Groupe de travail Réseau
Request for Comments : 5083
RFC mise à jour : 3852
Catégorie : Sur la voie de la normalisation

R. Housley, Vigil Security
novembre 2007

Traduction Claude Brière de L'Isle

Type de contenu Authenticated-Enveloped-Data dans la syntaxe de message cryptographique (CMS)

Résumé
Le présent document décrit un type de contenu supplémentaire pour la syntaxe de message cryptographique (CMS, *Cryptographic Message Syntax*). Le type de contenu Authenticated-enveloped-data est destiné à être utilisé avec des modes de chiffrement authentifiés. Toutes les diverses techniques de gestion de clé qui sont prises en charge dans le type de contenu de CMS enveloped-data sont aussi pris en charge par le type de contenu de CMS Authenticated-enveloped-data.

Table des Matières

1. Introduction

Le présent document décrit un type de contenu supplémentaire pour la syntaxe de message cryptographique (CMS, *Cryptographic Message Syntax*) [RFC3852]. Le type de contenu authenticated-enveloped-data est destinté à être utilisé avec des modes de chiffrement authentifiés, où un contenu arbitraire est à la fois authentifié et chiffré. Aussi, certaines données associées sous la forme d'attributs authentifiés peuvent aussi être authentifiées. Toutes les diverses techniques de gestion de clé qui sont prises en charge dans le type de contenu de CMS enveloped-data sont aussi pris en charge par le type de contenu de CMS authenticated-enveloped-data.

Les conventions pour utiliser le compteur standard de chiffrement évolué avec les algorithmes de chiffrement authentifié de code d'authentification de message en chaînage de bloc de chiffrement (AES-CCM, *Cipher Block Chaining-Message Authentication Code*) et le mode compteur AES-Galois (GCM) avec le type de contenu de CMS authenticated-enveloped-data définies dans le présent document peuvent être trouvées dans la [RFC5084].

Le type de contenu authenticated-enveloped-data , comme tous les autres types de contenu de CMS, emploie l'ASN.1 [X.208-88], et il utilise les règles de codage de base (BER, *Basic Encoding Rules*) [X.209-88] et les règles de codage distinctif (DER, *Distinguished Encoding Rules*) [X.509-88].

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].

1.2 Numéros de version

La structure de données majeure (AuthEnvelopedData) inclut un numéro de version comme premier élément dans la structure des données. Le numéro de version est destiné à éviter des erreurs de décodage ASN.1. Certaines mises en œuvre ne vérifient pas le numéro de version avant de tenter un décodage, et si une erreur de décodage survient alors, le numéro de version est vérifié au titre de la routine de traitement d'erreur. C'est une approche raisonnable ; elle place le traitement d'erreur en dehors du plus court chemin. Cette approche est aussi utile quand un numéro de version incorrect est utilisé par l'envoyeur.

Chaque fois que la structure est mise à jour, un numéro de version supérieur va être alloué. Cependant, pour assurer une interopérabilité maximum, le numéro de version supérieur est seulement utilisé quand la nouvelle caractéristique de syntaxe est employée. C'est-à-dire que le plus faible numéro de version qui prend en charge la syntaxe générée est utilisé.

2. Type de contenu Authenticated-Enveloped-Data

Le type de contenu authenticated-enveloped-data *(données authentifiées enveloppées)* consiste en un contenu authentifié et chiffré de tout type et des clés chiffrées de content-authenticated-encryption *(chiffrement de contenu authentifié)* pour un ou plusieurs receveurs. La combinaison du contenu authentifié et chiffré et d'une clé chiffrée de content-authenticated-encryption pour un receveur est une "enveloppe numérique" pour ce receveur. Tout type de contenu peut être enveloppé pour un nombre arbitraire de receveurs en utilisant toutes les techniques de gestion de clé prises en charge pour chaque receveur. De plus, des attributs authentifiés mais non chiffrés peuvent être fournis par l'origine.

L'application normale du type de contenu authenticated-enveloped-data va représenter les enveloppes numériques de un ou plusieurs receveurs dans un contenu encapsulé.

Authenticated-enveloped-data est construit selon les étapes suivantes :

1. Une clé de content-authenticated-encryption pour un algorithme de content-authenticated-encryption particulier est générée au hasard.

2. La clé de content-authenticated-encryption est chiffrée pour chaque receveur. Les détails de ce chiffrement dépendent de l'algorithme de gestion de clés utilisé, mais quatre techniques générales sont prises en charge :

   Transport de clé : la clé de content-authenticated-encryption est chiffrée dans la clé publique du receveur ;

   Accord de clé : la clé publique du receveur et la clé privée de l'envoyeur sont utilisées pour générer une paire de clés de chiffrement de clé symétriques, puis la clé de content-authenticated-encryption est chiffrée dans la paire de clés de chiffrement de clé symétriques ;

   Clés symétriques de chiffrement de clé : la clé de content-authenticated-encryption est chiffrée dans une clé de chiffrement de clé symétrique précédemment distribuée ; et

   Mots de passe : la clé de content-authenticated-encryption est chiffrée dans une clé de chiffrement de clé déduite d'un mot de passe ou autre valeur de secret partagé.

3. Pour chaque receveur, la clé de chiffrement chiffrée de content-authenticated-encryption et les autres informations spécifiques du receveur sont collectées dans une valeur RecipientInfo, définie au paragraphe 6.2 de la [RFC3852].

4. Tous les attributs qui sont à authentifier mais non à chiffrer sont collectés dans les attributs authentifiés.

5. Les attributs collectés dans l'étape 4 sont authentifiés et le contenu de CMS est authentifié et chiffré avec la clé de content-authenticated-encryption. Si l'algorithme de chiffrement authentifié exige soit des données authentifiés supplémentaires (AAD, *additional authenticated data*) soit que le contenu soit bourré à un multiple d'une certaine taille

de bloc, alors le bourrage est ajouté comme décrit au paragraphe 6.3 de la [RFC3852].

6. Tous les attributs qui sont à fournir sans authentification ou chiffrement sont collectés dans les attributs non authentifiés.

7. Les valeurs de RecipientInfo pour tous les receveurs, les attributs authentifiés, les attributs non authentifiés, et le contenu authentifié et chiffré sont collectés ensemble pour former une valeur AuthEnvelopedData comme défini au paragraphe 2.1.

Un receveur ouvre l'enveloppe numérique en déchiffrant une des clés chiffrées de content-authenticated-encryption, et en utilisant ensuite la clé récupérée pour déchiffrer et vérifier l'intégrité du contenu authentifié et chiffré ainsi que l'intégrité des attributs authentifiés.

Le receveur DOIT vérifier l'intégrité du contenu reçu avant le libérer aucune information, en particulier le texte en clair du contenu. Si la vérification d'intégrité échoue, le receveur DOIT détruire tout le texte en clair du contenu.

Cette section est divisée en trois paragraphes. Le premier décrit le type de contenu AuthEnvelopedData, le second décrit le processus d'authentification et de chiffrement, et le troisième décrit le processus de chiffrement de clé.

2.1 Type AuthEnvelopedData

L'identifiant d'objet suivant identifie le type de contenu authenticated-enveloped-data :

IDENTIFIANT D'OBJET id-ct-authEnvelopedData ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) ct(1) 23 }

Le type de contenu authenticated-enveloped-data DOIT avoir le type ASN.1 AuthEnvelopedData :

```
AuthEnvelopedData ::= SEQUENCE {
  version    CMSVersion,
  originatorInfo    [0] IMPLICIT OriginatorInfo FACULTATIF,
  recipientInfos   RecipientInfos,
  authEncryptedContentInfo   EncryptedContentInfo,
  authAttrs     [1] IMPLICITE AuthAttributes FACULTATIF,
  mac    MessageAuthenticationCode,
  unauthAttrs [2] IMPLICITE UnauthAttributes FACULTATIF }
```

Les champs du type AuthEnvelopedData ont la signification suivante :

version est le numéro de version de la syntaxe. Il DOIT être réglé à 0.

originatorInfo fournit facultativement des informations sur l'origine. Il n'est présent que si c'est exigé par l'algorithme de gestion de clés. Il peut contenir des certificats et des listes de révocation de certificat (CRL, *Certificate Revocation List*) et le type OriginatorInfo est défini au paragraphe 6.1 de la [RFC3852].

recipientInfos est une collection d'informations par receveur. Il DOIT y avoir au moins un élément dans la collection. Le type RecipientInfo est défini au paragraphe 6.2 of [RFC3852].

authEncryptedContentInfo est contenu authentifié et chiffré. Le type de contenu de CMS enveloped-data utilise le même type pour porter le contenu chiffré. Le type EncryptedContentInfo est défini au paragraphe 6.1 de la [RFC3852].

authAttrs contient facultativement les attributs authentifiés. Le type de contenu de CMS authenticated-data utilise le même type pour porter les attributs authentifiés. L'élément authAttrs DOIT être présent si le type de contenu porté dans EncryptedContentInfo n'est pas id-data. Les attributs authentifiés DOIVENT être codés en DER, même si le reste de la structure AuthEnvelopedData est codé en BER. Le type AuthAttributes est défini au paragraphe 9.1 de la [RFC3852] ; cependant, dans ce cas, l'attribut Résumé de message NE DEVRAIT PAS être inclus. Les types d'attribut utiles sont définis à la Section 11 de la [RFC3852].

mac est la valeur de la vérification d'intégrité (ICV, *integrity check value*) ou le code d'authentification de message (MAC) qui est généré par l'algorithme de chiffrement authentifié. Le type de contenu de CMS authenticated-data utilise le

même type pour porter un MAC. Dans ce cas, le MAC couvre directement les attributs authentifiés et le contenu, et un algorithme de résumé n'est pas utilisé. Le type MessageAuthenticationCode est défini au paragraphe 9.1 de la [RFC3852].

unauthAttrs contient facultativement les attributs non authentifiés. Le type de contenu de CMS authenticated-data utilise le même type pour porter les attributs non authentifiés. Le type UnauthAttributes est défini au paragraphe 9.1 de la [RFC3852]. Les types d'attribut utiles sont définis à la Section 11 de la [RFC3852].

2.2 Processus d'authentification et de chiffrement

La clé content-authenticated-encryption pour l'algorithme désiré de content-authenticated-encryption est généré au hasard.

Si l'algorithme de chiffrement authentifié exige que le contenu soit bourré à un multiple d'une certaine taille de bloc, alors le bourrage DOIT être ajouté comme décrit au paragraphe 6.3 de la [RFC3852]. Cette méthode de bourrage n'est bien définie que si et seulement si la taille de bloc est inférieure à 256 octets.

Si des attributs authentifiés facultatifs sont présents, ils sont alors codés en DER. Un codage séparé du champ authAttrs est effectué pour construire l'entrée de données authentifiées associées (AAD) à l'algorithme de chiffrement authentifié. Pour les besoins de la construction des AAD, l'étiquette IMPLICITE [1] dans le champ authAttrs n'est pas utilisée pour le codage DER : une étiquette universelle ENSEMBLE DE est plutôt utilisée. C'est-à-dire que le codage DER de l'étiquette ENSEMBLE DE, plutôt que l'étiquette IMPLICITE [1], est à inclure dans la construction de l'entrée d'AAD avec la longueur et les octets de contenu de la valeur de authAttrs. Si l'algorithme de chiffrement authentifié exige que les AAD soient bourrées à un multiple d'une certaine taille de bloc, le bourrage DOIT alors être ajouté comme décrit au paragraphe 6.3 de la [RFC3852]. Cette méthode de bourrage n'est bien définie que si et seulement si la taille de bloc est inférieure à 256 octets.

Si il n'y a pas d'attribut facultatif authentifié, alors des bits zéro d'entrée sont fournis pour l'entrée d'AAD à l'algorithme de chiffrement authentifié.

Les entrées à l'algorithme de chiffrement authentifié sont le contenu (les données, qui sont bourrées si nécessaire) les attributs authentifiés codés en DER (les AAD, qui sont bourrées si nécessaire) et la clé content-authenticated-encryption. Sous le contrôle d'une clé content-authenticated-encryption, l'opération de chiffrement authentifié transpose une chaîne arbitraire d'octets (les données) en une autre chaîne d'octets (le texte chiffré) et elle calcule une étiquette d'authentification sur les AAD et les données. Les données chiffrées sont incluses dans le contenu chiffré *(encryptedContent)* authEncryptedContentInfo de AuthEnvelopedData comme une CHAINE D'OCTETS, et l'étiquette d'authentification est incluse dans le MAC de AuthEnvelopedData.

2.3 Processus de chiffrement de clé

L'entrée au processus de chiffrement de clé -- la valeur fournie à l'algorithme de chiffrement de clé du receveur -- est juste la "valeur" de la clé de content-authenticates-encryption.

Toutes les techniques de gestion de clé susmentionnées peuvent être utilisées pour chaque receveur du même contenu chiffré.

3. Considérations sur la sécurité

La présente spécification définit un type de contenu de CMS supplémentaire. Les considérations de sécurité fournies dans la [RFC3852] s'appliquent aussi à ce type de contenu.

De nombreux algorithmes de chiffrement authentifié utilisent un chiffrement de bloc en mode compteur pour fournir le chiffrement. Quand il est utilisé de façon appropriée, le mode compteur fournit une forte confidentialité. Bellare, Desai, Jokipii, et Rogaway montrent dans [BDJR] que les garanties de confidentialité fournies par le mode compteur sont au moins aussi fortes que celles du mode de chaînage de bloc de chiffrement (CBC, *Cipher Block Chaining*) quand on utilise le même chiffrement de bloc.

Malheureusement, il est aisé de faire un mauvais usage du mode compteur. Si les valeurs du bloc compteur sont utilisées pour plus d'une opération de chiffrement avec la même clé, alors le même flux de clés va être utilisé pour chiffrer les deux

textes en clair, et les garanties de confidentialité sont vidées de sens.

Heureusement, le type de contenu de CMS authenticated-enveloped-data fournit tous les outils nécessaires pour éviter une mauvaise utilisation du mode compteur. Toutes les techniques de gestion de clé existantes permettent qu'une clé de chiffrement de contenu fraîche soit générée pour chaque contenu. De plus, les algorithmes existants de chiffrement authentifié qui utilisent le mode compteur prennent en charge l'utilisation d'une valeur imprévisible de nom occasionnel dans le bloc compteur. Cette valeur de nom occasionnel imprévisible (parfois appelée un "sel") devrait être portée dans un paramètre Identifiant d'algorithme.

Les mises en œuvre doivent générer au hasard des clés de chiffrement de contenu authentifié, le bourrage, et les valeurs imprévisibles de nom occasionnel. Aussi, la génération des paires de clés publique/privée s'appuie sur des nombres aléatoires. L'utilisation de générateurs de nombres pseudo-aléatoiress (PRNG, *pseudo-random number generator*) inadéquats pour générer des clés de chiffrement peut résulter en peu ou pas de sécurité. Un attaquant peut trouver beaucoup plus facile de reproduire l'environnement de PRNG qui a produit les clés, et de faire ses recherches sur le petit ensemble résultant de possibilités, plutôt qu'une recherche en force brute sur l'espace de clé entier. La génération de nombres aléatoires de qualité est difficile. La [RFC4086] offre d'importantes lignes directrices dans ce domaine.

Si l'attribut Résumé de message est inclus dans les AuthAttributes, alors la valeur de l'attribut va contenir la valeur de hachage unidirectionnel non chiffrrée du texte en clair du contenu. La divulgation de cette valeur de hachage permet de retracer le contenu, et elle peut être utilisée pour déterminer si le texte en clair correspond à un ou plusieurs contenus candidats. Pour ces raisons, AuthAttributes NE DEVRAIT PAS contenir d'attribut Résumé de message.

La CMS est souvent utilisée pour fournir le chiffrement dans des environnements de messagerie. Dans les environnements de messagerie, diverses formes de messages non sollicités (comme des pourriels et des fausses annonces) représentent un volume significatif de trafic indésiré. Les stratégies d'atténuation présentes pour le trafic de message non désiré impliquent l'analyse du texte en clair des messages. Quand les receveurs acceptent des messages chiffrés non sollicités, ils deviennent encore plus vulnérables au trafic non désiré parce que de nombreuses stratégies d'atténuation présentes vont être incapables d'accéder au texte source. Donc, le logiciel qui reçoit des messages qui ont été chiffrés en utilisant la CMS a besoin de fournir un ou plusieurs mécanismes pour traiter le trafic de messages non désirés. Une approche qui n'exige pas la divulgation du matériel de chiffrement à un serveur est de rejeter ou d'éliminer les messages chiffrés sauf si ils proviennent d'un membre d'une liste de correspondants acceptables.

4. Module ASN.1

```
CMS-AuthEnvelopedData-2007 { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) modules(0)
                                cms-authEnvelopedData(31) }

ÉTIQUETTES DE DÉFINITIONS IMPLICITES ::=
DÉBUT

-- EXPORTE tout
-- Les types et valeurs définis dans ce module sont exportés pour être utilisés dans les autres modules ASN.1. D'autres
applications peuvent les utiliser pour leurs propres besoins.

IMPORTE

-- Importe de la [RFC3852], paragraphe 12.1
  AuthAttributes, CMSVersion, EncryptedContentInfo, MessageAuthenticationCode, OriginatorInfo, RecipientInfos,
   UnauthAttributes
  DE CryptographicMessageSyntax2004
    { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) modules(0) cms-2004(24) } ;

IDENTIFIANT D'OBJET id-ct-authEnvelopedData ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9)
                                                  smime(16) ct(1) 23 }

AuthEnvelopedData ::= SEQUENCE {
   version CMSVersion,
   originatorInfo [0] IMPLICIT OriginatorInfo FACULTATIF,
   receveurInfos RecipientInfos,
```

```
    authEncryptedContentInfo EncryptedContentInfo,
    authAttrs [1] IMPLICIT AuthAttributes FACULTATIF,
    mac MessageAuthenticationCode,
    unauthAttrs [2] IMPLICIT UnauthAttributes FACULTATIF }

FIN -- de CMS-AuthEnvelopedData-2007
```

5. Références

5.1 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)

[RFC3852] R. Housley, "Syntaxe de message cryptographique (CMS)", juillet 2004. *(Obsolète, voir la* RFC5652)

[X.208] Recommandation UIT-T X.208, "Spécification de la notation numéro un de syntaxe abstraite (ASN.1)", Genève, novembre 1988.

[X.209] Recommandation UIT-T X.209, "Spécification des règles de codage de base pour la notation numéro un de syntaxe abstraite (ASN.1)", Genève, 1988.

[X.509] Recommandation UIT-T X.509, "L'annuaire - cadre d'authentification", Genève, 1988.

5.2 Références pour information

[BDJR] Bellare, M., Desai, A., Jokipii, E., et P. Rogaway, "A Concrete Security Treatment of Symmetric Encryption: Analysis of the DES Modes of Operation", Proceedings 38th Annual Symposium on Foundations of Computer Science, 1997.

[RFC4086] D. Eastlake 3rd, J. Schiller, S. Crocker, "Exigences d'aléa pour la sécurité", juin 2005. (*Remplace* RFC1750) (BCP0106)

[RFC5084] R. Housley, "Utilisation des chiffrements authentifiés AES-CCM et AES-GCM dans la syntaxe de message cryptographique (CMS)", novembre 2007. *(P.S.)*

Adresse de l'auteur

Russell Housley
Vigil Security, LLC
918 Spring Knoll Drive
Herndon, VA 20170
USA
mél : housley@vigilsec.com

Déclaration complète de droits de reproduction

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 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.