Groupe de travail Réseau
Request for Comments : 4073
Catégorie : Sur la voie de la normalisation

R. Housley, Vigil Security
mai 2005
Traduction Claude Brière de L'Isle

Protéger plusieurs contenus avec la syntaxe de message cryptographique (CMS)

Statut de ce mémoire
Le présent document spécifie un protocole de l'Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. Prière de se référer à l'édition en cours des "Normes officielles des protocoles de l'Internet" (STD 1) pour connaître l'état de la normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé
Le présent document décrit une convention pour utiliser la syntaxe de message cryptographique (CMS, *Cryptographic Message Syntax*) pour protéger une collection de contenus. Si on le désire, des attributs peuvent être associés au contenu.

Table des Matières

1. Introduction

Le présent document décrit une convention pour utiliser la syntaxe de message cryptographique (CMS, *Cryptographic Message Syntax*) [RFC3852] pour protéger une collection de contenus. Le type de contenu ContentCollection est utilité pour transférer un ou plusieurs contenus, identifiés chacun par un type de contenu. Si on le désire, le type de contenu ContentWithAttributes peut être utilisé pour associer des attributs arbitraires au contenu.

La convention décrite dans le présent document n'est pas nécessaire lorsque la CMS est utilisée avec MIME [RFC3851]. MIME multipart [RFC2045] fournit un mécanisme direct et largement déployé pour porter plus d'un élément de contenu, dont chacun est associé à un type MIME.

Cependant, la CMS n'est pas toujours utilisée avec MIME. Parfois, la CMS est utilisée dans un environnement exclusivement ASN.1 [ASN1]. Dans ce cas, le type de contenu ContentCollection est utilisé pour rassembler plus d'un élément de contenu, chacun ayant un identifiant d'objet pour spécifier le type de contenu.

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].

1.1 Exemple de collection de contenus

Ce paragraphe donne un exemple simple pour illustrer le besoin du type de contenu ContentCollection. Considérons un

collectionneur d'art qui veut vendre une de ses pièces, une urne ancienne grecque appelée une amphore. Le collectionneur veut composer une offre de vente signée numériquement. Cela comporte trois parties. La première partie contient l'offre de vente du propriétaire, incluant le prix demandé. La seconde partie contient une image de haute qualité de l'amphore. La dernière partie contient une appréciation d'un expert en céramiques bien connu. La dernière partie est signée numériquement par l'expert. La Figure 1 illustre la structure, et le type de contenu CMS SignedData est utilisé pour les deux signatures numériques.

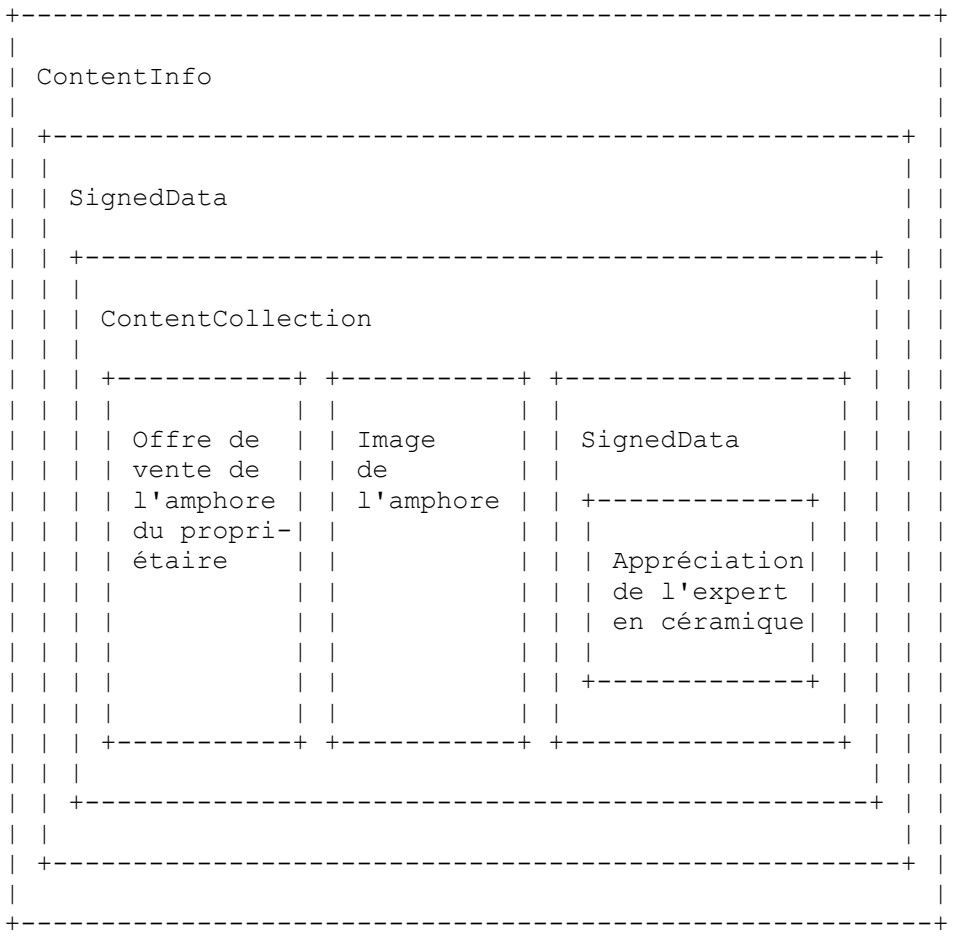
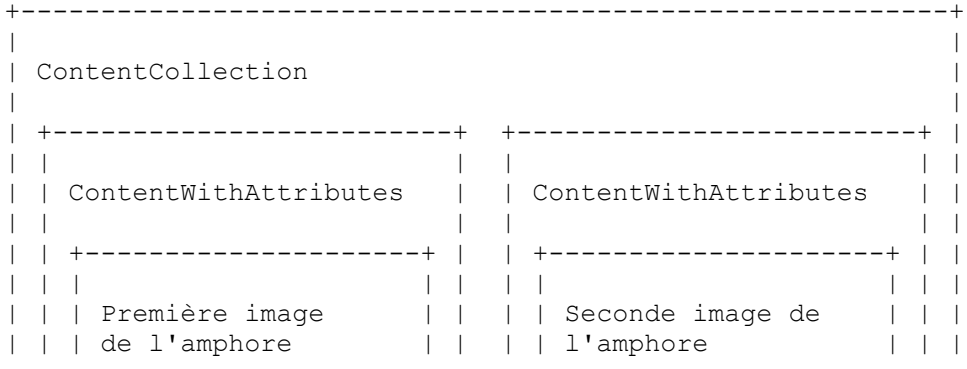


Figure 1. Exemple d'utilisation du type de contenu ContentCollection

1.2. Exemple de contenu avec attributs

Ce paragraphe donne un exemple simple pour illustrer le besoin du type de contenu ContentWithAttributes. Considérons le collectionneur d'art de l'exemple précédent. Au lieu de fournir une seule image de l'amphore, le collectionneur fournit plusieurs images. Pour aider les acheteurs potentiels, le collectionneur attache plusieurs attributs à chaque image. Les attributs donnent des informations sur la résolution de l'image, la date de la prise de vue, le photographe, et ainsi de suite. La Figure 2 illustre la collection d'images, montrant seulement deux images, chacune avec trois attributs. Cette collection entière de contenus d'images pourrait être portée au lieu de la seule image de la Figure 1, lui permettant d'être couverte par la signature numérique du collectionneur.



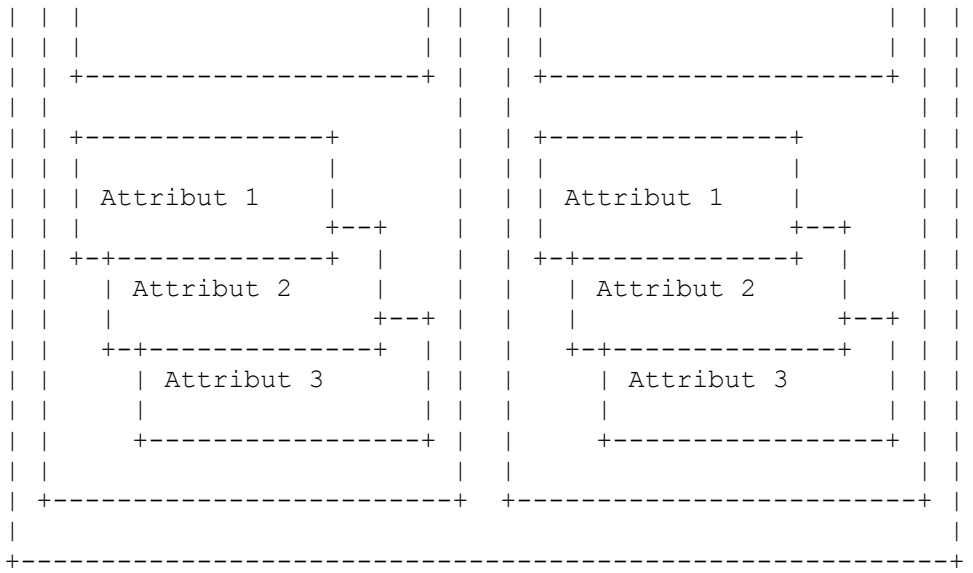


Figure 2. Exemple d'utilisation de type de contenu ContentWithAttributes

2. Type de contenu ContentCollection

Le type de contenu ContentCollection est utilisé pour transférer une collection d'éléments de contenu, identifiés chacun par un type de contenu. La syntaxe traite les contenus avec divers niveaux de protection. Par exemple, une collection de contenus pourrait inclure des types de contenu avec protection CMS ainsi que des types de contenus sans protection. Une collection de contenus est supposée être encapsulée dans un ou plusieurs types de contenus CMS protecteurs, mais ceci n'est pas exigé par la présente spécification.

L'identifiant d'objet suivant désigne le type de contenu "collection de contenus" :

IDENTIFIANT D'OBJET id-ct-contentCollection ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9)
smime(16) ct(1) 19 }

Le contenu ContentCollection a la syntaxe suivante :

ContentCollection ::= SEQUENCE SIZE (1..MAX) OF ContentInfo

ContentCollection contient une séquence de ContentInfo, une pour chaque contenu de la collection. La structure de ContentInfo est définie dans la CMS. L'identifiant d'objet contentType au sein de ContentInfo indique le type du contenu associé. Les mises en œuvre de la présente spécification DEVRAIENT être prêtes à traiter des identifiants d'objet pour les types de contenu SignedData, EncryptedData, EnvelopedData, et AuthenticatedData, comme spécifié dans la [RFC3852]. Les mises en œuvre de la présente spécification DEVRAIENT aussi être prêtes à traiter l'identifiant d'objet pour le type de contenu CompressedData comme spécifié dans la [RFC3274].

3. Type de contenu ContentWithAttributes

Le type de contenu ContentWithAttributes est utilisé pour transférer un seul contenu, qui est identifié par un type de contenu et une collection d'attributs associée à ce contenu. La syntaxe s'accommode d'un nombre arbitraire d'attributs ; cependant, il doit y avoir au moins un attribut.

L'identifiant d'objet suivant désigne le type de contenu ContentWithAttributes :

IDENTIFIANT D'OBJET id-ct-contentWithAttrs ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9)
smime(16) ct(1) 20 }

Le contenu ContentWithAttributes a la syntaxe suivante :

```
ContentWithAttributes ::= SEQUENCE {
   content     ContentInfo,
   attrs       SEQUENCE SIZE (1..MAX) OF Attribute }
```

ContentWithAttributes contient une séquence d'un seul élément ContentInfo suivi par une séquence d'attributs. La structure ContentInfo est définie dans la CMS. L'identifiant d'objet contentType au sein de ContentInfo indique le type du contenu. La structure "Attribute" était à l'origine définie dans [X501], et sa définition est répétée dans la CMS [RFC3852].

4. Considérations sur la sécurité

Le type de contenu ContentCollection est utilisé pour transférer un ou plusieurs contenus, identifiés chacun par un type de contenu. La syntaxe s'accommode de contenus avec divers niveaux de protection. Par exemple, une collection de contenus pourrait inclure des types de contenu avec protection de la CMS ainsi que des types de contenu non protégés. Une collection de contenus est supposée être encapsulée dans un ou plusieurs types de contenus protégés par CMS, mais ceci n'est pas exigé par la présente spécification. Il s'ensuit que les mises en œuvre DOIVENT être prêtes à traiter plusieurs niveaux d'encapsulation.

Les considérations sur la sécurité exposées dans la [RFC3852] sont pertinentes lorsque la CMS est utilisée pour protéger plus d'un contenu en utilisant le type de contenu ContentCollection ou le type de contenu ContentWithAttributes.

5. Références

5.1 Références normatives

[ASN1] Recommandation UIT-T X.208, "Spécification de la notation n° 1 de syntaxe abstraite (ASN.1)". 1988.

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174)

[RFC3274] P. Gutmann, "Type de contenu Données compressées pour la syntaxe de message cryptographique (CMS)", juin 2002. *(P.S.)*

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

5.2 Références pour information

[RFC2045] N. Freed et N. Borenstein, "Extensions de messagerie Internet multi-objets (MIME) Partie 1 : Format des corps de message Internet", novembre 1996. *(D. S., MàJ par* 2184, 2231, 5335.)

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

[X501] Recommandation UIT-T X.501. "L'annuaire – Modèles". 1988.

Appendice A: Module ASN.1

Le module ASN.1 contenu dans cet appendice définit les structures dont la mise en œuvre est nécessaire pour la présente spécification. Il doit être utilisé en conjonction avec les modules ASN.1 de la [RFC3852] et de la [RFC3274].

```
ContentCollectionModule
   { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) modules(0) 26 }

ÉTIQUETTES IMPLICITES DE DÉFINITIONS ::=
DÉBUT
```

```
IMPORTE
  Attribute, ContentInfo
      DE CryptographicMessageSyntax2004 -- [RFC3852]
     { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) modules(0) cms-2001(14) };

-- Type de contenu ContentCollection et identifiant d'objet

IDENTIFIANT D'OBJET  id-ct-contentCollection ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9)
                                                   smime(16) ct(1) 19 }

ContentCollection ::= SEQUENCE SIZE (1..MAX) OF ContentInfo

-- Type de contenu ContentWithAttributes et identifiant d'objet

IDENTIFIANT D'OBJET  id-ct-contentWithAttrs ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9)
                                                   smime(16) ct(1) 20 }

ContentWithAttributes ::= SEQUENCE {
   content     ContentInfo,
   attrs       SEQUENCE SIZE (1..MAX) OF Attribute }

FIN
```

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

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 actuellement fourni par la Internet Society.