Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

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

Référentiel Général de Sécurité

version 2.0

Annexe A1

Règles relatives à la mise en œuvre des fonctions de sécurité basées sur l'emploi de certificats électroniques

Version 3.0 du 27 février 2014

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
27/02/2014	3.0	*Document constitutif du Référentiel Général de Sécurité – RGSv2.0, annexe A1* Fusion des annexes A1 à A5 du RGS version 1.0 Modifications des exigences sur les dispositifs de protection des clés privées des services applicatifs. Modifications des exigences de qualification des applications de création de signature électronique.	ANSSI

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

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_A1].

Il fixe les règles de sécurité applicables aux différents « composants » nécessaires à la mise en œuvre des fonctions de sécurité basées sur l'emploi des certificats électroniques et décrites dans le [RGS]. Ces fonctions de sécurité sont les suivantes :

- signature électronique ;
- authentification de personne ;
- double usage signature électronique et authentification ;
- confidentialité ;
- cachet ;
- authentification de serveur.

Ces composants sont les suivants :

- les bi-clés et certificats électroniques délivrés par des prestataires de service de certification électronique pour les usages listés ci-dessus ;
- le dispositif de protection des éléments secrets ;
- les applications qui assurent l'interface avec les usagers (ou les machines), les dispositifs de protection et les éléments secrets.

Il s'adresse aux autorités administratives (AA) qui ont décidé, après analyse des risques, de mettre en œuvre, pour un niveau de sécurité donné parmi *, ** et ***, l'une ou plusieurs des fonctions de sécurité du [RGS] précisées ci-dessus.

Les règles spécifiques à une fonction de sécurité donnée seront précédées du nom de la fonction de sécurité entre « [] » (exemple [Signature électronique]). De la même manière, les règles applicables aux certificats électroniques délivrés à des personnes seront précédées par [Personne] et celles applicables aux services applicatifs par [Service applicatif].

II. Présentation des fonctions de sécurité

II.1. Fonction de sécurité « signature électronique »

La signature électronique est l'une des fonctions de sécurité apportant de la confiance dans les échanges dématérialisés entre usagers et autorités administratives ou entre autorités administratives.

Dans le cadre du [RGS] et de son utilisation dans l'administration, les types de relations couverts par le service de signature sont notamment les suivants :

- signature électronique par un usager, puis vérification de cette signature par un téléservice d'une autorité administrative accessible par voie électronique ;
- signature électronique par un usager, puis vérification de cette signature par un agent d'une autorité administrative ;
- signature électronique par un agent d'une autorité administrative, puis vérification de cette signature par un usager ;
- signature électronique par un agent d'un acte administratif puis vérification de cette signature par un autre agent.

La signature électronique peut être requise et mise en œuvre lorsque 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...).

Le recours à la signature électronique est imposé seulement pour la validité des actes administratifs établis sous la forme électronique[1].

Le principe de fonctionnement et d'interaction des composants entre eux est le suivant :

- l'application de création de signature, déployée sur une machine (PC, borne publique, serveur...) peut réaliser les premières itérations de calcul d'un condensat, à l'aide d'une fonction de hachage, à partir des informations à signer ;
- elle transmet les informations nécessaires à la réalisation de la signature (informations à signer complètes ou partielles, condensat partiel le cas échéant) au dispositif de création de signature (exemples : carte à puce, clé USB) également connecté à la machine.
- le dispositif de création de signature réalise les itérations restantes (a minima la dernière itération) du calcul du condensat, à l'aide d'une fonction de hachage, à partir des informations transmises par l'application de création de signature ;le dispositif de signature réalise un calcul cryptographique de signature du condensat en utilisant la clé privée de signature de l'agent ou de l'usager, activée le cas échéant par un code d'activation (code PIN par exemple) ;
- ce condensat signé, dit signature électronique, est retourné à l'application ;
- la vérification de la signature s'effectue à l'aide d'un module de vérification de signature et du certificat électronique délivré par PSCE qui lie l'identité de l'agent ou de l'usager avec sa clé publique : un calcul cryptographique est effectué à l'aide de la clé publique sur la signature électronique et comparé au condensat obtenu par hachage des informations à signer.

Dans le cadre du [RGS], l'utilisation de la clé privée de signature du porteur et du certificat mono-usage associé est strictement limitée à la signature électronique[2].

La mise en œuvre d'un procédé de signature électronique respectant les exigences définies pour le niveau *** permet de bénéficier de la présomption de fiabilité du procédé de signature telle que prévue dans l'article 1316-4 du code civil. En effet, les exigences formulées dans le [RGS] (annexe [RGS_A_X2]) à l'égard des prestataires de services de certification électronique et des dispositifs de

[1] Art. 8 de l'[Ordonnance]

[2] L'utilisation de certificats électronique dits « double usage » (authentification et signature) tels que décrits dans le document [RGS_A2] est également tolérée.

création de signature pour le niveau *** répondent respectivement aux exigences de l'article 6 et de l'article 3 du [Décret2001-272-].

II.2. Fonction de sécurité « confidentialité »

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

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 mono-usage associé est strictement limitée au service de confidentialité.

II.3. Fonction de sécurité « authentification »

L'authentification est l'une des fonctions de sécurité apportant de la confiance dans les échanges dématérialisés entre usagers et autorités administratives ou entre autorités administratives.

Dans le cadre du [RGS] et de son utilisation dans l'administration, les types de relations couverts par le service d'authentification sont notamment les suivants :

- authentification d'un usager vis-à-vis d'un service de l'administration accessible par voie électronique,
- authentification d'un usager vis-à-vis d'un agent d'une autorité administrative,
- authentification d'un agent d'une autorité administrative vis-à-vis d'un usager.

Cette fonction de sécurité permet à un usager ou à un agent de s'authentifier dans le cadre des types de

relations mentionnés ci-dessus. Ce document ne traite que de l'authentification basée sur des mécanismes cryptographiques asymétriques.

Le principe de fonctionnement et d'interaction des composants entre eux est le suivant :

- l'application de création de cachet, déployée sur une ou plusieurs machines calcule un condensat, à l'aide d'une fonction de hachage, à partir des informations à signer ;
- elle transmet ce condensat au dispositif de création de cachet ;
- le dispositif de création de cachet réalise un calcul cryptographique de signature du condensat en utilisant la clé privée de signature du service de création de cachet, activée le cas échéant par un code d'activation (code PIN par exemple) par le responsable du certificat de cachet ;
- ce condensat signé, dit cachet, est retourné à l'application ;

la vérification du cachet s'effectue à l'aide d'un module de vérification de cachet et du certificat électronique délivré par PSCE qui lie l'identité du service de création de cachet avec sa clé publique : un calcul cryptographique est effectué à l'aide de la clé publique sur la signature électronique et comparé au condensat obtenu par hachage des informations à signer.

Dans le cadre du [RGS], l'utilisation de la clé privée d'authentification du porteur et du certificat mono-usage associé est strictement limitée à l'authentification[3].

II.4. Fonction de sécurité « cachet »

Le cachet, apposé par un service de création de cachet, est l'une des fonctions de sécurité apportant de la confiance dans les échanges dématérialisés entre usagers et autorités administratives ou entre autorités administratives. Le terme « cachet » est utilisé par un service applicatif, se différenciant ainsi de la « signature électronique » qui est un terme consacré réservé à une personne physique.

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

- apposition d'un cachet sur des données par un service applicatif d'une autorité administrative et vérification de ce cachet par un usager ;
- apposition d'un cachet sur des données par un service applicatif et vérification de ce cachet par un agent d'une autorité administrative ;
- apposition d'un cachet sur des données par un service applicatif et vérification de ce cachet par un autre service applicatif.

Le principe de fonctionnement et d'interaction des composants entre eux est le suivant :

- l'application de création de cachet, déployée sur une machine (PC, borne publique, serveur...) peut réaliser les premières itérations de calcul d'un condensat, à l'aide d'une fonction de hachage, à partir des informations à signer ;
- Elle transmet les informations nécessaires à la réalisation du cachet (informations à signer complètes ou partielles, condensat partiel le cas échéant) au dispositif de création de cachet (exemples : carte à puce, clé USB) également connecté à la machine ;
- le dispositif de création de cachet réalise les itérations restantes (a minima la dernière itération) du calcul du condensat, à l'aide d'une fonction de hachage, à partir des informations transmises par l'application de création de cachet ; ce condensat signé, dit cachet, est retourné à l'application ;
- la vérification du cachet s'effectue à l'aide d'un module de vérification de cachet et du certificat électronique délivré par PSCE qui lie l'identité du service de création de cachet avec sa clé publique : un calcul cryptographique est effectué à l'aide de la clé publique sur la signature électronique et comparé au condensat obtenu par hachage des informations à signer.

Dans le cadre du [RGS], l'utilisation de la clé privée du service de création de cachet et du certificat

[3] L'utilisation de certificats électronique dits « double usage » (à des fins d'authentification et de signature) tels que décrits dans le document [RGS_A2] est également tolérée.

mono-usage associé est strictement limitée au service de cachet.

II.5. Fonction de sécurité « authentification serveur »

L'authentification d'un serveur est l'une des fonctions de sécurité apportant de la confiance dans les échanges dématérialisés entre usagers et autorités administratives ou entre autorités administratives.

Dans le cadre du [RGS] et de son utilisation dans l'administration, les types de relations couverts par le service d'authentification serveur sont notamment les suivants :

- établissement d'une session sécurisée entre un serveur d'une autorité administrative et un usager,
- établissement d'une session sécurisée entre un serveur et un agent d'une autorité administrative,
- établissement d'une session sécurisée entre deux serveurs.

Cette fonction de sécurité permet à un serveur de s'authentifier et d'établir des sessions sécurisées dans le cadre des types de relations mentionnés ci-dessus.

Le principe de fonctionnement et d'interaction des composants entre eux est le suivant :

- l'application d'authentification transmet une requête d'authentification (un « challenge ») au dispositif d'authentification dans lequel la clé privée d'authentification du serveur est confinée et protégée notamment en confidentialité ;
- le dispositif d'authentification réalise un calcul cryptographique de signature du « challenge » en utilisant la clé privée, une fois celle-ci activée par le responsable du serveur, le cas échéant à l'aide d'un code d'activation (code PIN par exemple) ;
- ce challenge signé est retourné à l'application ;
- la vérification de l'authentification s'effectue à l'aide d'un module de vérification et du certificat électronique délivré par PSCE qui lie l'identité du serveur avec sa clé publique : un calcul cryptographique « inverse » est effectué à l'aide de la clé publique sur le challenge signé et comparé au challenge initial.

Dans le cadre du [RGS], l'utilisation de la clé privée d'authentification du serveur et du certificat mono-usage associé est strictement limitée au service d'authentification et d'établissement de session sécurisée.

III. Exigences relatives à la mise en œuvre des fonctions de sécurité

Ce paragraphe regroupe toutes les exigences de sécurité, d'interopérabilité ainsi que les bonnes pratiques pour les composants participant aux fonctions de sécurité.

III.1. Les certificats délivrés par les PSCE

Les exigences que doit respecter un PSCE, délivrant des certificats électroniques sont définies dans les politiques de certification type (PC Type) « Personne » et « Service applicatif » [RGS_A2] et [RGS_A3]. Ces deux PC Types distingue les exigences spécifiques à chacune des fonctions de sécurité ainsi que trois niveaux de sécurité aux exigences croissantes *, ** et *** (à l'exception de l'usage combiné « Authentification et Signature » qui n'en compte que deux : * et **).

En l'occurrence, la PC Type « Personne » traite des fonctions de sécurité « signature électronique », « authentification » et « confidentialité ». La PC Type « Service applicatif » traite des fonctions de sécurité « cachet » et « authentification serveur ». Ces deux PC Types distinguent également les règles spécifiques au porteur ou au secteur pour lesquels le certificat électronique est délivré : particulier, agent de l'Etat, employé de société, secteur public, secteur privé.

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 réserve que le niveau du dispositif de protection de la clé privée et le niveau du certificat soient cohérents. Par exemple, un certificat électronique conforme aux exigences du niveau (***) pourra être employé dans des téléservices de niveaux inférieurs, sous réserve de son interopérabilité.

Ces PC Type s'appuient sur l'annexe [RGS_A4] du [RGS] qui définit 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 électroniques 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 à l'usage et au niveau visé et respecter ensuite l'ensemble des engagements pris.

III.2. Les dispositifs de protection des éléments secrets

Le dispositif de protection des éléments secrets est un logiciel ou le matériel (carte à puce par exemple) qui stocke la clé privée dédiée à une fonction de sécurité donnée, les éléments permettant de la déverrouiller (code PIN par exemple), qui permet sa mise en œuvre et, le cas échéant, leur génération.

III.2.1. Dispositifs de protection des éléments secrets d'une personne physique

III.2.1.1. Exigences de sécurité

Les exigences sont décrites dans l'annexe 3 des PC Type [RGS_A2].

Quel que soit le niveau visé, le dispositif de protection des éléments secrets de la personne doit répondre aux exigences de sécurité suivantes :

- si la bi-clé 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 ;

- garantir la confidentialité et l'intégrité de la clé privée ;
- assurer la correspondance entre la clé privée et la clé publique ;
- permettre de garantir l'authenticité et l'intégrité de la clé publique lors de son export hors du dispositif.
- [Tous usages sauf Confidentialité]
- disposer de techniques sûres de destruction de la clé privée en cas de re-génération de la clé privée ou de destruction des clés privées qui ne sont plus utilisées ;

[Confidentialité]

- permettre de garantir la confidentialité, l'authenticité et l'intégrité de la clé symétrique lors de son export hors du dispositif à destination de l'application de déchiffrement des données.

III.2.1.2. Exigences sur la qualification

Le respect des règles suivantes n'est exigé que lorsque le PSCE souhaite faire qualifier son offre de certificats électroniques au(x) niveau(x) de sécurité considéré(s) selon la procédure décrite dans le [DécretRGS] et délivre au porteur final ou au responsable du certificat électronique du service applicatif le dispositif de protection des éléments secrets. Dans tous les autres cas, leur respect est recommandé.

Au niveau *** :
Le dispositif de protection des éléments secrets doit être qualifié au niveau renforcé[4], selon le processus décrit dans le [RGS], et être conforme aux exigences du chapitre ci-dessus.

Au niveau ** :

Le dispositif de protection des éléments doit être qualifié au minimum au niveau standard[5], selon le processus décrit dans le [RGS], et être conforme aux exigences du chapitre ci-dessus.

Il est toutefois recommandé d'utiliser un dispositif de protection éléments secrets qualifié au niveau renforcé.

Au niveau * :

Le dispositif de protection des éléments secrets doit être qualifié au minimum au niveau élémentaire[6], selon le processus décrit dans le [RGS], et être conforme aux exigences du chapitre ci-dessus.

Il est toutefois recommandé d'utiliser un dispositif de protection des éléments secrets qualifié au niveau standard.

III.2.2.Dispositifs de protection des éléments secrets d'un service applicatif

III.2.2.1. Exigences de sécurité

Les exigences sont décrites dans l'annexe 3 des PC Type [RGS_A3].

Quel que soit le niveau visé, le dispositif de protection des éléments secrets du service applicatif doit répondre aux exigences de sécurité suivantes :

[4], [5] et [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 électroniques doit obtenir une dérogation de l'ANSSI.

- si la bi-clé 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 ;
- assurer la correspondance entre la clé privée et la clé publique.

Par ailleurs, des mesures de sécurité organisationnelles, procédurales ou techniques doivent être mises en place afin de :

- détecter les défauts lors des phases d'initialisation, et d'opération et disposer de techniques sûres de destruction de la clé privée en cas de re-génération de la clé privée ;
- garantir la confidentialité et l'intégrité de la clé privée ;
- permettre de garantir l'authenticité et l'intégrité de la clé publique lors de son export hors du dispositif.

Cachet
➢ assurer pour le serveur légitime uniquement la fonction de génération des cachets électroniques et protéger la clé privée contre toute utilisation par des tiers.

Authentification Serveur
➢ assurer pour le serveur légitime uniquement, d'une part, la fonction d'authentification et, d'autre part, la fonction de déchiffrement de clés symétriques de session, et protéger la clé privée contre toute utilisation par des tiers ; ➢ permettre de garantir l'authenticité et l'intégrité de la clé symétrique de session, une fois déchiffrée, lors de son export hors du dispositif à destination de l'application de déchiffrement des données.

Nota - Les dispositifs matériels, de types cartes à puces ou modules cryptographiques qualifiés par l'ANSSI, respectent ces exigences. Toutefois, des solutions logicielles sont susceptibles de respecter ces exigences pourvues que des mesures de sécurité additionnelles propres à l'environnement dans lequel est déployée la clé privée soient mises en place.

III.2.2.2. Exigences en terme d'évaluation et d'audit

Les composantes de l'IGC qui mettent en œuvre la clé privée doit faire l'objet d'un audit de sécurité. Pour les niveaux ** et ***, l'audit technique de la sécurité doit être effectué au minimum tous les deux ans. Cet audit doit comprendre :

- un audit de l'architecture réseau (liaison entre les différentes zones et entités, filtrage),
- un audit de configuration (équipements réseau et de sécurité, serveurs d'infrastructure)
- un audit organisationnel.

Au-delà des strictes composantes de l'IGC, l'environnement dans lequel est déployée la clé privé peut faire l'objet d'un audit de sécurité.

III.3. Les Applications

III.3.1.Exigences de sécurité

[Signature] Il est recommandé d'utiliser une application de création de signature conforme au profil de

protection [PP_Appli]. De la même manière, il est recommandé d'utiliser un module de vérification de signature conforme au profil de protection [PP_Vérif].

[Confidentialité] 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].

[Confidentialité] 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 :

- 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 des applications qualifiées au niveau standard.

Au niveau *, il est recommandé d'utiliser des applications qualifiées au niveau élémentaire.

III.3.3.Bonnes pratiques

Avant de se fier à un certificat électronique, 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 ;
- correspond au niveau de sécurité cohérent avec l'usage pour lequel il est destiné.

Il est recommandé pour ce faire d'élaborer une politique de vérification des certificats électroniques.

III.4. Environnement d'utilisation

Les fonctions de sécurité « Signature », « Authentification » et « Confidentialité » sont notamment mises en œuvre sur une borne publique ou un ordinateur dans un cadre privé ou professionnel pour un usage par une personne physique.

Les fonctions de sécurité « Cachet » et « Authentification Serveur » sont notamment mises en œuvre sur un ou plusieurs serveurs hébergeant un service applicatif, pour un usage relevant d'une personne morale et sous le contrôle d'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.

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

[Confidentialité] 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*
[Décret2001-272]	*Décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique.*

IV.2. Documents techniques

Renvoi	Document
[PP_Appli]	*Profil de protection application de création de signature électronique Version 1.6 d'août 2008*
[PP_Vérif]	*Profil de protection module de vérification de signature électronique Version 1.6 d'août 2008*
[RGS]	*Référentiel Général de Sécurité - Version 2.0*
[RGS_A2]	*Politique de Certification Type « Personne » - Version 3.0*
[RGS_A3]	*Politique de Certification Type « Service applicatif » - Version 3.0*
[RGS_A4]	*Profils de certificats, de LCR et OCSP et algorithmes cryptographiques – Version 2.3*

5