Groupe de travail Réseau
Request for Comments : 4543
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

D. McGrew, Cisco Systems, Inc.
J. Viega, McAfee, Inc.
mai 2006

Utilisation du code d'authentification de message de Galois (GMAC) dans IPsec ESP et AH

Statut du présent 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 "Protocoles officiels de l'Internet" (STD 1) pour voir l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé
Le présent mémoire décrit l'utilisation du code d'authentification de message de Galois (GMAC, *Galois Message Authentication Code*) dans la norme de chiffrement évolué (AES, *Advanced Encryption Standard*) comme mécanisme pour assurer l'authentification de l'origine des données, mais pas la confidentialité, au sein de l'encapsulation de charge utile de sécurité (ESP, *Encapsulating Security Payload*) et de l'en-tête d'authentification (AH, *Authentication Header*) IPsec. GMAC se fonde sur le mode de fonctionnement Galois/compteur (GCM, *Galois/Counter Mode*) et peut être efficacement mis en œuvre dans les matériels à des vitesses de 10 gigabits par seconde et au-dessus, et il convient bien aussi aux mises en œuvre de logiciels.

Table des matières

1. Introduction

Le présent document décrit l'utilisation du mode AES-GMAC comme un mécanisme pour l'authentification de l'origine des données dans ESP [RFC4303] et AH [RFC4302]. On se réfère à ces méthodes comme respectivement ENCR_NULL_AUTH_AES_GMAC et AUTH_AES_GMAC. ENCR_NULL_AUTH_AES_GMAC est un accompagnement pour le mode ESP Galois/compteur [RFC4106] d'AES, qui assure l'authentification ainsi que la confidentialité. ENCR_NULL_AUTH_AES_GMAC est destiné aux cas où la confidentialité n'est pas désirée. Comme GCM, GMAC est efficace et sûr, et convient pour les mises en œuvre de matériels à hauts débits. ENCR_NULL_AUTH_AES_GMAC et AUTH_AES_GMAC sont conçus de telle façon que le coût incrémentaire de mise en œuvre, dans AES-GCM-ESP, est faible.

Le présent document ne traite pas des détails de la mise en œuvre de GCM ou GMAC. Ces détails se trouvent dans [GCM], avec les vecteurs d'essai.

1.1 Conventions utilisées dans le document

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].

2. AES-GMAC

GMAC est un mode de fonctionnement de chiffrement de bloc qui assure l'authentification de l'origine des données. Il est défini dans les termes de l'opération de chiffrement authentifié de CGM comme suit. L'opération de chiffrement authentifié CGM a quatre entrées : une clé secrète, un valeur d'initialisation (IV), un texte source, et une entrée pour des données authentifiées supplémentaires (AAD, *additional authenticated data*). Il a deux sorties, un texte chiffré dont la longueur est identique au texte source et une étiquette d'authentification. GMAC est le cas particulier de GCM dans lequel le texte source a une longueur de zéro. Le résultat de texte chiffré (de longueur zéro) est ignoré, bien sûr, de sorte que le seul résultat de la fonction est l'étiquette d'authentification. Dans ce qui suit, on décrit comment la IV GMAC et les AAD sont formées à partir des champs ESP et AH, et comment les paquets ESP et AH sont formés à partir de l'étiquette d'authentification.

On se réfère ci-dessous à l'entrée d'IV AES-GMAC comme à un nom occasionnel, afin de le distinguer des champs IV dans les paquets. La même combinaison de nom occasionnel et de clé NE DOIT PAS être utilisée plus d'une fois, car la réutilisation d'une combinaison de nom occasionnel et de clé détruit les garanties de sécurité de AES-GMAC.

À cause de cette restriction, il peut être difficile d'utiliser ce mode de façon sûre quand on utilise des clé à configuration statique. Pour une bonne sécurité, les mises en œuvre DOIVENT utiliser un système de gestion de clé automatique, comme l'échange de clé Internet (IKE, *Internet Key Exchange*) (soit la version deux [RFC4306] soit la version une [RFC2409]) pour s'assurer que cette exigence est satisfaite.

3. Utilisation de AES-GMAC dans ESP

L'algorithme AES-GMAC pour ESP est défini comme un algorithme ESP "en mode combiné" (voir le paragraphe3.2.3 de la [RFC4303]) plutôt qu'un algorithme d'intégrité ESP. Il est appelé ENCR_NULL_AUTH_AES_GMAC pour souligner le fait qu'il n'effectue pas de chiffrement et n'assure aucune confidentialité.

Raison : ESP n'a aucune disposition pour que les transformations d'intégrité placent une valeur d'initialisation au sein du champ Charge utile ; seules les transformations de chiffrement sont supposées utiliser des IV. Définir GMAC comme une transformation de chiffrement évite ce problème, et permet à GMAC de bénéficier du même traitement en parallèle que le fait GCM.

Comme tous les modes combinés d'ESP, il est enregistré dans IKEv2 comme une transformation de chiffrement, ou transformation de "Type 1". Il NE DOIT PAS être utilisé conjointement avec toute autre transformation de chiffrement ESP (dans une encapsulation ESP particulière). Si la confidentialité est désirée, alors ESP GCM [RFC4106] DEVRAIT être utilisé à la place.

3.1 Valeur d'initialisation

Avec ENCR_NULL_AUTH_AES_GMAC, une valeur d'initialisation (IV) explicite est incluse dans la charge utile ESP, à la sortie de ce champ. La IV DOIT faire huit octets. Pour une certaine clé, la IV NE DOIT PAS se répéter. La façon la plus naturelle de satisfaire cette exigence est de régler la IV en utilisant un compteur, mais les mises en œuvre sont libres de régler le champ IV de toute façon qui garantisse son unicité, comme un registre à décalage avec réinjection linéaires (LFSR, *linear-feedback shift register*) . Noter que l'envoyeur peut utiliser toute méthode de génération d'IV qui satisfait à l'exigence d'unicité sans coordination avec le receveur.

3.2 Format de nom occasionnel

Le nom occasionnel passé à l'algorithme d'authentification AES-GMAC a la disposition suivante :

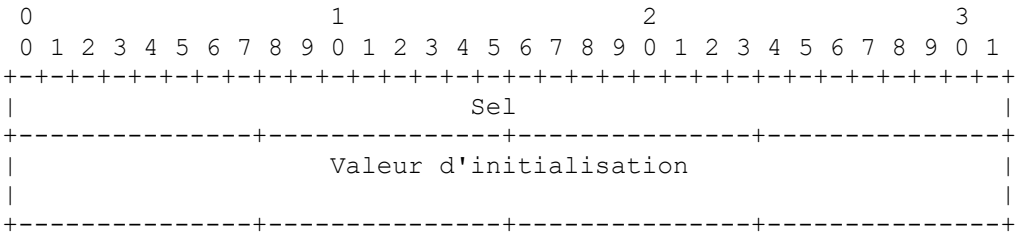

Figure 1 : Format de nom occasionnel

Les composants du nom occasionnel sont les suivants :

Sel : le champ Sel est une valeur de quatre octets qui est allouée au début de l'association de sécurité, et qui reste constante pour toute la vie de l'association de sécurité. Le sel DEVRAIT être imprévisible (c'est-à-dire, choisi au hasard) avant son choix, mais n'a pas besoin d'être secret. On décrit comment régler le sel pour une association de sécurité établie via l'échange de clé Internet au paragraphe 5.4.

Valeur d'initialisation : le champ IV est décrit au paragraphe 3.1.

3.3 Construction AAD

L'intégrité et l'authentification d'origine des données sont fournies par les champs SPI, Numéro de séquence (étendu), Charge utile authentifiée, Bourrage, Longueur de bourrage, et Prochain en-tête. C'est fait en incluant ces champs dans le champ Données authentifiées supplémentaires (AAD, *Additional Authenticated Data*) de AES-GMAC. Deux formats de AAD sont définis : un pour les numéros de séquence de 32 bits, et un pour les numéros de séquence étendus de 64 bits. Le format avec les numéros de séquence de 32 bits est montré à la Figure 2, et le format avec les numéros de séquence étendus de 64 bits est montré à la Figure 3.

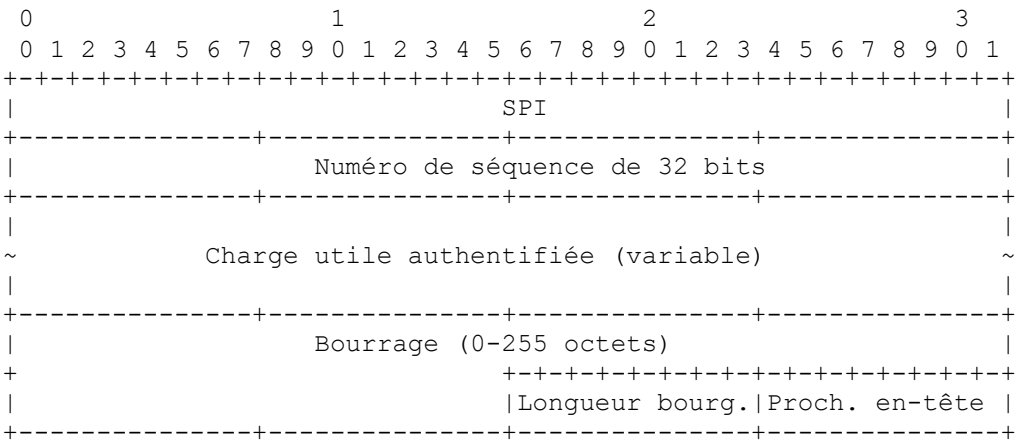

Figure 2 : Format d'AAD avec numéro de séquence de 32 bits

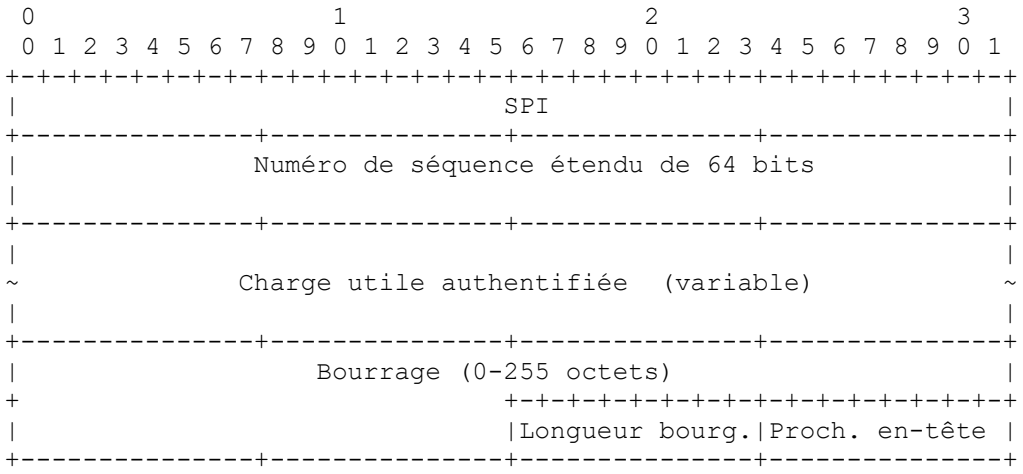

Figure 3 : Format d'AAD avec numéro de séquence étendu de 64-bits

L'utilisation de numéros de séquence de 32 bits plutôt que numéros étendus de 64 bits est déterminée par le protocole de gestion d'association de sécurité (SA) qui a été utilisé pour créer la SA. Pour IKEv2 [RFC4306] c'est négocié via le type 5 de transformation, et par défaut pour ESP on utilise les numéros de séquence étendus de 64 bits en l'absence de négociation (par exemple, voir le paragraphe 2.2.1 de la [RFC4303]).

3.4 Valeur de vérification d'intégrité

La valeur de vérification d'intégrité (ICV, *Integrity Check Value*) consiste seulement en l'étiquette d'authentification AES-GMAC. L'étiquette d'authentification NE DOIT PAS être tronquée, afin que la longueur de l'ICV soit de 16 octets.

3.5 Différences avec AES-GCM-ESP

Dans ce paragraphe, on souligne les différences entre la présente spécification et AES-GCM-ESP [RFC4106]. La différence essentielle est que dans le présent document, l'AAD consiste en le SPI, le numéro de séquence, et la charge utile ESP, et que le texte source AES-GCM est de longueur zéro, tandis que dans AES-GCM-ESP, le AAD ne comporte que le SPI et le numéro de séquence, et que le texte source AES-GCM consiste en la charge utile ESP. Ces différences sont illustrées par la Figure 4. Cette figure montre le cas où l'option Numéro de séquence étendu n'est pas utilisée. Quand elle l'est, le champ Numéro de séquence dans la figure serait remplacé par le numéro de séquence étendu.

Il est important de noter que ENCR_NULL_AUTH_AES_GMAC *n'est pas* équivalent à AES-GCM-ESP avec le chiffrement "en moins". Cependant, le calcul de l'ICV effectué dans les deux cas est similaire à cause de la structure de la fonction GHASH [GCM].

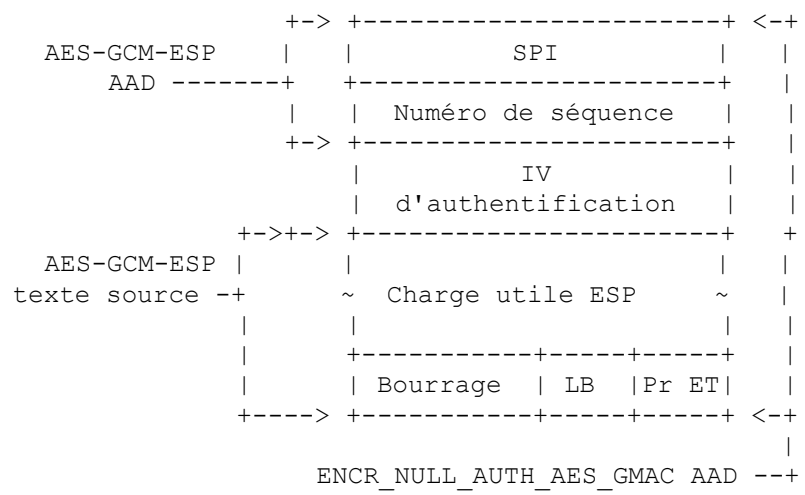

Figure 4 : Différences entre ENCR_NULL_AUTH_AES_GMAC et AES-GCM-ESP

3.6 Expansion de paquet

L'IV ajoute huit octets supplémentaires au paquet et l'ICV ajoute 16 octets supplémentaires. Ce sont les seules sources d'expansion de paquet, en dehors des 10 à 13 octets pris par les champs ESP SPI, Numéro de séquence, Bourrage, Longueur de bourrage, et Prochain en-tête (si la quantité minimale de bourrage est utilisée).

4. Utilisation de AES-GMAC dans AH

Dans AUTH_AES_GMAC, le champ Données d'authentification AH consiste en l'IV et l'étiquette d'authentification, comme le montre la Figure 5. À la différence du cas AH usuel, le champ Données d'authentification contient à la fois une entrée de l'algorithme d'authentification (l'IV) et le résultat de l'algorithme d'authentification (l'étiquette). Aucun bourrage n'est requis dans le champ Données d'authentification, parce que sa longueur est un multiple de 64 bits.

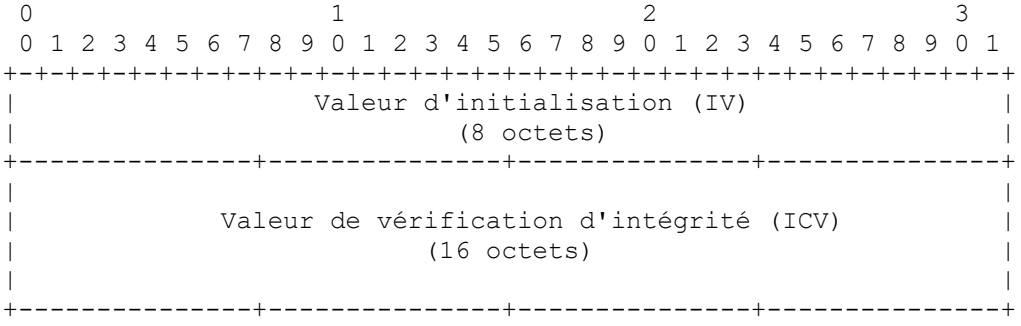

Figure 5 : Format des données d'authentification AUTH_AES_GMAC

L'IV est comme décrite au paragraphe 3.1. La valeur de vérification d'intégrité (ICV) est décrite au paragraphe 3.4.

L'entrée de nom occasionnel GMAC est formée comme décrit au paragraphe 3.2. L'entrée d'AAD GMAC consiste en les données authentifiées comme défini au paragraphe 3.1 de la [RFC4302]. Ces valeurs, fournies selon cet algorithme, avec la clé secrète et l'étiquette d'authentification résultante, données comme résultat, sont utilisées pour former l'ICV.

5. Conventions IKE

Cette section décrit les conventions utilisées pour générer le matériel de chiffrement et les valeurs de sel à utiliser avec ENCR_NULL_AUTH_AES_GMAC et AUTH_AES_GMAC en utilisant l'échange de clé Internet (IKE) versions une [RFC2409] et deux [RFC4306].

5.1 Identifiant de phase 1

Le présent document ne spécifie pas les conventions d'utilisation de AES-GMAC pour les négociations de IKE phase 1. Pour utiliser AES-GMAC de cette manière, une spécification distincte sera nécessaire , et un identifiant d'algorithme de chiffrement devra être alloué. Les mises en œuvre DEVRAIENT utiliser un chiffrement IKE phase 1 qui soit au moins aussi fort que AES-GMAC. L'utilisation de AES-CBC [RFC3602] avec la même taille de clé AES qu'utilisé par ENCR_NULL_AUTH_AES_GMAC ou AUTH_AES_GMAC est RECOMMANDÉE.

5.2 Identifiant de phase 2

Pour les négociations de IKE phase 2, l'IANA a alloué des identifiants comme décrit à la Section 9.

5.3 Attribut de longueur de clé

AES-GMAC peut être utilisé avec une des trois longueurs de clé AES. La façon dont la longueur de clé est indiquée est différente pour AH et ESP.

Pour AH, chaque longueur de clé a son propre identifiant de transformation d'intégrité séparé et son propre nom d'algorithme (Section 9). L'attribut Longueur de clé IKE NE DOIT PAS être utilisé avec ces identifiants. Cette transformation NE DOIT PAS être utilisée avec ESP.

Pour ESP, il y a un seul identifiant de transformation de chiffrement (qui représente la transformation combinée) (Section 9). L'attribut Longueur de clé IKE DOIT être utilisé avec chaque utilisation de cet identifiant pour indiquer la longueur de clé. L'attribut Longueur de clé DOIT avoir une valeur de 128, 192, ou 256.

5.4 Matériel de chiffrement et valeurs de sel

IKE utilise une fonction pseudo aléatoire (PRF, *pseudo-random function*) pour déduire le matériel de chiffrement. La PRF est itérée pour déduire du matériel de chiffrement de taille arbitraire, appelé KEYMAT. Le matériel de chiffrement est extrait de la chaîne de sortie sans considération des frontières.

La taille de KEYMAT pour ENCR_NULL_AUTH_AES_GMAC et AUTH_AES_GMAC DOIT être de quatre octets de plus que nécessaire pour la clé AES associée. Le matériel de chiffrement est utilisé comme suit :

ENCR_NULL_AUTH_AES_GMAC avec clé de 128 bits et AUTH_AES_128_GMAC
Le KEYMAT demandé pour chaque clé AES-GMAC fait 20 octets. Les 16 premiers octets sont la clé AES de 128 bits, et les quatre octets restants sont utilisés comme valeur de sel dans le nom occasionnel.

ENCR_NULL_AUTH_AES_GMAC avec clé de 192 bits et AUTH_AES_192_GMAC
Le KEYMAT demandé pour chaque clé AES-GMAC fait 28 octets. Les 24 premiers octets sont la clé AES de 192 bits, et les quatre octets restants sont utilisés comme valeur de sel dans le nom occasionnel.

ENCR_NULL_AUTH_AES_GMAC avec clé de 256 bits et AUTH_AES_256_GMAC
Le KEYMAT demandé pour chaque clé AES-GMAC fait 36 octets. Les 32 premiers octets sont la clé AES de 256 bits, et les quatre octets restants sont utilisés comme valeur de sel dans le nom occasionnel.

6. Valeurs d'essai

L'Appendice B de [GCM] fournit les vecteurs d'essai qui vont aider à la mise en œuvre avec AES-GMAC.

7. Considérations sur la sécurité

Dans la mesure ou la couverture de l'authentification est différente dans AES-GCM-ESP et dans la présente spécification (voir la Figure 4) il faut souligner que les deux spécifications sont sûres. Dans ENCR_NULL_AUTH_AES_GMAC, la IV n'est incluse ni dans le texte source ni dans les données authentifiées supplémentaires. Cela n'a pas d'effet négatif sur la sécurité, parce que le champ IV ne fournit d'entrée que pour l'IV GMAC, qui n'est pas obligée d'être authentifiée (voir [GCM]). Dans AUTH_AES_GMAC, l'IV est incluse dans les données authentifiées supplémentaires. Ce fait n'a pas d'effet négatif sur la sécurité ; il résulte de la propriété que GMAC est sûr même contre les attaques dans lesquelles l'adversaire peut manipuler l'IV et le message. Même un adversaire qui a ces puissantes capacités ne peut pas falsifier une étiquette d'authentification pour un message (autre qu'un qui a été soumis à l'oracle de message choisi). Comme un tel adversaire pourrait facilement choisir des messages qui contiennent les IV avec lesquelles ils correspondent, il n'y a pas de problème de sécurité avec l'inclusion de l'IV dans l'AAD.

GMAC est d'une sûreté démontrable contre des adversaires qui peuvent choisir des textes source adaptables, des ICV et le champ AAD, dans les conditions de chiffrement standard (en gros, que le résultat du chiffrement sous-jacent sous une clé choisie au hasard soit indistinguable d'un résultat choisi au hasard). Essentiellement, cela signifie que, utilisé dans les limites de ces paramètres, un cassage de GMAC implique celui du chiffrement de bloc sous-jacent. La preuve de sécurité est disponible dans [GCMP].

Le plus important souci de sécurité est que l'IV ne se répète jamais pour une clé donnée. En partie, ceci est traité par l'interdiction d'utiliser AES-GMAC avec des clés configurées statiquement, comme discuté à la Section 2.

Quand IKE est utilisé pour établir des clés fraîches entre deux entités homologues, des clés séparées sont établies pour les deux flux de trafic. Si un mécanisme différent est utilisé pour établir des clés fraîches, un qui établit seulement une clé pour protéger les paquets, il y a alors une forte probabilité pour que les homologues choisissent les mêmes valeurs d'initialisation pour certains paquets. Donc, pour éviter des collisions de compteur de blocs, les mise en œuvre de ESP ou AH qui permettent l'utilisation de la même clé pour protéger les paquets avec le même homologue DOIVENT s'assurer que les deux homologues allouent des valeurs de sel différentes à l'association de sécurité.

L'autre considération est que, comme avec tout mode de fonctionnement en chiffrement de bloc, la sécurité de toutes les données protégées sous une certaine association de sécurité diminue légèrement à chaque message.

Pour protéger contre ce problème, les mises en œuvre DOIVENT générer une clé fraîche avant d'avoir traité 2^64 blocs de données avec une certaine clé. Noter qu'il est impossible d'atteindre cette limite quand on utilise des numéros de séquence de 32 bits.

Noter que, pour chaque message, GMAC n'appelle le chiffrement de bloc qu'une seule fois.

8. Raison de la conception

La présente spécification a été conçue comme similaire à AES-GCM-ESP [RFC4106] autant que possible. On réutilise le dessin et l'expérience de mise en œuvre de cette spécification. On inclut les trois tailles de clé AES car AES-GCM-ESP les prend toutes trois en charge, et les plus grandes tailles de clé donnent aux futurs utilisateurs plus d'options de haute sécurité.

9. Considérations relatives à l'IANA

L'IANA a alloué les paramètres IKEv2 suivants. Pour l'utilisation de AES GMAC dans AH, les identifiants de transformation d'intégrité (type 3) suivants ont été alloués :
"9" pour AUTH_AES_128_GMAC
"10" pour AUTH_AES_192_GMAC
"11" pour AUTH_AES_256_GMAC

Pour l'utilisation de AES-GMAC dans ESP, l'identifiant de transformation de chiffrement (type 1) suivant a été alloué :
"21" pour ENCR_NULL_AUTH_AES_GMAC

10. Remerciements

Nos discussions avec Fabio Maino et David Black ont significativement amélioré cette spécification, et Tero Kivinen nous a fourni d'utiles commentaires. Steve Kent nous a donné des conseils sur les interactions ESP. Le présent travail suit étroitement le modèle de AES-GCM, qui lui-même suit étroitement la transformation AES-CCM de Russ Housley [RFC4309]. De plus, le mode de fonctionnement GCM a été à l'origine conçu comme une amélioration du mode CWC [CWC] dans lequel Doug Whiting et Yoshi Kohno ont participé. Nous exprimons nos remerciements à Fabio, David, Tero, Steve, Russ, Doug, et Yoshi.

9. Références

9.1 Références normatives

[GCM] McGrew, D. and J. Viega, "The Galois/Counter Mode of Operation (GCM)", Submission to NIST, janvier 2004.

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

[RFC3602] S. Frankel, R. Glenn, S. Kelly, "Algorithme de chiffrement AES-CBC et utilisation avec IPsec", septembre 2003. *(P.S.)*

11.2 Références pour information

[CWC] Kohno, T., Viega, J., and D. Whiting, "CWC: A high-performance conventional authenticated encryption mode", Fast Software Encryption. février 2004.

[GCMP] McGrew, D. and J. Viega, "The Security and Performance of the Galois/Counter Mode (GCM)", Proceedings of INDOCRYPT '04, décembre 2004.

[RFC2409] D. Harkins et D. Carrel, "L'échange de clés Internet (IKE)", novembre 1998. *(Obsolète, voir la* RFC4306)

[RFC4106] J. Viega, D. McGrew, "Utilisation du mode Galois/Compteur (GCM) dans une encapsulation IPsec de charge utile de sécurité (ESP)", juin 2005. *(P.S.)*

[RFC4302] S. Kent, "En-tête d'authentification IP", décembre 2005. *(P.S.)*

[RFC4303] S. Kent, "Encapsulation de charge utile de sécurité dans IP (ESP)", décembre 2005. (*Remplace* RFC2406) *(P.S.)*

[RFC4306] C. Kaufman, "Protocole d'échange de clés sur Internet (IKEv2)", décembre 2005. *(Obsolète, voir la* RFC5996)

[RFC4309] R. Housley, "Utilisation du mode CCM de la norme de chiffrement évolué (AES) avec l'encapsulation de charge utile de sécurité (ESP) dans IPsec", décembre 2005. *(P.S.)*

Adresse des auteurs

David A. McGrew
Cisco Systems, Inc.
510 McCarthy Blvd.
Milpitas, CA 95035
US
téléphone : (408) 525 8651
mél : mcgrew@cisco.com

John Viega
McAfee, Inc.
1145 Herndon Parkway, Suite 500
Herndon, VA 20170
US
mél : viega@list.org

Déclaration complète de droits de reproduction

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 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 administatif (IASA) de l'IETF.