Groupe de travail Réseau
Request for Comments : 4262
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

S. Santesson, Microsoft

décembre 2005

Extension de certificat X.509 pour capacités d'extension de messagerie Internet sécurisée/multi objets (S/MIME)

Résumé
Le présent document définit une extension de certificat pour l' inclusion de capacités d'extensions de messagerie Internet sécurisée/multi parties (S/MIME, *Secure/Multipurpose Internet Mail Extensions*) dans les certificats de clé publique X.509, comme défini par la [RFC3280]. Cette extension de certificat fournit une méthode facultative pour indiquer les capacités cryptographiques d'une entité en complément de l'attribut de capacités S/MIME dans les messages S/MIME conformément à la [RFC3851].

1. Introduction

Le présent document définit une extension de certificat pour l'inclusion de capacités S/MIME dans les certificats de clés publiques X.509, comme défini par la [RFC3280].

L'attribut Capacités S/MIME, défini dans la [RFC3851], indique les capacités cryptographiques de l'envoyeur d'un message S/MIME signé. Ces informationsc peuvent être utilisées par le receveur dans les échanges S/MIME sécurisés ultérieurs pour choisir les propriétés cryptographiques appropriées.

Cependant, S/MIME implique aussi le scénario où, par exemple, un envoyeur d'un message chiffré n'a pas de connaissance établie à priori des capacités cryptographiques du receveur par les échanges S/MIME récents.

Dans un tel cas, l'envoyeur est forcé de s'appuyer sur des moyens hors bande ou sur sa configuration par défaut pour choisir un algorithme de chiffrement de contenu pour les messages chiffrés aux receveurs dont les capacités de chiffrement ne sont pas connues. Une telle configuration par défaut peut cependnat être incompatible avec les capacités du receveur et/ou sa politique de sécurité.

La solution définie dans la présente spécification s'appuie sur le fait que le chiffrement S/MIME exige la possession du certificat de clé publique du receveur. Ce certificat contient déjà des informations sur la clé publique du receveur et sur les capacités cryptographiques de cette clé. Grâce au mécanisme d'extension défini dans cette spécification, le certificat peut aussi identifier les capacités cryptographiques S/MIME du sujet. Cela peut alors être utilisé comme une ressource d'informations facultatives pour choisir les réglages de chiffrement appropriés pour la communication.

Le présent document se limite à l'approche "statique" où les capacités cryptographiques affirmées restent inchangées jusqu'à ce que le certificat arrive à expiration ou soit révoqué. D'autres approches "dynamiques", qui permettent la restitution de capacités certifiées mises à jour de façon dynamique pendant la durée de vie d'un certificat, sortent du domaine d'application du présent document.

1.1 Terminologie

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].

2. Extension de capacités S/MIME

Cette section définit l'extension "Capacités S/MIME".

La structure des données de l'extension "Capacités S/MIME" utilisée dans la présente spécification est identique à la structure des données de l'attribut "SMIMECapabilities" défini dans la [RFC3851]. (La structure ASN.1 de smimeCapabilities est donnée ci-dessous à des fins purement illustratives.)

IDENTIFIANT D'OBJET smimeCapabilities ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) 15}

SMIMECapabilities ::= SEQUENCE DE SMIMECapability
SMIMECapability ::= SEQUENCE {
  capabilityID IDENTIFIANT D'OBJET,
  parametres TOUS DÉFINIS PAR capabilityID FACULTATIF}

Toutes les exigences de contenu définies pour l'attribut SMIMECapabilities dans la [RFC3851] s'appliquent aussi à cette extension.

De nombreux types différents de capacités S/MIME ont été définis dans divers documents. Bien que toutes les différentes capacités puissent être placées dans cette extension, l'intention de la présente spécification est principalement de soutenir l'inclusion de capacités S/MIME qui spécifient des algorithmes de chiffrement de contenu.

Les autorités de certification (CA, *Certification Authorities*) DEVRAIENT limiter le type de capacités S/MIME incluses dans cette extension aux types qui sont considérés pertinents pour l'utilisation prévue du certificat.

Les applications de client qui traitent cette extension PEUVENT à leur discrétion ignorer toutes les capacités S/MIME présentes et DEVRAIENT toujours ignorer en douceur toutes les capacités S/MIME présentes qui ne sont pas considérées comme pertinentes pour l'utilisation particulière du certificat.

Cette extension NE DOIT PAS être marquée comme critique.

3. Utilisation dans les applications

Les applications qui utilisent l'extension Capacités S/MIME NE DEVRAIENT PAS utiliser les informations de l'extension si des informations de capacités authentifiées plus fiables et pertinentes sont disponibles à l'application.

Il sort du domaine d'application de la présente spécification de définir ce qui est, ou n'est pas, considéré comme une source d'informations plus fiables par l'application qui utilise le certificat.

4. Considérations sur la sécurité

L'extension Capacités S/MIME contient une déclaration sur les capacités du sujet faite au moment de la production du certificat. Les mises en œuvre devraient donc prendre en compte tous les effets causés par le changement de ces capacités pendant la durée de vie du certificat.

Le changement des capacités du sujet pendant la durée de vie d'un certificat peut exiger la révocation du certificat. La révocation ne devrait cependant être motivée que si un des algorithmes mentionnés sur la liste est considéré comme ayant été cassé ou comme trop faible pour la politique de sécurité en vigueur.

Les mises en œuvre devraient prendre en compte que l'utilisation ce cette extension ne change pas le fait qu'il est toujours de la responsabilité de l'envoyeur de choisir un chiffrement suffisamment fort pour la divulgation de ses 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)

[RFC3280] R. Housley, W. Polk, W. Ford et D. Solo, "Profil de certificat d'infrastructure de clé publique X.509 et de liste de révocation de certificat (CRL) pour l'Internet", avril 2002. *(Obsolète, voir* RFC5280)

[RFC3851] B. Ramsdell, "Spécification du message d'extensions de messagerie Internet multi-objets/sécurisé (S/MIME) version 3.1", juillet 2004. *(Obsolète, voir* RFC5751)

Adresse de l'auteur

Stefan Santesson
Microsoft
Tuborg Boulevard 12
2900 Hellerup
Danemark

méi l: stefans@microsoft.com

Déclaration complète de droits de reproduction

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