

Groupe de travail Réseau  
**Request for Comments : 4056**  
Catégorie : Sur la voie de la normalisation

J. Schaad, Soaring Hawk Consulting  
juin 2005  
Traduction Claude Brière de L'Isle

## Utilisation de l'algorithme RSASSA-PSS dans la syntaxe de message cryptographique (CMS)

### Statut de ce mémoire

Le présent document spécifie un protocole de l'Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. Prière de se référer à l'édition en cours des "Normes officielles des protocoles de l'Internet" (STD 1) pour connaître l'état de la normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

### Notice de copyright

Copyright (C) The Internet Society (2005).

### Résumé

Le présent document spécifie les conventions pour utiliser l'algorithme de signature numérique RSASSA-PSS (*RSA Probabilistic Signature Scheme*) avec la syntaxe de message cryptographique (CMS, *Cryptographic Message Syntax*).

## 1. Vue d'ensemble

Le présent document spécifie les conventions pour utiliser l'algorithme de signature numérique de schéma RSA de signature probabiliste (RSASSA-PSS, *RSA Probabilistic Signature Scheme*) [RFC3447] avec le type de contenu signed-data de la syntaxe de message cryptographique [RFC3852].

Les valeurs de CMS sont générées en utilisant l'ASN.1 [X.208-88], avec les règles de codage de base (BER, *Basic Encoding Rules*) [X.209-88] et les règles de codage distinctives (DER, *Distinguished Encoding Rules*) [X.509-88].

Le présent document est rédigé pour être utilisé en conjonction avec la [RFC4055]. Toutes les structures ASN.1 référencées dans le présent document sont définies dans la RFC 4055.

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

### 1.1 Algorithme PSS

Bien qu'il n'y ait pas de défauts connus de l'algorithme de signature PKCS n° 1 v1.5 [RFC2313], RSASSA-PSS [RFC3447] a été développé dans un effort pour avoir une sécurité plus démontrable mathématiquement. Les signatures PKCS n° 1 v1.5 ont été développées de façon ad hoc ; RSASSA-PSS a été développé sur la base de fondements mathématiques.

## 2. Identifiants et paramètres d'algorithme

### 2.1 Identifiants de certificat

L'algorithme de signature RSASSA-PSS est défini dans la [RFC3447]. Les conventions pour le codage de la clé publique sont définies dans la [RFC4055].

Deux identifiants d'algorithmes sont utilisés pour les clés publiques RSA sujettes dans les certificats. Ce sont :

IDENTIFIANT D'OBJET rsaEncryption ::= { pkcs-1 1 }

et

IDENTIFIANT D'OBJET id-RSASSA-PSS ::= { pkcs-1 10 }

Lorsque l'identifiant d'algorithme `rsaEncryption` est utilisé pour une clé publique, le champ de paramètres `AlgorithmIdentifier` DOIT contenir `NULL`. Les détails complets se trouvent dans la [RFC4055].

Lorsque l'identifiant d'algorithme `id-RSASSA-PSS` est utilisé pour une clé publique, le champ de paramètres `AlgorithmIdentifier` DOIT soit être absent, soit contenir `RSASSA-PSS-params`. Là encore, les détails complets se trouvent dans la [RFC4055].

Dans les deux cas, la clé publique RSA, qui est composée d'un module et d'un exposant public, DOIT être codée en utilisant le type `RSAPublicKey`. Le résultat de ce codage est porté dans la clé publique de certificat sujette.

```
RSAPublicKey ::= SEQUENCE {
    modulus ENTIER, -- n
    publicExponent ENTIER } -- e
```

## 2.2 Identifiants de signature

L'identifiant d'algorithme pour les signatures RSASSA-PSS est :

```
IDENTIFIANT D'OBJET id-RSASSA-PSS ::= {pkcs-1 10 }
```

Lorsque l'identifiant d'algorithme `id-RSASSA-PSS` est utilisé pour une signature, le champ de paramètres `AlgorithmIdentifier` DOIT contenir `RSASSA-PSS-params`. On trouve les informations sur `RSASSA-PSS-params` dans la [RFC4055].

Lors d'une signature, l'algorithme RSA génère une seule valeur, et cette valeur est utilisée directement comme valeur de signature.

## 3. Conventions de données signées

Les algorithmes de résumé DEVRAIENT contenir la fonction de hachage unidirectionnelle utilisée pour calculer le résumé de message sur la valeur de `eContent`.

La même fonction de hachage unidirectionnelle DEVRAIT être utilisée pour calculer le résumé de message sur les deux valeurs de `eContent` et de `signedAttributes` si `signedAttributes` existe.

La même fonction de hachage unidirectionnelle DOIT être utilisée pour calculer le résumé de message sur le `signedAttributes` et comme algorithme de hachage dans la structure `RSA-PSS-params`.

L'algorithme de signature DOIT contenir `id-RSASSA-PSS`. Le champ des paramètres d'algorithme DOIT contenir `RSASSA-PSS-params`.

La signature contient la seule valeur résultant de l'opération de signature.

Si l'identifiant d'algorithme `subjectPublicKeyInfo` pour la clé publique dans le certificat est `id-RSASSA-PSS` et si le champ `Paramètres` est présent, les étapes supplémentaires suivantes DOIVENT être suivies au titre de la validation de la signature :

1. Le champ `hashAlgorithm` dans les paramètres `subjectPublicKey.algorithm` du certificat et les paramètres `signatureAlgorithm` DOIT être le même.
2. Le champ `maskGenAlgorithm` dans les paramètres `subjectPublicKey.algorithm` du certificat et les paramètres `signatureAlgorithm` DOIT être le même.
3. La longueur du sel dans les paramètres `signatureAlgorithm` DOIT être supérieure ou égale à la longueur de sel dans les paramètres `subjectPublicKey.algorithm` du certificat.
4. Le champ `trailerField` dans les paramètres `subjectPublicKey.algorithm` du certificat et les paramètres `signatureAlgorithm` DOIT être le même.

En faisant les comparaisons ci-dessus, les valeurs par défaut sont considérées comme les mêmes que les valeurs existantes.

Si une des quatre étapes ci-dessus n'est pas vérifiée, l'algorithme de vérification de signature DOIT refuser la validation.

#### 4. Considérations sur la sécurité

Les mises en œuvre doivent protéger la clé privée RSA. La compromission de la clé privée RSA peut résulter en la capacité à falsifier les signatures.

La génération de la clé privée RSA s'appuie sur des nombres aléatoires. L'utilisation de générateurs de nombres pseudo aléatoire (PRNG, *pseudo-random number generator*) inadéquats pour générer ces valeurs peut résulter en une sécurité amoindrie ou inexistante. Un attaquant peut trouver beaucoup plus facile de reproduire l'environnement du PRNG qui a produit les clés, et chercher dans le petit ensemble de possibilités résultant, plutôt qu'une recherche en force brute sur tout l'espace de clés. La génération de nombres aléatoires de qualité est difficile. La [RFC1750] offre des directives importantes dans ce domaine.

Utiliser la même clé privée pour différents algorithmes offre à un attaquant la possibilité d'obtenir des informations supplémentaires sur la clé. Il est fortement suggéré que la même clé ne soit pas utilisée pour les algorithmes de signature PKCS n° 1 v1.5 et RSASSA-PSS.

Lors du calcul de signatures, la même fonction de hachage devrait être utilisée pour toutes les opérations. Cela réduit le nombre de points de défaillance dans le processus de signature.

Les procédures de vérification de paramètres mentionnées à la Section 3 sont d'une importance particulière. Il est possible de falsifier des signatures en changeant (particulièrement avec des valeurs plus faibles) ces valeurs de paramètres. Les signataires qui utilisent cet algorithme devraient veiller à ce qu'un seul jeu de valeurs de paramètres soit utilisé car cela diminue la possibilité de fuites d'informations.

#### 5. Références normatives

- [RFC2119] S. Bradner, "[Mots clés à utiliser](#) dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. (*MàJ par RFC8174*)
- [RFC3447] J. Jonsson et B. Kaliski, "[Normes de cryptographie à clés publiques](#) (PKCS) n° 1 : Spécifications de la cryptographie RSA version 2.1", février 2003. (*Obsolète, remplacée par RFC8017*) (*Information*)
- [RFC3852] R. Housley, "Syntaxe de message cryptographique (CMS)", juillet 2004. (*Obsolète, voir la RFC5652*)
- [RFC4055] J. Schaad et autres, "[Algorithmes et identifiants supplémentaires pour la cryptographie RSA](#) à utiliser dans le profil de certificat d'infrastructure de clé publique X.509 et de liste de révocation de certificat (CRL) pour l'Internet", juin 2005.
- [X.208-88] Recommandation UIT-T X.208, "Spécification de la notation n° 1 de syntaxe abstraite (ASN.1)", 1998.
- [X.209-88] Recommandation UIT-T X.209, " Spécification des règles de codage de base pour la notation n° 1 de syntaxe abstraite (ASN.1)", 1998
- [X.509-88] Recommandation UIT-T X.509, "Cadre d'authentification de l'annuaire", 1988.

#### 6. Références pour information

- [RFC1750] D. Eastlake 3rd et autres, "Recommandations d'[aléa pour la sécurité](#)", décembre 1994. (*Info., remplacée par RFC4086*)
- [RFC2313] B. Kaliski, "PKCS n° 1 : Chiffrement RSA version 1.5", mars 1998.

## Adresse de l'auteur

Jim Schaad  
Soaring Hawk Consulting  
PO Box 675  
Gold Bar, WA 98251  
USA  
mél : [jimsch@exmsft.com](mailto:jimsch@exmsft.com)

## Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (2005).

Le présent document est soumis aux droits, licences et restrictions contenus dans le BCP 78, et à [www.rfc-editor.org](http://www.rfc-editor.org), et sauf pour ce qui est mentionné ci-après, les auteurs conservent tous leurs droits.

Le présent document et les informations contenues sont fournies sur une base "EN L'ÉTAT" et le contributeur, l'organisation qu'il ou elle représente ou qui le/la finance (s'il en est), la INTERNET SOCIETY et la INTERNET ENGINEERING TASK FORCE déclinent toutes garanties, exprimées ou implicites, y compris mais non limitées à toute garantie que l'utilisation des informations ci encloses ne violent aucun droit ou aucune garantie implicite de commercialisation ou d'aptitude à un objet particulier.

### Propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourraient être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur répertoire en ligne des IPR de l'IETF à <http://www.ietf.org/ipr> .

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à [ietf-ipr@ietf.org](mailto:ietf-ipr@ietf.org) .

### Remerciement

Le financement de la fonction d'édition des RFC est actuellement fourni par la Internet Society.