



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 A4

Fonction de sécurité

« Authentification Serveur »

Version 2.3 du 11 février 2010

HISTORIQUE DES VERSIONS			
DATE	VERSION	EVOLUTION DU DOCUMENT	REDACTEUR
12/12/2008	2.2	<i>Document constitutif du Référentiel Général de Sécurité – RGSv0.98, annexe A4.</i> Création du document.	DCSSI / DGME
11/02/2010	2.3	<i>Document constitutif du Référentiel Général de Sécurité – RGSv1.0, annexe A4.</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 A4 au RGSv1.0 : Fonction de sécurité - Authentification Serveur				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.1.10	2.3	11/02/2010	PUBLIC	2/9

SOMMAIRE

I. OBJET ET CONTENU DU DOCUMENT	4
II. PRÉSENTATION DE LA FONCTION DE SÉCURITÉ « AUTHENTIFICATION SERVEUR »	5
III. EXIGENCES POUR LA MISE EN ŒUVRE DE LA FONCTION DE SÉCURITÉ « AUTHENTIFICATION SERVEUR »	6
III.1. Certificats délivrés par les PSCE	6
III.2. Dispositifs de protection des clés privées.....	7
III.2.1. Exigences de sécurité.....	7
III.2.2. Exigences sur la qualification.....	7
III.3. Application d'authentification	8
III.4. Module de vérification d'authentification	8
III.5. Environnement d'utilisation.....	8
IV. DOCUMENTS DE RÉFÉRENCE	9
IV.1. Réglementation	9
IV.2. Documents techniques	9

Annexe A4 au RGSv1.0 : Fonction de sécurité - Authentification Serveur

Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.1.10	2.3	11/02/2010	PUBLIC	3/9

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_4].

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

- les bi-clés et certificats électroniques permettant l'authentification de serveur et l'établissement de session sécurisée¹ ;
- le dispositif de protection des clés privées du serveur ;
- le module de vérification d'authentification ;
- l'application d'authentification du serveur.

Dans le présent document, le terme « serveur » représente un ou plusieurs serveurs physiques détenant un même FQDN (fully qualified domain name).

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 « Authentification Serveur » 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 Authentification Serveur » [RGS_A_9].

Annexe A4 au RGSv1.0 : Fonction de sécurité - Authentification Serveur				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.1.10	2.3	11/02/2010	PUBLIC	4/9

II. Présentation de la 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 AA ou entre AA.

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 associé est strictement limitée au service d'authentification et d'établissement de session sécurisée.

Annexe A4 au RGSv1.0 : Fonction de sécurité - Authentification Serveur				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.1.10	2.3	11/02/2010	PUBLIC	5/9

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

III.1. Certificats délivrés par les PSCE

Les exigences que doit respecter un PSCE, délivrant des certificats à des fins d'authentification, sont définies dans la politique de certification type (PC Type) [RGS_A_9].

La PC Type Authentification Serveur 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 garantie². Ainsi, par exemple, un certificat électronique d'authentification serveur 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 quelque 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 de serveurs 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 même, cette PC Type concerne les certificats pour des serveurs de type serveur SSL/TLS ou des serveurs qui, lors de l'établissement d'une session sécurisée avec un autre serveur, se trouvent être en mode client⁴. 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 d'authentification serveur 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.

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.

⁴ Le certificat d'authentification serveur est associé au FQDN et pas au serveur physique sur lequel la bi-clé est déployée. Autrement dit, une bi-clé d'authentification serveur peut être déployée sur plusieurs machines physiques rattachées à ce FQDN (cas notamment d'architecture de répartition de charge).

Annexe A4 au RGSv1.0 : Fonction de sécurité - Authentification Serveur				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.1.10	2.3	11/02/2010	PUBLIC	6/9

III.2. Dispositifs de protection des clés privées

III.2.1.Exigences de sécurité

Dans le cadre d'un serveur devant s'authentifier auprès d'un usager, d'un agent ou d'un autre serveur dans le but d'établir une session sécurisée, celui-ci doit utiliser un dispositif de protection des clés privées répondant à un minimum d'exigences de sécurité. Ces exigences sont décrites dans l'annexe 3 de la PC Type Authentication Serveur [RGS_A_9] et reprises ci-dessous.

Quel que soit le niveau, un dispositif de protection des clés privées utilisé par le serveur 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 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 une authentification qui ne peut être falsifiée sans la connaissance de la clé privée ;
- 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 ;
- 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 d'authentification serveur au(x) niveau(x) de sécurité considéré(s) selon la procédure décrite dans le [DécretRGS] et délivre au responsable du certificat d'authentification serveur 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 serveur doit être qualifié au niveau renforcé⁵, 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 serveur doit être qualifié au minimum au niveau standard⁶, selon le processus décrit dans le [RGS], et être conforme aux exigences du chapitre

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 d'authentification machine 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 d'authentification machine doit obtenir

Annexe A4 au RGSv1.0 : Fonction de sécurité - Authentification Serveur				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.1.10	2.3	11/02/2010	PUBLIC	7/9

ci-dessus.

Au niveau * :

Le dispositif de protection des clés privées utilisé par le serveur doit être qualifié au minimum au niveau élémentaire⁷, selon le processus décrit dans le [RGS], et être conforme aux exigences du chapitre ci-dessus.

III.3. Application d'authentification

Aux niveaux *** et **, il est recommandé d'utiliser une application d'authentification qualifiée au niveau standard.

III.4. Module de vérification d'authentification

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

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.

III.5. Environnement d'utilisation

La fonction de sécurité « Authentification Serveur » est notamment mise en œuvre sur un serveur (machine) hébergeant une application, 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 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.

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 certificat de signature doit obtenir une dérogation de l'ANSSI.

Annexe A4 au RGSv1.0 : Fonction de sécurité - Authentification Serveur				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.1.10	2.3	11/02/2010	PUBLIC	8/9

IV. Documents de référence

IV.1. Réglementation

Renvoi	Document
[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>

IV.2. Documents techniques

Renvoi	Document
[RGS]	<i>Référentiel Général de Sécurité - Version 1.0</i>
[RFC3647]	<i>IETF - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework - 11/2003</i>
[RGS_A_10]	<i>Politique de Certification Type Authentification Serveur - 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 A4 au RGSv1.0 : Fonction de sécurité - Authentification Serveur				
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.1.10	2.3	11/02/2010	PUBLIC	9/9