Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Premier ministre	Ministère du budget, des comptes publics et de la réforme de l'État
Agence nationale de la sécurité des systèmes d'information	Direction générale de la modernisation de l'État

Référentiel Général de Sécurité

version 1.0

Annexe A1

Fonction de sécurité

« Confidentialité »

Version 2.3 du 11 février 2010

HISTORIQUE DES VERSIONS			
DATE	**VERSION**	**EVOLUTION DU DOCUMENT**	**REDACTEUR**
06/11/2006	2.1	*Document constitutif de la Politique de Référencement Intersectorielle de Sécurité – PRISv2.1.*	DCSSI / SDAE
12/12/2008	2.2	*Document constitutif du Référentiel Général de Sécurité – RGSv0.98, annexe A1.* Restructuration du document.	DCSSI / DGME
11/02/2010	2.3	*Document constitutif du Référentiel Général de Sécurité – RGSv1.0, annexe A1.* Principales modifications : • Suppression des exigences des chapitres III.2, III.3.2 et III.4.2 et III.5.2 ; • Rajout de chapitres relatifs à la qualification des produits de sécurité et des offres de PSCE.	ANSSI / DGME

Les commentaires sur le présent document sont à adresser à :

Agence nationale de la sécurité des systèmes d'information

SGDSN/ANSSI

51 boulevard de La Tour-Maubourg
75700 Paris 07 SP

rgs@ssi.gouv.fr

Direction générale de la modernisation de l'État

Service Projets

64-70 allée de Bercy
75012 Paris

rgs.dgme@finances.gouv.fr

SOMMAIRE

I. Objet et contenu du document

Le présent document fait partie des documents constitutifs du Référentiel Général de Sécurité [RGS]. Il en constitue l'annexe [RGS_A_1].

Il regroupe toutes les règles de sécurité applicables pour les différents « composants » nécessaires à la mise en œuvre de la fonction de sécurité « Confidentialité » basée sur la cryptographie asymétrique. Ces composants sont les suivants :

- les bi-clés et certificats électroniques dont l'usage est le chiffrement[1] ;
- le dispositif de protection des clés privées ;
- le module de chiffrement ;
- le module de déchiffrement.

Il s'adresse aux autorités administratives (AA) qui ont décidé après leur analyse de risque, de mettre en œuvre, pour un niveau de sécurité donné parmi *, ** et ***, la fonction de sécurité « Confidentialité » basée sur des mécanismes cryptographiques asymétriques.

[1] Les règles relatives à la délivrance et la gestion du cycle de vie des certificats de chiffrement sont regroupées dans le document « Politique de Certification Type Confidentialité » [RGS_A_6].

II. Présentation de la fonction de sécurité « Confidentialité »

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

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

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

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

Un tel chiffrement peut être requis et mis en œuvre lorsque, par exemple, l'usager est en relation avec une application d'échange dématérialisé depuis son ordinateur personnel ou depuis une borne d'accès dans un lieu public (mairie, CPAM, ...) et que les informations échangées nécessitent d'être protégées en confidentialité en raison de leur sensibilité.

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

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

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

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

III. Exigences pour la mise en œuvre de la fonction de sécurité « Confidentialité »

Ce paragraphe regroupe toutes les exigences de sécurité, d'interopérabilité ainsi que les bonnes pratiques pour tous les composants participant à la fonction de sécurité « Confidentialité ».

III.1. Certificats délivrés par les PSCE

Les exigences que doit respecter un PSCE, délivrant des certificats à des fins de confidentialité sont définies dans la politique de certification type (PC Type) Confidentialité [RGS_A_6].

La PC Type Confidentialité distingue trois niveaux de sécurité aux exigences croissantes *, ** et ***.

Il est autorisé d'utiliser au sein d'un système d'information un certificat électronique de niveau de sécurité supérieur à celui de la fonction de sécurité sous réserves, d'une part, que le niveau du dispositif de stockage et de mise en œuvre de la clé privée et le niveau du certificat soient cohérents et, d'autre part, que l'interopérabilité du certificat ait été par ailleurs garantie[2]. Ainsi, par exemple, un certificat électronique de confidentialité conforme aux exigences du niveau (***) et référencé pourra être employé dans des téléservices de niveaux (*) et (**).

Les exigences applicables à un ou à plusieurs des niveaux spécifiques sont clairement identifiées et mises en évidence dans la PC Type. Cette architecture documentaire permet de disposer d'une PC Type homogène quel que soit le niveau et permet également d'identifier facilement et rapidement sur quels sujets il y a des différences entre les niveaux et quelles sont ces différences.

Cette PC Type concerne à la fois les porteurs de certificats du secteur privé de types "entreprises"[3] et "particuliers". Elle concerne également tous les agents des autorités administratives porteurs de certificats. Les exigences spécifiques à l'un ou à l'autre de ces types d'utilisateurs, lorsqu'elles existent, sont clairement identifiées.

De plus, cette PC Type s'appuie sur deux documents communs à toutes les PC Types :

- l'annexe [RGS_A_13] du [RGS] : document définissant des variables de temps concernant différents évènements du cycle de vie des clés cryptographiques et des certificats ;
- l'annexe [RGS_A_14] du [RGS] : document définissant les règles et recommandations sur les profils des certificats, les listes de certificats révoqués et le protocole OCSP ainsi que des exigences sur les algorithmes cryptographiques mis en œuvre.

Un PSCE peut faire qualifier à un niveau de sécurité donné l'offre de certificats de chiffrement selon les modalités prévues dans le [DécretRGS]. Dans ce cas, il doit intégrer dans sa PC l'ensemble des exigences de la PC Type correspondant au niveau visé et, bien entendu, respecter ensuite l'ensemble des engagements pris dans cette PC.

III.2. Dispositifs de protection de clés privées

III.2.1.Exigences de sécurité

L'usager ou l'agent qui reçoit des données chiffrées doit utiliser un dispositif de protection de clés privées répondant à un minimum d'exigences de sécurité. Ces exigences sont décrites dans l'annexe 3

[2] Attestée par la procédure de référencement, conformément à l'article 12 de l'ordonnance.

[3] La dénomination "entreprise" recouvre les entreprises au sens le plus large et également les personnes morales de droit privé : sociétés, associations ainsi que les artisans et les travailleurs indépendants.

de la PC Type Confidentialité [RGS_A_6], et reprises ci-dessous.

Quel que soit le niveau, un dispositif de protection de clés privées utilisé par le porteur pour stocker et mettre en œuvre sa clé privée de déchiffrement, et le cas échéant, générer sa bi-clé, doit répondre aux exigences de sécurité suivantes :

- si la bi-clé de confidentialité du porteur est générée par le dispositif, garantir que cette génération est réalisée exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique de la bi-clé générée ;
- détecter les défauts lors des phases d'initialisation, de personnalisation et d'opération et disposer de techniques sûres de destruction des clés privées qui ne sont plus utilisées ;
- garantir la confidentialité et l'intégrité des clés privées[4] ;
- assurer la correspondance entre la clé privée et la clé publique ;
- assurer la fonction de déchiffrement, de clés symétriques, de fichiers ou de messages, pour le porteur légitime uniquement et protéger la clé privée contre toute utilisation par des tiers ;
- permettre de garantir l'authenticité et l'intégrité de la clé symétrique, d'un fichier ou d'un message, une fois déchiffré, lors de son export hors du dispositif à destination de l'application de déchiffrement des données ;
- permettre de garantir l'authenticité et l'intégrité de la clé publique lors de son export hors du dispositif ;
- le cas échéant, permettre de garantir la confidentialité, l'authenticité et l'intégrité de la clé privée lors de son export hors du dispositif, à destination d'une fonction de séquestre ou d'archivage des clés privées.

III.2.2.Exigences sur la qualification

Le respect des règles suivantes n'est exigé que lorsque le PSCE souhaite faire qualifier son offre de certificats de chiffrement au(x) niveau(x) de sécurité considéré(s) selon la procédure décrite dans le [DécretRGS] et délivre au porteur final le dispositif de protection des clés privées ; dans tous les autres cas, leur respect est recommandé.

Au niveau *** :
Le dispositif de protection des clés privées utilisé par le porteur doit être qualifié au niveau renforcé[5], selon le processus décrit dans le [RGS], et être conforme aux exigences du chapitre ci-dessus.

Au niveau ** :

Le dispositif de protection des clés privées utilisé par le porteur doit être qualifié au minimum au niveau standard[6], selon le processus décrit dans le [RGS], et être conforme aux exigences du chapitre ci-dessus.

Il est toutefois recommandé d'utiliser dispositif de protection des clés privées qualifié au niveau renforcé.

[4] A un instant donné, un dispositif de protection de clés privées peut disposer de plusieurs clés privées : la clé privée courante ainsi que la ou les clés privées précédentes afin que le porteur puisse continuer à accéder aux messages / fichiers qui avaient été chiffrés à l'aide des clés publiques correspondantes.

[5] Sous réserve qu'il existe au moins une telle référence au catalogue des produits qualifiés par l'ANSSI. Dans le cas contraire, le PSCE souhaitant faire qualifier son offre de certificats de chiffrement doit obtenir une dérogation de l'ANSSI.

[6] Sous réserve qu'il existe au moins une telle référence au catalogue des produits qualifiés par l'ANSSI. Dans le cas contraire, le PSCE souhaitant faire qualifier son offre de certificats de chiffrement doit obtenir une dérogation de l'ANSSI.

Au niveau * :

Le dispositif de protection des clés privées utilisé par le porteur doit être qualifié au minimum au niveau élémentaire[7], selon le processus décrit dans le [RGS], et être conforme aux exigences du chapitre ci-dessus.

Il est toutefois recommandé d'utiliser dispositif de protection des clés privées qualifié au niveau standard.

III.3. Module de chiffrement

III.3.1.Exigences de sécurité

Les opérations cryptographiques de chiffrement sont mises en œuvre dans un module de chiffrement qui va procéder au chiffrement.

Quel que soit le niveau, un module de chiffrement doit répondre aux exigences de sécurité suivantes :

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

III.3.2.Exigences sur la qualification

Aux niveaux *** et **, il est recommandé d'utiliser un module de chiffrement qualifié au minimum au niveau standard.

III.3.3.Bonnes pratiques

Lors de l'utilisation d'un certificat, il faut notamment vérifier que celui-ci :

- contient une indication d'usage conforme à ce qui est attendu ;
- est valide et n'est pas révoqué ;
- a une chaîne de certification qui est correcte à tous les niveaux.

III.4. Module de déchiffrement

III.4.1.Exigences de sécurité

Les opérations cryptographiques de déchiffrement sont mises en œuvre dans un module de déchiffrement qui va procéder au déchiffrement.

Quel que soit le niveau, un module de déchiffrement doit répondre aux exigences de sécurité suivantes :

[7] Sous réserve qu'il existe au moins une telle référence au catalogue des produits qualifiés par l'ANSSI. Dans le cas contraire, le PSCE souhaitant faire qualifier son offre de certificats de chiffrement doit obtenir une dérogation de l'ANSSI.

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

III.4.2.Exigences sur la qualification

Aux niveaux *** et **, il est recommandé d'utiliser un module de déchiffrement qualifié au minimum au niveau standard.

III.5. Environnement d'utilisation

La fonction de sécurité « Confidentialité » est notamment mise en œuvre sur une borne publique ou un ordinateur dans un cadre privé ou professionnel pour un usage par une personne physique.

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

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

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

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

IV. Documents de référence

IV.1. Réglementation

Renvoi	Document
[ORDONNANCE]	*Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives*
[DécretRGS]	*Décret pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005*

IV.2. Documents techniques

Renvoi	Document
[RGS]	*Référentiel Général de Sécurité - Version 1.0*
[RGS_A_6]	*Politique de Certification Type Confidentialité - Version 2.3*
[RGS_A_13]	*Variables de Temps - Version 2.3*
[RGS_A_14]	*Profils de certificats, de LCR et OCSP et algorithmes cryptographiques – Version 2.3*