



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 A3

Fonction de sécurité

« Signature »

Version 2.3 du 11 février 2010

HISTORIQUE DES VERSIONS			
DATE	VERSION	EVOLUTION DU DOCUMENT	REDACTEUR
06/11/2006	2.1	<i>Document constitutif de la Politique de Référencement Intersectorielle de Sécurité – PRISv2.1.</i>	DCSSI / SDAE
12/12/2008	2.2	<i>Document constitutif du Référentiel Général de Sécurité – RGSv0.98, annexe A3.</i> Restructuration du document.	DCSSI / DGME
11/02/2010	2.3	<i>Document constitutif du Référentiel Général de Sécurité – RGSv1.0, annexe A3.</i> Principales modifications : <ul style="list-style-type: none"> • 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

Annexe A3 au RGSv1.0 : Fonction de sécurité - Signature				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.1.6	2.3	11/02/2010	PUBLIC	2/10

SOMMAIRE

I. OBJET ET CONTENU DU DOCUMENT	4
II. PRÉSENTATION DE LA FONCTION DE SÉCURITÉ « SIGNATURE »	5
III. EXIGENCES POUR LA MISE EN ŒUVRE DE LA FONCTION « SIGNATURE »	6
III.1. Certificats délivrés par les PSCE	6
III.2. Dispositifs de création de signature	6
III.2.1. Exigences de sécurité.....	6
III.2.2. Exigences sur la qualification.....	7
III.3. Application de création de signature	8
III.3.1. Exigences de sécurité.....	8
III.3.2. Exigences sur la qualification.....	8
III.4. Module de vérification de signature	8
III.4.1. Exigences de sécurité.....	8
III.4.2. Exigences sur la qualification.....	8
III.4.3. Bonnes pratiques.....	8
III.5. Environnement d'utilisation.....	8
IV. DOCUMENTS DE RÉFÉRENCE	10
IV.1. Réglementation	10
IV.2. Documents techniques	10

Annexe A3 au RGSv1.0 : Fonction de sécurité - Signature

Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.1.6	2.3	11/02/2010	PUBLIC	3/10

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_3].

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

- les bi-clés et certificats électroniques permettant la création et la vérification de signatures électroniques¹ ;
- le dispositif de création de signature électronique ;
- le module de vérification de signature électronique ;
- l'application de création de signature électronique.

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

¹ Les règles relatives à la délivrance et la gestion du cycle de vie des certificats de signature sont regroupées dans le document « Politique de Certification Type Signature » [RGS_A_8] ou dans le cas de certificat double usage « Politique de Certification Type Authentification et Signature » [RGS_A_11].

Annexe A3 au RGSv1.0 : Fonction de sécurité - Signature				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.1.6	2.3	11/02/2010	PUBLIC	4/10

II. Présentation de la fonction de sécurité « Signature »

La signature électronique 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 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'utilisateur 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 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, ...) 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 signature (exemples : carte à puce, clé USB) également connecté à la machine ;
- 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'utilisateur, 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'utilisateur 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 associé est strictement limitée à la signature électronique².

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_8]) à l'égard des prestataires de services de certification électronique et des dispositifs de création de signature pour le niveau *** répondent respectivement aux exigences de l'article 6 et de l'article 3 du décret [SIG].

² L'utilisation de certificats électronique dits « double usage » (authentification et signature) tels que décrits dans le document [RGS_A_11] est également permise.

Annexe A3 au RGSv1.0 : Fonction de sécurité - Signature				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.1.6	2.3	11/02/2010	PUBLIC	5/10

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

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

III.1. Certificats délivrés par les PSCE

Les exigences que doit respecter un PSCE délivrant des certificats à des fins de signature sont définies dans la politique de certification type (PC Type) Signature [RGS_A_8] ou, dans le cas du double usage, de la PC Type Authentification et Signature [RGS_A_11].

La PC Type Signature distingue trois niveaux de sécurité aux exigences croissantes *, ** et *** (tandis que la PC Type Authentification et Signature n'en distingue que deux : * 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 garantie³. Ainsi, par exemple, un certificat électronique de signature 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 les PC Types. 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 certificats du secteur privé de types "entreprises"⁴ 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 événements 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 signature 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 création de signature

III.2.1. Exigences de sécurité

Dans le cadre d'un téléservice requérant une signature électronique l'utilisateur et/ou l'agent doivent utiliser un dispositif de création de signature répondant à un minimum d'exigences de sécurité. Ces

³ Attestée par la procédure de référencement, conformément à l'article 12 de l'ordonnance.

⁴ 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.

Annexe A3 au RGSv1.0 : Fonction de sécurité - Signature				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.1.6	2.3	11/02/2010	PUBLIC	6/10

exigences sont décrites dans l'annexe 3 de la PC Type Signature et reprises ci-dessous.

Le dispositif de création de signature, utilisé par le porteur pour stocker et mettre en œuvre sa clé privée et, le cas échéant, générer sa bi-clé, doit répondre aux exigences de sécurité suivantes :

- si la bi-clé de signature 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 de la clé privée en cas de re-génération de la clé privée ;
- garantir la confidentialité et l'intégrité de la clé privée ;
- assurer la correspondance entre la clé privée et la clé publique ;
- générer une signature qui ne peut être falsifiée sans la connaissance de la clé privée ;
- assurer la fonction de signature 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 publique lors de son export hors du dispositif.

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 signature électronique au(x) niveau(x) de sécurité considéré(s) selon la procédure décrite dans le [DécretRGS] et délivre au porteur final le dispositif de création de signature ; dans tous les autres cas, leur respect est recommandé.

Au niveau *** :

Le dispositif de création de signature utilisé par le porteur doit être qualifié au niveau renforcé⁵, selon le processus décrit dans le [RGS], et être conforme aux exigences⁶ du chapitre ci-dessus.

Au niveau ** :

Le dispositif de création de signature utilisé par le porteur doit être qualifié au minimum au niveau standard⁷, selon le processus décrit dans le [RGS], et être conforme aux exigences du chapitre ci-dessus.

Il est toutefois recommandé d'utiliser dispositif de création de signature qualifié au niveau renforcé.

Au niveau * :

Le dispositif de création de signature utilisé par le porteur doit être qualifié au minimum au niveau

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 signature doit obtenir une dérogation de l'ANSSI.

⁶ Une cible de sécurité conforme au profil de protection [CWA14169] Annexe A (CWA14169-1) permet au dispositif de création de signature d'être considéré comme conforme aux exigences du chapitre ci-dessus relatives à la fonction de génération des données de création et de vérification de signature électronique.

Une cible de sécurité conforme au profil de protection [CWA14169] Annexe B (CWA14169-2) permet au dispositif de création de signature d'être considéré comme conforme aux exigences du chapitre ci-dessus relatives à la fonction de création de signature électronique.

Une cible de sécurité conforme au profil de protection [CWA14169] Annexe C (CWA14169-3) permet au dispositif de création de signature d'être considéré comme conforme à toutes les exigences du chapitre ci-dessus

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 signature doit obtenir une dérogation de l'ANSSI.

Annexe A3 au RGSv1.0 : Fonction de sécurité - Signature				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.1.6	2.3	11/02/2010	PUBLIC	7/10

élémentaire⁸, selon le processus décrit dans le [RGS], et être conforme aux exigences du chapitre ci-dessus.

Il est toutefois recommandé d'utiliser dispositif de création de signature qualifié au niveau standard.

III.3. Application de création de signature

III.3.1. Exigences de sécurité

Aux niveaux *** et **, il est recommandé d'utiliser une application de création de signature conforme au profil de protection [PP_Appli].

III.3.2. Exigences sur la qualification

Aux niveaux *** et **, il est recommandé d'utiliser une application de création de signature qualifiée au niveau standard selon le processus décrit dans le [RGS].

III.4. Module de vérification de signature

III.4.1. Exigences de sécurité

Aux niveaux *** et **, il est recommandé d'utiliser un module de vérification de signature conforme au profil de protection [PP_Vérif].

III.4.2. Exigences sur la qualification

Aux niveaux *** et **, il est recommandé d'utiliser un module de vérification de signature qualifié au niveau standard selon le processus décrit dans le [RGS].

III.4.3. Bonnes pratiques

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

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

Il est recommandé pour ce faire d'élaborer et d'appliquer une Politique de vérification de signature.

III.5. Environnement d'utilisation

La fonction de sécurité « Signature » 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 mise 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 celle-ci (différenciation compte utilisateur/administrateur) ;
- installation et mise à jour de logiciels et de composants sur la machine sous le contrôle de

⁸ 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 signature doit obtenir une dérogation de l'ANSSI.

Annexe A3 au RGSv1.0 : Fonction de sécurité - Signature				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.1.6	2.3	11/02/2010	PUBLIC	8/10

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 création de signature, il est recommandé, et tout particulièrement au niveau ***, d'utiliser un lecteur de carte à puce avec PIN/PAD intégré permettant de saisir son code d'activation et de le vérifier sans que celui-ci ne transite via l'ordinateur ou la borne d'accès publique utilisés.

Annexe A3 au RGSv1.0 : Fonction de sécurité - Signature				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.1.6	2.3	11/02/2010	PUBLIC	9/10

IV. Documents de référence

IV.1. Réglementation

Renvoi	Document
[DIRSIG]	<i>Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques.</i>
[ORDONNANCE]	<i>Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives</i>
[DécretRGS]	<i>Décret pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005</i>
[SIG]	<i>Décret n°2001-272 du 30 mars 2001 pris pour application de l'article 1316-4 du code civil et relatif à la signature électronique.</i>

IV.2. Documents techniques

Renvoi	Document
[PP_Appli]	<i>Profil de protection application de création de signature électronique Version 1.6 d'août 2008</i>
[PP_Vérif]	<i>Profil de protection module de vérification de signature électronique Version 1.6 d'août 2008</i>
[RGS]	<i>Référentiel Général de Sécurité - Version 1.0</i>
[RGS_A_3]	<i>Fonction de sécurité « Signature » - Version 2.3</i>
[RGS_A_8]	<i>Politique de certification type Service Signature - Version 2.3</i>
[RGS_A_11]	<i>Politique de certification type Services Authentification et Signature - Version 2.3</i>
[RGS_A_13]	<i>Variables de Temps - Version 2.3</i>
[RGS_A_14]	<i>Profils de certificats, de LCR et OCSP et algorithmes cryptographiques – Version 2.3</i>

Annexe A3 au RGSv1.0 : Fonction de sécurité - Signature				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.1.6	2.3	11/02/2010	PUBLIC	10/10