Groupe de travail Réseau
Request for Comments : 3853
RFC mise à jour : 3261
Catégorie : En cours de normalisation

J. Peterson
Neustar
juillet 2004
Traduction Claude Brière de L'Isle

S/MIME exige la norme de chiffrement évolué (AES) pour le protocole d'initialisation de session (SIP)

Résumé
La RFC 3261 spécifie actuellement 3DES comme suite de chiffrement de mise en oeuvre obligatoire pour les mises en oeuvre de S/MIME dans le protocole d'initialisation de session (SIP, *Session Initiation Protocol*). Le présent document met à jour les lignes directrices normatives de la RFC 3261 pour exiger la norme de chiffrement évolué (AES, *Advanced Encryption Standard*) pour S/MIME.

1 Introduction

La spécification du protocole d'initialisation de session (SIP, *Session Initiation Protocol*) (RFC 3261 [1]) précise actuellement la prise en charge facultative (un PEUT normatif) de l'utilisation de MIME sécurisé, ou S/MIME (RFC 2633 [8]). Depuis la publication de la RFC 3261, la spécification S/MIME et la syntaxe de message chiffré (CMS, *Cryptographic Message Syntax*, RFC 3369 [3]) sous-jacente ont subi quelques révisions. Le travail effectué a identifié AES comme un algorithme qui pourrait être utilisé pour le chiffrement du contenu dans S/MIME.

La norme de chiffrement évolué (AES, *Advanced Encryption Standard* [6]) est estimé largement comme étant plus rapide que le Triple-DES (3DES, dont l'utilisation était précédemment rendu obligatoire avec S/MIME) et comme étant d'une sécurité comparable. AES est aussi estimé avoir des exigences de mémoire comparativement faible, ce qui la rend convenable pour l'utilisation dans les appareils mobiles ou incorporés, ce qui est un cas d'utilisation important pour SIP.

Comme considération supplémentaire, la spécification SIP a une recommandation (un DEVRAIT normatif) de prise en charge de la sécurité de la couche transport (TLS, *Transport Layer Security*, RFC 2246 [7]). La prise en charge de TLS dans SIP exige l'utilisation de AES. Cela signifie qu'actuellement, les mises en oeuvre qui prennent en charge à la fois TLS et S/MIME doivent prendre en charge à la fois 3DES et AES. Une duplication d'efforts similaire existe avec DSS dans S/MIME comme algorithme de signature numérique (la suite de chiffrement TLS obligatoire utilisée par SIP exige RSA). Unifier les exigences de la suite de chiffrement et l'algorithme de signature pour TLS et S/MIME simplifierait les mises en oeuvre de sécurité.

Il est donc désirable de mettre les exigences de S/MIME pour SIP à parité avec le travail en cours sur la norme S/MIME, ainsi que d'unifier les exigences d'algorithme pour TLS et S/MIME. À ce jour, S/MIME n'a pas encore connu un grand développement dans les agents d'utilisateur SIP, et donc un minimum de suites de chiffrement pour S/MIME pourrait être mises à jour sans rendre obsolètes des quantités substantielles de mises en oeuvre de S/MIME pour SIP (en fait, ces changements rendront probablement plus facile la prise en charge de S/MIME). Le présent document met donc à jour les exigences normatives pour S/MIME dans la RFC 3261.

Noter que le travail sur ces révisions est toujours en cours dans le groupe de travail S/MIME. Le présent document va continuer de suivre l'évolution de ce travail. En initiant maintenant ce processus dans le groupe de travail SIP, nous

fournissons une opportunité précoce d'adopter les changements proposés et donnons aux développeurs l'avertissement que les exigences de S/MIME pour SIP peuvent encore changer.

2 Terminologie

Dans le présent document, les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" sont à interpréter comme décrit dans la RFC 2119 [2] et indiquent les niveaux d'exigence pour les mises en œuvre SIP conformes.

3 Exigences de la suite de chiffrement de S/MIME pour SIP

Les mises à jour suivantes visent le paragraphe 23.3 de la RFC 3261, et spécifiquement le cinquième point. Le texte dit actuellement :

- Les mises en œuvre S/MIME DOIVENT au minimum prendre en charge SHA1 comme algorithmes de signature numérique, et 3DES comme algorithme de chiffrement. Tous les autres algorithmes de signature et de chiffrement PEUVENT être acceptés. Les mises en œuvre peuvent négocier la prise en charge de ces algorithmes avec l'attribut "SMIMECapabilities".

Ce texte est mis à jour comme suit :

Les mises en œuvre S/MIME DOIVENT au minimum prendre en charge RSA comme algorithme de signature numérique et SHA1 comme algorithme de résumé [5], et AES comme algorithme de chiffrement (comme spécifié dans [4]. Pour le transport des clés, les mises en œuvre de S/MIME DOIVENT prendre en charge le transport de clés RSA comme spécifié au paragraphe 4.2.1. de [5]. Les mises en œuvre S/MIME d'AES DOIVENT prendre en charge les clés de 128 bits d'AES, et DEVRAIENT prendre en charge les clés de 192 et 256 bits. Noter que la spécification S/MIME [8] rend obligatoire la prise en charge de 3DES comme algorithme de chiffrement, DH pour le chiffrement de clés et DSS comme algorithme de signature. Dans le profil SIP de S/MIME, la prise en charge de 3DES, DH et DSS est RECOMMANDÉE mais pas exigée. Tous les autres algorithmes de signature et de chiffrement PEUVENT être pris en charge. Les mises en oeuvre peuvent négocier la prise en charge des algorithmes avec l'attribut "SMIMECapabilities".

Comme SIP est entièrement en 8 bits, toutes les mises en œuvre DOIVENT utiliser le codage de transfert de contenu binaire à 8 bits pour S/MIME dans SIP. Les mises en oeuvre PEUVENT aussi être capables de recevoir le codage de transfert de contenu en base 64.

4 Considérations pour la sécurité

La migration des exigences de S/MIME de Triple-DES à AES n'introduit aucun nouveau problème de sécurité connu.

5 Références

5.1 Références normatives

[1] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley et E. Schooler, "SIP: Protocole d'initialisation de session", RFC 3261, juin 2002.

[2] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, RFC 2119, mars 1997.

[3] R. Housley, "Syntaxe de message cryptographique (CMS)", RFC 3369, août 2002.

[4] J. Schaad, "Utilisation de l'algorithme de chiffrement de la norme de chiffrement évolué (AES) dans la syntaxe de message cryptographique (CMS)", RFC 3565, juillet 2003.

[5] R. Housley, "Algorithmes de la syntaxe de message cryptographique (CMS)", RFC 3394, août 2002.

5.2 Références informatives

[6] National Institute of Standards & Technology, "Advanced Encryption Standard (AES).", FIPS 197, novembre 2001.

[7] T. Dierks et C. Allen, "Le protocole TLS version 1.0", RFC 2246, janvier 1999.

[8] B. Ramsdell, éd., "Spécification de message S/MIME version 3.1", RFC 3851, juillet 2004.

6 Remerciements

Merci à Rohan Mahy, Gonzalo Camarillo, et Eric Rescorla pour leur révision de ce document.

7 Adresse de l'auteur

Jon Peterson
NeuStar, Inc.
1800 Sutter St
Suite 570
Concord, CA 94520
USA
téléphone : +1 925/363-8720
mél : jon.peterson@neustar.biz
URI : http://www.neustar.biz/

8 Déclaration complète de droits de reproduction

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