Groupe de travail Réseau
Request for Comments : 2984
Catégorie : En cours de normalisation

C. Adams, Entrust Technologies
octobre 2000
Traduction Claude Brière de L'Isle

Utilisation de l'algorithme de chiffrement CAST-128 dans CMS

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

Résumé
Le présent document spécifie comment incorporer CAST-128 (RFC2144) dans la syntaxe de message cryptographique S/MIME comme algorithme supplémentaire pour le chiffrement symétrique. Les OID pertinents et les étapes de traitement sont fournis de façon que CAST-128 puisse être inclus dans la spécification de CMS (RFC2630) pour le contenu symétrique et le chiffrement de clé.

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 le BCP 14, [RFC2119].

1. Motifs

S/MIME (Extensions sécurisées multi objets de messagerie Internet) [RFC2311], [RFC2632] est un ensemble de spécifications pour le transport sûr d'objets MIME. Dans les spécifications actuelles (S/MIME v3) l'algorithme symétrique d'application obligatoire pour le chiffrement du contenu et le chiffrement de clé est le triple-DES (3DES). Bien que ce soit parfaitement acceptable dans de nombreux cas parce que la sécurité de 3DES est généralement considérée comme élevée, pour certains environnements 3DES peut être vu comme trop lent. Pour aider en partie à améliorer de tels soucis de performances, S/MIME a permis qu'un certain nombre d'algorithmes supplémentaires (facultatifs) soient utilisés pour le chiffrement symétrique du contenu et de la clé.

L'algorithme de chiffrement CAST-128 [RFC2144], [Adams] est un chiffrement symétrique bien étudié qui a un certain nombre de caractéristiques séduisantes, incluant des performances relativement élevées et une taille de clé variable (de 40 à 128 bits). Il est disponible sans redevance et sans licence pour des utilisations commerciales et non commerciales dans le monde entier [IPR], et est donc largement utilisé dans nombre d'applications sur l'Internet. Il semble donc être un algorithme de chiffrement facultatif convenable pour S/MIME.

Le présent document décrit comment utiliser CAST-128 au sein de la spécification CMS de S/MIME.

2. Spécification

Cette section donne les OID et les informations de traitement nécessaires pour que CAST-128 soit utilisé pour le chiffrement de contenu et de clé dans CMS.

2.1 OID pour chiffrement de contenu et de clé

CAST-128 est ajouté à l'ensemble des algorithmes de chiffrement symétriques facultatifs dans CMS en fournissant deux identifiants d'objet (OID, *object identifier*) uniques. Un OID définit l'algorithme de chiffrement de contenu et l'autre définit l'algorithme de chiffrement de clé. Ainsi un agent de CMS peut appliquer CAST-128 pour le chiffrement de contenu ou de clé en choisissant l'identifiant d'objet correspondant, en fournissant les paramètres requis, et en commençant le code de programme.

Pour le chiffrement de contenu, l'utilisation de CAST-128 en mode de chaînage de bloc de chiffrement (CBC, *cipher block chaining*) est RECOMMANDÉ. La longueur de clé est variable (de 40 à 128 bits en incréments de un octet).

L'algorithme de chiffrement de contenu CAST-128 en mode CBC a l'identifiant d'objet suivant :

IDENTIFIANT D'OBJET cast5CBC ::= {iso(1) member-body(2) us(840) nt(113533) nsn(7) algorithms(66) 10}

Le paramètre associé à cet identifiant d'objet contient le vecteur initial IV et la longueur de clé

```
cast5CBCParameters ::= SEQUENCE {iv  CHAINE D'OCTETS PAR DEFAUT 0,        -- Vecteur
    d'initialisation
keyLength  ENTIER                                                        -- Longueur de clé, en
    bits
 }
```

On trouvera les commentaires concernant l'utilisation de l'IV dans la [RFC2144].

Les procédures d'enveloppement/développement de clé utilisées pour chiffrer/déchiffrer une clé de chiffrement de contenu CAST-128 avec une clé de chiffrement de clé CAST-128 sont spécifiées au paragraphe 2.2. La génération et la distribution des clés de chiffrement de clé sortent du domaine d'application du présent document.

L'algorithme de chiffrement de clé CAST-128 a l'identifiant d'objet suivant :

```
IDENTIFIANT D'OBJET cast5CMSkeywrap  ::= { iso(1)
   member-body(2) us(840) nt(113533) nsn(7)
   algorithms(66) 15}
```

Le paramètre associé à cet identifiant d'objet ne contient que la longueur de clé (parce que la procédure d'enveloppe de clé elle-même définit comment et quand utiliser un IV):

```
cast5CMSkeywrapParameter ::= ENTIER                    -- longueur de clé, en bits
```

2.2 Enveloppe et développement de clé

L'enveloppe et le développement de clé de CAST-128 est fait conformément à la CMS [RFC2630].

2.2.1 Enveloppe de clé CAST-128

L'enveloppe de clé avec CAST-128 est identique à celle de la [RFC2630], paragraphes 12.6.1 et 12.6.4, avec "RC2" remplacé par "CAST-128" dans l'introduction du 12.6.4. Seules des clés CAST-128 de 128 bits peuvent être utilisées comme clés de chiffrement de clé, et elles DOIVENT être utilisées dans le paramètre cast5CMSkeywrapParameter réglées à 128. Il est RECOMMANDÉ que la taille de la clé de chiffrement de contenu et la taille de la clé de chiffrement de clé soient égales (car la sécurité du contenu sera au plus celle de la plus petite de ces deux valeurs).

2.2.2 Développement de clé CAST-128

Le développement de clé avec CAST-128 est identique à celui de la [RFC2630], paragraphes 12.6.1 et 12.6.5, avec "RC2" remplacé par "CAST-128" dans l'introduction à 12.6.5.

3. Utilisation de CAST-128 dans les clients S/MIME

Un client S/MIME DEVRAIT annoncer l'ensemble des fonctions cryptographiques qu'il prend en charge en utilisant l'attribut de capacités S/MIME. Cet attribut donne une liste partielle des OID des fonctions cryptographiques et DOIT être signé par le client. Les OID des fonctions DEVRAIENT être séparés logiquement en catégories fonctionnelles et DOIVENT être ordonnés selon leur préférence. Si un client S/MIME est obligé de prendre en charge le chiffrement symétrique avec CAST-128, l'attribut "capabilities" DOIT contenir l'OID cast5CBC spécifié ci-dessus dans la catégorie des algorithmes symétriques. Le paramètre associé à cet OID (voir ci-dessus) DOIT être utilisé pour indiquer la longueur de clé acceptée. Par exemple, lorsque la longueur de clé acceptée est 128 bits, la SEQUENCE SMIMECapability qui représente CAST-128 DOIT être codée en DER comme la chaîne hexadécimale suivante :

301106092A864886F67D07420A300402020080.

Lorsque un agent envoyeur crée un message chiffré, il doit décider quel type d'algorithme de chiffrement utiliser. En général, le processus de décision implique des informations obtenues des listes de capacités incluses dans les messages reçus du receveur, ainsi que d'autres informations comme des accords privés, les préférences de l'utilisateur, des restrictions légales, et ainsi de suite. Si les usagers exigent CAST-128 pour le chiffrement symétrique, il DOIT être pris en charge par les clients S/MIME sur les deux côtés envoyeur et receveur, et il DOIT être établi dans les préférences de l'utilisateur.

4. Considérations pour la sécurité

Le présent document spécifie l'utilisation du chiffrement symétrique CAST-128 pour le chiffrement du contenu d'un message de CMS et pour le chiffrement de la clé symétrique utilisée pour chiffrer le contenu d'un message de CMS. Bien que CAST-128 permette d'utiliser des clés de longueur variable, on doit reconnaître que les plus petites tailles de clé (par exemple, 40, 56, ou 64 bits) peuvent être d'une faiblesse inacceptable pour certains environnements. L'utilisation des plus grandes tailles de clé (par exemple, 128 bits) est toujours RECOMMANDÉE (lorsque les lois pertinentes sur l'importation, l'exportation, ou autres, le permettent). Il est aussi RECOMMANDÉ que la taille de la clé de chiffrement de contenu et la taille de la clé de chiffrement de clé soient égales (car la sécurité du contenu sera au plus celle de la plus petite de ces deux valeurs).

Références

[Adams] C. Adams, "Constructing Symmetric Ciphers using the CAST Design Procedure", Designs, Codes, and Cryptography, vol.12, n° 3, novembre 1997, pp.71-104.

[IPR] Voir la page de l'IETF Notices des droits de propriété intellectuelle à http://www.ietf.cnri.reston.va.us/ipr.html

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

[RFC2144] C. Adams, "L'algorithme de chiffrement CAST-128", mai 1997. *(Information)*

[RFC2311] S. Dusse et autres, "Spécification de message S/MIME, version 2", mars 1998. *(Information)*

[RFC2312] S. Dusse, P. Hoffman, B. Ramsdell, J. Weinstein, "Traitement de certificat S/MIME version 2", mars 1998. *(Information)*

[RFC2630] R. Housley, "Syntaxe de message cryptographique", juin 1999. *(Obsolète, voir 3369, 3370) (P.S.)*

[RFC2632] B. Ramsdell, éd., "Traitement de certificat S/MIME version 3", juin 1999. (*Obsolète, voir* RFC3850) *(P.S.)*

[RFC2633] B. Rmasdell, "Spécification de message S/MIME version 3", juin 1999. (*Obsolète, voir* RFC3851) *(P.S.)*

Adresse de l'auteur

Carlisle Adams
Entrust Technologies
1000 Innovation Drive,
Kanata, Ontario, Canada K2K 3E7
mél : cadams@entrust.com

Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d’éditeur des RFC est actuellement fourni par la Internet Society.