux systèmes d'information destinés à échanger des informations entre les usagers et les autorités administratives, ainsi qu'entre les différentes autorités administratives.

L'[Ordonnance] prévoit, en son article 9.I, l'établissement d'un Référentiel Général de Sécurité (RGS), dans le but de fixer, selon le niveau de sécurité requis, les règles que doivent respecter certaines fonctions contribuant à la sécurité des informations. Les règles formulées dans le RGS s'imposent ainsi et sont modulées en fonction du niveau de sécurité retenu par l'AA pour la fonction concernée.

Conformément à l'article 14.I, les AA doivent mettre leurs systèmes d'information (SI) existants à la date de publication du présent RGS en conformité avec ce référentiel dans un délai de trois ans à compter de sa publication. Les systèmes créés dans les six mois qui suivent la publication du RGS doivent être mis en conformité dans un délai de 12 mois.

Conformément à l'article 15, les systèmes d'information traitant d'informations relevant du secret de la défense nationale n'entrent pas dans le champ d'application de l'[Ordonnance].

L'[Ordonnance] renvoie à des décrets les conditions d'application des mesures qu'elle prévoit. En particulier, le décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'[Ordonnance], ci-après désigné [DécretRGS], traite des points suivants :

- les conditions d'élaboration, d'approbation et de publication par arrêté du RGS (en application de l'article 9.I de l'[Ordonnance]) ;
- les fonctions de sécurité (en application de l'articles 9.II de l'[Ordonnance]) ;
- la qualification des produits de sécurité (en application de l'article 9.III de l'[Ordonnance]) ;
- la qualification des prestataires de services de confiance (en application de l'article 9.III de l'[Ordonnance]) ;
- la validation des certificats électroniques (en application de l'article 10 de l'[Ordonnance]), dont les modalités d'application sont précisées par deux arrêtés du Premier ministre.

Référentiel Général de Sécurité (RGS)		
Version	Date	Page
0.99	19/02/2010	5/33

1.3 - Elaboration, approbation et publication du RGS

Extrait du [DécretRGS] : Chapitre Ier : Référentiel Général de Sécurité :

« Article 2 :

Le référentiel général de sécurité ainsi que ses mises à jour sont approuvées par arrêté du Premier ministre publié au Journal officiel de la République française. L'Agence nationale de la sécurité des systèmes d'information concourt à l'élaboration de ce référentiel et à sa mise à jour en liaison avec la direction générale de la modernisation de l'Etat. Ce référentiel est mis à disposition du public par voie électronique.»

Conformément à l'article ci-dessus, le RGS est élaboré par l'agence nationale de la sécurité des systèmes d'information (ANSSI) en liaison avec la direction générale de la modernisation de l'Etat (DGME).

Au cours de l'élaboration de cette première version, différents acteurs ont été consultés, notamment des autorités administratives qui seront chargées de mettre en application ce référentiel, des éditeurs de produits de sécurité et des prestataires de services de confiance qui devront respecter les exigences techniques du référentiel, ainsi que plus généralement le public à l'aide d'un appel à commentaires sur internet. A l'issue de cette phase, le RGS v1.0 est approuvé par un arrêté du Premier ministre, et est mis à disposition du public sur le site internet mentionné dans l'arrêté.

Cette première version du référentiel est appelée à évoluer. Des mises à jour seront nécessaires pour prendre en compte l'évolution des techniques et des menaces, ainsi que pour compléter le RGS avec de nouvelles fonctions de sécurité. Ces mises à jour seront effectuées selon la même procédure d'élaboration, d'approbation et de publication de cette première version.

1.4 - Autorités administratives concernées

L'[Ordonnance] précise que les AA sont les administrations de l'État, les collectivités territoriales, les établissements publics à caractère administratif, les organismes gérant des régimes de protection sociale relevant du code de la sécurité sociale et du code rural ou mentionnés aux articles L. 223-16 et L. 351-21 du code du travail et les autres organismes chargés de la gestion d'un service public administratif.

Par ailleurs, seules sont concernées, parmi ces AA, celles qui mettent en œuvre des systèmes d'information susceptibles d'échanger des informations avec d'autres AA ou avec des usagers.

1.5 - Objectif du RGS

Conformément à sa vocation première, le RGS contient un ensemble de règles de sécurité, fixées dans le présent document ou dans ses annexes, qui s'imposent aux AA et aux prestataires qui les assistent.

En complément à ces règles, ont été insérées dans le RGS des bonnes pratiques en matière de sécurité des systèmes d'information (SSI), dans le but de guider les AA et les prestataires dans les choix qui se présentent à eux pour sécuriser au mieux les systèmes d'information. Le RGS apporte également des éclairages nécessaires sur la marche à suivre pour prendre en compte pleinement les dispositions de l'[Ordonnance].

L'objectif du RGS n'est pas d'imposer une technologie, une architecture, ou une solution technique, ni même les fonctions de sécurité décrites dans le RGS. En revanche, lorsqu'une AA juge nécessaire, à l'issue d'une analyse de risque, de mettre en œuvre des fonctions de sécurité qui sont prévues dans le RGS, elle doit alors respecter les règles correspondantes.

1.6 - Documents constitutifs du RGS

Le RGS est constitué du présent document, appelé « corps » du RGS, et d'annexes.

1.6.1 - Le corps du RGS

Le corps du RGS se veut accessible aux non experts en informatique, et notamment aux autorités qui doivent respecter, ou faire respecter, le RGS. Il comporte les chapitres suivants :

Chapitre 1^{er} : Introduction

Chapitre 2 : Un cadre pour gérer la sécurité des systèmes d'information

Référentiel Général de Sécurité (RGS)		
Version	Date	Page
0.99	19/02/2010	6/33

Ce chapitre fournit un ensemble de règles et de bonnes pratiques relatives à la gestion globale de la SSI, ainsi qu'à l'intégration de la SSI dans le cycle de vie des systèmes d'information.

Chapitre 3 : Fonctions de sécurité

Il s'agit du chapitre central du RGS, celui répondant pleinement aux dispositions de l'article 9.I de l'[Ordonnance]. Les fonctions de sécurité sont déclinées par niveaux de sécurité, les règles étant fixées pour chacun de ces niveaux. Il est de la responsabilité d'une AA de déterminer, dans le cadre de la mise en œuvre d'un système d'information, les fonctions de sécurité nécessaires au niveau de sécurité requis. Lorsque la fonction de sécurité est traitée dans le RGS, l'AA applique les règles adéquates au niveau considéré.

Chapitre 4 : Accusés d'enregistrement et accusés de réception

Ce chapitre présente les règles de sécurité relatives aux fonctions d'accusé d'enregistrement et d'accusé de réception.

Chapitre 5 : Qualification

La qualification est un label pouvant être délivré à un produit de sécurité ou à un prestataire de services de confiance (PSCO). Ce chapitre présente les trois processus de qualification des produits de sécurité (élémentaire, standard, renforcé) ainsi que le schéma de qualification des PSCO.

Chapitre 6 : Les infrastructures de gestion de clés (IGC)

Ce chapitre contient les règles et recommandations relatives à la mise en œuvre et à l'exploitation d'une IGC par les AA.

Il présente également le cas particulier de la validation des certificats par l'État, notamment la validation au moyen de l'infrastructure « IGC/A » (Infrastructure de Gestion de la Confiance de l'Administration).

Chapitre 7 : Liste des documents applicables

Chapitre 8 : Liste des profils de protection

Chapitre 9 : Glossaire

Chapitre 10 : Références documentaires

1.6.2 - Les annexes du RGS

Le RGS comprend les annexes A traitant de l'utilisation de certificats électroniques dans les fonctions de sécurité et les annexes B constituant le référentiel cryptographique :

[RGS_A_1]	Fonction de sécurité "Confidentialité"
[RGS_A_2]	Fonction de sécurité "Authentification"
[RGS_A_3]	Fonction de sécurité "Signature"
[RGS_A_4]	Fonction de sécurité "Authentification Serveur"
[RGS_A_5]	Fonction de sécurité "Cachet"
[RGS_A_6]	Politique de certification Type "Confidentialité"
[RGS_A_7]	Politique de certification Type "Authentification"
[RGS_A_8]	Politique de certification Type "Signature"
[RGS_A_9]	Politique de certification Type "Authentification Serveur"
[RGS_A_10]	Politique de certification Type "Cachet"
[RGS_A_11]	Politique de certification Type "Authentification et Signature"
[RGS_A_12]	Politique d'horodatage Type
[RGS_A_13]	Variables de temps
[RGS_A_14]	Profils de certificats, CRL, OCSP et algorithmes cryptographiques
[RGS_B_1]	Référentiel cryptographique : règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques
[RGS_B_2]	Référentiel cryptographique : règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques
[RGS_B_3]	Référentiel cryptographique : règles et recommandations concernant les mécanismes d'authentification

Référentiel Général de Sécurité (RGS)		
Version	Date	Page
0.99	19/02/2010	7/33

1.7 - A qui s'adresse le RGS ?

Le RGS s'adresse au personnel ou aux organismes ayant une responsabilité dans le système d'information d'une AA, qu'ils relèvent de l'autorité directe de cette AA ou qu'ils interviennent à son profit, ainsi qu'aux éditeurs de produits de sécurité et aux PSCO qui souhaitent voir leurs produits ou services de confiance choisis par les AA.

Différents acteurs sont plus particulièrement concernés par le RGS. Leurs objectifs ne sont pas les mêmes. Ces acteurs sont notamment :

Maîtrise d'ouvrage (MOA) des AA :

La MOA est responsable de la définition des besoins lors de la conception d'un système d'information. Elle fixe l'organisation du projet, ses objectifs, ses enjeux et ses contraintes. D'une manière générale, elle est responsable de l'identification des objectifs de sécurité et du pilotage du projet.

Les chapitres 2 et 6 sont particulièrement destinés à la MOA d'une AA.

Maîtrise d'œuvre (MOE) des AA :

La MOE est responsable des propositions techniques et de l'évaluation des charges de réalisation. D'une manière générale, elle est responsable de la détermination des exigences de sécurité devant satisfaire les objectifs de sécurité, et de leur mise en œuvre.

Les chapitres 3, 4 et 6 seront étudiés avec attention par la MOE d'un projet de système d'information. En effet, une fois les fonctions de sécurité et niveaux de sécurité déterminés, la MOE y trouvera les règles de sécurité à respecter.

Responsable de la sécurité des systèmes d'information (RSSI) d'une AA :

En fonction des organismes, le RSSI, ou la personne faisant office de RSSI, peut avoir différents rattachements. Rattaché à la direction générale, il est chargé de proposer la politique de sécurité du système d'information (PSSI) qui sera fixée par l'AA, et de veiller à son application. Dans le cadre d'un projet, il conseille l'autorité d'homologation. Rattaché à la direction informatique, il intervient en tant qu'expert auprès de la direction de projet et valide les livrables SSI au regard de la PSSI. Dans le cadre du processus d'homologation de sécurité d'un système d'information, il a la charge de présenter l'analyse de risques.

Le RSSI sera tout particulièrement concerné par les chapitres 2, 3 et 4.

Editeurs de produits de sécurité :

L'AA détermine les fonctions de sécurité au niveau de sécurité qu'elle estime adéquat et recourt à des produits de sécurité afin de les mettre en œuvre au sein du système d'information. Ces produits de sécurité peuvent avoir fait l'objet d'une qualification, le cas échéant à un degré donné, attestant de la robustesse des mécanismes de sécurité qu'ils offrent et de leur conformité à un niveau de sécurité traité dans le RGS.

Les éditeurs de produits de sécurité exploiteront en priorité le chapitre 5.1 qui expose le processus de qualification des produits de sécurité.

Par ailleurs, les éditeurs de produits de sécurité se référeront utilement au chapitre 3 afin de prendre en compte les exigences techniques que doivent notamment respecter les mécanismes cryptographiques implémentés dans les produits de sécurité.

Prestataire de services de confiance (PSCO) :

Une AA peut, en complément de la mise en place de produits de sécurité dans son système d'information, faire appel aux services d'un PSCO, que ce dernier soit public ou privé. Une AA peut aussi décider d'être elle-même PSCO en fournissant le service pour son propre usage.

Le chapitre 5.2 présente le schéma de qualification des PSCO. D'autre part, les PSCO se référeront utilement au chapitre 3 afin que les mécanismes cryptographiques éventuellement implémentés dans leurs offres en respectent les exigences. Enfin, dans l'optique de faire valider par l'État les certificats électroniques qu'ils émettent, les prestataires de services de certification électronique (PSCE) se reporteront au chapitre 6.

Référentiel Général de Sécurité (RGS)		
Version	Date	Page
0.99	19/02/2010	8/33

Le schéma ci-dessous illustre les domaines d'intérêts du RGS selon les acteurs :

Familles de lecteurs	RGS Corps du document	Annexes (Règles de sécurité)	Références (Bonnes pratiques SSI)
RSSI, MOA et MOE d'une autorité administrative	<p>Chapitre 2 : Un cadre pour gérer la SSI</p> <p>6 principes SSI à appliquer</p> <p>Intégration de la SSI dans le cycle de vie des systèmes d'information</p>		<p>Norme ISO 2700X</p> <p>Guide de rédaction d'un Politique SSI</p> <p>Guide d'intégration de la SSI dans les projets</p> <p>Guide d'évaluation de la maturité d'un SI</p> <p>Méthode d'analyse de risques « EBIOS »</p> <p>Fiches types d'expression rationnelle d'objectifs de sécurité</p>
<p>RSSI et MOE d'une autorité administrative</p> <p>Editeurs de produits de sécurité</p> <p>Prestataires de services de confiance</p>	<p>Chapitre 3 : Fonctions de sécurité</p> <p>Règles relatives aux fonctions de sécurité :</p> <ul style="list-style-type: none"> •Signature électronique •Authentification •Chiffrement •Horodatage <p>Règles relatives aux mécanismes cryptographiques (symétriques et asymétriques)</p>	<p>[RGS_A_1] [RGS_A_2] [RGS_A_3] [RGS_A_4] [RGS_A_5] [RGS_A_6] [RGS_A_7] [RGS_A_8] [RGS_A_9] [RGS_A_10] [RGS_A_11] [RGS_A_12] [RGS_A_13] [RGS_A_14]</p> <p>[RGS_B_1] [RGS_B_2] [RGS_B_3]</p>	
MOE d'une autorité administrative	<p>Chapitre 4 : Accusés de réception / accusés d'enregistrements</p> <p>Règles de sécurité des AE / AR</p>	<p>[RGS_A_3] [RGS_A_8] [RGS_A_12]</p>	
<p>Editeurs de produits de sécurité</p> <p>Prestataires de services de confiance</p>	<p>Chapitre 5 : Qualification</p> <p>Qualification des produits de sécurité</p> <p>Qualification des PSCO</p>	<p>[RGS_A_6] [RGS_A_7] [RGS_A_8] [RGS_A_9] [RGS_A_10] [RGS_A_11] [RGS_A_12]</p> <p>[RGS_B_1] [RGS_B_2] [RGS_B_3]</p>	<p>Processus de qualification au niveau élémentaire</p> <p>Processus de qualification au niveau standard</p> <p>Processus de qualification au niveau renforcé</p>
<p>RSSI et MOA d'une autorité administrative</p> <p>Prestataires de services de certification électronique</p>	<p>Chapitre 6 : Les IGC</p> <p>Recommandations sur la mise en œuvre d'IGC</p> <p>Validation des certificats par l'Etat</p>		<p>Politique de certification de l'IGC/A</p>

Référentiel Général de Sécurité (RGS)		
Version	Date	Page
0.99	19/02/2010	9/33

2 - Un cadre pour gérer la sécurité des systèmes d'information

2.1 - Introduction à la sécurité des systèmes d'information

La sécurité des systèmes d'information (SSI) recouvre l'ensemble des moyens techniques, organisationnels et humains qui doivent être mis en place dans le but de garantir, au juste niveau requis, la sécurité des informations d'un organisme et des systèmes qui en assurent l'élaboration, le traitement, la transmission ou le stockage.

Ce besoin de sécurité doit être déterminé en fonction de la menace et des enjeux.

D'une part, les enjeux se mesurent à l'aune de la gravité des impacts que provoquerait, pour l'organisme, une perte de :

- la disponibilité des informations : quel impact en cas d'impossibilité d'accéder aux données ou d'utiliser le système d'information ? ;
- l'intégrité des informations : quel impact en cas de modification non désirée de données ou de composants du système d'information ? ;
- la confidentialité des informations : quel impact en cas d'accès par une personne non autorisée à des données confidentielles ?

D'autre part, les menaces à prendre en compte sont celles qui pèsent réellement sur le système d'information et sur les informations qu'il traite, transmet et stocke, dans l'environnement dans lequel il se situe. Le système d'information, et donc les informations qu'il contient, est-il isolé, ou est-il accessible depuis Internet ? Les postes de travail, les serveurs, les réseaux utilisés sont-ils dans une enceinte protégée, ou dans un lieu public ? Le système est-il dans une zone inondable, une zone sismique ? Le personnel est-il habilité dans sa totalité à connaître les données, à piloter les processus ou à administrer le système, ou faut-il considérer comme une menace l'accès de certaines personnes aux données, aux processus ou au système ?

Il est maintenant fait obligation aux AA, par l'article 3 du [décret RGS], de conduire cette démarche, en utilisant une méthode d'analyse de risque afin d'identifier les risques de manière factuelle et exhaustive, ainsi que de déterminer formellement le besoin de sécurité. En effet, la SSI ne peut être correctement assurée qu'en explicitant clairement les risques auxquels le système est réellement exposé.

Les risques ainsi appréciés, le responsable du système d'information peut énoncer, en toute connaissance de cause, les objectifs de sécurité à satisfaire. Ces objectifs se rapportent aux trois grands domaines de la sécurité :

- la disponibilité des données et du système d'information ;
- l'intégrité des données et du système d'information ;
- la confidentialité des données, et celle des éléments critiques du système d'information¹ ;

auxquels peuvent s'ajouter deux domaines complémentaires :

- l'authentification, pour garantir que seules les personnes autorisées peuvent accéder aux données et aux processus ;
- la traçabilité, pour pouvoir vérifier que les actions sur les données et sur les processus ont été effectuées par des personnes autorisées, et permettre de déceler toute action ou tentative d'action illégitime.

¹ La connaissance des éléments critiques d'un système relatifs à sa conception et à son fonctionnement peut aider une personne malveillante à accéder aux données confidentielles traitées par ce système.

Référentiel Général de Sécurité (RGS)		
Version	Date	Page
0.99	19/02/2010	10/33

De ces objectifs généraux découlent les fonctions de sécurité qui peuvent être mises en œuvre pour les atteindre. Il est alors possible de choisir les moyens aptes à assurer les fonctions retenues. Ces moyens pourront être :

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

La démarche de sécurité présentée dans le présent chapitre permet ainsi de s'assurer que les objectifs sont bien atteints, que les risques résiduels sont acceptés en toute responsabilité, que les fonctions de sécurité mises en place sont nécessaires et suffisantes et qu'elles ne génèrent pas de nouveaux risques.

La suite de ce chapitre présente un ensemble de recommandations pour la gestion de la SSI dans un organisme (§ 2.2) et dans un projet de système d'information (§2.3).

2.2 - Six grands principes de gestion de la SSI

2.2.1 - Adopter une démarche globale

L'objectif est la cohérence d'ensemble de la démarche de sécurisation des systèmes d'information. Il convient à ce titre de n'oublier aucun élément pertinent, pour éviter toute faille qui réduirait la sécurité globale du SI. Il est également nécessaire que chacune des décisions relatives à la sécurité soit prise au juste niveau hiérarchique.

Il est ainsi recommandé :

- de considérer tous les aspects qui peuvent avoir une influence sur la sécurité des systèmes d'information, techniques (matériels, logiciels, réseaux, ...) et non techniques (organisations, infrastructure, personnel, ...)
- de considérer tous les risques et menaces, d'origine humaine ou naturelle, accidentelle ou délibérée;
- de prendre en compte la SSI au juste niveau hiérarchique, car comme tous les autres domaines de la sécurité, la SSI repose sur une vision stratégique, et nécessite des choix d'autorité (les enjeux, les moyens humains et financiers, les risques résiduels acceptés), et un contrôle des actions et de leur légitimité ;
- de responsabiliser tous les acteurs (décideurs, maîtrise d'ouvrage, maîtrise 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).

2.2.2 - Adapter la SSI selon les enjeux

Il est recommandé que la SSI soit adaptée aux enjeux du système d'information et aux besoins de sécurité de l'AA, afin d'y consacrer les moyens financiers et humains juste nécessaires et suffisants. L'article 3 du [DécretRGS] précise ainsi, dans son 2°, que la réponse aux besoins de protection doit être proportionnée.

Une aide dans cette démarche est proposée dans le document [MaturitéSSI], qui explique comment déterminer rapidement les enjeux relatifs à la sécurité d'un système d'information, comment mesurer l'écart entre le niveau nécessaire de prise en compte de la sécurité et le niveau effectif, et comment en déduire les actions à mettre en œuvre pour atteindre le niveau de sécurité nécessaire.

Référentiel Général de Sécurité (RGS)		
Version	Date	Page
0.99	19/02/2010	11/33

2.2.3 - Gérer les risques SSI

Extrait du [DécretRGS] : Chapitre II : Fonctions de sécurité des systèmes d'information :

« Article 3 :

Dans les conditions fixées par le référentiel général de sécurité mentionné à l'article 2 du présent décret, l'autorité administrative doit, afin de protéger un système d'information :

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

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

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

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

La démarche de gestion des risques SSI, que l'AA doit mener conformément à l'article ci-dessus, consiste principalement à :

- établir le contexte de mise en œuvre du système ;
- identifier, apprécier et hiérarchiser les risques ;
- traiter les risques (les réduire ou les éviter, et accepter de prendre les risques résiduels).

Cette démarche peut être conduite de manière allégée dans le cas de systèmes simples ou sans enjeux importants de sécurité, ou au contraire de manière très approfondie si le système d'information est complexe et les enjeux élevés.

A cet effet, il est recommandé de s'appuyer sur la norme [ISO27005], qui fixe un cadre théorique de la gestion des risques, et de s'appuyer sur la méthode [EBIOS] pour sa mise en œuvre pratique grâce notamment aux explications et aux outils qu'elle propose.

2.2.4 - Élaborer une politique SSI

Il est recommandé d'élaborer et de formaliser une politique SSI globale au niveau de l'AA. Selon les besoins, cette politique SSI pourra être déclinée et complétée notamment pour un domaine particulier, ou pour un système d'information précis.

Le guide [PSSI] fournit une aide pour élaborer une politique SSI.

2.2.5 - Utiliser les produits et prestataires labellisés pour leur sécurité

Extrait du [DécretRGS] : Chapitre II : Fonctions de sécurité des systèmes d'information :

« Article 4 :

Pour mettre en œuvre dans un système d'information les fonctions de sécurité ainsi déterminées, l'autorité administrative recourt à des produits de sécurité et à des prestataires de services de confiance ayant fait l'objet d'une qualification dans les conditions prévues au présent décret ou à tout autre produit ou prestataire pour lesquels elle s'est assurée de la conformité de leurs fonctions de sécurité au référentiel général de sécurité. »

La qualification est un label créé par l'[Ordonnance], qui permet d'attester de la confiance que l'on peut accorder à des produits de sécurité et à des PSCO. D'autres labels existent pour attester de la compétence des professionnels, notamment en matière de SSI. Il est recommandé :

- d'utiliser chaque fois que possible des produits de sécurité qualifiés (§5.1) par l'ANSSI (les catalogues de ces produits sont disponibles sur le site www.ssi.gouv.fr), après s'être assuré que le produit répond bien au besoin et au contexte d'utilisation prévu ;
- de recourir chaque fois que possible à des PSCO qualifiés (§ 5.2) ;
- de prendre en considération, dans le choix des prestataires, en plus de leur qualification, leur éventuelle certification de services ou d'organismes selon la norme [ISO27001] ou d'autres normes équivalentes ;

Référentiel Général de Sécurité (RGS)		
Version	Date	Page
0.99	19/02/2010	12/33

- de prendre en considération, dans le choix de prestataires, la certification de leurs personnels lorsque des compétences particulières sont requises pour une fonction.

2.2.6 - Viser une amélioration continue

Il est recommandé de chercher une amélioration constante de la SSI, par exemple en mettant en place un « système de management de la sécurité de l'information » (SMSI), tel qu'il est défini dans l'[ISO27001], pour :

- planifier la SSI : définir le cadre du SMSI, apprécier les risques SSI et définir leur traitement ;
- mettre en œuvre la SSI : mettre en place et maintenir les mesures de sécurité ;
- vérifier la SSI : vérifier que les mesures de sécurité fonctionnent conformément à l'étape « Planifier » et identifier les améliorations possibles du SMSI ;
- améliorer la SSI : étudier et mettre en place les améliorations identifiées pour le SMSI.

2.3 - Intégration de la SSI dans le cycle de vie des systèmes d'information

Dans tout projet de mise en place d'un système d'information, le besoin de sécurité doit être pris en compte avec la même attention et en même temps et au même titre que les besoins fonctionnels que vise à satisfaire le système, le téléservice ou l'application.

Prise très en amont du projet, son efficacité sera bien supérieure, et son coût bien moindre, que s'il faut corriger les spécifications, voire les équipements ou l'architecture du système, du fait d'une intégration tardive.

Au-delà de la phase de définition (voire même de l'étude d'opportunité en cas de doute sur la possibilité de sécuriser le système d'information au niveau requis), la SSI doit être prise en compte tout au long de la vie d'un système d'information, notamment lors de toute modification, jusqu'à son retrait du service. Cette démarche de réévaluation et d'amélioration constante de la SSI s'appuie notamment sur des audits réguliers de sécurité. En fin de vie, il convient, par exemple, de veiller à la destruction des données et des composants confidentiels, avant de céder, de jeter ou de détruire le système.

Dans ce cycle, une étape essentielle est l'homologation de sécurité du système d'information (§2.3.2), qui doit intervenir avant la mise en service du système, puis être régulièrement réexaminée, afin de prendre les mesures que peuvent imposer les évolutions du système, de ses composants, de son emploi, du contexte humain ou organisationnel, ou encore bien sûr de la menace.

2.3.1 - Des efforts proportionnés aux enjeux SSI

La démarche de sécurité doit être adaptée aux enjeux du projet. Dans ce but, il est recommandé d'utiliser le guide [GISSIP] de l'ANSSI pour l'intégration de la sécurité dans les différentes phases des projets informatiques, et en particulier pour :

- lors de la conception générale, identifier les objectifs généraux de sécurité ;
- lors de la conception détaillée, affiner les objectifs de sécurité et identifier le niveau de risque maximum que l'autorité responsable se déclare prête à accepter ;
- lors de la réalisation du système, décrire concrètement les mesures de sécurité et la manière de les appliquer dans l'environnement effectif d'utilisation ;
- à la fin de la phase de développement et au plus tard avant la phase d'exploitation, prononcer la décision d'homologation (§2.3.2) ;
- tout au long de la vie du système, jusqu'au retrait du service, maintenir la sécurité.

2.3.2 - Un engagement systématique : l'homologation de sécurité

Extrait du [DécretRGS] : Chapitre II : Fonctions de sécurité des systèmes d'information : Article 5 :

Référentiel Général de Sécurité (RGS)		
Version	Date	Page
0.99	19/02/2010	13/33

L'autorité administrative atteste formellement auprès des utilisateurs de son système d'information que celui-ci est protégé conformément aux objectifs de sécurité fixés en application de l'article 3.

Dans le cas d'un téléservice, cette attestation est rendue accessible aux usagers selon les mêmes modalités que celles prévues à l'article 4 de l'ordonnance du 8 décembre 2005 susvisée pour la décision de création du téléservice.»

Cette « attestation formelle », évoquée à l'article 5 *supra*, correspond à une « homologation de sécurité du système d'information ». Celle-ci est obligatoire et est un préalable à la mise en service opérationnelle de tout système d'information. Elle est prononcée par une autorité dite d'homologation, désignée par l'AA, habituellement au sein même de cette AA. Lorsque le système est sous la responsabilité de plusieurs AA, l'autorité d'homologation est désignée conjointement par les AA concernées.

Au sens de l'article 5 *supra*, la décision d'homologation, ou « attestation formelle », est l'engagement par lequel l'autorité d'homologation atteste, au nom de l'AA, que le projet a bien pris en compte les contraintes opérationnelles établies au départ, que les exigences de sécurité sont bien déterminées et satisfaites, et que les risques résiduels sont maîtrisés et acceptés, et que le système d'information est donc apte à entrer en service.

Afin que sa décision soit motivée et justifiée, il est recommandé que l'autorité d'homologation s'appuie sur un dossier de sécurité, constitué selon le modèle décrit dans le guide [GISSIP].

Selon les résultats de l'analyse effectuée lors de la démarche d'homologation, l'autorité d'homologation pourra prononcer :

- une homologation provisoire, assortie de réserves et d'un délai de mise en conformité des défauts de sécurité rencontrés ;
- une homologation, assortie le cas échéant de conditions, pour une durée déterminée (recommandée entre 3 et 5 ans) ;
- un refus d'homologation, si les résultats de l'audit font apparaître des risques résiduels jugés inacceptables.

2.3.3 - Des outils spécifiques pour différentes familles de téléservices

Il est recommandé que les experts SSI et les responsables de système d'information utilisent, pour exprimer les besoins de sécurité et identifier les objectifs de sécurité, des fiches d'expression rationnelle d'objectifs de sécurité (FEROS). Pour faciliter ce travail, et pour les familles les plus usuelles de téléservices qu'une AA peut mettre en œuvre, sept FEROS génériques [FEROSTypes] sont proposées :

- Téléservice de candidature (exemples : candidature dans l'enseignement supérieur, au permis de conduire, ...)
- Téléservice de consultation (exemples : consultation des remboursements de la sécurité sociale, des résultats d'examens, de concours, ...)
- Téléservice de déclaration (exemples : dossier fiscal du particulier (TéléIR), compte fiscal des professionnels, déclaration de changement d'adresse, ...)
- Téléservice de demande (exemples : demande d'extraits d'état civil, de permis de construire, de licence IV, de stage d'étudiants, ...)
- Téléservice d'inscription (exemple : inscription à un concours de la fonction publique)
- Téléservice de paiement en ligne (exemples : paiement d'amendes, règlement de la TVA, règlement d'impôts sur le revenu, ...)
- Téléservice de simulation (exemples : calcul de revalorisation des pensions alimentaires, simulateur de calcul de retraite, d'impôt sur le revenu, ...).

En complément, le guide d'exigences de sécurité [ExigencesTélé] propose un ensemble d'exigences de sécurité qui permettent de répondre aux objectifs de sécurité exprimés dans les [FEROSTypes].

Il est recommandé de s'appuyer sur ces documents chaque fois que le téléservice mis en place entre dans l'une famille présentée *supra*.

Référentiel Général de Sécurité (RGS)		
Version	Date	Page
0.99	19/02/2010	14/33

3 - Fonctions de sécurité

3.1 - Introduction

Extrait de l'Ordonnance]

Article 9.I. - « Un référentiel général de sécurité fixe les règles que doivent respecter les fonctions des systèmes d'information contribuant à la sécurité des informations échangées par voie électronique telles que les fonctions d'identification, de signature électronique, de confidentialité et d'horodatage ».

Extrait du [DécretRGS] : Chapitre I : Référentiel Général de Sécurité :

« Article 1 :

Le référentiel général de sécurité, prévu par l'article 9 de l'ordonnance du 8 décembre 2005 susvisée, fixe les règles auxquelles les systèmes d'information mis en place par les autorités administratives doivent se conformer pour assurer la sécurité des informations échangées, et notamment leur confidentialité et leur intégrité, ainsi que la disponibilité et l'intégrité de ces systèmes et l'identification de leurs utilisateurs.

Ces règles sont définies selon des niveaux de sécurité prévus par le référentiel pour des fonctions de sécurité, telles que l'identification, la signature électronique, la confidentialité ou l'horodatage, qui permettent de répondre aux objectifs de sécurité mentionnés à l'alinéa précédent ... ».

Ce chapitre et les annexes auxquelles il renvoie contiennent les règles de sécurité à respecter pour les fonctions de sécurité d'authentification (§3.2), de signature électronique (§3.3), de confidentialité (§3.4) et d'horodatage (§3.5). Ces règles sont différenciées selon des niveaux de sécurité, définis dans ces mêmes annexes.

En fonction de leur besoin de sécurité, il appartient aux AA de déterminer les fonctions de sécurité ainsi que leurs niveaux de sécurité associés, en s'appuyant sur les méthodes, les outils et les bonnes pratiques proposés au chapitre 2 du présent document.

Lorsque de telles fonctions sont traitées dans le présent chapitre du RGS, l'AA respecte les règles correspondantes aux niveaux de sécurité requis parmi ceux prévus dans ce référentiel.

Dans les cas particuliers suivants, où l'AA détermine :

- un besoin pour un niveau de sécurité non prévu dans ce référentiel, elle doit soit appliquer les règles du niveau juste supérieur, soit appliquer celles du niveau juste inférieur et reconduire alors une analyse des risques résultant de ce choix ;
- un besoin pour un niveau de sécurité supérieur au plus haut niveau du référentiel, elle doit appliquer les règles de ce plus haut niveau, si possible, mettre en place des fonctions et mesures de sécurité complémentaires (non prévues dans le RGS) pour atteindre ses objectifs de sécurité ;
- un besoin pour un niveau de sécurité inférieur au plus bas niveau du référentiel, elle peut n'appliquer que les seules règles de ce plus bas niveau qui répondent à ses objectifs de sécurité.

3.2 - Authentification

L'authentification a pour but de vérifier l'identité dont se réclame une personne ou une machine (ci-après désignée « entité »). Généralement, l'authentification est précédée d'une identification, qui permet à cette entité de se faire reconnaître du système au moyen d'un élément dont on l'a doté. En d'autres termes, s'identifier consiste à communiquer une identité préalablement enregistrée, s'authentifier consiste à apporter la preuve de cette identité. La suite de ce chapitre ne traite que de la fonction d'authentification.

Référentiel Général de Sécurité (RGS)		
Version	Date	Page
0.99	19/02/2010	15/33

Les fonctions d'authentification présentées ci-dessous concernent les mécanismes à base de mots de passe (§3.2.2) et ceux à base de certificats électroniques (§3.2.3 et §3.2.4). Dans tous les cas, lorsque ces mécanismes font appel à des mécanismes cryptographiques, ils doivent respecter les exigences fixées dans les référentiels mentionnés au chapitre 3.2.1.

3.2.1 - Utilisation de mécanismes cryptographiques

Lorsqu'elles mettent en place une fonction d'authentification reposant sur des mécanismes cryptographiques, les AA doivent respecter les règles, et si possible les recommandations, indiquées dans les référentiels [RGS_B_1] et [RGS_B_2], communs à tous les mécanismes cryptographiques, et le référentiel [RGS_B_3], dédié aux mécanismes d'authentification.

3.2.2 - Authentification d'une personne par l'utilisation d'identifiants et de mots de passe statiques

L'authentification d'une personne auprès d'un système d'information *distant* fait intervenir trois entités :

- l'utilisateur : ce dernier souhaite effectuer des opérations sur le système d'information *distant* et doit pour cela prouver son identité ;
- l'environnement de confiance *local* (exemple : le PC d'un agent administratif) ;
- le système d'information *distant* (exemples : une base de donnée, le serveur hébergeant un téléservice).

De manière générale, il n'est pas recommandé de permettre une authentification par « identifiant / mot de passe » de façon directe entre l'utilisateur et le système d'information *distant*. En effet, un dispositif basé sur un identifiant et un mot de passe, du fait de la faiblesse intrinsèque qu'il présente en raison de la possibilité de rejeu, constitue un mécanisme de déverrouillage et non pas un réel mécanisme d'authentification. Un tel dispositif ouvre des possibilités de fraude largement employées, comme le hameçonnage, qui vise à récupérer les informations de connexion (identifiant et mot de passe) de l'utilisateur et permet donc d'usurper son identité.

Ce mécanisme d'authentification ne peut donc offrir qu'un niveau de sécurité limité, qui peut cependant suffire dans certaines applications. Cette section n'impose aucune règle ni niveau de sécurité et se borne à donner quelques recommandations d'usage des identifiants et des mots de passe dans un processus d'authentification d'une personne sur un système d'information *local* ou *distant*.

Il est ainsi recommandé de :

- respecter les bonnes pratiques proposées dans le document [CERTA] pour la création d'un mot de passe fiable et sa bonne gestion ;
- donner la capacité au système d'information de vérifier, au moment de son enregistrement, la complexité du mot de passe choisi par l'utilisateur, de façon à refuser les mots de passe qu'il serait trop aisé de deviner ;
- limiter ce mécanisme d'authentification au contrôle de l'accès à l'environnement local de confiance de l'utilisateur (par exemple, un mécanisme de déverrouillage par identifiant et mot de passe) ;
- mettre en place un dispositif d'authentification reposant sur des mécanismes cryptographiques, qui permet à l'environnement de confiance local, une fois déverrouillé par l'utilisateur, de s'authentifier auprès du système d'information distant au nom de l'utilisateur. Il est également recommandé que ces mécanismes permettent d'assurer la confidentialité et l'intégrité des données auxquelles accède l'utilisateur sur le système d'information distant.

3.2.3 - Authentification d'une personne par certificat électronique

La mise en œuvre par une AA de la fonction de sécurité « authentification » par des mécanismes cryptographiques asymétriques et l'emploi de certificats électroniques peut se faire selon trois niveaux de sécurité aux exigences croissantes : une étoile (*), deux étoiles (**) et trois étoiles (***).

Référentiel Général de Sécurité (RGS)		
Version	Date	Page
0.99	19/02/2010	16/33

Ces exigences, décrites à l'annexe [RGS_A_2], couvrent l'ensemble des composants nécessaires à la mise en œuvre de cette fonction de sécurité, pour les trois niveaux de sécurité. L'AA, après avoir déterminé le niveau de sécurité (*), (**) ou (***) de la fonction de sécurité « authentification » qu'elle souhaite mettre en œuvre au sein de son système d'information, respecte les exigences correspondantes pour chacun des composants suivants :

- le 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.

Les exigences concernant le composant « certificat électronique » portent non seulement sur son contenu, mais également sur les conditions dans lesquelles il est émis par un PSCE ainsi que sur le dispositif de stockage de la clé privée. Ces exigences font l'objet d'une autre annexe du RGS, [RGS_A_7], appelée « Politique de Certification Type authentification ». Le RGS offre également la possibilité d'avoir un certificat électronique unique, dit à « double usage », pour les fonctions d'authentification et de signature. Dans ce cas, le certificat doit respecter les exigences fixées dans la PC Type [RGS_A_11], et ne peut être prévu qu'aux niveaux (*) et (**).

3.2.4 - Authentification d'un serveur par certificat électronique

La mise en œuvre par une AA de la fonction de sécurité « authentification de serveur » par des mécanismes cryptographiques asymétriques et l'emploi de certificats électroniques peut se faire selon trois niveaux de sécurité aux exigences croissantes : une étoile (*), deux étoiles (**) et trois étoiles (***) .

Ces exigences, décrites dans l'annexe [RGS_A_4], couvrent l'ensemble des composants nécessaires à la mise en œuvre de cette fonction de sécurité, pour les trois niveaux de sécurité. L'AA, après avoir déterminé le niveau de sécurité parmi (*), (**) ou (***) de la fonction de sécurité « authentification de serveur » qu'elle souhaite mettre en œuvre au sein de son système d'information, respecte les exigences correspondantes pour chacun des composants suivants :

- le bi-clé et le certificat électronique dont l'usage est l'authentification du serveur et l'établissement d'une session sécurisée ;
- le dispositif de protection des clés privées du serveur ;
- le module de vérification d'authentification ;
- l'application d'authentification du serveur.

Les exigences concernant le composant « certificat électronique » portent non seulement sur son contenu, mais également sur les conditions dans lesquelles il est émis par un PSCE ainsi que sur le dispositif de stockage de la clé privée. Ces exigences font l'objet d'une autre annexe du RGS, [RGS_A_9], appelée « Politique de Certification Type authentification serveur ».

3.3 - Signature électronique

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 serveurs (serveurs applicatifs, téléservices fonctionnant sur une machine ou un groupe de machines), la fonction de « cachet électronique » permet de garantir l'intégrité des informations échangées et l'identification de la machine ayant « cachetée » ces informations. Cette fonction de « cachet » est pour une machine l'équivalent de la fonction signature pour une personne.

Les fonctions de signature (§3.3.2) et de cachet (§3.3.3) sont présentées ci-dessous. Dans tous les cas, lorsque ces fonctions font appel à des mécanismes cryptographiques, ils doivent respecter les exigences fixées dans les référentiels mentionnés au chapitre 3.3.1.

Référentiel Général de Sécurité (RGS)		
Version	Date	Page
0.99	19/02/2010	17/33

3.3.1 - Utilisation de mécanismes cryptographiques

Lorsqu'elles mettent en place une fonction de signature ou de cachet électronique reposant sur des mécanismes cryptographiques, les AA doivent respecter les règles, et si possible les recommandations, indiquées dans les référentiels [RGS_B_1] et [RGS_B_2], communs à tous les mécanismes cryptographiques.

3.3.2 - Signature d'une personne par certificat électronique

La mise en œuvre par une AA de la fonction de sécurité « signature électronique », reposant sur des mécanismes cryptographiques asymétriques et l'emploi de certificats électroniques, peut se faire selon trois niveaux de sécurité aux exigences croissantes : une étoile (*), deux étoiles (**) et trois étoiles (***) .

Ces exigences, décrites dans l'annexe [RGS_A_3], couvrent l'ensemble des composants nécessaires à la mise en œuvre de cette fonction de sécurité, pour les trois niveaux de sécurité. L'AA, après avoir déterminé le niveau de sécurité parmi (*), (**) ou (***) de la fonction de sécurité « signature électronique » qu'elle souhaite mettre en œuvre au sein de son système d'information, respecte les exigences correspondantes pour chacun des composants suivants :

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

Les exigences concernant le composant « certificat électronique » portent non seulement sur son contenu mais également sur les conditions dans lesquelles il est émis par un PSCE ainsi que sur le dispositif de stockage de la clé privée. Ces exigences font l'objet d'une autre annexe du RGS, [RGS_A_8], appelée « Politique de Certification Type signature électronique ». Le RGS offre également la possibilité d'avoir un certificat électronique unique, dit à « double usage », pour les fonctions d'authentification et de signature. Dans ce cas, le certificat doit respecter les exigences fixées dans la PC Type [RGS_A_11], et ne peut être prévu qu'aux niveaux (*) et (**).

Cas particulier de la signature des actes administratifs au sens de l'[Ordonnance] :

Extrait de l'[Ordonnance]

Article 8 : « Les actes des autorités administratives peuvent faire l'objet d'une signature électronique. Celle-ci n'est valablement apposée que par l'usage d'un procédé, conforme aux règles du référentiel général de sécurité mentionné au I de l'article 9, qui permette l'identification du signataire, garantisse le lien de la signature avec l'acte auquel elle s'attache et assure l'intégrité de cet acte ».

L'AA 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, et respecte 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'[Arrêté260704] et portant sur la délivrance de certificats électroniques dits « qualifiés » au sens du [décret2001-272], sont requises pour la génération de signatures électroniques « présumées fiables » au sens du [décret2001-272].

Ces exigences constituent un sous-ensemble de celles contenues dans le document [RGS_A_8] pour le niveau de sécurité (***), 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 [décret2001-272], établie avec un dispositif sécurisé de création de signature certifié conforme dans les conditions de l'article 3 du [décret2001-272] et mettant en œuvre des certificats de signature électronique conformes au niveau de sécurité (***) de [RGS_A_8] est *de facto* « présumée fiable » selon le [décret2001-272] et donc au sens de l'article 1316-4 du code civil.

Référentiel Général de Sécurité (RGS)		
Version	Date	Page
0.99	19/02/2010	18/33

3.3.3 - Cachet d'un serveur par certificat électronique

La mise en œuvre par une AA de la fonction de sécurité « cachet », reposant sur des mécanismes cryptographiques asymétriques et l'emploi de certificats électroniques, peut se faire selon trois niveaux de sécurité aux exigences croissantes : une étoile (*), deux étoiles (***) et trois étoiles (***).

Ces exigences, décrites dans l'annexe [RGS_A_5], couvrent l'ensemble des composants nécessaires à la mise en œuvre de cette fonction de sécurité, pour les trois niveaux de sécurité. L'AA, après avoir déterminé le niveau de sécurité parmi (*), (***) ou (****) de la fonction de sécurité « cachet » qu'elle souhaite mettre en œuvre au sein de son système d'information, respecte les exigences correspondantes pour chacun des composants suivants :

- le bi-clé et le certificat électronique dont l'usage est la création d'un cachet par une machine ;
- le dispositif de création d'un cachet par une machine ;
- le module de vérification d'un cachet ;
- l'application de création d'un cachet.

Les exigences concernant le composant « certificat électronique » portent non seulement sur son contenu mais également sur les conditions dans lesquelles il est émis par un PSCE ainsi que sur le dispositif de stockage de la clé privée. Ces exigences font l'objet d'une autre annexe du RGS, [RGS_A_10], appelée « Politique de Certification Type cachet ».

3.4 - Confidentialité

La confidentialité est le caractère réservé d'une information dont l'accès est limité aux seules personnes autorisées à la connaître.

Le chiffrement est un procédé cryptographique garantissant la confidentialité des données chiffrées contre toute personne ne possédant pas la clé de déchiffrement. Il s'agit du mécanisme essentiel de protection de la confidentialité et fait l'objet du chapitre 3.4.2.

Par ailleurs, 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. Ces droits d'accès sont déterminés, en fonction du strict besoin d'en connaître des usagers et de celui des agents dans le cadre de leurs missions. A cet effet, il est recommandé que des mécanismes techniques soient mis en place pour s'assurer que seules les personnes autorisées puissent accéder aux données en fonction de leur besoin d'en connaître. Il est recommandé également que ces mécanismes soient robustes et implémentés au plus près du lieu de stockage des données.

Dans tous les cas, les mécanismes de chiffrement et les mécanismes techniques de gestion des droits d'accès, dès lors qu'ils font appel à des mécanismes cryptographiques, doivent respecter les exigences fixées dans les référentiels mentionnés au chapitre 3.4.1.

3.4.1 - Utilisation de mécanismes cryptographiques

Lorsqu'elles mettent en place une fonction de confidentialité reposant sur des mécanismes cryptographiques, les AA doivent respecter les règles, et si possible les recommandations, indiquées dans les référentiels [RGS_B_1] et [RGS_B_2], communs à tous les mécanismes cryptographiques.

3.4.2 - Confidentialité par certificat électronique

La mise en œuvre par une AA de la fonction de sécurité « confidentialité », reposant sur des mécanismes cryptographiques asymétriques et l'emploi de certificats électroniques, peut se faire selon trois niveaux de sécurité aux exigences croissantes : une étoile (*), deux étoiles (***) et trois étoiles (***).

Référentiel Général de Sécurité (RGS)		
Version	Date	Page
0.99	19/02/2010	19/33

Ces exigences, décrites dans l'annexe [RGS_A_1], couvrent l'ensemble des composants nécessaires à la mise en œuvre de cette fonction de sécurité, pour les trois niveaux de sécurité. L'AA, après avoir déterminé le niveau de sécurité parmi (*), (**) ou (***) de la fonction de sécurité « confidentialité » qu'elle souhaite mettre en œuvre au sein de son système d'information, respecte les exigences correspondantes pour chacun des composants suivants :

- le bi-clé et le certificat électronique dont l'usage est le chiffrement ;
- le dispositif de protection des clés privées ;
- le module de chiffrement ;
- le module de déchiffrement.

Les exigences concernant le composant « certificat électronique » portent non seulement sur son contenu mais également sur les conditions dans lesquelles il est émis par un PSCE ainsi que sur le dispositif de stockage de la clé privée. Ces exigences font l'objet d'une autre annexe du RGS, [RGS_A_6], appelée « Politique de Certification Type confidentialité ».

3.5 - Horodatage

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 qui devra respecter les exigences mentionnées au chapitre 3.5.1. De plus, cette contremarque sera délivrée par un prestataire de service d'horodatage électronique (PSHE) qui devra respecter les exigences du chapitre 3.5.2.

3.5.1 - Utilisation des mécanismes cryptographiques

Lorsqu'elles mettent en place une fonction d'horodatage reposant sur des mécanismes cryptographiques, les AA doivent respecter les règles, et si possible les recommandations, indiquées dans les référentiels [RGS_B_1] et [RGS_B_2], communs à tous les mécanismes cryptographiques.

3.5.2 - Horodatage par contremarques de temps

Les contremarques de temps doivent être émises conformément aux exigences de l'annexe [RGS_A_12], appelée « Politique d'Horodatage Type ». Cette annexe ne distingue qu'un unique niveau de sécurité auquel les AA doivent se conformer dès lors qu'elles désirent mettre en œuvre la fonction d'horodatage au sein de leur système d'information.

Référentiel Général de Sécurité (RGS)		
Version	Date	Page
0.99	19/02/2010	20/33

4 - Accusé d'enregistrement et accusé de réception

4.1 - Introduction

Extrait de l'Ordonnance]

Article 5.I - « Toute demande, déclaration ou production de documents adressée par un usager à une autorité administrative par voie électronique ainsi que tout paiement opéré dans le cadre d'un téléservice fait l'objet d'un accusé de réception électronique et, lorsque celui-ci n'est pas instantané, d'un accusé d'enregistrement électronique. Cet accusé de réception et cet accusé d'enregistrement sont émis selon un procédé conforme aux règles fixées par le référentiel général de sécurité mentionné au I de l'article 9 ».

L'article 5.II a modifié comme suit le premier alinéa de l'article 16 de la loi n° 2000-321 du 12 avril 2000 modifiée relative aux droits des citoyens dans leurs relations avec les administrations :

« Toute personne tenue de respecter une date limite ou un délai pour présenter une demande, déposer une déclaration, exécuter un paiement ou produire un document auprès d'une autorité administrative peut satisfaire à cette obligation au plus tard à la date prescrite au moyen d'un envoi postal, le cachet de la poste faisant foi, ou d'un envoi par voie électronique, auquel cas fait foi la date figurant sur l'accusé de réception ou, le cas échéant, sur l'accusé d'enregistrement adressé à l'utilisateur par la même voie conformément aux dispositions du I de l'article 5 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. Ces dispositions ne sont applicables ni aux procédures régies par le code des marchés publics, ni à celles relevant des articles L. 1411-1 et suivants du code général des collectivités territoriales, ni à celles pour lesquelles la présence personnelle du demandeur est exigée en application d'une disposition particulière ».

L'article 5 de l'Ordonnance] prévoit que les accusés d'enregistrement et les accusés de réception soient 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, qui sont prévues au chapitre 3 du présent document telles que les fonctions de signature, de cachet et d'horodatage. Le chapitre 4.2 fixe ainsi les règles et donne des recommandations pour l'utilisation de ces fonctions dans la création et la gestion des accusés d'enregistrement et de réception.

4.2 - Règles et recommandations de sécurité

Les accusés d'enregistrement et de réception sont générés et émis par les AA à destination des usagers, il revient donc aux AA de mettre en place les systèmes d'information à cet effet.

Les AA doivent déterminer les fonctions de sécurité nécessaires à la protection de ces accusés et leur niveau de sécurité. Comme pour tout système d'information, il est recommandé de recourir à la démarche générale de sécurité présentée au chapitre 2 pour conduire cette analyse.

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] :

- soient horodatés avec des contremarques de temps conformes aux exigences du document [RGS_A_12] pour le niveau de sécurité unique prévu par ce document ;
- soient signés par un agent d'une AA (ou cachetés par une machine d'une AA) conformément aux exigences des documents [RGS_A_3] et [RGS_A_8] (ou [RGS_A_5] et [RGS_A_10]) pour le niveau de sécurité choisi par l'AA 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], la date figurant sur les accusés devant faire foi, cela impose de garantir aux usagers un niveau de fiabilité supplémentaire des accusés. Les AA 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, il est recommandé dans tous les cas d'assurer la sauvegarde des accusés d'enregistrement et de réception tant que peuvent survenir d'éventuelles réclamations de la part des usagers.

Référentiel Général de Sécurité (RGS)		
Version	Date	Page
0.99	19/02/2010	21/33

5 - Qualification

Extrait de l'[Ordonnance] :

Article 9.III - « Les produits de sécurité et les prestataires de services de confiance peuvent obtenir une qualification qui atteste de leur conformité à un niveau de sécurité du référentiel général de sécurité. Un décret précise les conditions de délivrance de cette qualification. Cette délivrance peut, s'agissant des prestataires de services de confiance, être confiée à un organisme privé habilité à cet effet ».

Extrait du [DécretRGS] : Chapitre II : Fonctions de sécurité des systèmes d'information :

« Article 4 :

Pour mettre en œuvre dans un système d'information les fonctions de sécurité ainsi déterminées, l'autorité administrative recourt à des produits de sécurité et à des prestataires de services de confiance ayant fait l'objet d'une qualification dans les conditions prévues au présent décret ou à tout autre produit ou prestataire pour lesquels elle s'est assurée de la conformité de leurs fonctions de sécurité au référentiel général de sécurité. »

L'objet de ce chapitre est de décrire les procédures de qualification des produits de sécurité et des prestataires de services de confiance qui permettent d'obtenir une attestation de conformité au RGS.

5.1 - Qualification de produits de sécurité

Extrait du [DécretRGS] chapitre III : Qualification des produits de sécurité :

« Article 6

La demande de qualification d'un produit de sécurité, prévue par l'article 9 de l'ordonnance du 8 décembre 2005 susvisée, est adressée à l'Agence nationale de la sécurité des systèmes d'information, par tout commanditaire, notamment un fabricant ou un fournisseur du produit ou une autorité administrative. La qualification est obtenue à l'issue d'une évaluation des fonctions de sécurité du produit au regard des règles du référentiel général de sécurité.

Article 7

La demande de qualification contient une description du produit et de ses fonctions de sécurité ainsi que les objectifs de sécurité qu'il vise à satisfaire.

L'Agence nationale de la sécurité des systèmes d'information s'assure que le niveau et les objectifs de sécurité sont cohérents avec le besoin de sécurité des autorités administratives. Elle instruit cette demande lorsque l'ensemble des matériels, des logiciels et de la documentation nécessaires pour réaliser l'évaluation sont disponibles et accessibles.

Article 8

L'évaluation du produit est effectuée dans les conditions et avec les garanties prévues par le décret du 18 avril 2002 susvisé.

Article 9

Le Premier ministre délivre la qualification du produit pour l'un des niveaux fixés par le référentiel, attestant ainsi de sa conformité aux exigences fixées par ce dernier.

Cette attestation est assortie, le cas échéant, de conditions et de réserves et précise sa durée de validité. Elle mentionne les objectifs de sécurité que le produit satisfait et, le cas échéant, le degré de qualification obtenu.

Tout changement des circonstances dans lesquelles la qualification a été délivrée peut conduire le Premier ministre à suspendre ou à retirer la qualification, après que le commanditaire a pu faire valoir ses observations »

La procédure de qualification des produits de sécurité est définie par les articles ci-dessus extraits du [DécretRGS].

Les produits de sécurité, selon l'article 1^{er} de l'[Ordonnance], sont des dispositifs, matériels ou logiciels, qui mettent en œuvre des fonctions contribuant à la sécurité des informations échangées par voie électronique.

Référentiel Général de Sécurité (RGS)		
Version	Date	Page
0.99	19/02/2010	22/33

La sécurité du système d'information repose principalement sur les produits de sécurité. L'efficacité de la protection du SI dépend non seulement des qualités techniques intrinsèques des produits mais également des conditions d'emploi des produits², celles-ci étant de la responsabilité de l'AA. Cette dernière attend en revanche légitimement des produits qu'ils tiennent leurs « promesses » en matière de sécurité, en couvrant effectivement les objectifs de sécurité qu'elle s'est fixés. Afin de l'attester, un produit de sécurité peut obtenir une qualification délivrée par l'ANSSI.

L'ANSSI procède à la qualification de produits de sécurité et ainsi atteste de la conformité des fonctions de sécurité d'un produit aux règles définies au chapitre 3 du présent document. Dans cette version du RGS, les fonctions d'authentification, de signature, de cachet, de confidentialité et d'horodatage peuvent faire l'objet d'une qualification. Dans le cas de fonctions utilisant des mécanismes cryptographiques, la qualification atteste de la conformité aux référentiels techniques [RGS_B_1] et [RGS_B_2].

L'ANSSI s'appuie sur des centres d'évaluation qu'elle a agréés pour mener les évaluations des fonctions de sécurité préalablement à la délivrance de la qualification.

La mise en œuvre détaillée de la procédure de qualification fait l'objet des trois documents suivants :

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

Ces différentes procédures se distinguent principalement par le degré d'assurance dans l'évaluation du produit. Le choix de la procédure à suivre est précisé dans les annexes du RGS, il dépend notamment du type de produits et du niveau de sécurité.

Dans tous les cas, il sera demandé au commanditaire d'une évaluation en vue d'une qualification de produire une cible de sécurité du produit. Pour garantir une bonne cohérence des objectifs et des exigences de sécurité, il est recommandé que la cible de sécurité soit conforme à un profil de protection (PP) proposé par l'ANSSI au chapitre 8, chaque fois que possible.

L'ANSSI publie sur son site internet le catalogue des produits de sécurité qualifiés.

5.2 - Qualification des Prestataires de Services de Confiance (PSCO)

Extrait du [DécretRGS] : (Chapitre IV – Qualification des prestataires de services de confiance) :

« Section 2 : Qualification des prestataires de services de confiance par des organismes habilités

Article 15

Un prestataire de services de confiance peut recevoir une qualification qui atteste de la conformité des services à un niveau de sécurité défini par le référentiel général de sécurité. Il adresse sa demande auprès d'un organisme habilité dans les conditions prévues à la section précédente. L'organisme habilité évalue la conformité des fonctions de sécurité mises en œuvre par le service offert par le prestataire au regard des règles du référentiel général de sécurité correspondant au niveau de sécurité pour lequel la demande de qualification a été faite. L'organisme adresse un rapport d'évaluation à l'Agence nationale de la sécurité des systèmes d'information et à la direction générale de la modernisation de l'État.

Article 16

Lorsqu'il prononce la qualification, l'organisme habilité délivre à cet effet au prestataire une attestation précisant les fonctions de sécurité couvertes par la qualification et les conditions s'y attachant. La qualification est valable pour une durée maximale de trois ans et peut être renouvelée dans les mêmes conditions. L'organisme habilité rend publiques les attestations

² Telles que l'exposition aux menaces, la configuration et le paramétrage, l'application des correctifs de sécurité, le code développé pour l'intégrer dans le SI, la présence d'autres mécanismes de sécurité externes au produit, le personnel exploitant ...

Référentiel Général de Sécurité (RGS)		
Version	Date	Page
0.99	19/02/2010	23/33

de qualification qu'il délivre.

Article 17

Lorsque l'organisme habilité décide de suspendre ou de retirer une qualification ou d'en modifier les conditions, il informe sans délais des raisons à l'origine de ces décisions la direction générale de la modernisation de l'État et l'Agence nationale de la sécurité des systèmes d'information. Il rend publique cette décision.

Article 18

Lorsqu'elles recourent à un prestataire de services de confiance qualifié dans les conditions du présent chapitre, les administrations de l'État en informent l'Agence nationale de la sécurité des systèmes d'information.

Article 19

Une autorité administrative qui agit comme prestataire de services de confiance pour ses besoins propres ou au profit d'autres autorités administratives peut être qualifiée par un organisme habilité, dans les conditions du présent chapitre.

Lorsque le prestataire de services de confiance est une administration de l'État, il doit solliciter au préalable l'avis de l'Agence nationale de la sécurité des systèmes d'information, qui peut proposer de procéder elle-même à l'évaluation des fonctions de sécurité mises en œuvre par cette autorité en vue de sa qualification. Dans ce cas, le Premier ministre délivre la qualification et décide le cas échéant de sa suspension ou de son retrait lorsque les conditions s'y attachant ne sont plus satisfaites. »

La procédure de qualification des prestataires de services de confiance est définie par les articles ci-dessus extraits du [DécretRGS].

Un prestataire de services de confiance, selon l'article 1^{er} de l'[Ordonnance], est une personne offrant des services tendant à la mise en œuvre de fonctions qui contribuent à la sécurité des informations échangées par voie électronique.

La qualification permet d'attester de la conformité des fonctions de sécurité mises en œuvre par le service offert par le prestataire au regard des règles définies au chapitre 3 du présent document.

Dans cette version du RGS, deux familles de PSCO peuvent faire qualifier leurs services :

- les prestataires de services de certification électronique pour les fonctions d'authentification, de signature (ou de cachet) et de confidentialité ;
- les prestataires de services d'horodatage électronique pour la fonction d'horodatage.

Cette qualification de prestataire permet d'attester de leur conformité aux référentiels techniques suivants :

- Politique de Certification Type « Confidentialité » [RGS_A_6] ;
- Politique de Certification Type « Authentification » [RGS_A_7] ;
- Politique de Certification Type « Signature » [RGS_A_8] ;
- Politique de Certification Type « Authentification serveur » [RGS_A_9] ;
- Politique de Certification Type « Cachet » [RGS_A_10] ;
- Politique de Certification Type « Authentification et signature » [RGS_A_11] ;
- Politique d'Horodatage Type [RGS_A_12].

Référentiel Général de Sécurité (RGS)		
Version	Date	Page
0.99	19/02/2010	24/33

6 - Validation des certificats électroniques

Extrait de l'[Ordonnance] :

Article 10 : « Les certificats électroniques délivrés aux autorités administratives et à leurs agents en vue d'assurer leur identification dans le cadre d'un système d'information font l'objet d'une validation par l'État dans des conditions précisées par décret ».

Extrait du [DécretRGS] : chapitre V : Validation des certificats électroniques :

« Article 20

Au sens du présent chapitre, on entend par :

1° « Certificat électronique » : des données sous forme électronique attestant du lien entre une autorité administrative ou un agent d'une autorité administrative et des éléments cryptographiques qui lui sont propres et qui sont utilisés par une fonction de sécurité assurant l'identification de cette autorité ou de cet agent dans un système d'information ;

2° « Validation d'un certificat électronique » : la procédure mise en place par l'État pour garantir que le certificat électronique d'un agent ou d'une autorité administrative a été délivré par une autorité administrative.

Article 21

En application de l'article 10 de l'ordonnance du 8 décembre 2005 susvisée, l'Agence nationale de la sécurité des systèmes d'information met en place une procédure de validation des certificats électroniques délivrés aux autorités administratives ou à leurs agents.

Article 22

La validation des certificats électroniques d'une autorité administrative ou de ses agents est subordonnée au respect par cette autorité des règles du référentiel général de sécurité relatives à la délivrance de ces certificats. L'Agence nationale de la sécurité des systèmes d'information peut vérifier sur place les conditions de délivrance de ces certificats.

Dans le cas d'un téléservice, les autorités administratives mettent à la disposition de leurs usagers les informations, dont la liste est fixée par un arrêté du Premier ministre, relatives à la délivrance et à la validation de leurs certificats électroniques.

Article 23

Un arrêté du Premier ministre précise les modalités de mise en œuvre de la procédure de validation. Les autorités administratives doivent obtenir la validation de leurs certificats électroniques et de ceux de leurs agents au plus tard dans les trois ans à compter de la publication de cet arrêté »

L'article 10 de l'[Ordonnance] prévoit que les certificats électroniques délivrés aux AA et à leurs agents sont validés par l'État. Les articles 20 à 23 du [DécretRGS] précisent les conditions de cette validation.

Ces certificats électroniques sont mis en œuvre dans le but d'assurer les fonctions de sécurité exposées au chapitre 3 :

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

L'objet de cette validation est de garantir à ceux qui doivent se fier à ces certificats électroniques que leurs porteurs sont bien les autorités administratives ou les agents identifiés dans ces certificats.

L'AA doit ainsi mettre en place une procédure de délivrance de certificats qui permet de garantir la fiabilité des informations contenues dans ces certificats. Cette procédure comporte notamment les fonctions :

- d'identification et de vérification de l'identité des agents à qui seront délivrés des certificats ;
- de fabrication technique des certificats ;
- de remise des certificats aux porteurs ;
- de révocation et de renouvellement des certificats.

Référentiel Général de Sécurité (RGS)		
Version	Date	Page
0.99	19/02/2010	25/33

Une AA recourt à un PSCE pour la délivrance de ces certificats. L'AA peut être son propre PSCE ou peut recourir aux services d'un prestataire externe pour tout ou partie des fonctions techniques citées ci-dessus. Dans tous les cas, l'AA reste seule responsable du processus global de délivrance.

La procédure de validation (§ 6.2) consiste à vérifier que la procédure de délivrance de certificats est fiable et conforme aux règles de sécurité du RGS (§ 6.1).

En outre, en application de l'article 22 du [décretRGS], la liste des informations que les AA doivent mettre à la disposition de leurs usagers est précisée au § 6.3.

Enfin, le rôle de l'IGC/A dans la validation des certificats est décrit au § 6.4.

6.1 - Règles de sécurité

Le PSCE chargé de la délivrance des certificats doit :

- rédiger une Politique de Certification (PC) conforme aux modèles des Politiques de Certification Types (annexes [RGS_A_6] à [RGS_A_11]) pour chacune des autorités de certification (AC) relevant de ce PSCE ;
- respecter les règles du chapitre 3 relatives aux fonctions de sécurité mettant en œuvre de tels certificats, et notamment les exigences prévues par les Politiques de Certification Types (PC-Types).

Les AC mentionnées à l'alinéa précédent peuvent elles-mêmes être certifiées par des AC, dites « AC intermédiaires », qui à leur tour peuvent être certifiées par d'autres AC intermédiaires, ainsi de suite jusqu'à l'AC de plus haut niveau dite « AC racine ». Cet ensemble d'AC est appelé « chaîne de certification ».

L'AA doit rédiger une PC globale contenant l'ensemble des exigences de sécurité applicables aux AC intervenant dans la chaîne de certification (AC racine et les éventuelles AC intermédiaires). Ces exigences doivent être issues des PC-Types et adaptées au contexte particulier de la certification d'AC.

6.2 - Procédure de validation

Conformément à l'article 21 du [DécretRGS], l'ANSSI est chargée de mettre en place cette procédure de validation.

Conformément à l'article 23 du [DécretRGS], les AA disposent d'un délai de trois ans à compter de la publication du présent arrêté pour obtenir la validation de leurs certificats. A cet effet, l'AA adresse à l'ANSSI un dossier de demande de validation. Pour les systèmes d'information mis en place après ce délai de trois ans, la demande de validation devra donc être préalable à la mise en place du système.

Le dossier de demande comporte :

- l'identification précise de l'AA ;
- les politiques de certification rédigées pour les AC (y compris pour les AC intermédiaires et AC racine) concernées par la demande ;
- les procédures relatives à la délivrance des certificats ;
- le cas échéant, les documents permettant d'attester de la conformité des AC aux PC-Types, tels que des attestations de qualification au sens du [DécretRGS] ou des résultats d'audit ;
- le certificat de l'AC racine concernée par la demande.

Conformément à l'article 22 du [DécretRGS], l'ANSSI peut demander à vérifier sur place les conditions de délivrance des certificats électroniques. L'objet de cet audit est de s'assurer que les procédures mises en place par le PSCE sont bien conformes aux règles du RGS. Cet audit porte

Référentiel Général de Sécurité (RGS)		
Version	Date	Page
0.99	19/02/2010	26/33

notamment sur les PC de l'AC racine, des éventuelles AC intermédiaires de la chaîne de certification et de la ou des AC délivrant des certificats à l'AA, sur leur application, notamment pour les demandes, la remise et la gestion du cycle de vie des certificats, ainsi que sur les procédures établies entre l'AA et les éventuels prestataires externes.

A l'issue de l'audit, et en l'absence de non-conformité, le certificat de l'AC racine utilisée par l'AA peut alors, sur demande de l'AA, être mis à disposition du public par voie électronique par l'ANSSI sur son site internet www.ssi.gouv.fr. Ce certificat de l'AC racine permet aux usagers et agents d'AA, s'ils le souhaitent, de vérifier la chaîne de certification.

6.3 - Liste des informations relatives à la délivrance et à la validation

En application de l'article 22 du [DécretRGS], les AA sont tenues de mettre à la disposition des usagers de leurs téléservices au minimum les informations suivantes relatives à la délivrance et à la validation des certificats électroniques :

- la politique de certification de l'AC délivrant les certificats des agents, des serveurs et des services applicatifs de l'AA mettant en œuvre le téléservice ;
- la liste des AC intervenant dans la chaîne de certification ;
- le certificat de l'AC racine ;
- la mention de la validation, au sens des présentes dispositions, des certificats délivrés.

6.4 - Rôle de l'IGC/A

L'infrastructure de gestion de clés cryptographiques de l'administration, dite IGC/A, est un service de certification électronique mis en œuvre par l'ANSSI.

L'objectif de ce service est de mettre à disposition des utilisateurs devant se fier à des certificats les éléments techniques permettant de vérifier simplement la chaîne de certification, jusqu'au certificat racine de l'AC « IGC/A », qui a fait l'objet d'un avis [AvisCertificatsIGC/A] publié au *Journal Officiel* de la République française du 17 février 2007.

Lorsque le certificat racine de l'IGC/A est intégré dans les logiciels installés sur les ordinateurs des utilisateurs, la vérification de la chaîne est alors automatique (sous réserve de la bonne configuration du logiciel).

Ce service ne peut fonctionner que si l'AC racine de l'AA a été préalablement certifiée par l'AC de l'IGC/A. Actuellement seules les AC racines des administrations de l'Etat peuvent demander à bénéficier de ce service. Celles-ci devront faire la preuve du respect des exigences de [PC_IGC/A] avant la certification par l'IGC/A.

Référentiel Général de Sécurité (RGS)		
Version	Date	Page
0.99	19/02/2010	27/33

7 - Liste des documents constitutifs du RGS

Ces documents contiennent les règles de sécurité, le cas échéant selon différents niveaux de sécurité, des fonctions de sécurité traitées au chapitre 3. Ils font à ce titre partie intégrante du RGS et sont classés en deux catégories :

- utilisation de certificats électroniques dans les fonctions de sécurité ([RGS_A_x]) ;
- utilisation de mécanismes cryptographiques dans les fonctions de sécurité ([RGS_B_y]).

7.1 - Documents applicables concernant l'utilisation de certificats électroniques dans les fonctions de sécurité

- [RGS_A_1] Fonction de sécurité « Confidentialité » - version 2.3
- [RGS_A_2] Fonction de sécurité « Authentification » - version 2.3
- [RGS_A_3] Fonction de sécurité « Signature électronique » - version 2.3
- [RGS_A_4] Fonction de sécurité « Authentification serveur » - version 2.3
- [RGS_A_5] Fonction de sécurité « Cachet » - version 2.3
- [RGS_A_6] Politique de Certification Type « Confidentialité » - version 2.3
- [RGS_A_7] Politique de Certification Type « Authentification » - version 2.3
- [RGS_A_8] Politique de Certification Type « Signature électronique » - version 2.3
- [RGS_A_9] Politique de Certification Type « Authentification serveur » - version 2.3
- [RGS_A_10] Politique de Certification Type « Cachet » - version 2.3
- [RGS_A_11] Politique de Certification Type « Authentification et Signature » - version 2.3
- [RGS_A_12] Politique d'Horodatage Type - version 2.3
- [RGS_A_13] Variables de temps - version 2.3
- [RGS_A_14] Profils de certificats, CRL, OCSP et algorithmes cryptographiques - version 2.3

Tous ces documents sont consultables à l'adresse <http://www.ssi.gouv.fr/rgs>.

7.2 - Documents applicables concernant l'utilisation de mécanismes cryptographiques dans les fonctions de sécurité

- [RGS_B_1] Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques - version 1.20
- [RGS_B_2] Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques - version 1.1
- [RGS_B_3] Règles et recommandations concernant les mécanismes d'authentification - version 1.0

Ces documents sont consultables à l'adresse <http://www.ssi.gouv.fr/rgs>.

Référentiel Général de Sécurité (RGS)		
Version	Date	Page
0.99	19/02/2010	28/33

8 - Liste des Profils de Protection

Un profil de protection (PP) définit un ensemble d'objectifs et d'exigences de sécurité, indépendant de l'implémentation, pour une catégorie de produits qui couvre des besoins de sécurité communs à plusieurs utilisateurs. Les profils de protection sont réutilisables et normalement publics.

Le concept de profil de protection permet le développement de standards fonctionnels et constitue une aide à la formulation du cahier des charges d'un produit de sécurité.

Les profils de protection peuvent être certifiés, attestant ainsi de leur conformité aux exigences définies dans les Critères Communs.

La liste des PP ci-dessous est donnée à titre d'information. Certains ont été produits et certifiés par l'ANSSI (<http://www.ssi.gouv.fr/archive/fr/confiance/pp.html>), d'autres sont issus de normes européennes.

Référence du PP	Nom du PP	Date du PP
CWA 14167-1	Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1	Juin 2003
CWA 14167-2	Cryptographic Module for CSP Signing operation with Backup (PP certifié le 18 décembre 2003 sous la référence PP/0308)	octobre 2003
CWA 14167-3	Cryptographic Module for CSP Key Generation Services	Février 2004
CWA 14167-4	Cryptographic Module for CSP Signing operation without Backup (PP certifié le 18 décembre 2003 sous la référence PP/0309)	octobre 2003
CWA 14169 type 1	Dispositif sécurisé de création de signature (EAL4+). Fonction de génération des données de création et de vérification de signature électronique. (PP certifié par le BSI en avril 2002)	Avril 2002
CWA 14169 type 2	Dispositif sécurisé de création de signature (EAL4+). Fonction de création de signature électronique. (PP certifié par le BSI en avril 2002)	Avril 2002
CWA 14169 type 3	Dispositif sécurisé de création de signature (EAL4+). Fonction de génération des données de création et de vérification de signature électronique. et de création de signature électronique (PP certifié par le BSI en avril 2002)	Avril 2002
CWA 14365-2	Protection Profile for Software Signature Creation Devices	Mars 2004
PP-CIP-CCv3.1 Version 1.9	Chiffreur IP EAL3+ (PP certifié le 22 août 2008 sous la référence DCSSI-PP 2008/08)	Juillet 2008
PP-PFP-CCv3.1 Version 1.7	Pare feu personnel EAL3+ (PP certifié le 30 mai 2008 sous la référence DCSSI-PP 2008/01)	mai 2008
PP-ACSE-CCv3.1 Version 1.6	Application de création de signature EAL3+ (PP certifié le 8 août 2008 sous la référence DCSSI-PP 2008/05)	17 juillet 2008
PP-MVSE-CCv3.1 Version 1.6	Module de vérification de signature EAL3+ (PP certifié le 8 août 2008 sous la référence DCSSI-PP 2008/06)	17 juillet 2008
PP-SH-CCv3.1 Version 1.7	Système d'horodatage EAL3+ (PP certifié le 23 octobre 2008 sous la référence DCSSI-PP 2008/07)	18 juillet 2008

Référentiel Général de Sécurité (RGS)		
Version	Date	Page
0.99	19/02/2010	29/33

9 - Glossaire

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

Autorité de certification (AC) – Au sein d'un PSCE, une Autorité de Certification a en charge, au nom et sous la responsabilité de ce PSCE, l'application d'au moins une politique de certification et est identifiée comme telle, en tant qu'émetteur (champ "issu" du certificat), dans les certificats émis au titre de cette politique de certification.

Autorité d'horodatage (AH) – Au sein d'un prestataire de services d'horodatage électronique (PSHE), une Autorité d'Horodatage a en charge, au nom et sous la responsabilité de ce PSHE, l'application d'au moins une politique d'horodatage en s'appuyant sur une ou plusieurs Unités d'Horodatage.

Autorité d'homologation – Personne qui, au sein de l'AA responsable du système d'information, est désignée pour prononcer la décision d'homologation de sécurité.

Certificat électronique – Fichier électronique attestant qu'un bi-clé appartient à une personne physique, une personne morale, un élément matériel ou un logiciel identifié, directement ou indirectement (pseudonyme). Il est délivré par un PSCE. En signant le certificat, l'AC valide le lien entre l'identité et la clé publique. Le certificat est valide pendant une durée limitée précisée dans celui-ci.

Contremarque de temps – Donnée qui lie une représentation d'une information à un temps particulier, exprimé en heure UTC, établissant ainsi la preuve que l'information existait à cet instant-là.

Fonction de sécurité – Fonction mise en œuvre au sein d'un système d'information contribuant à la sécurité des informations échangées par voie électronique.

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

Jeton d'horodatage – Même signification que contremarque de temps.

Politique d'horodatage (PH) – Ensemble de règles, identifié par un nom ou un numéro unique (appelé « OID » pour « Object IDentifier »), définissant les exigences auxquelles un PSHE se conforme pour la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'une contremarque de temps à une communauté particulière et/ou une classe d'application avec des exigences de sécurité communes. Une PH peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les abonnés et les utilisateurs de contremarques de temps.

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

Référentiel Général de Sécurité (RGS)		
Version	Date	Page
0.99	19/02/2010	30/33

Prestataire de services de certification électronique (PSCE) – Toute personne ou entité qui est responsable de la gestion de certificats électroniques tout au long de leur cycle de vie, vis-à-vis des porteurs et utilisateurs de ces certificats. Un PSCE peut fournir différentes familles de certificats correspondant à des finalités différentes et/ou des niveaux de sécurité différents. Un PSCE comporte au moins une AC mais peut en comporter plusieurs en fonction de son organisation. Les différentes AC d'un PSCE peuvent être indépendantes les unes des autres et/ou liées par des liens hiérarchiques ou autres (AC Racines / AC Filles). Un PSCE est identifié, dans un certificat dont il a la responsabilité, au travers de son AC qui a émis ce certificat et qui est elle-même directement identifiée dans le champ "issuer" du certificat.

Prestataire de service de confiance (PSCO) – Toute personne ou entité offrant des services consistant en la mise en œuvre de fonctions qui contribuent à la sécurité des informations échangées par voie électronique.

Prestataire de services d'horodatage électronique (PSHE) – Toute personne ou entité qui est responsable de la génération et de la gestion de contremarques de temps, vis-à-vis de ses abonnés et des utilisateurs de ces contremarques de temps. Un PSHE peut fournir différentes familles de contremarques de temps correspondant à des finalités différentes. Un PSHE comporte au moins une AH mais peut en comporter plusieurs en fonction de son organisation. Un PSHE est identifié dans les certificats de clés publiques des Unités d'Horodatage dont il a la responsabilité au travers de ses Autorités d'Horodatage.

Profil de protection – Document public qui définit, pour une catégorie de produits, un ensemble d'exigences et d'objectifs de sécurité, indépendants de leur technologie et de leur implémentation, qui satisfont les besoins de sécurité communs à un groupe d'utilisateurs.

Qualification d'un PSCO – Acte par lequel un organisme de certification atteste de la conformité de tout ou partie de l'offre de services d'un PSCO aux exigences du [RGS], pour un niveau de sécurité donné et correspondant au service visé par le PSCO.

Qualification d'un produit de sécurité – Acte par lequel l'ANSSI atteste de la capacité d'un produit à assurer les services de sécurité objet de la qualification. L'attestation de qualification indique l'aptitude du produit à participer à la réalisation, à un niveau de sécurité donné, d'une ou plusieurs fonctions traitées dans le [RGS].

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

Sécurité des Systèmes d'Information (SSI) – Satisfaction des besoins de sécurité (disponibilité, intégrité, confidentialité, imputabilité, traçabilité) d'un système d'information.

Téléservice – Tout système d'information permettant aux usagers de procéder par voie électronique à des démarches ou formalités administratives.

Usager – Personne physique agissant pour son propre compte ou pour le compte d'une personne morale et procédant à des échanges électroniques avec des autorités administratives.

Référentiel Général de Sécurité (RGS)		
Version	Date	Page
0.99	19/02/2010	31/33

10 - Références documentaires

10.1 - Références réglementaires

- [Ordonnance] Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives (Journal Officiel du 9 décembre 2005). Disponible en ligne : <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000636232&dateTexte=vig>
- [DécretRGS] Décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'[Ordonnance]. Disponible en ligne : <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021779444&dateTexte=vig>
- [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. Disponible en ligne : <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005630796&dateTexte=exte>
- [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. Disponible en ligne : <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000441678&dateTexte=exte>
- [loi120400] Loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations. Disponible en ligne : <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005629288&dateTexte=exte>

10.2 - Références techniques

- [ISO2700x] Normes relatives à la sécurité de l'information. Disponible auprès de l'ISO ou de l'AFNOR.
- [PSSI] Guide « Politique SSI » de l'ANSSI. Disponible en ligne : http://www.ssi.gouv.fr/site_article46.html
- [MaturitéSSI] Guide « maturité SSI » de l'ANSSI. Disponible en ligne : http://www.ssi.gouv.fr/site_article85.html
- [EBIOS] Méthode d'analyse de risque de l'ANSSI. Disponible en ligne : http://www.ssi.gouv.fr/site_article45.html
- [GISSIP] Guide « Gestion et Intégration de la SSI dans les Projets » (souvent nommé guide GISSIP) de l'ANSSI : http://www.ssi.gouv.fr/site_article86.html
- [FEROSTypes] Collection documentaire des « FEROS Types » pour les téléservices (source DGME) <http://www.references.modernisation.gouv.fr/mise-en-oeuvre-du-rgs>
- [ExigencesTélé] Guide d'Exigences types de sécurité pour les téléservices (source DGME) <http://www.references.modernisation.gouv.fr/mise-en-oeuvre-du-rgs>
- [CERTA] Note d'information du CERTA sur les mots de passe, 12/04/2007 : <http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001>

Référentiel Général de Sécurité (RGS)		
Version	Date	Page
0.99	19/02/2010	32/33

- [CC] "Common Criteria for Information Technology Security Evaluation". Disponible en ligne : <http://www.commoncriteriaportal.org>
- [QE] Processus de qualification d'un produit de sécurité – Niveau Élémentaire – V1.0 http://www.ssi.gouv.fr/site_article39.html
- [QS] Processus de qualification d'un produit de sécurité – Niveau Standard – V1.2 http://www.ssi.gouv.fr/site_article39.html
- [QR] Processus de qualification d'un produit de sécurité – Niveau Renforcé – V1.0 http://www.ssi.gouv.fr/site_article39.html
- [PC_IGC/A] Politique de Certification de l'IGC/A – version 1.1RevA et suivantes. Disponible en ligne : http://www.ssi.gouv.fr/site_article15.html
- [AvisCertificatsIGC/A] <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000646696>

Référentiel Général de Sécurité (RGS)		
Version	Date	Page
0.99	19/02/2010	33/33