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 A5

Fonction de sécurité

« Cachet »

Version 2.3 du 11 février 2010

HISTORIQUE DES VERSIONS			
DATE	**VERSION**	**EVOLUTION DU DOCUMENT**	**REDACTEUR**
12/12/2008	2.2	*Document constitutif du Référentiel Général de Sécurité – RGSv0.98, annexe A5.* Création du document.	DCSSI / DGME
11/02/2010	2.3	*Document constitutif du Référentiel Général de Sécurité – RGSv1.0, annexe A5.* 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_5].

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

- les bi-clés et certificats électroniques permettant la création d'un cachet par un service applicatif déployé sur un ou plusieurs serveurs[1] ;
- le dispositif de création d'un cachet ;
- le module de vérification d'un cachet;
- l'application de création d'un cachet.

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 « Cachet » basée sur des mécanismes cryptographiques asymétriques.

[1] Les règles relatives à la délivrance et la gestion du cycle de vie de tels certificats sont regroupées dans le document « Politique de Certification Type Cachet » [RGS_A_10].

II. Présentation de la 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 AA ou entre AA.

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 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 du service de création de cachet et du certificat associé est strictement limitée au service de cachet.

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

III.1. Certificats délivrés par les PSCE

Les exigences que doit respecter un PSCE, délivrant des certificats de cachet, sont définies dans la politique de certification type (PC Type) Cachet [RGS_A_10].

La PC Type Cachet 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 cachet 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 certificats cachet du secteur privé, de types "entreprises"[3], et ceux du secteur public. Les exigences spécifiques à l'un ou à l'autre de ces secteurs, 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 cachet 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 cachet

III.2.1.Exigences de sécurité

Le service de création de cachet doit utiliser un dispositif de création de cachet répondant à un minimum d'exigences de sécurité. Ces exigences sont décrites dans l'annexe 3 de la PC Type Cachet [RGS_A_10] et reprises ci-dessous.

Quel que soit le niveau, un dispositif de création de cachet utilisé par le responsable du serveur pour stocker et mettre en œuvre la clé privée, et le cas échéant générer la bi-clé, doit répondre aux

[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.

exigences de sécurité suivantes :

- si la bi-clé de du serveur 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 un cachet qui ne peut être falsifiée sans la connaissance de la clé privée ;
- assurer pour le serveur légitime uniquement la fonction de génération des cachets 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 cachet au(x) niveau(x) de sécurité considéré(s) selon la procédure décrite dans le [DécretRGS] et délivre au responsable du certificat de cachet le dispositif de création de cachet ; dans tous les autres cas, leur respect est recommandé.

Au niveau *** :
Le dispositif de création de cachet 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 création de cachet 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.

Au niveau * :

Le dispositif de création de cachet 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.

III.3. Application de création de cachet

Aux niveaux *** et **, il est recommandé d'utiliser une application de création de cachet qualifiée au niveau standard[7] du [RGS].

---

[4] 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 cachet doit obtenir une dérogation de l'ANSSI.

[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 cachet 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 cachet doit obtenir une dérogation de l'ANSSI.

[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 cachet doit obtenir une dérogation de

III.4. Module de vérification de cachet

Aux niveaux *** et **, il est recommandé d'utiliser un module de vérification de cachet qualifiée au niveau standard du [RGS].

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 n'est pas révoqué ;
- a une chaîne de certification qui est correcte à tous les niveaux.

Il est recommandé pour ce faire d'élaborer une politique de vérification de cachet.

III.5. Environnement d'utilisation

La fonction de sécurité « Cachet » est notamment mise en œuvre sur un ou plusieurs serveurs (machines) 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 régulières ;
- 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 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.

l'ANSSI.

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*
[RFC3647]	*IETF - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework - 11/2003*
[RGS_A_10]	*Politique de Certification Type Service Cachet Serveur - 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*