Groupe de travail Réseau
Request for Comments : 5273
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

J. Schaad, Soaring Hawk Consulting
M. Myers, TraceRoute Security, Inc.
juin 2008

Gestion de certificats sur la CMS (CMC) : protocoles de transport

Résumé
Le présent document définit un certain nombre de mécanismes de transport qui sont utilisés pour déplacer les messages de gestion de certificats sur la syntaxe de message cryptographique (CMC, *Certificate Management over Cryptographic Message Syntax*). Les mécanismes de transport décrits dans ce document sont HTTP, le fichier, la messagerie, et TCP.

Table des matières

1. Généralités

Le présent document définit un certain nombre de méthodes de transport utilisées pour déplacer les messages de CMC (définis dans la [RFC5272]). Les mécanismes de transport décrits dans ce document sont HTTP, fichier, messagerie, et TCP.

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. Protocole fondé sur le fichier

Les messages et réponses d'adhésion peuvent être transférés entre clients et serveurs en utilisant des mécanismes fondés sur le système de fichiers, comme quand l'adhésion est effectué pour un client hors ligne. Quand des fichiers sont utilisés pour transporter des messages binaires, de demande PKI complète ou de réponse PKI complète, il DOIT y avoir seulement une instance d'un message de demande ou réponse dans un seul fichier. Les extensions de type de fichier suivantes DEVRAIENT être utilisées :

Type de message	Extension de fichier
Simple demande PKI	.p10
Demande PKI complète	.crq
Simple réponse PKI	.p7c
Réponse PKI complète	.crp

Identification de fichier de demande/réponse PKI

3. Protocole fondé sur la messagerie

L'enveloppement MIME est défini pour les environnements qui sont en MIME natif. L'enveloppement MIME de base dans cette Section est tiré de la [RFC3851]. Quand on utilise un protocole fondé sur la messagerie, l'enveloppement MIME entre les couches d'enveloppement de CMS est facultatif. Noter que ceci est différent du message standard S/MIME (MIME sécurisé).

Les simples demandes d'adhésion sont codées en utilisant le type de contenu "application/pkcs10". Un nom de fichier DOIT être inclus dans une déclaration content-type ou content-disposition. L'extension pour le fichier DOIT être ".p10".

Les messages de simple réponse d'adhésion DOIVENT être codés comme type de contenu "application/pkcs7-mime". Un paramètre smime-type DOIT être dans la déclaration de type de contenu avec une valeur de "certs-only". Un nom de fichier avec l'extension ".p7c" DOIT être spécifié au titre de la déclaration de type de contenu ou de disposition de contenu.

Les messages de demande d'adhésion complète DOIVENT être codés comme type de contenu "application/pkcs7-mime". Le paramètre smime-type DOIT être inclus avec une valeur de "CMC-Request". Un nom de fichier avec l'extension ".p7m" DOIT être spécifié au titre de la déclaration de type de contenu ou de disposition de contenu.

Les messages de réponse d'adhésion complète DOIVENT être codés comme type de contenu "application/pkcs7-mime". Le paramètre smime-type DOIT être inclus avec une valeur de "réponse CMC". Un nom de fichier avec l'extension ".p7m" DOIT être spécifié au titre de la déclaration de type de contenu ou de disposition de contenu.

Élément	Type MIME	Fichier d'extension	Type SMIME
Simple demande PKI	application/pkcs10	.p10	N/A
Demande PKI complète	application/pkcs7-mime	.p7m	CMC-request
Simple réponse PKI	application/pkcs7-mime	.p7c	certs-only
Réponse PKI complète	application/pkcs7-mime	.p7m	CMC-response |

Table 1 : Identification de demande/réponse PKI MIME

4. Protocole fondé sur HTTP/HTTPS

Cette section décrit les conventions pour l'utilisation de HTTP [RFC2616] comme couche de transport. Dans la plupart des circonstances, l'utilisation de HTTP sur TLS [RFC4346] fournit la protection nécessaire du contenu contre l'espionnage.

Afin que puissent inter opérer les clients et serveurs de CMC qui utilisent HTTP, les règles suivantes s'appliquent :

Les clients DOIVENT utiliser la méthode POST pour soumettre leurs demandes.

Les serveurs DOIVENT utiliser le code de réponse 200 pour les réponses de succès.

Les clients PEUVENT tenter d'envoyer des demandes HTTP en utilisant TLS 1.0 [RFC4346] ou plus, bien que les serveurs ne soient pas obligés de prendre en charge TLS.

Les serveurs NE DOIVENT PAS supposer que le client prend en charge un type d'authentification HTTP comme des mouchards, l'authentification de base, ou l'authentification par résumé.

On attend des clients et serveurs qu'ils suivent les autres règles et restrictions de la [RFC2616]. Noter que certaines de ces règles sont pour les méthodes HTTP autres que POST ; en clair, seules les règles qui s'appliquent à POST sont pertinentes

pour la présente spécification.

4.1 Demande PKI

Une demande PKI utilisant la méthode POST est construite comme suit :

L'en-tête Content-Type DOIT avoir la valeur appropriée tirée du tableau 1.

Le corps du message est la valeur binaire du codage de la demande PKI.

4.2 Réponse PKI

Un réponse PKI fondée sur HTTP est composée des en-têtes HTTP appropriés, suivis pa la valeur binaire du codage en BER (règles de codage de base) de la réponse PKI simple ou complète.

L'en-tête Content-Type DOIT avoir la valeur appropriée tirée du tableau 1.

5. Protocole fondé sur TCP

Quand les messages de CMC sont envoyés sur une connexion fondée sur TCP, aucun enveloppement du message n'est nécessaire. Les messages sont envoyés dans leur forme codée en binaire.

Le client ferme une connexion après la réception d'une réponse, ou il produit une autre demande au serveur en utilisant la même connexion. Réutiliser une connexion pour plusieurs demandes successives, au lieu d'ouvrir plusieurs connexions qui sont utilisées pour une seule demande, est RECOMMANDÉ pour des raisons de performances et de conservation des ressources. Un serveur PEUT clore une connexion après avoir été inactif pendant un certain temps ; cette temporisation sera normalement de plusieurs minutes.

Il n'y a pas d'accès spécifique à utiliser pour le transport fondé sur TCP. Seuls les accès privés 49152 à 65535 peuvent être utilisés de cette manière (sans enregistrement). Les accès dans la gamme de 1 à 49151 NE DEVRAIENT PAS être utilisés. L'accès à utiliser est configuré hors bande.

6. Considérations sur la sécurité

Des mécanismes pour déjouer les attaques de répétition peuvent être nécessaires dans des mises en œuvre particulières de ce protocole selon l'environnement de fonctionnement. Dans les cas où l'autorité de certification (CA) maintient des informations d'état significatives, les attaques de répétition peuvent être détectées sans l'inclusion de mécanismes facultatifs de nom occasionnel. Les mises en œuvre de ce protocole doivent considérer avec attention les conditions environnementales avant de choisir si elles mettent ou non en œuvre les attributs senderNonce et recipientNonce décrits au paragraphe 6.6 de la [RFC5272]. Les développeurs de clients PKI à contraintes d'état sont vivement encouragés à incorporer l'utilisation de ces attributs.

L'initiation d'un canal de communications sûr entre une entité d'extrémité et une autorité de certification (CA) ou une autorité d'enregistrement (RA) -- et, de façon similaire, entre une RA et une autre RA ou CA – exige nécessairement un mécanisme d'initiation de confiance hors bande. Par exemple, un canal sûr peut être construit entre l'entité d'extrémité et la CA via IPsec [RFC4301] ou TLS [RFC4346]. Il existe de nombreux schémas comme celui-là, et le choix d'un schéma particulier pour l'initiation de confiance sort du domaine d'application du présent document. Les mises en œuvre de ce protocole sont vivement encouragées à considérer les principes généralement acceptés de gestion sûre de clé quand elles intègrent cette capacité dans une architecture de sécurité globale.

Dans certaines instances, aucune confiance hors bande préalable n'aura été initiée avant l'utilisation de ce protocole. Cela peut arriver quand le protocole lui-même est utilisé pour télécharger sur le système l'ensemble des ancres de confiance à utiliser pour ces protocoles. Dans ce cas, le type de contenu EnvelopedData (paragraphe 3.2.1.3.3 de la [RFC5272]) doit être utilisé pour fournir la même protection qu'aurait fournie TLS.

7. Remerciements

Les auteurs et le groupe de travail PKIX remercient de leur participation Xiaoyi Liu et Jeff Weinstein qui les ont aidés dans les premières versions de ce document.

Les auteurs tiennent à remercier Brian LaMacchia pour son travail de développement et de rédaction de nombreux concepts présentés dans ce document. Les auteurs tiennent aussi à remercier Alex Deacon et Barb Fox de leurs contributions.

8. Références

8.1 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)

[RFC2616] R. Fielding et autres, "Protocole de transfert hypertexte -- HTTP/1.1", juin 1999. *(D.S., MàJ par* 2817, 6585)

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

[RFC4301] S. Kent et K. Seo, "Architecture de sécurité pour le protocole Internet", décembre 2005. *(P.S.) (Remplace la* RFC2401)

[RFC5272] J. Schaad, M. Myers, "Gestion de certificat sur CMS (CMC)", juin 2008. (*Remplace* RFC2797) *(P.S.)*

8.2 Références pour information

[RFC4346] T. Dierks et E. Rescorla, "Protocole de sécurité de la couche Transport (TLS) version 1.1", avril 2006. *(Remplace* RFC2246 *; Remplacée par* RFC5246 *; MàJ par* RFC4366, 4680, 4681, 5746, 6176, 7465, 7507, 7919)

Adresse des auteurs

Jim Schaad
Soaring Hawk Consulting
PO Box 675
Gold Bar, WA 98251
USA
téléphone : (425) 785-1031
mél : jimsch@nwlink.com

Michael Myers
TraceRoute Security, Inc.
mél : mmyers@fastq.com

Déclaration complète de droits de reproduction

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 le 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.

Remerciement

Le financement de la fonction d'édition des RFC est fourni par l'activité de soutien administratif de l'IETF (IASA).