Groupe de travail Réseau
Request for Comments : 5274
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

Messages de gestion de certificat sur CMS (CMC) : exigences de conformité

Résumé
Le présent document fournit un ensemble de déclarations de conformité sur le protocole d'adhésion à la gestion de certificat sur la CMS (CMC, *Certificate Management over CMS*). Les structures ASN.1 et les mécanismes de transport pour le protocole d'adhésion à la CMC sont couvertes dans d'autres documents. Le présent document fournit les informations nécessaires pour faire une version conforme à la CMC.

Table des matières

1. Vue d'ensemble

Le protocole de gestion de certificats sur la CMS (CMC, *Certificate Management over CMS*) est conçu dans les termes d'une relation client/serveur. Dans le cas le plus simple, le client est le demandeur du certificat (c'est-à-dire, l'entité d'extrémité (EE)) et le serveur est le producteur du certificat (c'est-à-dire, l'autorité de certification (CA, *Certification Authority*)). L'introduction d'une autorité d'enregistrement (RA, *Registration Authority*) dans l'ensemble des agents complique seulement un peu le tableau. La RA devient le serveur par rapport au demandeur de certificat, et elle devient le client par rapport au producteur du certificat. Un nombre quelconque de RA peuvent être insérées dans la scène de cette manière.

Les RA peuvent servir à des besoins spécialisés qui ne sont pas actuellement couverts par ce document. Un de ces besoins serait d'un agent courtier de clés. À ce titre, toutes les demandes de certificat pour les clés de chiffrement seraient dirigées à travers cette RA et elle prendrait les mesures appropriées pour faire l'archivage de clés. Les demandes de récupération de clé pourraient être définies dans la méthodologie de la CMC permettant à l'agent courtier de clés d'effectuer cette opération

en agissant comme serveur final dans la chaîne des agents.

Si il y a plusieurs RA dans le système, il est considéré comme normal que toutes les RA ne voient pas toutes les demandes de certificats. L'acheminement entre les RA peut dépendre du contenu des demandes de certificat impliquées.

Le présent document est divisé en six sections, chaque section spécifiant les exigences spécifiques d'une classe d'agents dans le modèle de CMC. Ce sont 1) tous les agents, 2) tous les serveurs, 3) tous les clients, 4) toutes les entitées d'extrémité, 5) toutes les entités d'enregistrement, 6) toutes les autorités de certification.

2. Terminologie

Différents termes, abréviations, et acronymes sont utilisés dans ce document qu'on définit ici à des fins pratiques et pour la cohérence de leur utilisation :

EE *(End-Entity)* entité d'extrémité se réfère à l'entité qui possède une paire de clés et pour laquelle un certificat est produit.

RA *(Registration Authority)* autorité d'enregistrement ou RA locale (LRA, *Local RA*) se réfère à une entité qui agit comme intermédiaire entre la EE et la CA. Plusieurs RA peuvent exister entre l'entité d'extrémité et l'autorité de certification. Les RA peuvent effectuer des services supplémentaires comme la génération ou l'archivage de clés. Le présent document utilise le terme de RA pour les deux RA et LRA.

CA *(Certification Authority)* autorité de certification, se réfère à l'entité qui produit les certificats.

Client, se réfère à une entité qui crée une demande PKI. Dans le présent document, les RA et les EE peuvent être des clients.

Serveur, se réfère aux entités qui traitent les demandes PKI et créent les réponses PKI. Dans le présent document les CA et les RA peuvent toutes deux être des serveurs.

PKCS n° 10, se réfère à la norme de chiffrement à clé publique n° 10 [RFC2986], qui définit la syntaxe de demande de certification.

CRMF, se réfère au format de message de demande de certificat [RFC4211]. La CMC utilise cette syntaxe de demande de certification définie dans ce document au titre du protocole.

CMS, se réfère à la syntaxe de message cryptographique [RFC3852]. Le présent document fournit les services cryptographiques de base incluant le chiffrement et la signature avec et sans gestion de clé.

demande/réponse PKI se réfère aux demandes/réponses décrites dans ce document. Les demandes PKI incluent des demandes de certification, des demandes de révocation, etc. Les réponses PKI incluent des messages certs-only, des messages d'échec, etc.

Preuve d'identité se réfère au client qui prouve qu'il est qui il dit qu'il est au serveur.

Preuve de possession (POP) se réfère à une valeur qui peut être utilisée pour prouver que la clé privée correspondant à une clé publique est en sa possession et peut être utilisée par une entité d'extrémité.

Enveloppe de transport se réfère à la couche d'enveloppe de CMS la plus externe.

3. Terminologie des exigences

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].

4. Exigences pour toutes les entités

Toutes les déclarations de conformité aux [RFC5272] et [RFC5273] DOIVENT être respectées sauf mention contraire explicite dans le présent document.

Toutes les entités DOIVENT prendre en charge les demandes PKI complètes, les simples réponses PKI, et les réponses PKI complètes. Les serveurs DEVRAIENT prendre en charge les simples demandes PKI.

Toutes les entités DOIVENT prendre en charge l'utilisation de la syntaxe de CRMF pour les demandes de certification. La prise en charge de la syntaxe de PKCS n° 10 pour les demandes de certification DEVRAIT être mise en œuvre par les serveurs.

Le champ extendedFailInfo NE DEVRAIT PAS être rempli dans l'objet CMCStatusInfoV2 ; le champ failInfo DEVRAIT être utilisé pour relayer cette information. Si le champ extendedFailInfo est utilisé, il est suggéré qu'un élément CMCStatusInfoV2 supplémentaire existe pour la même partie de corps avec un champ failInfo.

Toutes les entités DOIVENT mettre en œuvre le mécanisme de transport HTTP comme défini dans [RFC5273]. D'autres mécanismes de transport PEUVENT être mis en œuvre.

4.1 Exigences pour les algorithmes de chiffrement

Toutes les entités DOIVENT vérifier les signatures DSA-SHA1 et RSA-SHA1 dans SignedData (voir la [RFC3370]). Les entités PEUVENT vérifier d'autres algorithmes de signature. Il est fortement suggéré que RSA-PSS avec SHA-1 soit vérifié (voir la [RFC4056]). Il est fortement suggéré que SHA-256 utilisant RSA et RSA-PSS soit vérifié (voir la [RFC4055]).

Toutes les entités DOIVENT générer des signatures DSA-SHA1 ou RSA-SHA1 pour SignedData (voir la [RFC3370]). D'autres algorithmes de signature PEUVENT être utilisés pour la génération.

Toutes les entités DOIVENT prendre en charge la norme de chiffrement évolué (AES, *Advanced Encryption Standard*) comme algorithme de chiffrement de contenu pour EnvelopedData (voir la [RFC3565]). D'autres algorithmes de chiffrement de contenu PEUVENT être mis en œuvre.

Toutes les entités DOIVENT prendre en charge RSA comme algorithme de transport de clés pour EnvelopedData (voir la [RFC3370]). Toutes les entités DEVRAIENT prendre en charge RSA-OAEP (voir la [RFC3560]) comme algorithme de transport de clés. D'autres algorithmes de transport de clés PEUVENT être mis en œuvre.

Si une entité prend en charge l'accord de clés pour EnvelopedData, elle DOIT prendre en charge Diffie-Hellman (voir la [RFC2631]).

Si une entité prend en charge PasswordRecipientInfo pour EnvelopedData ou AuthenticatedData, elle DOIT prendre en charge PBKDF2 [RFC2898] pour les algorithmes de déduction de clés. Elle DOIT prendre en charge l'enveloppe de clé AES (voir la [RFC3394] comme algorithme de chiffrement de clé.

Si AuthenticatedData est pris en charge, PasswordRecipientInfo DOIT être pris en charge.

Les exigences de l'algorithme pour la commande Preuve d'identité version 2 (paragraphe 6.2.1 de la [RFC5272]) sont : SHA-1 DOIT être mis en œuvre pour hashAlgId. SHA-256 DEVRAIT être mis en œuvre pour hashAlgId. HMAC-SHA1 DOIT être mis en œuvre pour macAlgId. HMAC-SHA256 DEVRAIT être mis en œuvre pour macAlgId.

Les exigences de l'algorithme pour la commande Témoin de liaison POP version 2 (paragraphe 6.3.1 de la [RFC5272]) sont : SHA-1 DOIT être mis en œuvre pour keyGenAlgorithm. SHA-256 DEVRAIT être mis en œuvre pour keyGenAlgorithm. PBKDF2 [RFC2898] PEUT être mis en œuvre pour keyGenAlgorithm. HMAC-SHA1 DOIT être mis en œuvre pour macAlgorithm. HMAC-SHA256 DEVRAIT être mis en œuvre pour macAlgorithm.

Les exigences de l'algorithme pour les commandes POP chiffré et POP déchiffré (paragraphe 6.7 de la [RFC5272]) sont : SHA-1 DOIT être mis en œuvre pour witnessAlgID. SHA-256 DEVRAIT être mis en œuvre pour witnessAlgID. HMAC-SHA1 DOIT être mis en œuvre pour thePOPAlgID. HMAC-SHA256 DEVRAIT être mis en œuvre pour thePOPAlgID.

Les exigences de l'algorithme pour la commande Publier les ancres de confiance (paragraphe 6.15 de la [RFC5272]) sont : SHA-1 DOIT être mis en œuvre pour hashAlgorithm. SHA-256 DEVRAIT être mis en œuvre pour hashAlgorithm.

Si une EE génère des clés DH pour la certification, elle DOIT prendre en charge la Section 4 de la [RFC2875]. Les EE PEUVENT prendre en charge la Section 3 de la [RFC2875]. Les CA et les RA qui font la vérification POP DOIVENT prendre en charge la Section 4 de la [RFC2875] et DEVRAIENT prendre en charge la Section 3 de la [RFC2875].

Les EE qui ont besoin d'utiliser un algorithme de signature pour les clés qui ne peuvent pas produire une signature DOIVENT prendre en charge l'Appendice C de la [RFC5272] et DOIVENT prendre en charge les commandes POP chiffré/déchiffré. Les CA et RA qui font la vérification de POP DOIVENT prendre en charge cet algorithme de signature et DOIVENT prendre en charge les commandes POP chiffré/déchiffré.

4.2 Commandes

Le tableau qui suit fait la liste des noms et du niveau de prise en charge exigé pour chaque commande.

Commande	EE	RA	CA
Info d'état CMC étendu	DOIT	DOIT	DOIT
Info d'état CMC	DEVRAIT	DEVRAIT	DEVRAIT
Preuve d'identité version 2	DOIT	DOIT	DOIT
Preuve d'identité	DEVRAIT	DEVRAIT	DEVRAIT
Identification	DOIT	DOIT	DOIT
Liaison POP aléatoire	DOIT	DOIT	DOIT
Témoin de liaison POP v 2	DOIT	DOIT	DOIT
Témoin de liaison POP	DEVRAIT	DOIT	DOIT
Retour des données	DOIT	DOIT	DOIT
Modifier la demande de certification	N/A	DOIT	(2)
Ajouter des extensions	N/A	PEUVENT	(1)
Identifiant de transaction	DOIT	DOIT	DOIT
Nom occasionnel d'envoyeur	DOIT	DOIT	DOIT
Nom occasionnel de receveur	DOIT	DOIT	DOIT
POP chiffrée	(4)	(5)	DEVRAIT
POP déchiffrée	(4)	(5)	DEVRAIT
Témoin POP de RA	N/A	DEVRAIT	(1)
Obtenir un certificat	facultatif	facultatif	facultatif
Obtenir une CRL	facultatif	facultatif	facultatif
Demande de révocation	DEVRAIT	DEVRAIT	DOIT
Informations d'enregistrement	DEVRAIT	DEVRAIT	DEVRAIT
Informations de réponse	DEVRAIT	DEVRAIT	DEVRAIT
Interrogation en instance	DOIT	DOIT	DOIT
Confirmer l'acceptation du certificat	DOIT	DOIT	DOIT
Publier les ancres de confiance	(3)	(3)	(3)
Données authentifiées	(3)	(3)	(3)
Regrouper les demandes	N/A	DOIT	(2)
Regrouper les réponses	N/A	DOIT	(2)
Informations de publication	facultatif	facultatif	facultatif
Commande traitée	N/A	DOIT	(2)

Tableau 1 : Attributs des commandes CMC

Notes:
1. Les CA DEVRAIENT mettre en œuvre cette commande si elle est destinée à fonctionner avec des RA.
2. Les CA DOIVENT mettre en œuvre cette commande si elle est destinée à fonctionner avec des RA.
3. La mise en œuvre est facultative pour ces commandes. On suggère fortement qu'elle soit mise en œuvre afin de remplir les ancres de confiance du client.
4. Les EE ont seulement besoin de mettre en œuvre cela si (a) elles prennent en charge les algorithmes d'accord de clés ou (b) elles ont besoin de fonctionner dans des environnements où les clés de matériel ne peuvent pas fournir la POP.
5. Les RA DEVRAIENT mettre en œuvre cela si elles mettent en œuvre le témoin de POP de RA.

Une attention forte devrait être portée à la mise en œuvre des commandes Authentification des données et Publication des

ancres de confiance car cela donne une méthode simple pour distribuer les ancres de confiance aux clients sans intervention de l'utilisateur.

4.3 Exigences pour les caractéristiques de CRMF

Les restrictions supplémentaires suivantes sont placées sur les caractéristiques de CRMF :

Les jetons de commande d'enregistrement id-regCtrl-regToken et id-regCtrl-authToken NE DOIVENT PAS être utilisés. Aucune caractéristique spécifique de CMC n'est utilisée pour remplacer ces éléments, mais généralement les commandes d'identification de CMC et identityProof vont effectuer le même service et sont définis plus spécifiquement.

Le jeton de commande id-regCtrl-pkiArchiveOptions NE DEVRAIT PAS être pris en charge. Une méthode de remplacement est en cours de développement pour fournir cette fonctionnalité.

Le comportement de id-regCtrl-oldCertID n'est pas utilisé présentement. Il est remplacé par la production du nouveau certificat et par l'utilisation de id-cmc-publishCert pour supprimer l'ancien certificat de la publication. Cette opération ne va normalement pas être accompagnée d'une révocation immédiate de l'ancien certificat ; cependant, cela peut être réalisé par la commande id-cmc-revokeRequest.

La commande id-regCtrl-protocolEncrKey n'est pas utilisée.

4.4 Exigences pour les clients

Il n'y a pas d'exigence supplémentaire.

5. Exigences pour les serveurs

Il n'y a pas d'exigence supplémentaire.

6. Exigences pour les EE

Si une entité met en œuvres Diffie-Hellman, elle DOIT mettre en œuvre soit la preuve de possession DH-POP comme défini dans la Section 4 de la [RFC2875], soit les commandes de défi-réponse POP id-cmc-encryptedPOP et id-cmc-decryptedPOP.

7. Exigences pour les RA

Les RA DEVRAIENT être capables de faire la POP déléguée. Les RA qui mettent en œuvre cette caractéristique DOIVENT mettre en œuvre la commande id-cmc-lraPOPWitness.

Toutes les RA DOIVENT mettre en œuvre la promotion de id-aa-cmc-unsignedData comme décrit au paragraphe 3.2.3 de la [RFC5272].

8. Exigences pour les CA

Assurer que les CA fonctionnent dans un environnement avec des RA est fortement suggéré. La mise en œuvre d'une telle prise en charge est fortement suggérée car cela permet la délégation d'un interaction administrative substantielle sur une RA plutôt qu'à la CA.

Les CA DOIVENT effectuer au moins les vérifications minimales sur toutes les clés publiques avant de produire un certificat. Au minimum, une vérification de syntaxe devrait se faire avec l'opération POP. De plus, les CA DEVRAIENT effectuer des vérifications simples pour les mauvaises clés connues comme les petits sous groupes pour les clés DSA-

SHA1 et DH [RFC2785] ou les mauvais exposants pour les clés RSA.

Les CA DOIVENT appliquer la vérification de POP avant de produire un certificat. Les CA PEUVENT déléguer l'opération de POP à une RA pour les cas où 1) une paire de messages défi/réponse doit être utilisée, 2) une RA effectue le courtage de clé et vérifie la POP de cette manière, ou 3) un algorithme inhabituel est utilisé et cette validation est faite à la RA.

Les CA DEVRAIENT mettre en œuvre à la fois la preuve de possession DH-POP comme défini à la Section 4 de la [RFC2875], et les commandes de défi-réponse POP id-cmc-encryptedPOP et id-cmc-decryptedPOP.

9. Considérations sur la sécurité

Le présent document utilise les [RFC5272] et [RFC5273] comme blocs de construction de ce document. Les sections sur la sécurité de ces deux documents sont incluses par référence.

La connaissance de comment une entité est supposée fonctionner est vitale pour la détermination des sections des exigences qui sont applicables à cette entité. Il faut faire attention quand on détermine quelles sections s'appliquent et à mettre pleinement en œuvre le code nécessaire.

Les algorithmes de chiffrement ont été et seront cassés ou affaiblis. Les mises en œuvre et les utilisateurs doivent vérifier que les algorithmes de chiffrement mentionnés dans ce document ont un sens du point de vue du niveau de sécurité. L'IETF peut produire de temps en temps des documents qui traitent de l'état de l'art actuel. Deux exemples de ces documents sont les [RFC2785] et [RFC4270].

10. Remerciements

Les auteurs et le groupe de travail PKIX remercient de leur participation Xiaoyi Liu et Jeff Weinstein qui ont aidé les auteurs des versions originelles de ce document.

Les auteurs remercient Brian LaMacchia de son travail de développement et de rédaction de beaucoup des concepts présentés dans ce document. Les auteurs remercient aussi Alex Deacon et Barb Fox de leurs contributions.

11. Références

11.1 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)

[RFC2631] E. Rescorla, "Méthode d'accord de clé Diffie-Hellman", juin 1999. *(P.S.)*

[RFC2875] H. Prafullchandra, J. Schaad, "Algorithmes de preuve de possession Diffie-Hellman", juillet 2000. *(P.S.) (Remplacée par* RFC6955)

[RFC2898] B. Kaliski, "PKCS n° 5 : Spécification de la cryptographie fondée sur un mot de passe, version 2.0", septembre 2000. *(Info. ; remplacée par* RFC8018)

[RFC3370] R. Housley, "Algorithmes de syntaxe de message cryptographique (CMS)", août 2002. *(P.S. ; MàJ par* RFC8702*)*

[RFC3394] J. Schaad, R. Housley, "Algorithme d'enveloppe de clés pour la norme de chiffrement évoluée (AES)", septembre 2002. *(Information)*

[RFC3560] R. Housley, "Utilisation de l'algorithme de transport de clé RSAES-OAEP dans la syntaxe de message cryptographique (CMS)", juillet 2003. *(P.S.)*

[RFC3565] J. Schaad, "Utilisation de l'algorithme de chiffrement de la norme de chiffrement évolué (AES) dans la syntaxe de message cryptographique (CMS)", juillet 2003. *(P.S.)*

[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.

[RFC4056] J. Schaad, "Utilisation de l'algorithme de signature RSASSA-PSS dans la syntaxe de message cryptographique (CMS)", juin 2005. *(P.S.)*

[RFC4211] J. Schaad, "Format de message de demande de certificat d'infrastructure de clé publique X.509 pour l'Internet", septembre 2005. (*P.S. ; remplace* RFC2511 ; *MàJ par* RFC9045*)*

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

[RFC5273] J. Schaad, M. Myers, "Gestion de certificat sur CMS (CMC) : protocoles de transport", juin 2008. *(P.S.)*

11.2 Références pour information

[RFC2785] R. Zuccherato, "Méthodes pour éviter les attaques de "petit sous-groupe" sur la méthode d'accord de clés Diffie-Hellman pour S/MIME", mars 2000. *(Information)*

[RFC2986] M. Nystrom, B. Kaliski, "PKCS n° 10 : Spécification de la syntaxe de demande de certification, version 1.7", novembre 2000. *(Information)*

[RFC4270] P. Hoffman, B. Schneier, "Attaques contre les hachages cryptographiques dans les protocoles Internet", nov. 2005. *(Info.)*

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

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).