



PREMIER MINISTRE

Secrétariat général
de la défense
nationale

Paris, le 31 janvier 2007

N° 193/SGDN/DCSSI/SDS

*Direction centrale de la sécurité
des systèmes d'information*

Affaire suivie par : Florent Chabaud

ALGORITHMES CRYPTOGRAPHIQUES
pour l'interopérabilité du
Format V1 de signature électronique
XAdES de l'Administration

Version 0.4

Historique des versions

Version 0.1	07/11/2006	Document initial présenté en interne le 27/11/2006
Version 0.2	24/01/2007	Prise en compte des commentaires internes de Gwenaëlle Martinet
Version 0.3	25/01/2007	Prise en compte des commentaires internes d'Emmanuel Bresson
Version 0.4	31/01/2007	Version validée SDS

1 Contexte

Ce document complète le document [AdmXAdES] en restreignant les algorithmes spécifiés dans le document [ETSI] et dans des normes publiques à un sous-ensemble nécessaire et suffisant pour l'application des préconisations du [RGI]. Il applique les mêmes conventions que le document [AdmXAdES] en ce qui concerne la terminologie normative (OBLIGATOIRE, RECOMMANDE, FACULTATIF, DECONSEILLE, INTERDIT) et la distinction entre création (CRE) et vérification (VER) de signature.

Les RECOMMANDATIONS soulignées visent à permettre l'interopérabilité tout en ayant pour objectif une qualification au niveau standard des produits de création et de vérification de signature utilisés par l'Administration. Ces recommandations d'interopérabilité se veulent donc conformes au [RefCrypto] mais ne sont ni nécessaires ni suffisantes à l'obtention de la qualification de niveau standard. En effet d'autres mécanismes, sans influence sur l'interopérabilité, doivent toutefois respecter les règles et recommandations de [RefCrypto] pour

permettre une telle qualification, comme par exemple la génération d'aléa ou la génération de clés. Inversement, des mécanismes non interopérables peuvent cependant respecter les critères de sécurité de [RefCrypto].

Les différentes dénominations d'algorithmes utilisées sont tirées du document [ETSI], partie 11, pages 30 à 32. Ces dénominations (*short object names*) y sont reliées aux URI et références normatives à employer. Lorsqu'une dénomination n'est pas prévue dans ce document, elle est définie par référence à des documents normatifs existants.

2 Références

2.1 Références normatives

[AdmXAdeS] Format v1 de signature électronique XAdES de l'Administration version 0.93 du 24 octobre 2006

[ETSI] Spécification de l'ETSI concernant les algorithmes utilisables dans le contexte des signatures électroniques avancées, réf. ETSI TS 102 176-1 V1.2.1 (2005-07)

[FIPS-180-2] FIPS PUB 180-2 + change notice, Secure Hash Standard

<http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf>

[FIPS-186-2] FIPS PUB 186-2 + change notice, Digital Signature Standard

<http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf>

[FIPS-186-3] FIPS PUB 186-3 (DRAFT) Digital Signature Standard (DSS)

http://csrc.nist.gov/publications/drafts/fips_186-3/Draft-FIPS-186-3%20_March2006.pdf

[ISO 10118] ISO/IEC 10118-3 (2004): "Information technology - Security techniques - Hash functions - Part 3: Dedicated hash functions"

[PKCS#1] IETF RFC 3447 (2003): "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1". <http://www.ietf.org/rfc/rfc3447.txt>

2.2 Références informatives

[RefCrypto] Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard, version 1.10, note n°2741/SGDN/DCSSI/SDS/LCR du 19 décembre 2006

[RGI] Référentiel général d'interopérabilité, volet technique, version 0.90 du 13 avril 2006 (<https://www.ateliers.adele.gouv.fr/RGI>)

3 Fonctions de hachage

3.1 Dénominations de référence

Dénomination (<i>short object name</i>)	OID	Référence normative
id-sha1	Voir [ETSI]	
id-sha224		
id-sha256		
id-sha384	{ joint-iso-itu-t(2) country(16) us(840) organization(1)	[ISO 10118]

	gov(101) csor(3) nistalgorithm(4) hashalgs(2) 2 }	[FIPS-180-2]
id-sha512	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 3 }	[ISO 10118] [FIPS-180-2]

3.2 Contraintes normatives

a *Création*

Il est **OBLIGATOIRE** d'utiliser l'un des algorithmes de hachage dénommés ci-dessus. Il est **RECOMMANDE** d'utiliser l'algorithme id-sha256. Il est **FACULTATIF** d'implanter les algorithmes id-sha224, id-sha384 et id-sha512. Il est **DECONSEILLE** d'utiliser l'algorithme id-sha1.

b *Vérification*

Il est **OBLIGATOIRE** d'implanter les algorithmes id-sha1 et id-sha256. Il est **RECOMMANDE** d'implanter les algorithmes id-sha224, id-sha384 et id-sha512. Si l'algorithme id-sha1 est utilisé, il est **RECOMMANDE** de mentionner à l'utilisateur que l'algorithme de hachage utilisé n'est pas sûr.

Il est **DECONSEILLE** d'implanter d'autres algorithmes de hachage et il est **OBLIGATOIRE** dans ce cas de mentionner à l'utilisateur que l'algorithme de hachage utilisé n'est pas recommandé.

4 Suites de signature

4.1 Dénominations de référence

Dénomination (short object name)	OID	Référence normative
id-RSASSA-PSS (with mgf1SHA1Identifier)	Voir [ETSI]	
id-RSASSA-PSS (with mgf1SHA224Identifier)		
id-RSASSA-PSS (with mgf1SHA256Identifier)		
id-RSASSA-PSS (with mgf1SHA384Identifier)	{ pkcs-1 10 } + { pkcs-1 8 }	[PKCS#1]
id-RSASSA-PSS (with mgf1SHA512Identifier)		
(sha-1with)RSAEncryption	Voir [ETSI]	
(sha224With)RSAEncryption		
(sha256With)RSAEncryption		
(sha384With)RSAEncryption	{ pkcs-1 12 }	[PKCS#1]
(sha512With)RSAEncryption	{ pkcs-1 13 }	
id-dsa(-with-sha1)	Voir [ETSI]	
id-ecdsa(-with-sha1)		
id-ecdsa(-with-sha224)	id-ecPublicKey + id-sha224	
id-ecdsa(-with-sha256)	id-ecPublicKey + id-sha256	
id-ecdsa(-with-sha384)	id-ecPublicKey + id-sha384	
id-ecdsa(-with-sha512)	id-ecPublicKey + id-sha512	

4.2 Contraintes normatives

a Contraintes générales

a.1 Création

Il est OBLIGATOIRE d'utiliser l'une des suites de signature dénommées ci-dessus.

a.2 Vérification

Il est OBLIGATOIRE d'implanter les suites de signature comprenant les algorithmes id-RSASSA-PSS, RSAEncryption et id-dsa. Il est RECOMMANDE d'implanter les suites de signature comprenant l'algorithme id-ecdsa.

b Algorithmes id-RSASSA-PSS et RSAEncryption

b.1 Création

Il est RECOMMANDE d'employer des modules de taille supérieure ou égale à 2048 bits. Il est DECONSEILLE d'employer des modules de taille inférieure ou égale à 1024 bits. Il est INTERDIT d'employer des modules de taille inférieure ou égale à 768 bits.

Il est OBLIGATOIRE d'employer des modules composés de deux facteurs premiers. Il est RECOMMANDE d'utiliser des facteurs premiers de même taille choisis aléatoirement.

Il est RECOMMANDE d'employer un exposant public supérieur ou égal à 65537. Il est DECONSEILLE d'employer l'exposant public 3.

b.2 Vérification

Si la signature vérifiée emploie des modules de taille inférieure ou égale à 768 bits, il est OBLIGATOIRE de signaler à l'utilisateur qu'elle ne garantit pas l'authenticité de façon certaine. Si la signature vérifiée emploie des modules de taille inférieure ou égale à 1024 bits, il est RECOMMANDE de signaler à l'utilisateur que cette taille n'est pas recommandée. Si la signature vérifiée emploie des modules de taille strictement inférieure à 2048 bits, il est RECOMMANDE de signaler à l'utilisateur que cette taille n'est pas recommandée.

c Algorithme id-dsa

c.1 Création

Bien que ceci ne soit pas conforme au standard en vigueur [FIPS-186-2], il est RECOMMANDE d'utiliser un nombre premier de taille supérieure ou égale à 2048 bits conformément à la référence en cours de validation [FIPS-186-3]. Il est DECONSEILLE d'employer un nombre premier de taille inférieure ou égale à 1024 bits. Il est INTERDIT d'employer un nombre premier de taille inférieure ou égale à 768 bits.

Il est OBLIGATOIRE d'employer un sous-groupe dont l'ordre est un multiple d'un nombre premier de taille supérieure ou égale à 160 bits. Il est RECOMMANDE d'utiliser un sous-groupe dont l'ordre est multiple d'un nombre premier de taille supérieure ou égale à 256 bits.

c.2 Vérification

Si la signature vérifiée emploie un nombre premier de taille inférieure ou égale à 768 bits, il est OBLIGATOIRE de signaler à l'utilisateur qu'elle ne garantit pas l'authenticité de façon certaine. Si la signature vérifiée emploie un nombre premier de taille inférieure ou égale à 1024 bits, il est RECOMMANDE de signaler à l'utilisateur que cette taille n'est pas recommandée. Si la signature vérifiée emploie un nombre premier de taille strictement inférieure à 2048 bits, il est RECOMMANDE de signaler à l'utilisateur que cette taille n'est pas recommandée.

d *Algorithme id-ecdsa*

d.1 *Création*

Il est OBLIGATOIRE d'employer des sous-groupes dont l'ordre est multiple d'un nombre premier de taille supérieure ou égale à 160 bits. Il est RECOMMANDE d'employer des sous-groupes dont l'ordre est multiple d'un nombre premier de taille supérieure ou égale à 256 bits.

Il est RECOMMANDE d'employer un corps premier $GF(p)$.

Il est RECOMMANDE de ne pas employer de courbes particulières faisant reposer la sécurité sur un problème mathématique plus facile que le problème générique de calcul de logarithme discret sur courbe elliptique définie dans le corps de base.

Pour un corps premier $GF(p)$ il est RECOMMANDE d'employer l'une des courbes P-256, P-384 et P-521 définies dans [FIPS-186-2].

Pour un corps binaire $GF(2^n)$ il est RECOMMANDE d'employer l'une des courbes B-283, B-409 et B-571 définies dans [FIPS-186-2].

d.2 *Vérification*

Il est RECOMMANDE d'implanter l'algorithme pour toute courbe elliptique définie sur un corps premier $GF(p)$. Il est FACULTATIF d'implanter l'algorithme pour les corps binaires $GF(2^n)$.

Si la signature vérifiée emploie des sous-groupes dont l'ordre n'est pas multiple d'un nombre premier de taille supérieure ou égale à 160 bits, il est OBLIGATOIRE de signaler à l'utilisateur que la signature ne garantit pas l'authenticité de façon certaine. Si la signature vérifiée emploie un sous-groupe dont l'ordre n'est pas multiple d'un nombre premier de taille supérieure ou égale à 256 bits, il est RECOMMANDE de signaler à l'utilisateur que cette courbe n'est pas recommandée.