

Premier ministre	Ministère du budget, des comptes publics et de la fonction publique
Direction Centrale de la Sécurité des Systèmes d'information	Direction Générale de la Modernisation de l'Etat

Administration Electronique :

Référentiel Général de Sécurité

Annexe à l'arrêté du Premier ministre du XX XX XX

Référentiel Général de Sécurité

Référence		Date	
RGS0.98.doc		16/12/2008	
Identification d'objet (OID)		Racine OID et gestionnaire	
Responsables		Version	
MBCPFP/DGME et SGDN/DCSSI		0.98	
Critère de diffusion		Nombre de pages	
Public		33	

HISTORIQUE DES VERSIONS

DATE	VERSION	EVOLUTION DU DOCUMENT	REDACTEUR
16/12/08	V0.98		DCSSI + DGME

Référentiel Général de Sécurité				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
	0.98	16/12/2008	Public	2/33

Sommaire

1 - Introduction	5
1.1 - Préambule : Forces et faiblesses du numérique.....	5
1.2 - Contexte	6
1.3 - Autorités administratives concernées	6
1.4 - Objectif du RGS.....	6
1.5 - Structure du RGS	7
1.5.1 - Documents constitutifs du RGS.....	7
1.5.2 - Corps du document RGS	7
1.6 - 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	11
2.2.4 - Élaborer une politique SSI.....	11
2.2.5 - Utiliser les produits et prestataires labellisés SSI.....	11
2.2.6 - Viser une amélioration continue	12
2.3 - Intégration de la SSI dans le cycle de vie des systèmes d'information.....	12
2.3.1 - Des efforts proportionnés aux enjeux SSI.....	12
2.3.2 - Un engagement systématique : l'homologation de sécurité.....	12
2.3.3 - Des outils ciblés pour les projets de système d'information.....	13
3 - Fonctions de sécurité	14
3.1 - Introduction	14
3.2 - Authentification	14
3.2.1 - Utilisation de mécanismes cryptographiques.....	14
3.2.2 - Utilisation des identifiants / mots de passe statiques	14
3.2.3 - Authentification d'une personne par certificat électronique.....	15
3.2.4 - Authentification d'un serveur par certificat électronique.....	15
3.3 - Signature électronique	16
3.3.1 - Utilisation de mécanismes cryptographiques.....	16
3.3.2 - Signature d'une personne par certificat électronique.....	16
3.3.3 - Cachet d'un serveur par certificat électronique.....	17
3.4 - Confidentialité	17
3.4.1 - Utilisation de mécanismes cryptographiques.....	17
3.4.2 - Confidentialité par certificat électronique	17
3.4.3 - Habilitations	18
3.5 - Horodatage	18
3.5.1 - Utilisation des mécanismes cryptographiques	18
3.5.2 - Horodatage par contremarques de temps.....	18
4 - Accusé d'enregistrement et de réception.....	19
4.1 - Introduction	19
4.2 - Règles de sécurité.....	19
5 - Qualification	20

Référentiel Général de Sécurité				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
	0.98	16/12/2008	Public	3/33

5.1 - Qualification de produits de sécurité	20
5.1.1 - Introduction	20
5.1.2 - Qualification élémentaire	21
5.1.3 - Qualification standard.....	21
5.1.4 - Qualification renforcée.....	21
5.2 - Qualification des Prestataires de Service de Confiance (PSCo)	22
6 - Les Infrastructures de Gestion de Clés (IGC)	24
6.1 - Règles et recommandations générales	24
6.2 - Cas particulier de la validation des certificats par l'Etat	24
6.2.1 - Présentation de l'IGC/A	25
6.2.2 - Règles de sécurité.....	25
7 - Référencement	26
8 - Annexe 1 : Liste des documents constitutifs du RGS	27
8.1 - Documents applicables concernant l'utilisation de certificats électroniques dans les fonctions de sécurité	27
8.2 - Documents applicables concernant l'utilisation de mécanismes cryptographiques dans les fonctions de sécurité	28
9 - Annexe 2 : Liste des Profils de Protection	29
10 - Annexe 3 : Glossaire	30
11 - Annexe 4 : Références documentaires	32
11.1 - Références réglementaires	32
11.2 - Références techniques	32

Référentiel Général de Sécurité				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
	0.98	16/12/2008	Public	4/33

1 - Introduction

1.1 - Préambule : 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'Etat, 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 d'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 assurées par moyens informatiques, peut être dangereuse pour l'organisme, voire, quand ils concernent des secteurs d'activité vitaux ou industriels, 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. Les protocoles 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, 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 croissantes de ces réseaux. Les logiciels, de plus en plus complexes, présentent tous 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 de 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 institutions 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 certains 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 l'individu fraudé (exemple : faux sites marchands permettant de voler les données bancaires et de puiser dans les comptes de la personne usurpée). 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.

Référentiel Général de Sécurité				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
	0.98	16/12/2008	Public	5/33

1.2 - Contexte

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.

C'est dans ce contexte qu'a été publiée 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]).

S'inscrivant dans la démarche globale du Gouvernement de réforme de l'Etat, 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 de l'[Ordonnance], les AA doivent mettre leurs systèmes d'information en conformité avec le RGS dans un délai de trois ans à compter de la date de publication du présent RGS pour les systèmes existants, et dans un délai de douze mois à compter de la même date pour les applications créées dans les six mois après cette date.

L'article 15 exclut du champ d'application de l'[Ordonnance] les systèmes d'informations traitant d'informations relevant du secret de la défense nationale. Toutefois une instruction spécifique pourra imposer à ces systèmes d'informations le respect du RGS.

Par ailleurs, l'[Ordonnance] prévoit que l'application de ses articles 9, 10 et 12 est fixée par décret. Ce décret (ci-après désigné [décretRGS]) traite des points suivants :

- le RGS (en application de l'article 9.I de l'[Ordonnance]), qui sera approuvé par arrêté ;
- l'homologation de sécurité des systèmes d'information (en application de l'article 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 service 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 ;
- Le référencement des produits de sécurité et des prestataires de service de confiance (en application de l'article 12 de l'[Ordonnance]).

1.3 - Autorités administratives concernées

La loi n° 2004-1343 précise que les AA soumises à l'[Ordonnance], et donc au RGS, sont les administrations de l'Etat, 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. Autrement dit, le périmètre de l'[Ordonnance] concerne tous les services publics administratifs de l'Etat.

1.4 - Objectif du RGS

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

De plus, cet ensemble est complété par des bonnes pratiques en 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 les éclairages nécessaires pour les AA quant à la marche à suivre pour prendre en compte pleinement les dispositions de l'[Ordonnance].

Référentiel Général de Sécurité				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
	0.98	16/12/2008	Public	6/33

1.5 - Structure du RGS

1.5.1 - Documents constitutifs du RGS

En plus du corps du RGS dont le contenu est présenté au chapitre 1.5.2 -, le RGS est constitué d'un ensemble de documents qui en font partie intégrante.

Ces documents sont les suivants :

[RGS_A_1]	Service de Confiance "Confidentialité"
[RGS_A_2]	Service de Confiance "Authentification"
[RGS_A_3]	Service de Confiance "Signature"
[RGS_A_4]	Service de Confiance "Authentification Serveur"
[RGS_A_5]	Service de Confiance "Cachet Serveur"
[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 Serveur"
[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, CRLs, 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

1.5.2 - Corps du document RGS

Le corps du document RGS est construit comme suit :

- **Chapitre 2 : Gestion de la sécurité :**
Ce chapitre fournit un ensemble de bonnes pratiques en SSI et de règles sur les deux thèmes suivant :
 - Gestion globale de la SSI au sein d'une AA,
 - Intégration de la SSI dans le cycle de vie des systèmes d'information.
- **Chapitre 3 : Fonctions de sécurité :**
C'est le cœur du document RGS. 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, ainsi que le niveau de sécurité requis pour chacune de ces fonctions. Lorsque la fonction de sécurité est traitée dans le RGS, alors l'AA respecte les règles exposées pour le niveau considéré.
- **Chapitre 4 : Accusés d'Enregistrement / Accusés de Réception :**
Les règles de sécurité relatives à la fonction d'accusé d'enregistrement et d'accusé de réception sont présentées dans ce chapitre par niveau de sécurité.
- **Chapitre 5 : Qualification :**
La qualification peut être obtenue pour un produit de sécurité ou pour un prestataire de service de confiance (PSCo).
 - qualification des produits de sécurité : présentation des différents niveaux de qualification et des procédures associées ;
 - qualification des PSCo : présentation de la procédure d'obtention d'une qualification.
- **Chapitre 6 : Les Infrastructures de Gestion de Clés (IGC) :**
Ce chapitre liste des recommandations concernant la mise en œuvre et l'exploitation d'une IGC par les AA. Il présente également le cas particulier de la validation des certificats par l'Etat notamment via l'architecture « IGC/A » (Infrastructure de la Gestion de la Confiance de l'Administration).
- **Chapitre 7 : Référencement**
Le référencement des produits de sécurité ou des offres des PSCo peut être obtenu après leur qualification et après la vérification de leur conformité à des exigences d'interopérabilité.
- **Chapitre 8 : Liste des documents applicables :**
Ce chapitre liste un ensemble de documents contenant des règles de sécurité que les AA doivent respecter lorsque celles-ci sont concernées.

Référentiel Général de Sécurité				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
	0.98	16/12/2008	Public	7/33

1.6 - A qui s'adresse le RGS ?

Le RGS s'adresse à toute personne responsable ou concourant à la mise en service d'un système d'information dans une AA, aux éditeurs de produits de sécurité et aux PSCo.

Différentes familles de lecteurs sont plus particulièrement concernées et amenées à utiliser le RGS. Leurs finalités et objectifs ne sont pas les mêmes.

Les familles de lecteur sont notamment :

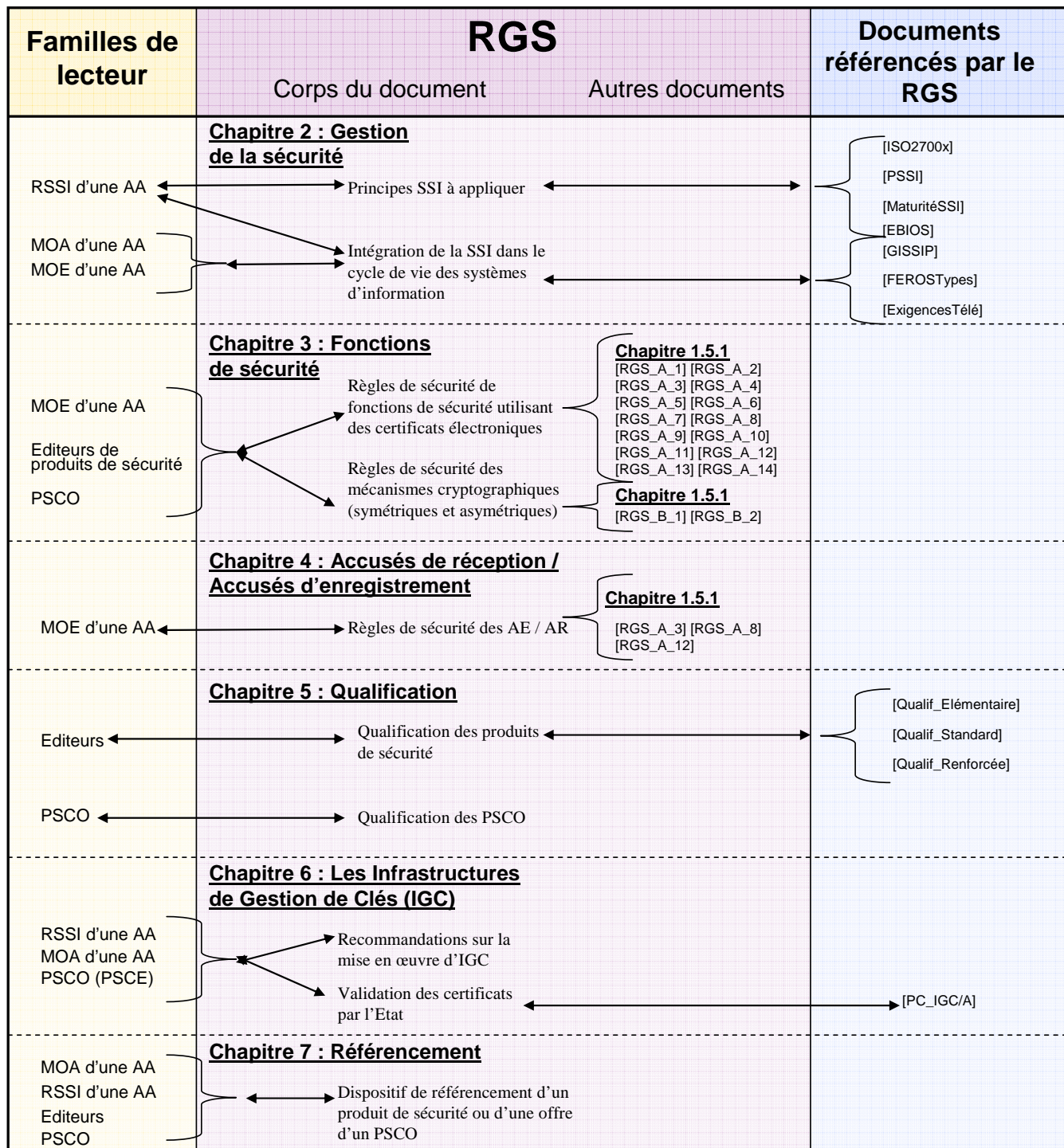
- **Maîtrise d'ouvrage (MOA) des AA :**
 - La MOA est responsable de la définition des besoins lors de la construction d'un système d'information. Elle fixe l'organisation du projet, ses objectifs, ses enjeux et ses contraintes. D'une manière générale, elle est responsable de l'identification des objectifs de sécurité et du pilotage du projet.
 - Les chapitres 2 6 et 7 sont particulièrement intéressants pour 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 lus avec attention par la MOE d'un projet de construction d'un système d'information. En effet, une fois les fonctions de sécurité et niveaux de sécurité déterminés, la MOE y trouvera les règles de sécurité devant être respectées.
- **Responsable de la sécurité des systèmes d'information (RSSI) d'une AA :**
 - En fonction des organismes, le RSSI¹ peut avoir différents rattachements. Rattaché à la direction générale, il est chargé de la définition et de l'application de la politique de sécurité du système d'information (PSSI). 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 de la commission d'homologation, il a la charge de présenter l'analyse de risques.
 - Le RSSI sera tout particulièrement intéressé par la lecture des chapitres 2, 3 et 4.
- **Editeurs de produits de sécurité :**
 - La mise en place d'un système d'information dans une AA s'accompagne du déploiement d'un ou plusieurs produits de sécurité dans le système d'information de l'AA. Ces produits de sécurité peuvent être qualifiés à un niveau donné. Cette qualification atteste que le produit respecte les règles de sécurité d'une fonction de sécurité pour un niveau de sécurité donné.
 - Les éditeurs de produits de sécurité exploiteront en priorité le chapitre 5.1 traitant de la qualification des produits de sécurité dans le cas où ceux-ci souhaitent suivre le processus de qualification pour un ou plusieurs de leurs produits de sécurité.
 - Lors des phases amont d'un projet de développement d'un produit de sécurité (spécifications, conception) un éditeur de produit de sécurité pourra se référer aux chapitres 3 et 4 afin de prendre en compte les règles imposées pour les fonctions de sécurité et niveaux de sécurité qu'il souhaite implémenter dans son produit. De plus si l'éditeur souhaite faire référencer un produit de sécurité, celui-ci se référera au chapitre 7 pour connaître la procédure à suivre.
- **Prestataire de service 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. L'AA peut aussi décider d'être un PSCo elle-même si elle gère elle-même le service correspondant. Un PSCo peut donc appartenir soit au secteur privé soit au secteur public.
 - Suivant le niveau de sécurité des services de sécurité qu'un PSCo souhaite offrir, la lecture du chapitre 5.2 apporte des précisions sur les règles et procédures de qualification propres à un PSCo. De même, afin de faire valider les certificats électroniques qu'il émet par l'Etat, un PSCo du secteur public lira attentivement le chapitre 6. De plus si le PSCo souhaite faire référencer une offre de services, il se référera au chapitre 7 pour connaître la procédure à suivre.

¹ Certaines AA n'ont pas nécessairement de poste de RSSI. Une personne ayant une autre fonction au sein de l'AA peut tout à fait faire office de RSSI.

Référentiel Général de Sécurité				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
	0.98	16/12/2008	Public	8/33

Le schéma ci-dessous présente le rôle central que remplit le RGS :

- à gauche : les familles de lecteur du RGS ;
- à droite : les documents référencés par le RGS.



Référentiel Général de Sécurité				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
	0.98	16/12/2008	Public	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 données informatiques d'un organisme et des systèmes qui assurent l'élaboration, le traitement, la transmission ou le stockage de ces données.

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

Les enjeux se mesurent à l'aune de la gravité des impacts que provoquerait, pour l'organisme, une défaillance dans chacun des trois grands domaines de sécurité que sont :

- la disponibilité, qui peut porter sur les données et sur le système d'information (quel serait l'impact en cas d'impossibilité d'accéder aux données ou d'utiliser le système d'information ?) ;
- l'intégrité, qui peut porter sur les données et sur le système d'information (quel serait l'impact en cas de modification non désirée de données ou d'un constituant du système d'information ?) ;
- la confidentialité, qui porte sur les données (quel serait l'impact en cas d'accès d'une personne non autorisée à des données ?).

La menace à prendre en compte est celle qui pèse sur le système d'information et sur les données qu'il traite, transmet et stocke, dans l'environnement dans lequel il se situe (le système d'information, et donc les données qu'il contient, est-il isolé, ou au accessibles par 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 ou à risque 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 certains aux données, aux processus ou au système ?).

Il est recommandé, pour des systèmes d'information complexes, de conduire cette démarche en utilisant une méthode d'analyse de risque, afin de déterminer sans faille le besoin de sécurité.

De ce besoin de sécurité, découlent les objectifs de sécurité à satisfaire, puis les fonctions qui peuvent être mises en œuvre pour atteindre ces objectifs, et enfin les moyens aptes à assurer les fonctions retenues. Une itération de la démarche peut être nécessaire pour assurer la sécurité des moyens ainsi mis en place.

Les objectifs de sécurité à satisfaire se rapportent à chacun des trois grands domaines cités :

- la disponibilité de tout ou partie des données et du système d'information ;
- l'intégrité de tout ou partie des données et du système d'information ;
- la confidentialité de tout ou partie des données, et celle des éléments critiques du système d'information (ceux qui assurent les fonctions de sécurité, comme par exemple les équipements de chiffrement, qu'il convient de protéger en confidentialité pour éviter qu'une personne non autorisée le désactive pour accéder aux données confidentielles) ;

auxquels peut 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, et prendre alors les mesures qui s'imposent.

Les moyens retenus pour assurer les fonctions de sécurité pourront être :

- techniques : informatiques (logiciels ou matériels), ou autre (blindage, détecteur d'intrusion, etc.) ;
- organisationnels : habilitation et accréditation du personnel, filtrage des accès, mises sous coffre des éléments sensibles, etc. ;
- ou humains : administrateur du système d'information, responsable de sécurité du système d'information, responsable de la protection physique du système.

La suite de ce chapitre présente des principes, règles et recommandations pour la gestion de la SSI dans un organisme, puis pour la gestion de la SSI dans un projet de système d'information.

Référentiel Général de Sécurité				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
	0.98	16/12/2008	Public	10/33

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 en effet de n'oublier aucun élément pertinent, pour éviter le maillon faible qui réduirait la sécurité apportée par tous les autres maillons, de faire prendre chacune des décisions au juste niveau.

Il faut pour cela :

- considérer tous les aspects qui peuvent avoir une influence sur la sécurité des systèmes d'information, techniques (matériels, logiciels, réseaux, etc.) et non techniques (organisations, sites, personnels, etc.) ;
- considérer toutes les origines de risques (origines humaines et naturelles, causes accidentelles et délibérées) ;
- prendre en compte la SSI au plus haut niveau hiérarchique, car comme tous les autres domaines de la sécurité, la SSI repose sur une vision stratégique, 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 ;
- responsabiliser tous les acteurs (décideurs, maîtrises d'ouvrage, maîtrises d'œuvre, utilisateurs, ...) ;
- intégrer la SSI tout le 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

La SSI doit être adaptée aux enjeux et besoins de sécurité de l'AA, afin d'y consacrer les moyens financiers et humains juste nécessaires et suffisants.

Une aide dans cette démarche peut être trouvée dans le document [MaturitéSSI]. Il a pour objectifs de déterminer rapidement les enjeux liés au système d'information de l'organisme, de mesurer l'écart entre le niveau nécessaire de prise en compte de la sécurité et le niveau effectif, et d'en déduire les actions à mettre en œuvre pour gérer la SSI de manière adéquate.

2.2.3 - Gérer les risques SSI

La démarche générale consiste principalement à :

- établir le contexte (délimiter et décrire la situation) ;
- apprécier les risques (les mettre en évidence et les hiérarchiser) ;
- traiter les risques (réduire, transférer, éviter les risques, ou accepter de les prendre).

Cette démarche, dont un cadre théorique est proposé par l'[ISO27005], peut être conduite de manière allégée dans les cas simples ou très détaillée si le système d'information est complexe et les enjeux élevés.

La mise en œuvre pratique de l'[ISO27005] doit s'appuyer sur les explications et les outils fournis dans les méthodes de gestion des risques telles que [EBIOS] (Expression des Besoins et Identification des Objectifs de Sécurité).

2.2.4 - Élaborer une politique SSI

Il est recommandé d'élaborer et de formaliser une politique SSI globale au niveau de la plus haute AA de la chaîne hiérarchique.

Selon les besoins, cette politique SSI pourra être déclinée et complétée dans les échelons subordonnés, ou pour un domaine particulier, ou pour un système d'information précis.

Le guide [PSSI] fournit une aide aux responsables SSI pour élaborer une politique de sécurité.

2.2.5 - Utiliser les produits et prestataires labellisés SSI

Des labels ont été créés par l'[Ordonnance] pour attester de la confiance que l'on peut accorder à des produits de sécurité et à des prestataires de service. D'autres existent pour les professionnels de la SSI. Il convient :

- d'utiliser chaque fois que possible des produits de sécurité qualifiés (cf. chapitre 5.1 -) ou certifiés par la DCSSI (le catalogue de ces produits est disponible sur son site Internet www.ssi.gouv.fr), après une analyse minutieuse de la cible de sécurité pour s'assurer qu'elle couvre bien le contexte d'utilisation prévu ;
- de recourir chaque fois que possible à des prestataires de services de confiance qualifiés (cf. chapitre 5.2 -) ;
- de prendre en considération, dans le choix des prestataires, leur éventuelle certification de services ou d'organismes (certification selon l'[ISO27001] par exemple) ;

Référentiel Général de Sécurité				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
	0.98	16/12/2008	Public	11/33

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

2.2.6 - Viser une amélioration continue

Il est recommandé de chercher une amélioration continue 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 : définir le cadre du SMSI, apprécier et spécifier le traitement des risques SSI ;
- mettre en œuvre : mettre en place et maintenir les mesures de sécurité ;
- vérifier : vérifier que les mesures de sécurité fonctionnent conformément à l'étape Planifier et identifier les améliorations possibles du SMSI ;
- améliorer : 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 réalisation ou de modification d'un système d'information ou d'une application informatique, le besoin de sécurité doit être pris en compte au même titre que les besoins fonctionnels que vise à satisfaire le système ou l'application. La SSI est une fonction à assurer au même titre que les autres. Prise très en amont du projet, son efficacité sera bien supérieure, et son coût bien moindre, que s'il faut corriger les spécifications, voire des équipements ou l'architecture du système, du fait d'une intégration tardive.

Conformément aux principes exposés ci-dessus, la SSI doit être prise en compte tout au long de la vie d'un système d'information, depuis sa définition, voire même dès son étude d'opportunité si un doute plane sur la possibilité de sécuriser le système d'information au niveau requis, puis tout au long de sa vie en service, dans une démarche de réévaluation et d'amélioration continue s'appuyant sur des audits, et à son retrait du service, en assurant notamment la destruction des données et des composants confidentiels avant de les céder ou de les mettre à la décharge.

Dans ce cycle, une étape essentielle est l'homologation de sécurité du système, qui doit intervenir avant sa mise en service, puis être régulièrement remise en cause, pour 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

Il est recommandé d'utiliser le guide de la DCSSI pour l'intégration de la sécurité dans les projets (guide [GISSIP]) afin d'adapter la démarche de sécurité en fonction des enjeux du projet, en particulier :

- la conception générale formulera les objectifs de sécurité ou recensera les bonnes pratiques pertinentes ;
- la conception détaillée affinera les éléments précédents, et déterminera comment la sécurité sera construite pour ne pas dépasser un niveau de risque que l'autorité responsable se déclare prête à accepter ;
- la réalisation du système permettra de décrire concrètement les mesures de sécurité et la manière de les appliquer dans l'environnement effectif d'utilisation ;
- la décision d'homologation marquera la transition du développement vers l'exploitation ;
- l'organisme ou le contrat avec un prestataire prendra en charge, le maintien de la sécurité et ceci jusqu'au retrait du service.

2.3.2 - Un engagement systématique : l'homologation de sécurité

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

PROJET

« Art. 3 – Afin de déterminer les fonctions de sécurité nécessaires à la protection d'un système d'information, en application des dispositions prévues à l'article 9 de l'ordonnance du 8 décembre 2005 susvisée, une autorité administrative doit :

- a) identifier l'ensemble des risques pesant sur la sécurité du système et des informations qu'il traite, au regard notamment des exigences de disponibilité et d'intégrité du système, des exigences de confidentialité et d'intégrité des informations, ainsi que du besoin d'authentification des utilisateurs du système ;
- b) fixer les objectifs de sécurité à satisfaire pour faire face aux risques identifiés ;
- c) en déduire les fonctions de sécurité, qui permettent d'atteindre ces objectifs de sécurité, en précisant leur niveau de sécurité.

L'autorité administrative peut décider que certains risques identifiés n'imposent pas la mise en place de fonctions de sécurité particulières, si les conditions d'emploi du système permettent de limiter ces risques à un niveau qu'elle estime acceptable.

Référentiel Général de Sécurité				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
	0.98	16/12/2008	Public	12/33

Art. 4 – Pour mettre en place dans un système d'information les fonctions de sécurité ainsi déterminées, l'autorité administrative recourt, à chaque fois que possible, à des produits de sécurité ou à des prestataires de services de confiance qualifiés dans les conditions prévues au présent décret. A défaut, elle s'assure par tout autre moyen de la conformité au référentiel général de sécurité, des produits et des prestataires auxquels elle recourt pour protéger son système d'information. Dans ce cas, la décision d'homologation visée à l'article suivant fait état des moyens utilisés pour s'assurer de cette conformité et des raisons ayant conduit à ne pas retenir de produits ou de prestataires qualifiés.

Art. 5 - Après avoir vérifié la mise en œuvre opérationnelle de ces produits et de ces prestataires dans son système d'information, l'autorité administrative prononce expressément l'homologation de sécurité du système, préalablement à son emploi, reconnaissant ainsi formellement que le système et les informations sont protégés conformément aux objectifs de sécurité. L'homologation est assortie le cas échéant de conditions, qui sont alors mentionnées dans la décision d'homologation.

L'autorité administrative réévalue, tout au long de la vie du système d'information, les risques pesant sur la sécurité du système et des informations. Elle peut modifier les conditions dont l'homologation est assortie ou retirer l'homologation lorsqu'elle estime que les risques encourus ne sont pas acceptables au regard du besoin de protection du système et des informations. Toute évolution du système ayant une répercussion sur la sécurité doit donner lieu à une nouvelle homologation de sécurité.

Art. 6 - Dans le cas d'un téléservice, la décision d'homologation de sécurité 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.

Art. 7 – Sur demande de la direction centrale de la sécurité des systèmes d'information, l'autorité administrative lui communique les documents établis au cours de la présente procédure d'homologation de sécurité du système ».

Tout système d'information doit faire l'objet d'une homologation de sécurité par une autorité d'homologation désignée par l'AA.

La décision d'homologation 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 le système d'information est donc apte à entrer en service avec des risques résiduels acceptés et maîtrisés.

L'autorité d'homologation peut s'appuyer sur une commission d'homologation qui lui fournira les éléments d'information et la synthèse nécessaires à sa décision. Si la responsabilité du système d'information n'est pas incarnée par une seule AA, l'homologation peut être collégiale ou confiée au représentant d'une des AA concernées.

L'autorité d'homologation peut prononcer :

- une homologation provisoire, assortie de réserves et d'un délai de mise en conformité.
- un refus d'homologation au vu des résultats d'audit et des risques résiduels encourus jugés inacceptables,
- une homologation, assortie le cas échéant de conditions, pour une durée déterminée (fréquemment entre 3 et 5 ans).

2.3.3 - Des outils ciblés pour les projets de système d'information

Conformément à l'article 3 du [DécretRGS], il est nécessaire :

- d'apprécier les risques pesant sur un système d'information ou sur ses utilisateurs ;
- d'identifier les objectifs de sécurité à atteindre pour réduire, le cas échéant, les risques mis en évidence à un niveau acceptable ;
- de définir les fonctions de sécurité et le niveau retenu pour chacune d'elles pour atteindre les objectifs de sécurité identifiés pour le système d'information, en fonction de la stratégie de traitement des risques adoptée par l'AA.

Une collection de sept expressions d'objectifs de sécurité génériques dites « FEROS Types » (Fiche d'Expression Rationnelle des Objectifs de Sécurité [FEROSTypes]), destinées aux experts SSI et aux responsables de système d'information, peuvent faciliter l'expression de leurs objectifs de sécurité.

Le « Guide d'Exigences Types » ([ExigencesTélé]), propose un ensemble d'exigences de sécurité qui répondent aux objectifs exprimés dans les [FEROSTypes].

Référentiel Général de Sécurité				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
	0.98	16/12/2008	Public	13/33

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 ».

Les fonctions de sécurité traitées dans ce chapitre contribuent à la sécurité des informations échangées par voie électronique.

Il est du ressort de l'AA de déterminer les fonctions de sécurité à utiliser ainsi que leur niveau de sécurité associé lorsque celle-ci met en place un projet de système d'information. Les méthodes, outils et bonnes pratiques pour y parvenir sont listés au chapitre 2 du RGS.

Le présent chapitre définit les règles que doivent respecter les fonctions de sécurité par niveau de sécurité (si plusieurs niveaux existent pour cette fonction). Ces règles s'appliquent aux AA.

3.2 - Authentification

En fonction de la sensibilité des données ou des traitements auxquels l'utilisateur ou l'agent ont accès dans le système d'information concerné, l'AA va choisir un procédé d'identification plus ou moins fort.

L'authentification a pour but de vérifier l'identité dont une entité (personne ou serveur) se réclame. Généralement, l'authentification est précédée d'une identification qui permet à cette entité de se faire reconnaître du système par un élément dont on l'a doté. En résumé, s'identifier c'est communiquer une identité préalablement enregistrée, s'authentifier c'est apporter la preuve de cette identité. La suite de ce chapitre ne traite que de la fonction d'authentification qui fait intervenir des éléments de sécurité informatique par opposition à l'identification qui repose sur des concepts organisationnels.

3.2.1 - Utilisation de mécanismes cryptographiques

Le référentiel [RGS_B_1] fixe les règles (et donne des recommandations), que les AA doivent respecter, lorsqu'elles mettent en place une fonction d'authentification reposant sur des mécanismes cryptographiques.

L'authentification par utilisation de mécanismes cryptographiques repose sur l'usage de clés. L'AA doit respecter les règles fixées dans le référentiel [RGS_B_2] pour la gestion de ces clés.

3.2.2 - Utilisation des identifiants / mots de passe statiques

Recommandations sur le choix et la gestion des mots de passe :

Il est recommandé aux AA de respecter les bonnes pratiques listées dans le document [CERTA] concernant la méthode de création d'un « bon » mot de passe ainsi que la gestion des mots de passe.

Recommandations sur l'usage des identifiants / mots de passe dans un processus d'authentification d'une personne sur un système d'information distant :

L'authentification d'une personne sur 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 local de confiance (exemple : le PC professionnel d'un agent administratif) ;
- le système d'information distant (exemples : une base de donnée, le serveur hébergeant un téléservice).

Il n'est pas recommandé de permettre une authentification par identification / 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 de par 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 / mot de passe) de l'utilisateur et permet donc d'usurper son identité.

Référentiel Général de Sécurité				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
	0.98	16/12/2008	Public	14/33

Il est donc recommandé de :

- mettre en place un mécanisme limitant l'accès à l'environnement local de confiance de l'utilisateur (par exemple, un mécanisme de déverrouillage par identifiant / 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. D'autre part, il est souhaitable que ces mécanismes permettent d'assurer la confidentialité et l'intégrité des données accédées par l'utilisateur sur le système d'information distant.

3.2.3 - Authentification d'une personne par certificat électronique

L'AA doit définir au préalable le niveau de sécurité relatif à la fonction « authentification d'une personne » et en déduit donc l'utilisation d'un certificat électronique dont le niveau de sécurité est au moins égal à une étoile (*), deux étoiles (**) ou trois étoiles (***) pour cette fonction.

Toutes les règles relatives aux exigences techniques complétées d'exigences de nature juridique et organisationnelle pour assurer la délivrance de certificats d'authentification sont regroupées dans un document appelé Politique de Certification Type Authentification [RGS_A_7]. Une Politique de Certification Type traite des exigences des 3 niveaux de sécurité croissants de une étoile (*) à trois étoiles (***). Ce document s'adresse plus particulièrement aux PSCE privés ou publics désirant offrir ce service d'émission de certificat d'une fonction donnée. Il s'adresse aussi aux AA pour connaître les critères de différenciation entre les niveaux de sécurité qu'elles ont déterminés.

Ainsi, les AA doivent utiliser des certificats d'authentification de personne d'un niveau de sécurité donné émis conformément aux exigences de la PC Type [RGS_A_7] (ou de la PC Type [RGS_A_11] dans le cas de certificats double usage authentification et signature) pour le niveau de sécurité retenu.

Toutes les règles relatives à la mise en œuvre de la fonction de sécurité « authentification » utilisant des certificats électroniques sont regroupées dans le document « Service Authentification² » [RGS_A_2]. Il présente d'une part la synthèse par niveau de sécurité des règles relatives à la délivrance de certificats électroniques d'authentification (dont l'exhaustivité se trouve dans les documents [RGS_A_7] et [RGS_A_11]) et définit d'autre part celles relatives aux applications et aux dispositifs nécessaires pour réaliser et vérifier cette fonction de sécurité. Il traite aussi des aspects de format et les bonnes pratiques

Ainsi, les AA utilisant une application d'authentification, un applicatif de vérification d'authentification et des dispositifs d'authentification doivent respecter les règles du document [RGS_A_2] pour le niveau de sécurité retenu.

Les AA veillent à suivre les règles de bonnes pratiques du document [RGS_A_2].

3.2.4 - Authentification d'un serveur par certificat électronique

L'AA doit définir au préalable le niveau de sécurité relatif à la fonction « authentification d'un serveur » et en déduit donc l'utilisation d'un certificat électronique de niveau au moins égal à *, ** ou *** pour cette fonction.

Toutes les règles relatives aux exigences techniques complétées d'exigences de nature juridique et organisationnelle pour assurer la délivrance de certificats d'authentification serveur sont regroupées dans un document appelé Politique de Certification Type Authentification serveur [RGS_A_9].

Ainsi, les AA doivent utiliser des certificats d'authentification de serveur d'un niveau de sécurité donné émis conformément aux exigences de la PC Type [RGS_A_9] pour le niveau de sécurité retenu.

Toutes les règles relatives à la mise en œuvre de la fonction de sécurité « authentification serveur » utilisant des certificats électroniques sont regroupées dans le document « Service Authentification Serveur » [RGS_A_4]. Il présente d'une part la synthèse par niveau de sécurité des règles relatives à la délivrance de certificats électronique d'authentification serveur (dont l'exhaustivité se trouve dans le document [RGS_A_9]) et définit d'autre part celles relatives aux applications et aux dispositifs nécessaires pour réaliser et vérifier cette fonction de sécurité. Il traite aussi des aspects de format et les bonnes pratiques

² Ce document s'adresse aux AA mettant en œuvre un tel service mais aussi aux PSCE et aux fournisseurs de produits matériels ou logiciels.

Référentiel Général de Sécurité				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
	0.98	16/12/2008	Public	15/33

Ainsi, les AA utilisant une application d'authentification, un applicatif de vérification d'authentification et des dispositifs de protection des clés privées doivent respecter les règles du document [RGS_A_4] pour le niveau de sécurité retenu.

Les AA veillent à suivre les règles de bonnes pratiques du document [RGS_A_4].

3.3 - Signature électronique

La signature d'une personne permet de garantir l'identité du signataire, l'intégrité du document signé ainsi que la manifestation du consentement du signataire quant au contenu des données électroniques ainsi 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 serveur » permet de garantir l'intégrité des données échangées et l'identification du serveur ayant cacheté ces données.

3.3.1 - Utilisation de mécanismes cryptographiques

Le référentiel [RGS_B_1] fixe les règles (et donne des recommandations), que les AA doivent respecter, lorsqu'elles mettent en place la fonction de signature dans un projet de système d'information.

La signature utilisant des mécanismes cryptographiques repose sur l'usage de clés. L'AA doit respecter les règles fixées dans le référentiel [RGS_B_2] pour la gestion de ces clés

3.3.2 - Signature d'une personne par certificat électronique

L'AA doit définir au préalable le niveau de sécurité relatif à la fonction « signature » et en déduit donc l'utilisation d'un certificat électronique de niveau au moins égal à *, ** ou *** pour cette fonction.

Toutes les règles relatives aux exigences techniques complétées d'exigences de nature juridique et organisationnelle pour assurer la délivrance de certificats de signature sont regroupées dans un document appelé Politique de Certification Type Signature [RGS_A_8].

Ainsi, les AA doivent utiliser des certificats de signature de personne d'un niveau de sécurité donné émis conformément aux exigences de la PC Type [RGS_A_8] (ou de la PC Type [RGS_A_11] dans le cas de certificats double usage authentification et signature) pour le niveau de sécurité retenu.

Toutes les règles relatives à la mise en œuvre de la fonction de sécurité « signature » utilisant des certificats électroniques sont regroupées dans le document « Service Signature » [RGS_A_3]. Il présente d'une part la synthèse par niveau de sécurité des règles relatives à la délivrance de certificats électronique de signature (dont l'exhaustivité se trouve dans les documents [RGS_A_7] et [RGS_A_11]) et définit d'autre part celles relatives aux applications et aux dispositifs nécessaires pour réaliser et vérifier cette fonction de sécurité. Il traite aussi des aspects de format et les bonnes pratiques

Ainsi, les AA utilisant une application de création de signature, un module de vérification de signature et des dispositifs de création de signature doivent respecter les règles du document [RGS_A_3] pour le niveau de sécurité retenu.

Les AA veillent à suivre les règles de bonnes pratiques du document [RGS_A_3].

Cas particulier de la signature des actes administratifs :

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 doit déterminer 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 respecter les règles définies dans ce paragraphe.

Référentiel Général de Sécurité				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
	0.98	16/12/2008	Public	16/33

Signature qualifiée :

Les exigences techniques des certificats qualifiés permettant de générer des signatures présumées fiables au sens du [décret2001-272] et définies dans l'[Arrêté260704] sont un sous ensemble des exigences techniques et des règles de sécurité devant être respectées pour être conforme à [RGS_A_8] niveau ***.

Les exigences supplémentaires introduites pour le niveau *** sont essentiellement des exigences de format et de variables de temps afin d'assurer l'interopérabilité avec tous les systèmes d'information des AA.

De ce fait, une signature électronique générée avec un dispositif de création de signature sécurisé certifié et avec des certificats électroniques de signature conformes au niveau trois étoiles (***) de [RGS_A_8] est présumée fiable et est conforme au [décret2001-272] ainsi qu'à la directive européenne 1999/93 CE.

3.3.3 - Cachet d'un serveur par certificat électronique

L'AA doit définir au préalable le niveau de sécurité relatif à la fonction « cachet serveur » et en déduit donc l'utilisation d'un certificat électronique de niveau au moins égal à *, ** ou *** pour cette fonction.

Toutes les règles relatives aux exigences techniques complétées d'exigences de nature juridique et organisationnelle pour assurer la délivrance de certificats cachet serveur sont regroupées dans un document appelé Politique de Certification Type Cachet Serveur [RGS_A_10].

Ainsi, les AA doivent utiliser des certificats de cachet serveur d'un niveau de sécurité donné émis conformément aux exigences de la PC Type [RGS_A_10] pour le niveau de sécurité retenu.

Toutes les règles relatives à la mise en œuvre de la fonction de sécurité « cachet serveur » utilisant des certificats électroniques sont regroupées dans le document « Service Cachet Serveur » [RGS_A_5]. Il présente d'une part la synthèse par niveau de sécurité des règles relatives à la délivrance de certificats électroniques cachet serveur (dont l'exhaustivité se trouve dans le document [RGS_A_10]) et définit d'autre part celles relatives aux applications et aux dispositifs nécessaires pour réaliser et vérifier cette fonction de sécurité. Il traite aussi des aspects de format et les bonnes pratiques

Ainsi, les AA utilisant une application de création de cachet, un applicatif de vérification de cachet et des dispositifs de création de cachet doivent respecter les règles du document [RGS_A_5] pour le niveau de sécurité retenu.

Les AA veillent à suivre les règles de bonnes pratiques du document [RGS_A_5].

3.4 - Confidentialité

La confidentialité est le caractère réservé d'une information ou d'un traitement dont l'accès est limité aux seules personnes admises à la ou le connaître. Le chiffrement est en cryptographie le procédé grâce auquel la compréhension de données chiffrées est impossible à toute personne ne possédant pas la clé de déchiffrement.

3.4.1 - Utilisation de mécanismes cryptographiques

Le référentiel [RGS_B_1] fixe les règles (et donne des recommandations), que les AA doivent respecter, lorsqu'elles mettent en place une fonction de confidentialité reposant sur des mécanismes cryptographiques.

La confidentialité utilisant des mécanismes cryptographiques repose sur l'usage de clés. L'AA doit respecter les règles fixées dans le référentiel [RGS_B_2] pour la gestion de ces clés.

3.4.2 - Confidentialité par certificat électronique

L'AA doit définir au préalable le niveau de sécurité relatif à la fonction « confidentialité » et en déduit donc l'utilisation d'un certificat électronique de niveau au moins égal à *, ** ou *** pour cette fonction.

Toutes les règles relatives aux exigences techniques complétées d'exigences de nature juridique et organisationnelle pour assurer la délivrance de certificats de confidentialité sont regroupées dans un document appelé Politique de Certification Type Confidentialité [RGS_A_6].

Ainsi, les AA doivent utiliser des certificats de confidentialité d'un niveau de sécurité donné émis conformément aux exigences de la PC Type [RGS_A_6] pour le niveau de sécurité retenu.

Toutes les règles relatives à la mise en œuvre de la fonction de sécurité « confidentialité » utilisant des certificats électroniques sont regroupées dans le document « Service confidentialité » [RGS_A_1]. Il présente d'une part la

Référentiel Général de Sécurité				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
	0.98	16/12/2008	Public	17/33

synthèse par niveau de sécurité des règles relatives à la délivrance de certificats électronique confidentialité (dont l'exhaustivité se trouve dans le document [RGS_A_6]) et définit d'autre part celles relatives aux applications et aux dispositifs nécessaires pour réaliser et vérifier cette fonction de sécurité. Il traite aussi des aspects de format et les bonnes pratiques

Ainsi, les AA utilisant un module de chiffrement, un module de déchiffrement et des dispositifs de protection des clés privées doivent respecter les règles du document [RGS_A_1] pour le niveau de sécurité retenu.

Les AA veillent à suivre les règles de bonnes pratiques du document [RGS_A_1].

3.4.3 - Habilitations

Comme indiqué au chapitre 2.1, certains moyens pour assurer les fonctions de sécurité peuvent être organisationnels. C'est le cas de l'accès aux données ou aux traitements.

Les AA doivent fixer des règles d'habilitation, destinées à déterminer, en fonction du strict besoin des usagers et de celui des agents dans le cadre de leurs fonctions, les autorisations d'accès à donner à chacun, en lecture, en écriture ou en modification, aux données contenues dans le système d'information.

3.5 - Horodatage

L'horodatage permet d'attester qu'une donnée existe à un instant donné.

3.5.1 - Utilisation des mécanismes cryptographiques

Le référentiel [RGS_B_1] fixe les règles (et donne des recommandations), que les AA doivent respecter, lorsqu'elles mettent en place une fonction d'horodatage reposant sur des mécanismes cryptographiques.

L'horodatage utilisant des mécanismes cryptographiques repose sur l'usage de clés. L'AA doit respecter les règles fixées dans le référentiel [RGS_B_2] pour la gestion de ces clés.

3.5.2 - Horodatage par contremarques de temps

Les AA utilisent des contremarques de temps émises conformément aux exigences de [RGS_A_12].

Les AA veillent à suivre les règles de bonnes pratiques qui se trouvent dans le document [RGS_A_3] et qui concernent la gestion de preuve.

Référentiel Général de Sécurité				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
	0.98	16/12/2008	Public	18/33

4 - Accusé d'enregistrement et 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 du 12 avril 2000 :
« 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'usager 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 ».

Le [décretAR/AE] d'application prévu à l'article 5.I de l'Ordonnance décrit les conditions et les délais d'émission de l'accusé d'enregistrement et de l'accusé de réception ainsi que les indications devant y figurer.

4.2 - Règles de sécurité

Il est de la responsabilité de l'AA de déterminer le niveau de sécurité requis pour la fonction d'accusé de réception et / ou d'enregistrement.

Selon que les relations entre les usagers et les AA s'inscrivent ou non dans le cadre de l'article 16 de la [loi120400], les exigences de sécurité seront différentes. Ainsi, si l'usager est tenu de respecter une date limite ou un délai dans le cadre de sa procédure, les AA veillent à mettre en place un dispositif de telle sorte que les accusés de réception et / ou d'enregistrement soient :

- horodatés avec des contremarques de temps émises conformément aux exigences du document [RGS_A_12] ;
- signés avec un certificat de signature (ou cachetés avec un certificat cachet serveur) de niveau une étoile (*) ou supérieur émis conformément aux exigences du document [RGS_A_8] (ou [RGS_A_10] pour les cachets serveur) pour ce niveau.

Par ailleurs, il est recommandé d'assurer la sauvegarde des accusés d'enregistrement et de réception tant que peuvent survenir d'éventuelles réclamations. La durée doit être déterminée par le responsable du système d'information.

Référentiel Général de Sécurité				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
	0.98	16/12/2008	Public	19/33

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 ».

5.1 - Qualification de produits de sécurité

5.1.1 - Introduction

Extrait du [décretRGS] (chapitre III : Qualification des produits de sécurité) :

PROJET

Art. 8 - 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 la direction centrale 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 correspondant au niveau de sécurité pour lequel la demande de qualification a été faite.

Art. 9 - La demande de qualification contient une description du produit et de ses fonctions de sécurité, les objectifs de sécurité qu'il vise à satisfaire ainsi que le niveau auquel il doit être qualifié. La direction centrale de la sécurité des systèmes d'information ne donne pas suite à cette demande lorsque :

- a) le niveau et les objectifs de sécurité identifiés ne sont pas cohérents avec le besoin de sécurité des autorités administratives ;
- b) l'ensemble des matériels, des logiciels et de la documentation nécessaires pour réaliser l'évaluation ne sont pas disponibles, et en particulier lorsque les conditions de développement du produit ne garantissent pas l'accès à ces éléments.

Art. 10 - L'évaluation du produit est effectuée dans les conditions prévues par le décret du 18 avril 2002 susvisé. La direction centrale de la sécurité des systèmes d'information peut procéder ou faire procéder à des évaluations complémentaires si elle l'estime nécessaire.

Art. 11 - Au vu des rapports d'évaluation, le Premier ministre délivre au commanditaire une attestation de qualification du produit, assortie le cas échéant de conditions et de réserves, portant notamment sur la durée de validité. L'attestation et les objectifs de sécurité que le produit peut satisfaire sont, avec l'accord du commanditaire, rendus publics. Tout changement des conditions dans lesquelles la qualification a été obtenue peut conduire le Premier ministre à suspendre ou à retirer la qualification, après que le commanditaire a pu faire valoir ses observations

Selon l'[Ordonnance], un produit de sécurité est un dispositif, matériel ou logiciel, mettant en œuvre des fonctions qui contribuent à la sécurité des informations échangées par voie électronique.

Ces produits de sécurité prennent en charge la majeure partie des mécanismes techniques sur lesquels repose la sécurité du système d'information. L'efficacité de la protection qui en résulte dépend d'une part des qualités et défauts techniques propres au produit et d'autre part des modalités d'emploi du produit dans son environnement (exposition aux menaces, présence d'autres mécanismes de sécurité externes au produit, paramétrage soigné, exploitation par du personnel formé, etc.)

Les modalités d'emploi restent de l'entière responsabilité de l'AA mais cette dernière attend légitimement du produit qu'il tienne ses promesses, afin d'atteindre effectivement les objectifs de sécurité qu'elle s'est fixés. Or un produit de sécurité trop « faible » peut compromettre l'atteinte de ces objectifs de sécurité.

Pour s'assurer de l'absence d'une telle brèche, un produit de sécurité peut obtenir une qualification délivrée par la DCSSI.

La DCSSI procède à la qualification de produits de sécurité afin d'apprécier la robustesse des mécanismes de sécurité mis en œuvre. La qualification comporte ainsi plusieurs niveaux : plus le niveau est élevé, plus la garantie de robustesse du produit apportée par la qualification est significative.

Référentiel Général de Sécurité				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
	0.98	16/12/2008	Public	20/33

Les trois niveaux de qualification de produits de sécurité sont les suivants :

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

Lors de la préparation de la qualification de leurs produits, les industriels peuvent s'appuyer sur des profils de protection. La DCSSI propose à titre informatif divers profils de protection (cf. annexe 2).

Pour un niveau de qualification donné, l'objectif est de vérifier que :

- le produit est conforme à ses spécifications de sécurité ;
- de coter ses mécanismes de façon théorique ;
- de recenser les vulnérabilités connues de produits de sa catégorie ;
- de soumettre le produit à des tests visant à contourner ses fonctions de sécurité.

5.1.2 - Qualification élémentaire

Analyse des mécanismes cryptographiques :

Les mécanismes cryptographiques et la gestion des clés utilisées par ces mécanismes au sein du produit de sécurité doivent être conformes aux règles définies dans [RGS_B_1] et [RGS_B_2].

Evaluation de l'implémentation matérielle et logicielle :

Le processus de délivrance de ce label de premier niveau repose sur la certification de sécurité de premier niveau (CSPN). Il s'agit d'attester que le produit a subi avec succès une évaluation par des centres d'évaluation agréés par la DCSSI dans un temps et une charge contraints. Cette évaluation est une expertise sur le produit de sécurité. Elle n'est pas basée sur les Critères Communs [CC].

Documents d'application :

Le document [Qualif_Élémentaire] détaille le processus de qualification de niveau élémentaire.

5.1.3 - Qualification standard

Analyse des mécanismes cryptographiques :

Identique à l'analyse des mécanismes cryptographiques de la qualification élémentaire.

Evaluation de l'implémentation matérielle et logicielle :

Cette évaluation se décompose en deux parties :

- Evaluation du produit selon les Critères Communs.
Le niveau d'assurance requis et sur lequel le produit de sécurité est évalué selon les [CC] est EAL 3 augmenté des paquets d'assurance ALC_FLR.3 et AVA_VLA.2 en [CC] V2.3 et ALC_FLR.3 et AVA_VAN.3 en [CC] V3.1.
- Expertise de l'implémentation de la cryptographie.

Document d'application :

Le document [Qualif_Standard] détaille le processus de qualification de niveau standard.

5.1.4 - Qualification renforcée

Analyse des mécanismes cryptographiques :

Identique à l'analyse des mécanismes cryptographiques de la qualification élémentaire.

Evaluation de l'implémentation matérielle et logicielle :

Cette évaluation se décompose en deux parties :

- Evaluation du produit selon les Critères Communs.
Le niveau d'assurance requis et sur lequel le produit de sécurité est évalué selon les [CC] est EAL 4 augmenté des paquets d'assurance ADV_IMP.2, ALC_DVS.2, ALC_FLR.3 et AVA_VLA.4 en [CC] V2.3 et ADV_IMP.2, ALC_DVS.2, ALC_FLR.3 et AVA_VAN.5 en [CC] V3.1.
- Expertise de l'implémentation de la cryptographie.

Document d'application :

Le document [Qualif_Renforcée] détaille le processus de qualification de niveau renforcé.

Référentiel Général de Sécurité				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
	0.98	16/12/2008	Public	21/33

5.2 - Qualification des Prestataires de Service de Confiance (PSCo)

Le processus de qualification d'un PSCo est détaillé dans le [DécretRGS].

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

PROJET

Section 1 : Habilitation des organismes qui procèdent à la qualification des prestataires de service de confiance.

Art. 12 – L'habilitation des organismes qui procèdent à la qualification des prestataires de services de confiance, prévue par l'article 9 de l'ordonnance du 8 décembre 2005 susvisée, est délivrée par le Premier ministre. L'organisme demandeur doit faire la preuve :

- a) de sa conformité aux normes d'accréditation en vigueur relatives notamment aux exigences d'impartialité, de responsabilité et de confidentialité applicables à ces organismes. Cette conformité est attestée par une accréditation délivrée par un organisme d'accréditation reconnu dans les conditions prévues par l'article R. 115-6 du code de la consommation, ou par tout organisme d'accréditation reconnu équivalent dans le cadre de la coopération européenne des organismes d'accréditation ;
- b) et de sa compétence technique à conduire l'évaluation de fonctions de sécurité mises en œuvre par un prestataire de services de confiance au regard du référentiel général de sécurité. Cette compétence est appréciée par la direction centrale de la sécurité des systèmes d'information à partir d'un audit des moyens, des ressources et de l'expérience de l'organisme.

Art. 13 – L'organisme d'accréditation définit conjointement avec la direction centrale de la sécurité des systèmes d'information et la direction générale de la modernisation de l'Etat, les règles et les procédures d'application des normes d'accréditation susmentionnées. Un organisme habilité dans le cadre des présentes dispositions est tenu de respecter ces règles et ces procédures qui sont disponibles auprès de l'organisme d'accréditation.

Art. 14 – La direction centrale de la sécurité des systèmes d'information et la direction générale de la modernisation de l'Etat sont informées par l'organisme d'accréditation, dans les meilleurs délais, de toute décision d'accréditation, de retrait ou de suspension d'accréditation prise dans le cadre des présentes dispositions.

Art. 15 – Lorsque, conformément à la norme d'accréditation, l'organisme accrédité met en place un comité chargé de préserver son impartialité, il doit inviter, si la norme le permet, un représentant de la direction centrale de la sécurité des systèmes d'information et un représentant de la direction générale de la modernisation de l'Etat à siéger à ce comité.

Art. 16 – La demande d'habilitation, prévue à la présente section, est adressée à la direction centrale de la sécurité des systèmes d'information. L'habilitation est subordonnée à l'accréditation de l'organisme dans les conditions prévues à la présente section. L'habilitation est valable pour une durée maximale de trois ans renouvelable. Elle peut énoncer des obligations particulières auxquelles est soumis l'organisme bénéficiaire. La direction centrale de la sécurité des systèmes d'information met à la disposition du public la liste des organismes habilités.

Art. 17 - La direction centrale de la sécurité des systèmes d'information peut s'assurer à tout moment que l'organisme continue de satisfaire aux critères au vu desquels il a été habilité. En cas de manquement à ces critères ou aux obligations fixées par la décision d'habilitation, le Premier ministre peut suspendre ou retirer l'habilitation, après qu'un représentant de l'organisme a pu faire valoir ses observations.

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

Art. 18 – Un prestataire de services de confiance peut demander une qualification auprès d'un organisme habilité dans les conditions prévues à la section précédente. L'organisme habilité évalue les fonctions de sécurité mises en œuvre 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.

Art. 19 - L'organisme habilité prononce la qualification du prestataire au vu du rapport d'évaluation, et lui délivre à cet effet une attestation précisant les fonctions de sécurité couvertes par la qualification et les conditions s'y attachant. La qualification est valable pour une durée de trois ans au plus et peut être renouvelée dans les mêmes conditions. L'organisme habilité adresse le rapport d'évaluation ainsi qu'une copie de l'attestation à la

Référentiel Général de Sécurité				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
	0.98	16/12/2008	Public	22/33

direction centrale de la sécurité des systèmes d'information et à la direction générale de la modernisation de l'Etat. Il rend publique la liste des prestataires auxquels il a délivré une qualification.

Art. 20 – Lorsque l'organisme habilité décide, conformément aux modalités prévues par la norme d'accréditation, de suspendre ou de retirer une qualification ou d'en modifier les conditions, il rend publiques ces décisions, dans les meilleurs délais. Il informe la direction centrale de la sécurité des systèmes d'information et la direction générale de la modernisation de l'Etat des raisons à l'origine de ces décisions.

Art. 21 - Lorsqu'elles recourent à un prestataire de services de confiance qualifié dans les conditions du présent chapitre, les administrations de l'Etat doivent en informer préalablement la direction centrale de la sécurité des systèmes d'information.

Art. 22 – 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.

Toutefois, lorsque cette autorité est une administration de l'Etat, elle doit solliciter au préalable l'avis de la direction centrale de la sécurité des systèmes d'information, qui peut proposer de procéder elle-même à la qualification de cette autorité. 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.

Référentiel Général de Sécurité				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
	0.98	16/12/2008	Public	23/33

6 - Les Infrastructures de Gestion de Clés (IGC)

6.1 - Règles et recommandations générales

Une AA souhaitant mettre en œuvre une IGC et exploiter des fonctions de sécurité à base de certificats électroniques est tenue de :

- rédiger une Politique de Certification (PC) ainsi qu'une Déclaration des Pratiques de Certification (DPC) pour ses autorités de certification ;
- respecter, pour les certificats d'utilisateurs finaux (de personne, serveur) qu'elle émet, les règles correspondantes du RGS, chapitre 3 – Fonctions de sécurité et plus particulièrement les exigences de la Politique de Certification Type de la fonction et du niveau de sécurité associés.

Une même autorité de certification peut émettre plusieurs types de certificats mais les exigences propres à chacun de ces types doivent être distinguées. Il convient pour ce faire d'attribuer un identifiant d'objet unique pour chacune des PC régissant l'émission de tels types de certificats.

Il est recommandé de porter dans une PC spécifique, les exigences de l'autorité de certification racine (appelée AC Racine de l'AA), et des éventuelles AC intermédiaires.

Il est recommandé qu'une AA rédige une politique de validation des certificats électroniques pour les téléservices les utilisant. Ce document est un ensemble de règles et dispositions définissant les exigences portant sur la vérification de la validité d'éléments tels que :

- des certificats électroniques ;
- des signatures électroniques ;
- des contremarques de temps.

Il s'applique aux utilisateurs de certificats, qu'ils en soient porteurs ou exploitants.

6.2 - Cas particulier de la validation des certificats par l'Etat

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'Etat dans des conditions précisées par décret ».

Le [DécretRGS] précise par ailleurs les modalités d'application de la validation des certificats par l'Etat dans son chapitre V (articles 23 à 26).

Extrait du [DécretRGS] :

PROJET

« Art. 23 - Au sens du présent chapitre, on entend par « 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.

Art. 24 - En application de l'article 10 de l'ordonnance du 8 décembre 2005 susvisée, la direction centrale de la sécurité des systèmes d'information met en place un service de validation des certificats électroniques délivrés aux autorités administratives ou à leurs agents permettant à ceux qui utilisent ces certificats d'en vérifier l'origine.

Art. 25 - Pour délivrer les certificats électroniques visés par les présentes dispositions, à une autorité administrative ou à ses agents, un prestataire de services de confiance doit demander, selon des modalités précisées par arrêté du Premier ministre, la validation de ces certificats. A titre transitoire, pour les certificats électroniques délivrés avant un délai de trois ans à compter de la date d'entrée en vigueur du présent chapitre, la demande de validation doit être effectuée, au plus tard, au terme de ce délai.

La validation des certificats électroniques est subordonnée au respect par le prestataire des règles du référentiel général de sécurité. La direction centrale de la sécurité des systèmes d'information peut demander à vérifier sur place les conditions de délivrance de ces certificats électroniques.

Art. 26 - Les autorités administratives veillent à ce que les systèmes d'information mis en œuvre pour la délivrance des certificats électroniques visés par les présentes dispositions

Référentiel Général de Sécurité				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
	0.98	16/12/2008	Public	24/33

soient mis en conformité avec le référentiel général de sécurité dans les délais prévus par l'ordonnance du 8 décembre 2005 susvisée.

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

6.2.1 - Présentation de l'IGC/A

L'objectif de cette validation est de mettre à disposition des usagers de systèmes d'information les éléments permettant de s'assurer de l'origine des certificats électroniques utilisés par les AA et leurs agents.

Dans ce but, l'autorité de certification (AC) racine de l'infrastructure de gestion de clé cryptographiques dite « IGC/A » (ou « Infrastructure de la Gestion de la Confiance de l'Administration »), qui est la racine centrale de l'administration française, délivre des certificats aux AC racines des AA.

Les certificats de la racine IGC/A sont publiés au Journal Officiel de la République française [AvisCertificatsIGC/A] pour permettre aux éditeurs de logiciels de communication d'en vérifier l'intégrité et l'authenticité avant de les intégrer définitivement dans leurs systèmes ou produits, et aux usagers d'effectuer les mêmes vérifications pour les certificats intégrés dans leurs systèmes informatiques.

Ainsi les certificats utilisés par une AA dotée d'un certificat délivré par l'IGC/A peuvent être validés grâce à la « chaîne de validation » qui les relie, par référence à une succession de certificats d'AC qui se font confiance, à celui de l'IGC/A, point de confiance reconnu.

6.2.2 - Règles de sécurité

Le respect des règles énoncées dans le chapitre 6.1 est un pré-requis pour une AA désirant faire signer son certificat d'AC Racine par l'IGC/A.

Avant de délivrer un certificat signé par l'IGC/A, la DCSSI peut demander à auditer les conditions dans lesquelles l'AA mettra en œuvre les certificats électroniques émis. Cet audit porte sur :

- l'AC racine de l'AA ;
- l'organisation et le champ d'application des AC subalternes constituant la chaîne de validation des certificats qui se trouveront validés par l'Etat ;
- l'ensemble des documents décrivant les engagements et exigences de l'AC racine de l'AA ;
- les pratiques, procédures et moyens mis en œuvre pour gérer le cycle de vie des certificats électroniques que l'AA délivre.

Cet audit vérifie également le respect des exigences portées dans [PC_IGC/A].

La PC d'une AC racine et les PC des AC subalternes doivent limiter la délivrance de leurs certificats électroniques à :

- des AC sous la responsabilité d'une ou plusieurs AA ;
- des agents de l'AA ;
- des machines (pour les certificats serveurs et les cachets serveurs) qui sont sous la responsabilité exclusive de l'AA.

Référentiel Général de Sécurité				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
	0.98	16/12/2008	Public	25/33

7 - Référencement

Extrait de l'Ordonnance

Article 12 : « Les produits de sécurité et les prestataires de services de confiance qualifiés à un niveau de sécurité dans les conditions prévues au III de l'article 9 peuvent faire en outre l'objet d'un référencement par l'Etat. Ils sont alors utilisables par les usagers pour l'ensemble des téléservices pour lesquels ce niveau de sécurité est requis.

Les agents des autorités administratives chargés du traitement et de l'exploitation des informations recueillies dans le cadre de systèmes d'information utilisent, pour accéder à ces systèmes, des produits de sécurité référencés.

Un décret précise les modalités d'application du présent article, notamment les conditions de délivrance des produits de sécurité aux agents des autorités administratives ».

Extrait du DécretRGS :

PROJET

Chapitre VI – Article 27 : « Le référencement d'un produit de sécurité ou d'un prestataire de services de confiance, mentionné à l'article 12 de l'ordonnance du 8 décembre 2005 susvisée, est subordonné au respect des prescriptions contenues dans un cahier des charges approuvé par arrêté du ministre chargé de la réforme de l'Etat. Ce cahier des charges détermine notamment les conditions dans lesquelles l'interopérabilité des produits de sécurité et des prestataires de services de confiance qualifiés dans les conditions prévues au présent décret, est vérifiée ainsi que les tests qui sont réalisés à cette fin.

Le référencement mentionné au premier alinéa est prononcé par décision du ministre chargé de la réforme de l'Etat ».

Référentiel Général de Sécurité				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
	0.98	16/12/2008	Public	26/33

8 - Annexe 1 : Liste des documents constitutifs du RGS

Ce chapitre liste les documents faisant partie intégrante du RGS. Il donne également les pointeurs permettant de se procurer ces documents. Ces documents sont classés en deux catégories :

- Documents applicables concernant l'utilisation de certificats électroniques dans les fonctions de sécurité ;
- Documents applicables concernant l'utilisation de mécanismes cryptographiques dans les fonctions de sécurité.

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

Acronyme	Titre du document	Nom complet du document	Version du document	Lien hypertexte
[RGS_A_1]	Service de Confiance "Confidentialité"	RGS_Service_Confidentialite_V2.2.pdf	2.2	http://www.references.modernisation.gouv.fr/documents-relatifs-a-lutilisation-de-certificats-en
[RGS_A_2]	Service de Confiance "Authentification"	RGS_Service_Authentification_V2.2.pdf	2.2	
[RGS_A_3]	Service de Confiance "Signature"	RGS_Service_Signature_V2.2.pdf	2.2	
[RGS_A_4]	Service de Confiance "Certificat Serveur"	RGS_Service_Authentification_Serveur_V2.2.pdf	2.2	
[RGS_A_5]	Service de Confiance "Cachet Serveur"	RGS_Service_Cachet_Serveur_V2.2.pdf	2.2	
[RGS_A_6]	Politique de Certification Type "Confidentialité"	RGS_PC-Type_Confidentialite_V2.2.pdf	2.2	
[RGS_A_7]	Politique de Certification Type "Authentification"	RGS_PC-Type_Authentification_V2.2.pdf	2.2	
[RGS_A_8]	Politique de Certification Type "Signature"	RGS_PC-Type_Signature_V2.2.pdf	2.2	
[RGS_A_9]	Politique de Certification Type "Certificat Serveur"	RGS_PC-Type_Authentification_Serveur_V2.2.pdf	2.2	
[RGS_A_10]	Politique de Certification Type "Cachet Serveur"	RGS_PC-Type_Cachet_Serveur_V2.2.pdf	2.2	
[RGS_A_11]	Politique de Certification Type "Authentification et Signature"	RGS_PC-Type_Authentification_Signature_V2.2.pdf	2.2	
[RGS_A_12]	Politique d'Horodatage Type	RGS_P_Horodatage-Type_V2.2.pdf	2.2	
[RGS_A_13]	Variables de temps	RGS_Variables_de_temps_V2.1.pdf	2.1	
[RGS_A_14]	Profils de Certificats, CRLs, OCSP et algorithmes cryptographiques	RGS_Profils_Certificat_LCR_OCSP_V2.2.pdf	2.2	

Référentiel Général de Sécurité				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
	0.98	16/12/2008	Public	27/33

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

Acronyme	Titre du document	Nom complet du document	Version du document	Lien hypertexte
[RGS_B_1]	Référentiel Cryptographique : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques	RGS_Mecanismes_cryptographiques_v1_11.pdf	1.11	http://www.ssi.gouv.fr/fr/RGS/
[RGS_B_2]	Référentiel Cryptographique : Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques	RGS_Gestion_clés_cryptographiques_v1_1.pdf	1.1	

Référentiel Général de Sécurité				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
	0.98	16/12/2008	Public	28/33

9 - Annexe 2 : Liste des Profils de Protection

Un profil de protection (PP) est un 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.

Les (PP) ci-dessous sont donnés à titre indicatif. Certains ont été produits et certifiés par la DCSSI (<http://www.ssi.gouv.fr/fr/confiance/pp.html>), d'autres sont issus de normes européennes.

Référence PP	Nom PP	Date PP
CWA14167-1	Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1	Juin 2003
PP CMSCOB PP PP 0308 CWA14167-2	Cryptographic Module for CSP Signing operation with Backup	Février 2004
CWA14167-3	Cryptographic Module for CSP Key Generation Services - Protection Profile (CMCKG-PP)	Février 2004
PP CMSCO PP 0309 CWA14167-4	Cryptographic Module for CSP Signing operation without Backup	2004
PP SSCD CWA14169 types 1, 2, 3	Dispositif sécurisé de création de signature (EAL4+)	Mars 2004
CWA14365-2	Guide on the Use of Electronic Signatures - Part 2: Protection Profile for Software Signature Creation Devices	Mars 2004
DCSSI-PP 2008/01 (PP-PFP-CCv3.1)	Pare feu personnel EAL3+	mai 2008
DCSSI-PP 2008/05 (PP-ACSE-CCv3.1)	Application de création de signature EAL3+	Juillet 2008
DCSSI-PP 2008/06 (PP-MVSE-CCv3.1)	Module de vérification de signature EAL3+	Juillet 2008
DCSSI-PP-2008/07 (PP-SH-CCv3.1)	Système d'horodatage EAL3+	Juillet 2008

Référentiel Général de Sécurité				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
	0.98	16/12/2008	Public	29/33

10 - Annexe 3 : 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 service 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 conformément au décret d'application de l'article 9.2 de l'[Ordonnance]

Certificat électronique - Fichier électronique attestant qu'une bi-clé appartient à la personne physique ou morale ou à l'élément matériel ou logiciel identifié, directement ou indirectement (pseudonyme), dans le certificat. Il est délivré par une Autorité de Certification. En signant le certificat, l'AC valide le lien entre l'identité de la personne physique ou morale ou de l'élément matériel ou logiciel et la bi-clé. Le certificat est valide pendant une durée limitée précisée dans celui-ci. Un certificat et une bi-clé sont généralement réservés à un usage unique. Seul le double usage authentification et signature est toléré pour certains types de certificats.

Certificat cachet serveur - Certificat électronique dont la bi-clé associée est utilisée pour générer une signature électronique par un élément matériel ou logiciel. Cette signature électronique n'est pas réalisée par une personne physique. Comme seule une personne physique peut signer au sens juridique du terme, il a donc été décidé de nommer ce certificat : cachet serveur, pour faire la distinction.

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

Fonction de sécurité - Fonctions des systèmes d'information contribuant à la sécurité des informations échangées par voie électronique.

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

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

HSM – Hardware Security Module. Appareil considéré comme inviolable offrant des fonctions cryptographiques. Il s'agit d'un matériel électronique offrant un service de sécurité qui consiste à générer, stocker et protéger des clés cryptographiques.

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

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 dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes. Une PC peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les porteurs et les utilisateurs de certificats.

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

Référentiel Général de Sécurité				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
	0.98	16/12/2008	Public	30/33

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 et/ou des niveaux de sécurité différents. Un PSHE comporte au moins une AH mais peut en comporter plusieurs en fonction de son organisation. Un PSHE est identifié dans les certificats de clés publiques des 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 prestataire de services de confiance - Acte par lequel un organisme de certification atteste de la conformité de tout ou partie de l'offre de service 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 la DCSSI atteste de la capacité d'un produit à assurer, avec un niveau de robustesse donné, les services de sécurité objet de la qualification. L'attestation de qualification indique le cas échéant l'aptitude du produit à participer à la réalisation, à un niveau de sécurité donné, d'une ou plusieurs fonctions traitées dans le [RGS].

Référencement - Opération réalisée par l'Administration et qui atteste que l'offre de service du PSCo ou le produit concerné est utilisable avec tous les systèmes d'information qui requièrent ce type de service ou de produit et exigent le niveau de sécurité correspondant. Une offre référencée pour un service donné et un niveau de sécurité donné du [RGS] peut être utilisée dans toutes les applications d'échanges dématérialisés requérant ce service et jusqu'à ce niveau de sécurité. Pour les usagers, le référencement permet de savoir quelles offres de service de sécurité ou quels produits ils peuvent utiliser pour tel ou tel échange dématérialisé. Le référencement des AC ou AH des autorités administratives répond aux mêmes critères.

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

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				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
	0.98	16/12/2008	Public	31/33

11 - Annexe 4 : Références documentaires

11.1 - 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=JORFTEXT00000636232&dateTexte=vig>
- [DécretRGS] Le décret regroupe l'ensemble de quatre décrets d'application des articles 9 et 10 de l'[Ordonnance].
Ce texte est encore à l'état de projet. Disponible en ligne : <http://www.ssi.gouv.fr/fr/RGS/>
- [DécretAR/AE] Décret relatif à l'accusé de réception électronique pris en application de l'article 5 de l'[Ordonnance].
Ce texte est encore à l'état de projet.
- [décret2001-272] Décret 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>
- [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=JORFTEXT00000441678&dateTexte>
- [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>

11.2 - Références techniques

- [ISO2700x] Normes relatives à la sécurité de l'information.
Disponible auprès de l'ISO ou via le service en ligne « Webport » de l'AFNOR.
- [PSSI] Guide « Politique SSI » de la DCSSI. Disponible en ligne : <http://www.ssi.gouv.fr/fr/confiance/pssi.html>
- [MaturitéSSI] Guide « maturité SSI » de la DCSSI
<http://www.ssi.gouv.fr/fr/confiance/documents/methodes/maturitessi-methode-2007-11-02.pdf>
- [EBIOS] Méthode d'analyse de risque de la DCSSI. Disponible en ligne : <http://www.ssi.gouv.fr/fr/confiance/ebiospresentation.html>
- [GISSIP] Guide « Gestion et Intégration de la SSI dans les Projets » (souvent nommé guide GISSIP) de la DCSSI
<http://www.ssi.gouv.fr/fr/confiance/documents/methodes/GISSIP-Methode-2006-12-11.pdf>
- [FEROSTypes] Collection documentaire des « FEROS Types » pour les téléservices (source DGME)
<http://www.referencesssi.gouv.fr/documents-relatifs-a-la-gestion-de-la-securite-dans-les-projets-si>
- [ExigencesTélé] Guide d'Exigences types de sécurité pour les téléservices (source DGME)
<http://www.referencesssi.gouv.fr/documents-relatifs-a-la-gestion-de-la-securite-dans-les-projets-si>

Référentiel Général de Sécurité				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
	0.98	16/12/2008	Public	32/33

- [CERTA] Note d'information du CERTA sur les mots de passe, dernière révision le 12 avril 2007.
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001>
- [CC] "Common Criteria for Information Technology Security Evaluation". Disponible en ligne :
<http://www.ssi.gouv.fr/fr/confiance/methodologie.html> ou <http://www.commoncriteriaportal.org>
- [Qualif_Elémentaire] Processus de qualification d'un produit de sécurité – Niveau Elémentaire – Version 1.0
<http://www.ssi.gouv.fr/fr/RGS/>
- [Qualif_Standard] Processus de qualification d'un produit de sécurité – Niveau Standard – Version 1.2
<http://www.ssi.gouv.fr/fr/RGS/>
- [Qualif_Renforcée] Processus de qualification d'un produit de sécurité – Niveau Renforcé – Version 1.0
<http://www.ssi.gouv.fr/fr/RGS/>
- [PC_IGC/A] Politique de Certification de l'IGC/A – version 1.1RevA et suivantes. Disponible en ligne :
http://www.ssi.gouv.fr/fr/sigelec/igca/igca-politique_certification.pdf
- [AvisCertificatsIGC/A]
http://www.legifrance.gouv.fr/jopdf/common/jo_pdf.jsp?numJO=0&dateJO=20070217&numT exte=126&pageDebut=02946&pageFin=02947

Référentiel Général de Sécurité				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
	0.98	16/12/2008	Public	33/33