Groupe de travail Réseau
Request for Comments : 5084
Catégorie : Sur la voie de la normalisation

R. Housley, Vigil Security
novembre 2007
Traduction Claude Brière de L'Isle

Utilisation du chiffrement authentifié par AES-CCM et AES-GCM dans la syntaxe de message cryptographique (CMS)

Résumé
Le présent document spécifie les conventions pour l'utilisation des algorithmes de chiffrement authentifié AES-CCM et AES-GCM avec le type de contenu authenticated-enveloped-data de la syntaxe de message cryptographique (CMS, *Cryptographic Message Syntax*).

Table des Matières

1. Introduction

Le présent document spécifie les conventions pour l'utilisation de la norme de chiffrement évolué en mode compteur avec code d'authentification de message et chaînage de bloc de chiffrement (AES-CCM, *Advanced Encryption Standard-Counter with Cipher Block Chaining-Message Authentication Code*) et des algorithmes de chiffrement authentifié AES-Galois/mode compteur (GCM) comme algorithme de chifrement de contenu authentifié avec le type de contenu authenticated-enveloped-data [RFC5083] de la syntaxe de message cryptographique [RFC3852].

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 ASN.1

Les valeurs de CMS sont générées en utilisant l'ASN.1 [X.208-88], qui 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].

1.3 AES

Les docteurs Joan Daemen et Vincent Rijmen, tous deux de Belgique, ont développé l'algorithme Rijndael de chiffrement de bloc, et l'ont soumis pour devenir la norme de chiffrement évolué (AES, *Advanced Encryption Standard*). Rijndael a été choisi par le National Institute for Standards and Technology (NIST), et il est spécifié dans la publication [AES] de l'U.S. Federal Information Processing Standard (FIPS). Le NIST a choisi l'algorithme Rijndael pour AES parce que il offre une combinaison de sécurité, performances, efficacité, facilité de mise en œuvre, et souplesse. Spécifiquement, l'algorithme fonctionne bien dans les matériels et logiciels sur une large gamme d'environnements de calcul. Aussi, les très faibles exigences de mémoire de l'algorithme conviennent très bien dans les environnements d'espace restreint. AES est largement utilisé par les organisations, institutions, et individus en dehors du gouvernement des États-Unis d'Amérique.

AES spécifie trois tailles de clés : 128, 192, et 256 bits.

1.4 AES-CCM

Le mode de fonctionnement compteur avec CBC-MAC (CCM) est spécifié dans la [RFC3610]. CCM est un mode de chiffrement de bloc générique de chiffrement authentifié. CCM est défini pour être utilisé avec tout chiffrement de bloc de 128 bits, mais dans le présent document, CCM est utilisé avec le chiffrement de bloc AES.

AES-CCM a quatre entrées : une clé AES, un nom occasionnel, un texte source, et des données authentifiées supplémentaires (AAD, *additional authenticated data*) facultatives. AES-CCM génère deux sorties : un texte chiffré *(ciphertext)* et un code d'authentification de message (aussi appelé une étiquette d'authentification).

Le nom occasionnel est généré par la partie qui effectue l'opération de chiffrement authentifié. Dans la portée de toute clé de chiffrement authentifié, la valeur de nom occasionnel DOIT être unique. C'est-à-dire que l'ensemble de valeurs de nom occasionnel utilisé avec toute clé NE DOIT PAS contenir de valeurs dupliquées. Utiliser le même nom occasionnel pour deux messages différents chiffrés avec la même clé détruit les propriétés de sécurité.

Les AAD sont authentifiées mais pas chiffrées. Donc, les AAD ne sont pas incluses dans le résultat de AES-CCM. Elles peuvent être utilisées pour authentifier les en-têtes de paquet en clair. Dans le type de contenu de CMS authenticated-enveloped-data, les attributs authentifiés comprennent les AAD.

1.5 AES-GCM

Le mode Galois/compteur (GCM, *Galois/Counter Mode*) est spécifié dans [GCM]. GCM est un mode de chiffrement de bloc générique de chiffrement authentifié. GCM est défini pour être utilisé avec tout chiffrement de bloc de 128 bits, mais dans le présent document, GCM est utilisé avec le chiffrement de bloc AES.

AES-GCM a quatre entrées : une clé AES, une valeur d'initialisation (IV), un contenu de texte source, et des données authentifiées supplémentaires (AAD) facultatives. AES-GCM génère deux résultats : un texte chiffré et un code d'authentification de message (aussi appelé une étiquette d'authentification). Pour avoir un ensemble commun de termes pour AES-CCM et AES-GCM, l'IV AES-GCM est appelée un nom occasionnel dans la suite du présent document.

Le nom occasionnel est généré par la partie qui effectue l'opération de chiffrement authentifié. Dans la portée de toute clé de chiffrement authentifié, la valeur de nom occasionnel DOIT être unique. C'est-à-dire que l'ensemble de valeurs de nom occasionnel utilisé avec toute clé NE DOIT PAS contenir de valeurs dupliquées. Utiliser le même nom occasionnel pour deux messages différents chiffrés avec la même clé détruit les propriétés de sécurité.

Les AAD sont authentifiées mais pas chiffrées. Donc, les AAD ne sont pas incluses dans le résultat de AES-GCM. Elles peuvent être utilisées pour authentifier les en-têtes de paquet en clair. Dans le type de contenu de CMS authenticated-enveloped-data, les attributs authentifiés comprennent les AAD.

2. Gestion de clé automatisée

La réutilisation d'une combinaison de nom occasionnel/clé AES-CCM ou AES-GCM détruit les garanties de sécurité. Par

suite, il peut être extrêmement difficile d'utiliser AES-CCM ou AES-GCM de façon sûre quand on utilise des clés configurées de façon statique. Pour être sûres, les mises en œuvre DOIVENT utiliser un système de gestion de clés automatisé [RFC4107].

Le type de contenu de CMS authenticated-enveloped-data prend en charge quatre techniques générales de gestion de clé :

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 symétriques, puis la clé de content-authenticated-encryption est chiffrée dans la paire de clés 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.

Toutes ces techniques de gestion de clé satisfont l'exigence de système automatisé de gestion de clé pour autant qu'une clé de chiffrement de contenu authentifié fraîche est générée pour la protection de chaque contenu. Noter que certaines de ces techniques de gestion de clé utilisent une clé de chiffrement de clé pour chiffrer plus d'une clé de chiffrement de contenu authentifié durant le cycle de vie du système. Tant qu'une clé fraîche de chiffrement de contenu authentifié est utilisée à chaque fois, AES-CCM et AES-GCM peuvent être utilisés en toute sécurité avec le type de contenu de CMS authenticated-enveloped-data.

En plus de ces quatre techniques générales de gestion de clé, la CMS prend en charge d'autres techniques de gestion de clé. Voir au paragraphe 6.2.5 de la [RFC3852]. Comme les propriétés de ces techniques de gestion de clé sont inconnues, aucune déclaration ne peut être faite sur si ces techniques de gestion de clé satisfont l'exigence du système automatisé de gestion de clé. Les concepteurs et les mises en œuvre doivent effectuer leur propre analyse de si une de ces autres techniques de gestion de clé est prise en charge.

3. Algorithmes de chiffrement Content-Authenticated

Cette Section spécifie les conventions employées par les mises en œuvre de CMS qui prennent en charge le chiffrement de contenu authentifié en utilisant AES-CCM ou AES-GCM.

Les identifiants d'algorithme de chiffrement de contenu authentifié sont localisés dans le champ contentEncryptionAlgorithm de EncryptedContentInfo AuthEnvelopedData.

Les algorithmes de chiffrement de contenu authentifié sont utilisés pour chiffrer le contenu localisé dans le champ encryptedContent de EncryptedContentInfo AuthEnvelopedData et pour fournir le code d'authentification de message pour le champ de MAC AuthEnvelopedData. Noter que le code d'authentification de message fournit la protection de l'intégrité pour les authAttrs AuthEnvelopedData et le encryptedContent de EncryptedContentInfo AuthEnvelopedData.

3.1 AES-CCM

L'algorithme de chiffrement authentifié AES-CCM est décrit dans la [RFC3610]. Un bref résumé des propriétés de AES-CCM est fourni au paragraphe 1.4.

Ni le contenu du texte source ni les entrées facultatives d'AAD n'ont besoin d'être bourrées avant d'invoquer AES-CCM.

Il y a trois identifiants d'algorithme pour AES-CCM, un pour chaque taille de clé AES :

```
IDENTIFIANT D'OBJET aes ::= { joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4)
                                  1 }
IDENTIFIANT D'OBJET id-aes128-CCM ::= { aes 7 }
IDENTIFIANT D'OBJET id-aes192-CCM ::= { aes 27 }
IDENTIFIANT D'OBJET id-aes256-CCM ::= { aes 47 }
```

Avec les trois identifiants d'algorithme AES-CCM, le champ de paramètres AlgorithmIdentifier DOIT être présent, et le champ Paramètres doit contenir un CCMParameter :

```
CCMParameters ::= SEQUENCE {
  aes-nonce         CHAINE D'OCTETS (TAILLE(7..13)),
  aes-ICVlen        AES-CCM-ICVlen DEFAUT 12 }
  AES-CCM-ICVlen ::= ENTIER (4 | 6 | 8 | 10 | 12 | 14 | 16)
```

Le champ de paramètre aes-nonce contient 15 L octets, où L est la taille du champ Longueur. Avec la CMS, la situation normale est que la clé de content-authenticated-encryption soit utilisée pour un seul contenu ; donc, L=8 est RECOMMANDÉ. Voir dans la [RFC3610] une discussion sur le compromis entre la taille maximum de contenu et la taille du nom occasionnel. Dans la portée de toute clé de chiffrement de contenu authentifié, la valeur de nom occasionnel DOIT être unique. C'est-à-dire que l'ensemble des valeurs de nom occasionnel utilisé avec toute clé NE DOIT PAS contenir de valeurs dupliquées.

Le champ de paramètre aes-ICVlen donne la taille du code d'authentification de message. Il DOIT correspondre à la taille en octets de la valeur dans le champ MAC AuthEnvelopedData. Une longueur de 12 octets est RECOMMANDÉE.

3.2 AES-GCM

L'algorithme de chiffrement authentifié AES-GCM est décrit dans [GCM]. Un bref résumé des propriétés de AES-CCM est donné au paragraphe 1.5.

Ni le contenu du texte source ni les entrées facultatives d'AAD n'ont besoin d'être bourrées avant d'invoquer AES-GCM.

Il y a trois identifiants d'algorithme pour AES-GCM, un pour chaque taille de clé AES :

```
IDENTIFIANT D'OBJET aes ::= { joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3)
                                    nistAlgorithm(4) 1 }
IDENTIFIANT D'OBJET id-aes128-GCM ::= { aes 6 }
IDENTIFIANT D'OBJET id-aes192-GCM ::= { aes 26 }
IDENTIFIANT D'OBJET id-aes256-GCM ::= { aes 46 }
```

Avec les trois identifiants d'algorithme AES-GCM, le champ de paramètres AlgorithmIdentifier DOIT être présent, et le champ Paramètres doit contenir un GCMParameter :

```
GCMParameters ::= SEQUENCE {
  aes-nonce       CHAINE D'OCTETS,              -- la taille recommandée est 12 octets
  aes-ICVlen      AES-GCM-ICVlen DEFAUT 12 }

AES-GCM-ICVlen ::= ENTIER (12 | 13 | 14 | 15 | 16)
```

aes-nonce est la valeur d'initialisation AES-GCM. La spécification de l'algorithme permet au nom occasionnel d'avoir tout nombre de bits entre 1 et 2^64. Cependant, l'utilisation de CHAINE D'OCTETS au sein de GCMParameters exige que le nom occasionnel soit un multiple de 8 bits. Dans la portée de toute clé de content-authenticated-encryption, la valeur du nom occasionnel DOIT être unique, mais elles n'ont pas besoin d'avoir des longueurs égales. Une valeur de nom occasionnel de 12 octets peut être traitée plus efficacement, de sorte que cette longueur est RECOMMANDÉE.

Le champ de paramètre aes-ICVlen donne la taille du code d'authentification de message. Il DOIT correspondre à la taille en octets de la valeur dans le champ MAC AuthEnvelopedData. Une longueur de 12 octets est RECOMMANDÉE.

4. Considérations sur la sécurité

AES-CCM et AES-GCM utilisent le chiffrement de bloc AES 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, la CMS AuthEnvelopedData fournit tous les outils nécessaires pour éviter une mauvaise utilisation du mode compteur. La gestion de clé automatisée est discutée à la Section 2.

Il y a des attaques très génériques de précalcul contre l'utilisation de tout chiffrement de bloc en mode compteur qui permettent une attaque par interposition contre les clés [H], [B], [MF]. AES-CCM et AES-GCM utilisent tous deux le mode compteur pour le chiffrement. Ces attaques de précalcul exigent la création et la recherche d'énormes tableaux de texte chiffré associé au texte source connu et aux clés connues. En supposant que les ressources de mémoire et de processeur sont disponibles pour une attaque de précalcul, alors la force théorique de tout chiffrement de bloc en mode compteur est limitée à 2^(n/2) bits, où n est le nombre de bits de la clé. L'utilisation de longues clés est la meilleure contre-mesure contre les attaques de précalcul. L'utilisation d'une valeur de nom occasionnel imprévisible dans le bloc compteur augmente significativement la taille du tableau que l'attaquant doit calculer pour monter une attaque de précalcul réussie.

Les mises en œuvre doivent générer au hasard des clés de chiffrement de contenu authentifié. L'utilisation de générateurs de nombres pseudo-aléatoires (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.

5. Références

5.1 Références normatives

[AES] NIST, FIPS PUB 197, "Advanced Encryption Standard (AES)", novembre 2001.

[GCM] Dworkin, M., "NIST Special Publication 800-38D, "Recommendation for Block Cipher Modes of Operation: Galois/mode counter (GCM) and GMAC", U.S. National Institute of Standards and Technology http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf

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

[RFC3610] D. Whiting, R. Housley, N. Ferguson, "Compteur avec CBC-MAC (CCM)", septembre 2003. *(Information)*

[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

[B] Biham, E., "How to Forge DES-Encrypted Messages in 2^28 Steps", Technion Computer Science Department Technical Report CS0884, 1996.

[BDJR] Bellare, M., Desai, A., Jokipii, E., and 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.

[H] Hellman, M. E., "A cryptanalytic time-memory trade-off", IEEE Transactions on Information Theory, juillet 1980, pp. 401-406.

[MF] McGrew, D., et S. Fluhrer, "Attacks on Additive Encryption of Redundant Plaintext et Implications on Internet Security", The Proceedings of the Seventh Annual Workshop on Selected Areas in Cryptography (SAC 2000), Springer-Verlag, août 2000.

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

[RFC4107] S. Bellovin, R. Housley, "Lignes directrices pour la gestion des clés de chiffrement", juin 2005. (BCP0107)

[RFC5083] R. Housley, "Type de contenu Authenticated-Enveloped-Data dans la syntaxe de message cryptographique (CMS)", novembre 2007. *(P.S. ; MàJ* RFC3852)

Appendice. Module ASN.1

```
CMS-AES-CCM-and-AES-GCM
  { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) modules(0) cms-aes-ccm-et-gcm(32) }

ÉTIQUETTES DE DÉFINITIONS IMPLICITES ::= DÉBUT

-- EXPORTE tout

-- Identifiants d'objet

IDENTIFIANT D'OBJET aes ::= { joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4)
                                  1 }

IDENTIFIANT D'OBJET id-aes128-CCM ::= { aes 7 }

IDENTIFIANT D'OBJET id-aes192-CCM ::= { aes 27 }

IDENTIFIANT D'OBJET  id-aes256-CCM ::= { aes 47 }

IDENTIFIANT D'OBJET id-aes128-GCM ::= { aes 6 }

IDENTIFIANT D'OBJET id-aes192-GCM ::= { aes 26 }

IDENTIFIANT D'OBJET id-aes256-GCM ::= { aes 46 }


-- Paramètres pour AigorithmIdentifier

CCMParameters ::= SEQUENCE {
  aes-nonce        CHAINE D'OCTETS (TAILLE(7..13)),
  aes-ICVlen       AES-CCM-ICVlen DEFAUT 12 }

AES-CCM-ICVlen ::= ENTIER (4 | 6 | 8 | 10 | 12 | 14 | 16)

GCMParameters ::= SEQUENCE {
  aes-nonce       CHAINE D'OCTETS,              -- la taille recommandée est 12 octets
  aes-ICVlen      AES-GCM-ICVlen DEFAUT 12 }

AES-GCM-ICVlen ::= ENTIER (12 | 13 | 14 | 15 | 16)

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