Équipe d'ingénierie de l'Internet (IETF)
Request for Comments : 6407
RFC rendue obsolète : 3547
Catégorie : En cours de normalisation
ISSN : 2070-1721

B. Weis, S. Rowles, Cisco Systems
T. Hardjono, MIT

octobre 2011
Traduction Claude Brière de L'Isle

Domaine d'interprétation de groupe

Résumé
Le présent document décrit le protocole de domaine d'interprétation de groupe (GDOI, *Group Domain of Interpretation*) spécifié dans la RFC3547. GDOI fournit la gestion de clé de groupe pour la prise en charge de communications de groupe sécurisées conformément à l'architecture spécifiée dans la RFC4046. GDOI gère les associations de sécurité de groupe, qui sont utilisées par IPsec et éventuellement d'autres protocoles de sécurité des données. Le présent document remplace la RFC3547.

Statut de ce mémoire
Ceci est un document de l'Internet en cours de normalisation.

Le présent document a été produit par l'équipe d'ingénierie de l'Internet (IETF). Il représente le consensus de la communauté de l'IETF. Il a subi une révision publique et sa publication a été approuvée par le groupe de pilotage de l'ingénierie de l'Internet (IESG). Tous les documents approuvés par l'IESG ne sont pas candidats à devenir une norme de l'Internet ; voir la Section 2 de la RFC5741.

Les informations sur le statut actuel du présent document, tout errata, et comment fournir des réactions sur lui peuvent être obtenues à http://www.rfc-editor.org/info/rfc6407

Table des matières

1. Introduction

Les applications de groupe et de diffusion sûres exigent une méthode par laquelle chaque membre du groupe partage une politique de sécurité et du matériel de clé communs. Le présent document décrit le domaine d'interprétation de groupe (GDOI, *Group Domain of Interpretation*) qui est un domaine d'interprétation (DOI, *Domain of Interpretation*) du protocole d'association de sécurité et de gestion de clé Internet (ISAMKP, *Internet Security Association et Key Management Protocol*) [RFC2408], un système de gestion de clés de groupe. Le GDOI distribue des associations de sécurité (SA, *Security Association*) pour les protocoles d'en-tête d'authentification (AH, *Authentication Header*) IPsec [RFC4302] et d'encapsulation de charge utile de sécurité (ESP, *Encapsulating Security Payload*) [RFC4303] et éventuellement d'autres protocoles de sécurité des données utilisés dans les applications de groupe. Le GDOI utilise le modèle de gestion de clé de groupe défini dans la [RFC4046], et décrit plus généralement par "l'architecture de sécurité de groupe de diffusion groupée" [RFC3740].

Dans ce modèle de gestion de clés de groupe, les participants au protocole GDOI sont un contrôleur de groupe/serveur de clés (GCKS, *Group Controller/Key Server*) et un membre du groupe (GM, *group member*). Un membre du groupe contacte ("s'enregistre auprès") d'un GCKS pour se joindre au groupe. Durant l'enregistrement, l'authentification mutuelle et l'autorisation sont réalisées, après quoi le GCKS distribue la politique actuelle du groupe et le matériel de clés au membre du groupe sur une session authentifiée et chiffrée. Le GCKS peut aussi initier le contact ("changer de clés") avec les membres du groupe pour fournir des mises à jour de la politique du groupe.

ISAKMP définit deux "phases" de négociation (paragraphe 2.3 de la [RFC2408]). Une association de sécurité de phase 1 assure l'authentification mutuelle et l'autorisation, et une association de sécurité qui est utilisée par les participants au protocole pour exécuter un échange de phase 2. Le présent document incorpore (c'est-à-dire, utilise mais ne redéfinit pas) la définition d'association de sécurité de phase 1 du DOI Internet des [RFC2407], [RFC2409]. Bien que les RFC 2407, 2408, et 2409 aient été rendues obsolètes par la [RFC4306] (et ensuite, la [RFC5996]) elles sont utilisées par le présent document parce que les définitions du protocole restent pertinentes pour les protocoles ISAKMP autres que IKEv2.

Le GDOI inclut deux nouveaux échanges (protocoles) ISAKMP de phase 2, ainsi que les nécessaires nouvelles définitions de charge utile à la norme ISAKMP (paragraphe 2.1 de la [RFC2408]). Ces deux nouveaux protocoles sont :

1. L'échange de protocole d'enregistrement GROUPKEY-PULL. Cet échange utilise le comportement "tiré" car le membre initie la restitution de ces SA à partir d'un GCKS. Il est protégé par un protocole ISAKMP de phase 1, comme décrit ci-dessus. Au point culminant d'un échange GROUPKEY-PULL, un membre autorisé du groupe a reçu et installé un ensemble de SA qui représentent la politique du groupe, et il est prêt à participer à des communications de groupe sûres.

2. L'échange de protocole de changement de clé GROUPKEY-PUSH. Le protocole de changement de clé est un datagramme initié ("poussé") par le GCKS, normalement délivré aux membres du groupe en utilisant une adresse de diffusion groupée IP. Le protocole de changement de clés est un protocole ISAKMP, où la politique de chiffrement et le matériel de clés ("Rekey SA") sont inclus dans la politique du groupe distribuée par le GCKS dans l'échange GROUPKEY-PULL. Au point culminant d'un échange GROUPKEY-PUSH, le serveur de clés a envoyé la politique du groupe à tous les membres autorisés du groupe, permettant aux membres receveurs du groupe de participer aux communications de groupe sécurisées. Si une méthode de gestion de groupe est incluse dans la politique du groupe (comme décrit au paragraphe 7.4) à la conclusion de l'échange GROUPKEY-PUSH, certains membres du groupe pourraient avoir perdu leur autorisation et ne plus être capables de participer aux communications de groupe sécurisées.

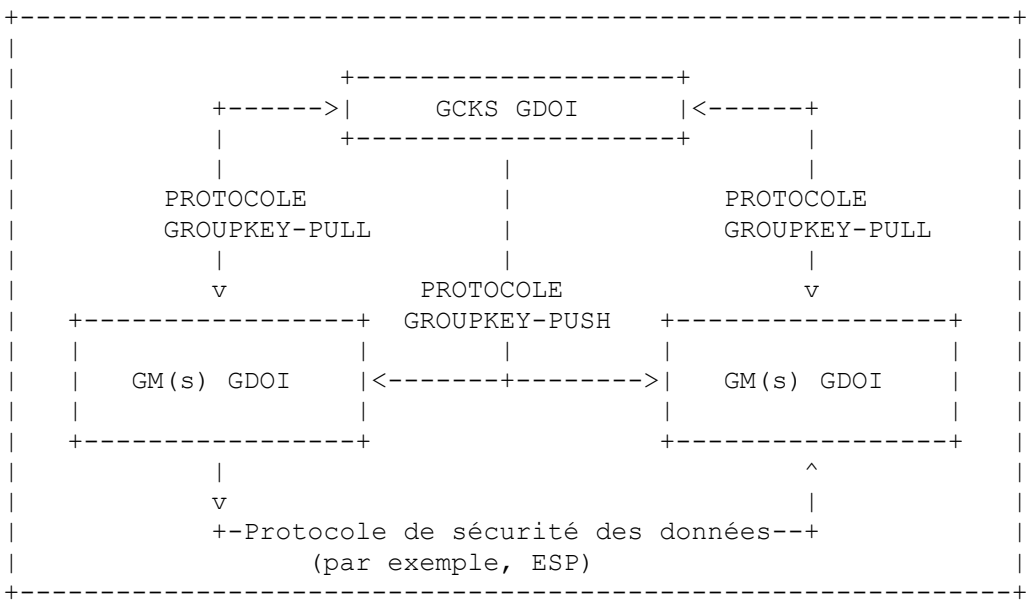


Figure 1 : Modèle de gestion de clé de groupe

Bien que le protocole GROUPKEY-PUSH spécifié par le présent document puisse être utilisé pour rafraîchir la SA Rekey qui protège le protocole GROUPKEY-PUSH, l'utilisation la plus courante de GROUPKEY-PUSH est d'établir le matériel et la politique de chiffrement pour un protocole de sécurité des données.

GDOI définit plusieurs types de charge utile utilisés pour distribuer la politique et le matériel de clés au sein des protocoles GROUPKEY-PULL et GROUPKEY-PUSH : les associations de sécurité (SA), SA KEK, SA TEK, la politique associée au groupe (GAP, *Group Associated Policy*), le numéro de séquence (SEQ), et le téléchargement de clé (KD, *Key Download*). Le format et l'usage de ces charges utiles sont définis dans les sections suivantes de ce mémoire.

En résumé, GDOI est un protocole de gestion d'association de sécurité de groupe : tous les messages GDOI sont utilisés pour créer, entretenir, ou supprimer les associations de sécurité pour un groupe. Comme on l'a décrit plus haut, ces associations de sécurité protègent une ou plusieurs SA de protocole de sécurité des données, une SA Rekey, et/ou d'autres données partagées par les membres du groupe pour les applications de sécurité de diffusion groupée et de groupes.

1.1 Notation des exigences

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 la [RFC2119].

1.2. Terminologie

Les termes clés suivants sont utilisés dans le présent document.

SA de sécurité des données : C'est la politique de sécurité distribuée par un GCKS GDOI qui décrit le trafic que les membres du groupe veulent protéger. Le présent document décrit la distribution des SA de sécurité des données d'AH et ESP IPsec.

Contrôleur de groupe/Serveur de clés : (GCKS) Appareil qui définit la politique du groupe et distribue les clés pour cette politique [RFC3740].

Membre du groupe : C'est un membre autorisé d'un groupe sûr, qui envoie et/ou reçoit des paquets IP en relation avec le groupe.

GROUPKEY-PULL : Protocole utilisé par un membre de groupe GDOI pour demander la politique du groupe et le matériel de clés.

GROUPKEY-PUSH : Protocole utilisé par un GCKS GDOI pour distribuer les mises à jour de politique du groupe et de matériel de clés aux membres du groupe autorisés.

Clé de chiffrement de clé : Clé de chiffrement symétrique utilisée pour protéger le message GROUPKEY-PUSH.

Hiérarchie logique de clés : Méthode de gestion de groupe définie au paragraphe 5.4 de la [RFC2627].

SA de changement de clé . C'est la politique de sécurité qui protège un protocole GROUPKEY-PUSH.

Charge utile d'attribut de SA : Charge utile qui suit la charge utile d'association de sécurité et qui décrit les attributs de sécurité de groupe associés à l'association de sécurité. Les charges utiles d'attribut de SA incluent les charges utiles SAK, SAT, et GAP.

Indice de paramètre de sécurité : (SPI) Valeur arbitraire qui est utilisée par un receveur pour identifier une association de sécurité telle qu'une association de sécurité ESP IPsec ou une SA de changement de clé.

Clé de chiffrement de trafic : Clé de chiffrement symétrique utilisée pour protéger un protocole de sécurité des données (par exemple, ESP d'IPsec).

1.3 Acronymes et abréviations

Les acronymes et abréviations suivants sont utilisés dans le présent document.

AH *(IP Authentication Header)* en-tête d'authentification IP

ATD *(Activation Time Delay)* retard d'heure d'activation

DOI *(Domain of Interpretation)* domaine d'interprétation

DTD *(Deactivation Time Delay)* retard d'heure de désactivation

ESP *(IP Encapsulating Security Payload)* encapsulation IP de charge utile de sécurité

GCKS *(Group Controller/Key Server)* contrôleur de groupe/serveur de clé

GDOI *(Group Domain of Interpretation)* domaine d'interprétation de groupe

GAP *(Group Associated Policy Payload)* charge utile de politique associée au groupe

GM *(Group Member)* membre du groupe

GSPD *(Group Security Policy Database)* base de données de politique de sécurité de groupe

IV *(Initialization Vector)* vecteur d'initialisation

KD *(Key Download Payload)* charge utile Téléchargement de clé

KEK *(Key Encryption Key)* clé de chiffrement de clé

LKH *(Logical Key Hierarchy)* hiérarchie de clé logique

SA *(Security Association)* association de sécurité

SAK *(SA KEK Payload)* charge utile KEK de SA

SEQ *(Sequence Number Payload)* charge utile Numéro de séquence

SAT *(SA TEK Payload)* charge utile TEK de SA

SID *(Sender-ID)* identifiant d'envoyeur

SPI *(Security Parameter Index)* indice de paramètre de sécurité

SSIV *(Sender-Specific IV)* vecteur d'initialisation spécifique de l'envoyeur

TEK *(Traffic Encryption Key)* clé de chiffrement de trafic

TLV Type/Longueur/Valeur

TV Type/Valeur

2. Protocole GDOI de phase 1

L'échange GROUPKEY-PULL GDOI est un protocole de "phase 2" qui DOIT être protégé par un protocole de "phase 1". Le protocole de "phase 1" peut être tout protocole qui fournit les protections suivantes :
- o Authentification des homologues
- o Confidentialité
- o Intégrité du message

Les paragraphes qui suivent décrivent un tel protocole de "phase 1". D'autres protocoles qui sont des protocoles de "phase 1" potentiels sont décrits à l'Appendice A. Cependant, l'utilisation des protocoles qui y sont énumérés n'est pas considérée comme faisant partie du document.

Le présent document définit comment les échanges ISAKMP phase 1 tels que définis dans la [RFC2409] peuvent être utilisés comme protocole de phase 1 pour GDOI. Les sections suivantes définissent les caractéristiques uniques des protocoles ISAKMP phase 1 pour ces échanges lorsque utilisés pour GDOI.

Le paragraphe 7.1 décrit comment les protocoles ISAKMP phase 1 satisfont aux exigences d'un protocole GDOI phase 1.

2.1 Valeur de DOI

La charge utile de SA de phase 1 a une valeur de DOI. Cette valeur DOIT être la valeur de DOI de GDOI comme défini plus loin dans le présent document.

2.2 Accès UDP

L'IANA a alloué l'accès 848 pour l'utilisation de GDOI ; cela permet à une mise en œuvre d'utiliser des instances séparées de ISAKMP pour servir GDOI et le protocole d'échange de clé Internet (IKE, *Internet Key Exchange Protocol*) [RFC5996]. Un GCKS DEVRAIT écouter sur cet accès les échanges GROUPKEY-PULL, et le GCKS PEUT utiliser cet accès pour distribuer les messages GROUPKEY-PUSH. Une mise en œuvre d'échange ISAKMP phase 1 qui prend en charge la traversée de NAT de la [RFC3947] PEUT passer à l'accès 4500 pour traiter l'échange GROUPKEY-PULL.

3. Échange GROUPKEY-PULL

Le but de l'échange GROUPKEY-PULL est d'établir des SA Rekey et/ou Data-security chez le membre pour un groupe particulier. Une SA de phase 1 protège le GROUPKEY-PULL ; il PEUT y avoir plusieurs échanges GROUPKEY-PULL pour une certaine SA de phase 1. L'échange GROUPKEY-PULL télécharge les clés de sécurité des données (TEK) et/ou la clé de chiffrement de clé de groupe (KEK) ou le dispositif KEK sous la protection de la SA de phase 1.

3.1 Autorisation

Il est important qu'un membre du groupe fasse explicitement confiance aux entités dont il attend qu'elles agissent comme un GCKS pour un groupe particulier. Lorsque aucune autorisation n'est effectuée, il est possible à un participant GDOI vicieux de perpétrer une attaque par interposition entre un membre du groupe et un GCKS [MP04]. Un membre du groupe DOIT faire une liste spécifique de tous les GCKS autorisés dans sa base de données d'autorisation des homologues du groupe (GPAD, *Group Peer Authorization Database*) [RFC5374]. Un membre du groupe DOIT s'assurer que l'identité de phase 1 du GCKS est un GCKS autorisé.

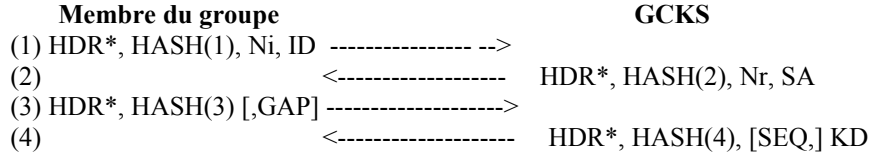
Il est important qu'un GCKS autorise explicitement les membres du groupe avant de leur fournir la politique du groupe et le matériel de clés. Une mise en œuvre de GCKS DEVRAIT avoir une méthode d'autorisation des membres du groupe (par exemple, en tenant une liste d'autorisations). Lorsque le GCKS effectue l'autorisation, il DOIT utiliser l'identité de phase 1 pour autoriser la demande GROUPKEY-PULL pour la politique du groupe et le matériel de clés.

3.2 Messages

Le GROUPKEY-PULL est un échange de phase 2. La phase 1 calcule le SKEYID_a qui est la "clé" dans le hachage de clé utilisé dans les charges utiles de hachage de GROUPKEY-PULL. Lors de l'utilisation de la phase 1 définie dans le présent document, SKEYID_a est déduit conformément à la [RFC2409]. Comme avec la génération de la charge utile IKE HASH au paragraphe 5.5 de la [RFC2409], chaque message GROUPKEY-PULL hache un ensemble de valeurs défini de façon univoque. Le nom occasionnel permute le hachage et fournit une certaine protection contre les attaques en répétition. La protection contre la répétition est importante pour protéger le GCKS contre les attaques qu'un serveur de gestion de clé va s'attirer.

Le GROUPKEY-PULL utilise des noms occasionnels pour garantir la "vitalité", ou contre la répétition d'un message GROUPKEY-PULL récent. L'attaque en répétition n'est utile que dans le contexte de la phase 1 en cours. Si un message GROUPKEY-PULL est répété sur la base d'une phase 1 précédente, le calcul du hachage va échouer à cause d'un SKEYID_a faux. Le traitement du message va échouer avant que le nom occasionnel soit même évalué.

Pour que l'un ou l'autre homologue tire parti de la protection contre la répétition, il doit retarder autant que possible le traitement jusqu'à ce qu'il reçoive le message dans le protocole qui prouve que l'homologue est bien vivant. Par exemple, le GCKS NE DOIT PAS ajuster son état interne (par exemple, en gardant un enregistrement du GM) jusqu'à ce qu'il ait reçu un message avec Nr inclus correctement dans la charge utile HASH. Cette exigence assure que les répétitions des messages GDOI ne causeront pas de changement de l'état du groupe par le GCKS tant qu'il n'a pas confirmation que le membre initiateur du groupe est vivant.



* Protégé par la SA de phase 1 ; le chiffrement survient après HDR

Figure 2 : Échange GROUPKEY-PULL

La Figure 2 montre les quatre messages qui font partie d'un échange GROUPKEY-PULL. HDR est une charge utile d'en-tête ISAKMP qui utilise des mouchards de phase 1 et un identifiant de message (M-ID) comme dans ISAKMP. À la suite de chaque HDR se trouve un ensemble de charges utiles qui portent les demandes (les messages 1 et 3 générés par le membre du groupe) ou la politique du groupe et/ou le matériel de clés (messages 2 et 4 générés par le GCKS).

Les hachages sont calculés de la façon décrite dans la [RFC2409]. Le calcul de HASH pour chaque message est unique ; il est montré à la Figure 2 et ci-dessous par HASH(n) où (n) représente le numéro de message GROUPKEY-PULL. Chaque

calcul de HASH est une fonction pseudo-aléatoire (prf, *pseudo-random function*) sur l'identifiant de message (M-ID) provenant de l'en-tête ISAKMP concaténé avec le message entier qui suit le hachage incluant tous les en-têtes de charge utile, mais excluant tout bourrage ajouté pour le chiffrement. Le GM s'attend à trouver son nom occasionnel, Ni, dans le HASH d'un message retourné, et le GCKS s'attend à voir son nom occasionnel, Nr, dans le HASH d'un message retourné. HASH(2), HASH(3), et HASH(4) incluent aussi des valeurs de nom occasionnel passées précédemment dans le protocole (c'est-à-dire, Ni ou Nr moins l'en-tête de charge utile). Le nom occasionnel passé dans Ni est représenté par Ni_b, et le nom occasionnel passé dans Nr est représenté par Nr_b. Les charges utiles HASH prouvent que l'homologue a le secret de phase 1 (SKEYID_a) et le nom occasionnel pour l'échange identifié par l'identifiant de message, M-ID.

HASH(1) = prf(SKEYID_a, M-ID | Ni | ID)
HASH(2) = prf(SKEYID_a, M-ID | Ni_b | Nr | SA)
HASH(3) = prf(SKEYID_a, M-ID | Ni_b | Nr_b [| GAP])
HASH(4) = prf(SKEYID_a, M-ID | Ni_b | Nr_b [| SEQ] | KD)

En plus des charges utiles de nom occasionnel et de HASH, le membre du groupe identifie le groupe auquel il souhaite se joindre au moyen de la charge utile d'identifiant ISAKMP.

Le GCKS informe le membre des politiques du chiffrement du groupe dans la charge utile SA, qui décrit le DOI, la KEK, et/ou le matériel de clés de TEK , les transformations d'authentification, et autres politiques du groupe. Chaque SPI est aussi déterminé par le GCKS et téléchargé dans la chaîne de charge utile SA (voir le paragraphe 5.2). L'attribut KEK SA contient la paire de mouchards ISAKMP pour la SA, qui n'est pas négociée mais téléchargée. Chaque attribut TEK SA contient un SPI comme défini au paragraphe 5.5.

Après avoir reçu et analysé la charge utile SA, le membre du groupe répond par un message d'accusé de réception qui prouve sa vivacité. Il inclut facultativement une charge utile GAP pour demander des ressources.

Le GCKS informe le membre du groupe de la valeur du numéro de séquence dans la charge utile SEQ. Ce numéro de séquence fournit un état anti-répétition associé à une KEK, et sa connaissance assure que le membre du groupe ne va pas accepter de message GROUPKEY-PUSH envoyé avant que le GM se soit joint au groupe. La charge utile SEQ n'a pas d'autre usage et est omise de l'échange GROUPKEY-PULL lorsque un attribut KEK n'est pas inclus dans la charge utile SA. Lorsque une charge utile SEQ est incluse dans l'échange GROUPKEY-PULL, elle inclut le numéro de séquence le plus récemment utilisé pour le groupe. À la conclusion d'un échange GROUPKEY-PULL, le membre initiateur du groupe NE DOIT PAS accepter de message Rekey avec à la fois la valeur du SPI d'attribut KEK et un numéro de séquence inférieur ou égal à celui reçu durant l'échange GROUPKEY-PULL. Lorsque le premier membre du groupe initie un échange GROUPKEY-PULL, le GCKS fournit un numéro de séquence de zéro, car aucun message GROUPKEY-PUSH n'a encore été envoyé. Noter que le numéro de séquence ne s'incrémente qu'avec les messages GROUPKEY-PUSH. L'échange GROUPKEY-PULL distribue le numéro de séquence actuel au membre du groupe. Le numéro de séquence se remet à une valeur de un avec l'utilisation d'un nouvel attribut KEK. Donc, le premier paquet envoyés pour une certaine SA Rekey aura un numéro de séquence de 1. Le numéro de séquence s'incrémente avec chaque changement de clé successif.

Le GCKS retourne toujours une charge utile KD contenant le matériel de clés au GM. Si une SA Rekey est définie dans la charge utile SA, KD va alors contenir la KEK ; si une ou plusieurs SA de sécurité des données sont définies dans la charge utile de SA, KD contiendra les TEK.

3.2.1 Initialisation d'en-tête ISAKMP

Les mouchards sont utilisés dans l'en-tête ISAKMP pour identifier une session GDOI particulière. L'échange GROUPKEY-PULL GDOI utilise des mouchards conformément à ISAKMP [RFC2408].

Prochaine charge utile identifie une charge utile ISAKMP ou GDOI (voir Section 5).

Version majeure est 1 et Version mineure est 0 conformément à ISAKMP, paragraphe 3.1 de la [RFC2408].

Type d'échange a la valeur de 32 pour l'échange GROUPKEY-PULL de GDOI.

Fanions, Identifiant de message, et Longueur sont selon ISAKMP, paragraphe 3.1 de la [RFC2408]. Le fanion Commit n'est pas utile parce que il n'y a pas de synchronisation entre l'échange GROUPKEY-PULL et le trafic de données protégé par la politique distribuée par l'échange GROUPKEY-PULL.

3.3 Opérations de membre du groupe

Avant qu'un membre du groupe ne contacte le GCKS, il doit déterminer l'identifiant de groupe et la politique de phase 1 acceptable via une méthode hors bande. La phase 1 est initiée en utilisant le DOI GDOI dans la charge utile SA. Une fois que la phase 1 est achevée, l'automate à états du GM passe au protocole GDOI.

Pour construire le premier message GDOI, le GM choisit Ni, crée une charge utile de nom occasionnel, construit une charge utile Identité incluant l'identifiant de groupe, et génère HASH(1).

À réception du second message GDOI, le GM valide HASH(2), extrait le nom occasionnel Nr, et interprète la charge utile SA (y compris ses charges utiles d'attribut SA). La charge utile SA contient la politique qui décrit le protocole de sécurité et les protocoles de chiffrement utilisés par le groupe. Cette politique décrit la SA Rekey (si elle est présente) les SA de sécurité des données, et autre politique du groupe. Si la politique dans la charge utile SA est acceptable pour le GM, il continue le protocole. Autrement, le GM DEVRAIT supprimer la session de phase 1 après avoir notifié le GCKS avec un échange d'informations ISAKMP contenant une charge utile Supprimer.

Lorsque il construit le troisième message GDOI, il revoit d'abord chaque SA de sécurité des données qui lui est donnée. Si l'une d'elles décrit l'utilisation d'un chiffrement en mode compteur, le GM détermine si il a besoin de plus d'un identifiant d'envoyeur (SID, *Sender-ID*) (voir au paragraphe 3.5). Si c'est le cas, il demande le nombre requis de SID pour son usage exclusif au sein du nom occasionnel en mode compteur comme décrit au paragraphe 5.4. Le GM complète alors la construction du troisième message GDOI en créant HASH(3).

À réception du quatrième message GDOI, le GM valide HASH(4).

Si la charge utile SEQ est présente, le numéro de séquence inclus dans la charge utile SEQ indique le plus bas numéro de séquence acceptable présent dans un futur message GROUPKEY-PUSH. Mais si la KEK associée à ce numéro de séquence avait été installée précédemment, du fait du traitement asynchrone des messages GROUPKEY-PULL et GROUPKEY-PUSH, ce numéro de séquence peut être inférieur au numéro de séquence contenu dans le plus récent message GROUPKEY-PUSH reçu. Dans ce cas, la valeur du numéro de séquence dans la charge utile SEQ DOIT être considérée comme périmée et ignorée.

Le GM interprète les paquets de clé KD, où chaque paquet de clé comporte le matériel de clés pour les SA distribuées dans la charge utile SA. Le matériel de clé est confronté en comparant le SPI de chaque paquet de clé aux valeurs de SPI précédemment envoyées dans les charges utiles SA. Une fois que les TEK et les politiques correspondent, le GM les fournit au sous-système de sécurité des données, et il est prêt à envoyer ou recevoir les paquets qui correspondent à la politique de TEK. Si ce groupe a une KEK, la politique de KEK et les clés sont marquées comme prêtes à l'utilisation, et le GM sait qu'il attend un numéro de séquence non inférieur à celui distribué dans la charge utile SEQ. Le GM est maintenant prêt à recevoir des messages GROUPKEY-PUSH.

Si la charge utile KD est incluse dans un dispositif de clés LKH, le GM prend la dernière clé dans le dispositif comme KEK de groupe. Le dispositif est alors mémorisé sans autre traitement.

3.4 Opérations du GCKS

Le GCKS écoute passivement les demandes entrantes provenant des membres du groupe. La phase 1 authentifie le membre du groupe et établit la session sécurisée avec eux.

À réception du premier message GDOI, le GCKS valide HASH(1), extrait le Ni et l'identifiant de groupe dans l'identifiant de charge utile. Il vérifie que sa base de données contient les informations de groupe pour cet identifiant de groupe et que le GM est autorisé à participer au groupe.

Le GCKS construit le second message GDOI, incluant un nom occasionnel Nr, et la politique pour le groupe dans une charge utile SA, suivie par les charges utiles Attribut SA (c'est-à-dire, les charges utiles KEK SA, GAP, et/ou TEK SA) conformément à la politique du GCKS. (Voir au paragraphe 5.2.1 les détails de la façon dont le GCKS choisit les charges utiles à envoyer.)

À réception du troisième message GDOI, le GCKS valide HASH(3). Si le message inclut une charge utile GAP, il met en antémémoire les demandes incluses dans cette charge utile pour les utiliser à la construction du quatrième message GDOI.

Le GCKS construit le quatrième message GDOI, incluant la charge utile SEQ (si le GCKS envoie des messages Rekey) et la charge utile KD contenant les clés correspondant à la politique envoyée précédemment dans les charges utiles TEK de

SA et KEK de SA. Si un algorithme de gestion de groupe est défini au titre de la politique du groupe, le GCKS va d'abord insérer le membre du groupe dans la structure de gestion de groupe (par exemple, une feuille dans l'arborescence LKH) et ensuite créer un dispositif LKH de clés et l'inclure dans la charge utile KD. La première clé dans le dispositif est associée au nœud feuille du membre du groupe, suivi par chaque nœud LKH au dessus dans l'arborescence, culminant avec le nœud racine (qui est aussi la KEK). Si une ou plusieurs SA de sécurité des données distribuées dans la charge utile SA incluaient un mode de fonctionnement compteur, le GCKS inclut au moins une valeur de SID dans la charge utile KD, et éventuellement plus, selon la demande reçue dans le troisième message GDOI.

3.5 Fonctionnement en mode compteur

Plusieurs nouveaux modes de fonctionnement fondés sur le compteur ont été spécifiés pour ESP (par exemple, AES-CTR [RFC3686], AES-GCM [RFC4106], AES-CCM [RFC4309], AES-GMAC [RFC4543]) et pour AH (par exemple, AES-GMAC [RFC4543]). Ces modes fondés sur le compteur exigent que jamais deux envoyeurs dans le groupe n'envoient un paquet avec le même vecteur d'initialisation (IV, *Initialization Vector*) en utilisant la même clé et le même mode de chiffrement. Cette exigence est satisfaite dans GDOI lorsque les exigences suivantes sont respectées :

- Le GCKS distribue une clé unique pour chaque SA de sécurité des données.
- Le GCKS utilise la méthode décrite dans la [RFC6054], qui alloue à chaque envoyeur une portion de l'espace d'IV en provisionnant chaque envoyeur avec une ou plusieurs valeurs uniques de SID.

Lorsque au moins une SA de sécurité des données incluse dans la politique du groupe inclut un mode compteur, le GCKS alloue automatiquement et distribue un SID à chaque membre du groupe agissant dans le rôle d'envoyeur sur la SA de sécurité des données. La valeur de SID est utilisée exclusivement par le membre du groupe auquel il a été alloué. Le membre du groupe utilise le même SID pour chaque SA de sécurité des données en spécifiant l'utilisation d'un mode de fonctionnement fondé sur le compteur. Un GCKS DOIT distribuer des clés uniques pour chaque SA de sécurité des données incluant un mode de fonctionnement fondé sur le compteur afin de conserver une utilisation de clé et nom occasionnel uniques.

Lorsque un membre du groupe reçoit une SA de sécurité des données dans une charge utile de SA TEK pour laquelle il est un envoyeur, il peut choisir de demander une ou plusieurs valeurs de SID. Demander une valeur de 1 n'est pas nécessaire car le GCKS va automatiquement en allouer exactement une au membre du groupe envoyeur. Un membre du groupe DOIT demander autant de SID que ce qui correspond au nombre de modules de chiffrement dans lesquels il va installer les TEK dans la direction sortante. Autrement, un membre du groupe PEUT demander plus d'un SID et les utiliser en série. Cela pourrait être utile lorsque on prévoit que le membre du groupe va épuiser la gamme des noms occasionnels de SA de sécurité des données en utilisant un seul SID trop rapidement (par exemple, avant l'expiration de la politique fondée sur le temps dans la TEK).

Lorsque la politique du groupe comporte un mode de fonctionnement fondé sur le compteur, un GCKS DEVRAIT utiliser la méthode suivante pour allouer les valeurs de SID, qui assure que chaque SID sera alloué à juste un membre du groupe.

1. Un GCKS tient un compteur de SID, qui enregistre les SID qui ont été alloués. Les SID sont alloués en séquence, le premier SID alloué étant zéro.

2. Chaque fois qu'un SID est alloué, la valeur courante du compteur est sauvegardée et allouée au membre du groupe. Le compteur de SID est ensuite incrémenté en préparation de la prochaine allocation.

3. Lorsque le GCKS distribue une SA de sécurité des données spécifiant un mode de fonctionnement fondé sur le compteur, et qu'un membre du groupe est un envoyeur, un membre du groupe peut demander un compte des SID dans une charge utile GAP. Lorsque le GCKS reçoit cette demande, il incrémente le compteur de SID une fois pour chaque SID demandé, et distribue chaque valeur de SID au membre du groupe.

4. Un GCKS alloue de nouvelles valeurs de SID pour chaque échange GROUPKEY-PULL généré par un envoyeur, sans considérer si un membre du groupe avait précédemment contacté le GCKS. De cette façon, le GCKS n'a pas d'obligation de tenir un enregistrement de quelles valeurs de SID il a précédemment alloué à chaque membre du groupe. Plus important, comme le GCKS ne peut pas fiablement détecter si le membre du groupe avait envoyé des données sur les SA de sécurité des données du groupe actuel, il ne sait pas quelles valeurs de nom occasionnel de sécurité des données en mode compteur a utilisé un membre du groupe. En distribuant de nouvelles valeurs de SID, le serveur de clés s'assure que chaque fois qu'un membre du groupe conforme installe une SA de sécurité des données, il va utiliser un ensemble unique de noms occasionnels en mode compteur.

5. Lorsque le compteur de SID tenu par le GCKS atteint sa valeur finale de SID, aucune autre valeur de SID ne peut être distribuée. Avant de distribuer toute nouvelle autre valeur de SID, le GCKS DOIT supprimer des SA de sécurité des

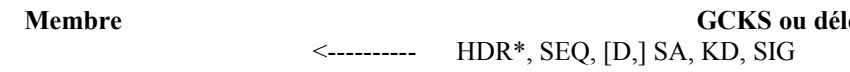
données pour le groupe, suivi par la création des nouvelles SA de sécurité des données, et remettre le compteur de SID à sa valeur initiale.

6. Le GCKS DEVRAIT envoyer un message GROUPKEY-PUSH supprimant toutes les SA de sécurité des données et la SA Rekey pour le groupe. Il en résultera que les membres du groupe initieront un nouvel échange GROUPKEY-PULL, dans lequel ils vont recevoir à la fois de nouvelles valeurs de SID et les nouvelles SA de sécurité des données. Les nouvelles valeurs de SID peuvent être utilisées en toute sécurité parce qu'elles ne sont utilisées qu'avec les nouvelles SA de sécurité des données. Noter que la suppression de la SA Rekey est nécessaire pour garantie que les membres du groupe recevant un échange GROUPKEY-PUSH avant de se réenregistrer ne vont pas utiliser par inadvertance leurs vieux SID avec les nouvelles SA de sécurité des données.

En utilisant la méthode ci-dessus, à aucun moment deux membres du groupe ne peuvent utiliser les mêmes valeurs d'IV avec la même clé de SA de sécurité des données.

4. Message GROUPKEY-PUSH

GDOI envoie en toute sécurité des informations de contrôle en utilisant les communications de groupe. Cela va normalement utiliser la distribution en diffusion groupée IP d'un message GROUPKEY-PUSH mais peut aussi être "poussé" en utilisant la livraison en envoi individuel si la diffusion groupée IP n'est pas possible. Le message GROUPKEY-PUSH remplace un dispositif Rekey SA KEK ou KEK, et/ou crée une nouvelle SA Data-security.



* Protégé par la KEK de SA Rekey ; le chiffrement survient après HDR

Figure 3 : Message GROUPKEY-PUSH

HDR est défini plus loin. La charge utile SEQ est définie dans la section 5, "Charges utiles". Une ou plusieurs charges utiles D (Delete, *Supprimer*) (décrit au paragraphe 5.9) spécifient facultativement la suppression de la politique du groupe existante. La SA définit la politique du groupe pour la SA Rekey et/ou les SA de sécurité des données de remplacement comme décrit à la Section 5, le KD fournissant la matériel de clés pour ces SA.

La charge utile SIG comporte une signature d'un hachage du message GROUPKEY-PUSH entier (excepté les octets de la charge utile SIG) avant qu'il ait été chiffré. Le HASH est pris sur la chaîne 'rekey', le HDR GROUPKEY-PUSH, suivi par toutes les charges utiles qui précèdent la charge utile SIG. La chaîne préfixée garantit que la signature du datagramme Rekey ne peut être utilisée pour aucun autre objet dans le protocole GDOI. La charge utile SIG est créée en utilisant la signature du hachage ci-dessus, le receveur vérifiant la signature à l'aide d'une clé publique récupérée lors d'un précédent échange GDOI. La KEK actuelle (elle aussi distribuée dans un précédent échange de message GROUPKEY-PULL ou GROUPKEY-PUSH) chiffre toutes les charges utiles qui suivent le GROUPKEY-PUSH HDR. Note : La raison de l'ordre de ces opérations est donnée au paragraphe 7.3.5.

Si la SA définit un dispositif KEK LKH ou une seule KEK, KD contient une KEK ou un dispositif de KEK pour une nouvelle SA Rekey, qui a une nouvelle paire de mouchards. Lorsque la charge utile KD porte un nouvel attribut KEK de SA (paragraphe 5.3) une SA Rekey est remplacée par une nouvelle SA ayant le même identifiant de groupe (ID spécifié dans le message 1 du paragraphe 3.2) et en incrémentant le même compteur de séquence, qui est initialisé dans le message 4 du paragraphe 3.2. Si la SA définit une charge utile TEK de SA, cela informe le membre qu'une nouvelle SA Data-security a été créée, avec le matériel de clé porté dans KD (paragraphe 5.6).

Si la SA définit un grand dispositif KEK LKH (par exemple, durant l'initialisation de groupe et le changement de clés par lots) des parties du dispositif PEUVENT être envoyées dans différents datagrammes GROUPKEY-PUSH uniques. Cependant, chacun des datagrammes GROUPKEY-PUSH DOIT être un datagramme GROUPKEY-PUSH pleinement formé. Il en résulte que chaque datagramme contiendra un numéro de séquence et la politique dans la charge utile SA, qui correspond à la portion du dispositif de KEK envoyé dans la charge utile KD.

4.1 Utilisation de clés de signature

Une clé de signature ne devrait pas être utilisée dans plus d'un contexte (par exemple, utilisée pour l'authentification d'hôte et aussi pour l'authentification de message). Donc, le GCKS NE DEVRAIT PAS, pour signer la charge utile SIG dans le message GROUPKEY-PUSH, utiliser la même clé que pour l'authentification de l'échange GROUPKEY-PULL.

4.2 Initialisation d'en-tête ISAKMP

À la différence de ISAKMP, la paire de mouchards est complètement déterminée par le GCKS. La paire de mouchards dans l'en-tête GDOI ISAKMP identifie la SA Rekey pour différencier les groupes sûrs gérés par un GCKS. Donc, GDOI utilise les champs de mouchard comme SPI.

Prochaine charge utile identifie une charge utile ISAKMP ou GDOI (voir la Section 5).

Version majeure est 1 et Version mineure est 0 conformément à ISAKMP (paragraphe 3.1 de la [RFC2408].

Type d'échange a la valeur 33 pour le message GROUPKEY-PUSH GDOI.

Fanions DOIT avoir le bit Chiffrement réglé conformément au paragraphe 3.1 de la [RFC2008]. Tous les autres bits DOIVENT être réglés à zéro.

ID de message DOIT être réglé à zéro.

Longueur est réglé conformément à ISAKMP (paragraphe 3.1 de la [RFC2408]).

4.3 Opérations du GCKS

Le GCKS peut initier un message Rekey pour une parmi plusieurs raisons, par exemple, les membres du groupe ont changé ou les clés vont arriver à expiration.

Pour commencer le datagramme de changement de clés, le GCKS construit un HDR ISAKMP avec la paire correcte de mouchards, et une charge utile SEQ qui inclut un numéro de séquence supérieur de un au précédent datagramme Rekey. Si le message utilise le nouvel attribut de KEK pour la première fois, le SEQ est remis à 1 dans ce message.

Une charge utile SA est ensuite ajoutée. Cela est identique en structure et signification à une charge utile SA envoyée dans un échange GROUPKEY-PULL. Si il y a des changements à la KEK (y compris dus à l'exclusion de membres du groupe, dans le cas de LKH) un attribut SA_KEK est ajouté à la SA. Si il y a une ou plusieurs nouvelles TEK, alors les attributs SA_TEK sont ajoutés pour décrire cette politique.

Une charge utile KD est alors ajoutée. Cela est identique en structure et signification à une charge utile KD envoyée dans un échange GROUPKEY-PULL. Si un attribut SA_KEK était inclus dans la charge utile SA, alors les KEK correspondantes (ou un dispositif de mise à jour de KEK) sont incluses. Un dispositif de mise à jour de KEK est créé en déterminant d'abord quels membres du groupe ont été exclus, en générant de nouvelles clés en tant que de besoin, et en distribuant ensuite les dispositifs de mise à jour LKH suffisamment pour fournir la nouvelle KEK aux membres du groupe restants (voir les détails au paragraphe 5.4.1 de la [RFC2627]). Les TEK sont aussi envoyées pour chaque attribut SA_TEK inclus dans la charge utile SA.

Dans l'avant-dernière étape, le GCKS crée la charge utile SIG et l'ajoute au datagramme.

Enfin, les charges utiles qui suivent le HDR sont chiffrées en utilisant la KEK actuelle. Le datagramme peut maintenant être envoyée.

4.4 Opérations de membre du groupe

Un membre du groupe qui reçoit le datagramme GROUPKEY-PUSH confronte la paire de mouchards dans le HDR ISAKMP à une SA existante. Le message est déchiffré, et la forme du datagramme est validée. Cela élimine les messages de malformation évidente (qui peuvent être envoyés au titre d'une attaque de déni de service contre le groupe).

Le numéro de séquence dans la charge utile SEQ est validé pour s'assurer qu'il est supérieur au numéro de séquence reçu précédemment. La charge utile SIG est alors validée. Si la signature échoue, le message est éliminé.

Les charges utiles SA et KD sont traitées, ce qui résulte en une nouvelle SA GDOI Rekey (si la charge utile SA incluait un attribut SA_KEK) et/ou de nouvelles SA IPsec qui sont ajoutées au système. Si la charge utile KD inclut un dispositif de mise à jour LKH, le membre du groupe compare l'identifiant de LKH, dans chaque paquet de mise à jour de clé, aux

identifiants de LKH qu'il détient. Si il trouve une correspondance, il déchiffre la clé en utilisant la clé qui la précède dans la matrice des clés et mémorise la nouvelle clé dans la matrice de clé du LKH qu'il détient. Le déchiffrement final donne la nouvelle KEK de groupe.

Si la charge utile SA inclut une ou plusieurs SA de sécurité des données incluant un mode de fonctionnement fondé sur le compteur et si le membre du groupe receveur est un envoyeur pour cette SA, le membre du groupe utilise sa valeur courante de SID avec les SA de sécurité des données pour créer des noms occasionnels en mode compteur. Si il est un envoyeur et ne détient pas une valeur de SID actuelle, il NE DOIT PAS installer les SA de sécurité des données. Il PEUT initier un échange GROUPKEY-PULL avec le GCKS afin d'obtenir une valeur de SID (ainsi que la politique du groupe actuelle).

5. Charges utiles et valeurs définies

Le présent document spécifie l'utilisation de plusieurs charges utiles ISAKMP, qui sont définies conformément à la [RFC2408]. Les charges utiles suivantes sont utilisées comme défini dans la [RFC2408].

Prochain type de charge utile	**Valeur**
Charge utile de hachage (HASH)	8
Signature (SIG)	9

Les charges utiles suivantes sont étendues ou mieux spécifiées.

Prochain type de charge utile	**Valeur**
Association de sécurité (SA)	1
Identification (ID)	5
Nom occasionnel (N)	10
Supprimer (Delete, D)	12

Plusieurs formats de charge utile sont exigés dans les échanges de sécurité de groupe.

Prochain type de charge utile	**Valeur**
Charge utile SA KEK (SAK)	15
Charge utile SA TEK (SAT)	16
Téléchargement de clé (KD)	17
Numéro de séquence (SEQ)	18
Politique associée au groupe (GAP)	22

Tous les champs multi-octet dans les charges utiles GDOI qui représentent des entiers sont disposées en ordre gros boutien (aussi appelé "octet de poids fort en premier" ou "ordre des octets du réseau").

Toutes les charges utiles qui incluent un en-tête générique de charge utile ISAKMP créent un champ Longueur de charge utile qui inclut la longueur de l'en-tête générique de charge utile (paragraphe 3.2 de la [RFC2408]).

5.1 Charge utile d'identification

La charge utile Identification est définie dans la [RFC2408]. Pour le GDOI, elle est utilisée pour identifier une identité de groupe qui sera ensuite associée à des associations de sécurité pour le groupe. Une identité de groupe peut se transposer en une adresse de diffusion groupée spécifique IPv4 ou IPv6, ou peut spécifier un identifiant plus général, comme celui qui représente un ensemble de flux de diffusion groupée en rapport.

Lorsque il est utilisé avec le GDOI, le champ Données d'identifiant spécifique de DOI DOIT être réglé à 0.

Lorsque il est utilisé avec le GDOI, le type d'identifiant ID_KEY_ID DOIT être pris en charge par une mise en œuvre conforme et DOIT spécifier comme valeur un identifiant de groupe de 4 octets. Les mises en œuvre PEUVENT aussi prendre en charge d'autres types d'identifiant.

5.2 Charge utile d'association de sécurité

La charge utile Association de sécurité est définie dans la [RFC2408]. Pour le GDOI, elle est utilisée par le GCKS pour affirmer les attributs de sécurité pour les SA Rekey et Sécurité des données.

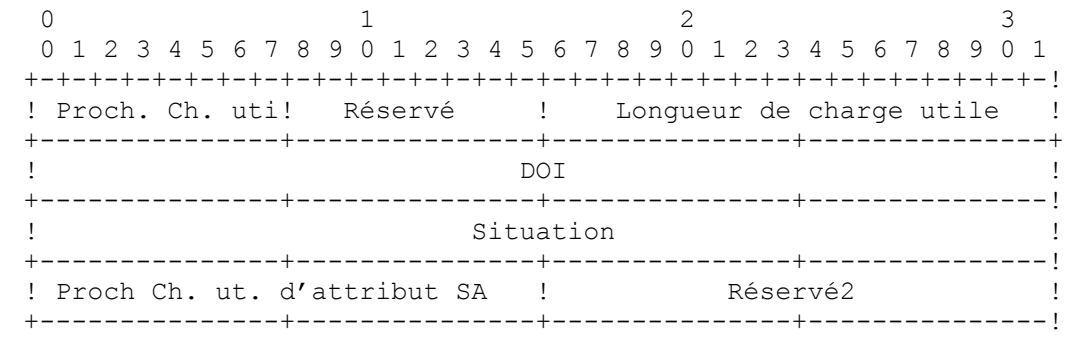


Figure 4 : Charge utile Association de sécurité

Les champs de charge utile Association de sécurité sont définis comme suit :

- Prochaine charge utile (1 octet) – Identifie la prochaine charge utile pour le message GROUPKEY-PULL ou GROUPKEY-PUSH comme défini ci-dessus. La prochaine charge utile NE DOIT PAS être une charge utile Attribut de SA ; elle DOIT être la prochaine charge utile qui suit la charge utile de type Association de sécurité.

- Réservé (1 octet) – Non utilisé, doit être zéro.

- Longueur de charge utile (2 octets) – C'est la longueur en octets de la charge utile en cours, incluant l'en-tête générique et toutes les charges utiles TEK et KEK.

- DOI (4 octets) – C'est le GDOI, dont la valeur est 2.

- Situation (4 octets) -- Doit être zéro.

- Prochaine charge utile Attribut de SA (2 octets) -- DOIT être le code pour un type de charge utile Attribut de SA. Voir au paragraphe 5.2.1 la description des circonstances requises pour que chaque type de charge utile soit présent.

- Réservé2 (2 octets) – DOIT être zéro (0).

5.2.1 Charges utiles d'attribut de SA

Les charges utiles qui définissent des attributs spécifiques d'association de sécurité pour la KEK et/ou les TEK utilisées par le groupe DOIVENT suivre la charge utile SA. Combien de chaque charge utile dépend de la politique du groupe. Il peut y avoir zéro ou une charge utile SAK, zéro ou une charge utile GAP, et zéro, une ou plusieurs charges utiles SAT, et soit une charge utile SAK, soit une charge utile SAT DOIT être présente. Lorsque elles sont présentes, l'ordre des charges utiles Attribut de SA DOIT être : SAK, GAP, et SAT.

Cette latitude à l'égard des charges utiles Attribut de SA permet à diverses politiques de groupe d'être accommodées. Par exemple, si la politique du groupe n'exige pas l'utilisation d'une SA Rekey, le GCKS n'a pas besoin d'envoyer un attribut SA KEK aux membres du groupe car toutes les mises à jour de SA vont être effectuées en utilisant la SA Enregistrement. Autrement, la politique du groupe peut utiliser une SA Rekey mais choisir de télécharger une KEK aux membres du groupe seulement au titre de la SA Enregistrement. Donc, la politique de KEK (dans l'attribut KEK SA) ne sera pas nécessaire au titre de la charge utile SA du message SA Rekey.

Spécifier plusieurs SAT permet que plusieurs sessions fassent partie du même groupe et que plusieurs flux soient associés à une session (par exemple, vidéo, audio, et texte) mais chacune avec une politique d'association de sécurité individuelle.

Une charge utile GAP permet la distribution d'une politique à l'échelle du groupe, comme des instructions sur le moment où activer et désactiver les SA.

5.3. Charge utile de KEK de SA

La charge utile SA KEK (SAK) contient des attributs de sécurité pour la méthode de KEK pour un groupe et des paramètres spécifiques de l'opération GROUPKEY-PULL. Les identités de source et de destination décrivent les identités utilisées pour le datagramme GROUPKEY-PULL.

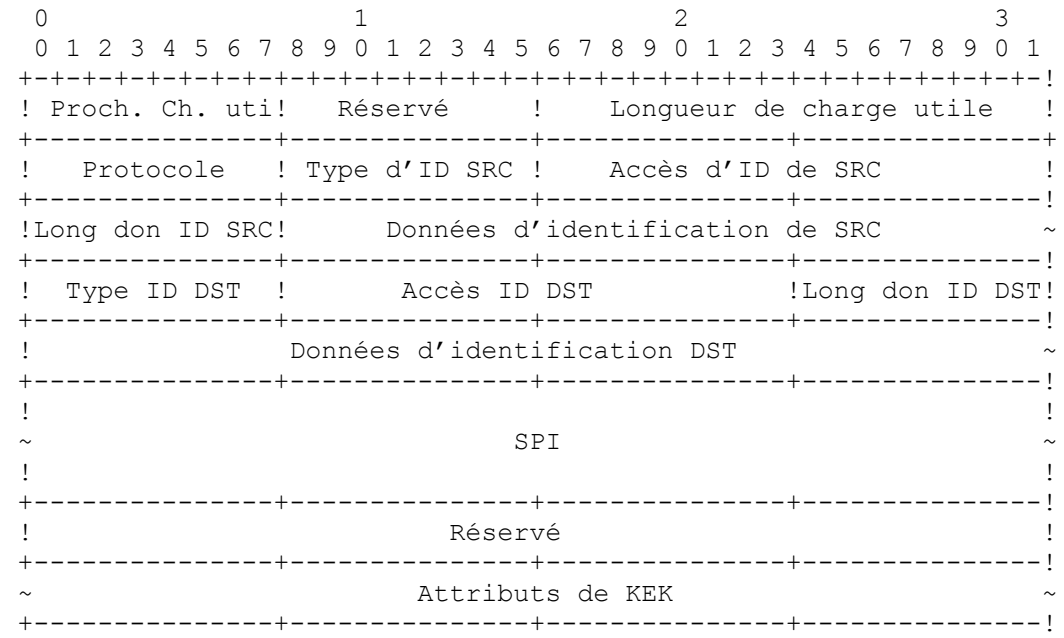


Figure 5 : Charge utile KEK de SA

Les champs de charge utile SAK sont définis comme suit :

- Prochaine charge utile (1 octet) – Identifie la prochaine charge utile pour le message GROUPKEY-PULL ou GROUPKEY-PUSH. Les seuls types de prochaine charge utile valides pour ce message sont une charge utile GAP, une charge utile SAT, ou zéro pour indiquer qu'il n'y a pas de charge utile Attribut de SA à suivre.
- Réservé (1 octet) -- DOIT être zéro.
- Longueur de charge utile (2 octets) – Longueur de cette charge utile, incluant les attributs de KEK
- Protocole (1 octet) -- Valeur qui décrit un ID de protocole IP (par exemple, UDP/TCP) [PROT-REG] pour le datagramme GROUPKEY-PUSH.
- Type d'ID de SRC (1 octet) – Valeur qui décrit les informations d'identité trouvées dans le champ Données d'identification de SRC. Les valeurs définies sont spécifiées par la section Type d'identification IPsec dans le registre IANA ISAKMP [ISAKMP-REG].
- Accès d'ID de SRC (2 octets) -- Valeur qui spécifie un accès associé à l'identifiant de source. Une valeur de zéro signifie que le champ Accès d'ID de SRC DOIT être ignoré.
- Longueur des données d'ID de SRC (1 octet) -- Valeur qui spécifie la longueur du champ Données d'identification de SRC.
- Données d'identification de source (longueur variable) -- Valeur, comme indiquée par le type d'ID de SRC.
- Type d'ID de DST (1 octet) -- Valeur qui décrit les informations d'identité trouvées dans le champ Données d'identification de destination. Les valeurs définies sont spécifiées par la section Type d'identification IPsec dans le registre IANA ISAKMP [ISAKMP-REG].
- Protocole d'ID de DST (1 octet) -- Valeur qui décrit un identifiant de protocole IP (par exemple, UDP/TCP) [PROT-REG].
- Accès d'ID de DST (2 octets) -- Valeur qui spécifie un accès associé à l'identifiant de destination.
- Longueur des données d'ID de DST (1 octet) -- Valeur spécifiant la longueur du champ Données d'identification de destination.
- Données d'identification de DST (longueur variable) -- Valeur, comme indiquée par le Type d'ID de DST.
- SPI (16 octets) – Indice de paramètre de sécurité pour la KEK. Le SPI est la paire de mouchards d'en-tête ISAKMP où les huit premiers octets deviennent le champ "Cookie initiateur" du HDR ISAKMP du message GROUPKEY-PUSH, et les huit octets suivants deviennent le "Cookie répondant" dans le même HDR. Comme décrit ci-dessus, ces mouchards sont alloués par le GCKS.
- Réservé2 (4 octets) -- DOIT être zéro. Ces octets représentent des champs précédemment définis mais qui ne sont plus utilisés par GDOI.
- Attributs de KEK – Contient les attributs de politique de KEK associés au groupe. Les attributs suivants peuvent être présents dans une charge utile SAK. Les attributs doivent suivre le format défini dans ISAKMP (paragraphe 3.3 de la

[RFC2408]). Dans le tableau qui suit, les attributs qui sont définis comme TV sont marqués comme basiques (B); les attributs qui sont définis comme TLV sont marqués comme variables (V).

Classe d'identifiant	Valeur	Type
Réservé	0	
KEK_MANAGEMENT_ALGORITHM	1	B
KEK_ALGORITHM	2	B
KEK_KEY_LENGTH	3	B
KEK_KEY_LIFETIME	4	V
SIG_HASH_ALGORITHM	5	B
SIG_ALGORITHM	6	B
SIG_KEY_LENGTH	7	B
Réservé	8	B
Non alloué	9-127	
Utilisation privée	128-255	
Non alloué	256-32767	

Les attributs KEK_ALGORITHM et SIG_ALGORITHM DOIVENT être inclus ; les autres sont FACULTATIFS et sont inclus selon la politique du groupe. L'attribut KEK_MANAGEMENT_ALGORITHM NE DOIT PAS être inclus dans un message GROUPKEY-PULL, et DOIT être ignoré s'il est présent.

5.3.1 KEK_MANAGEMENT_ALGORITHM

La classe KEK_MANAGEMENT_ALGORITHM spécifie l'algorithme de gestion de KEK de groupe utilisé pour fournir le contrôle d'accès vers l'avant ou vers l'arrière (c'est-à-dire, utilisé pour exclure des membres du groupe). Les valeurs définies sont spécifiées dans le tableau suivant.

Type de gestion de KEK	Valeur
Réservé	0
LKH	1
Non alloué	2-127
Utilisation privée	128-255
Non alloué	256-65 535

5.3.1.1 LKH

Ce type indique la méthode de gestion de groupe décrite au paragraphe 5.4 de la [RFC2627]. Une discussion générale du fonctionnement de LKH se trouve aussi au paragraphe 6.3 de "Multicast and Group Security" [HD03]

5.3.2 KEK_ALGORITHM

La classe KEK_ALGORITHM spécifie l'algorithme de chiffrement dans lequel la KEK est utilisée pour fournir la confidentialité au message GROUPKEY-PUSH. Les valeurs définies sont spécifiées dans le tableau suivant. Une mise en œuvre GDOI DOIT s'interrompre si elle rencontre un attribut ou capacité qu'elle ne comprend pas.

Type d'algorithme	Valeur
Réservé	0
KEK_ALG_DES	1
KEK_ALG_3DES	2
KEK_ALG_AES	3
Non alloué	4-127
Utilisation privée	128-255
Non alloué	256-32767

Si un KEK_MANAGEMENT_ALGORITHM est défini avec la spécification de plusieurs clés (par exemple, LKH) et si l'algorithme de gestion ne spécifie pas l'algorithme pour ces clés, l'algorithme défini par l'attribut KEK_ALGORITHM DOIT alors être utilisé pour toutes les clés qui sont incluses au titre de la gestion.

5.3.2.1 KEK_ALG_DES

Ce type spécifie DES en utilisant le mode de chaînage de bloc de chiffrement (CBC) comme décrit dans [FIPS81].

5.3.2.2 KEK_ALG_3DES

Ce type spécifie 3DES en utilisant trois clés indépendantes comme décrit dans "Keying Option 1" dans [FIPS46-3].

5.3.2.3 KEK_ALG_AES

Ce type spécifie AES comme décrit dans [FIPS197]. Le mode de fonctionnement pour AES est CBC comme défini dans [SP.800-38A].

5.3.3 KEK_KEY_LENGTH

La classe KEK_KEY_LENGTH spécifie la longueur de la clé d'algorithme de KEK (en bits). Le contrôleur de groupe/serveur de clé (GCKS) ajoute l'attribut KEK_KEY_LENGTH à la charge utile SA lors de la distribution de la politique de KEK aux membres du groupe. Le membre du groupe vérifie si il a ou non la capacité d'utiliser une clé de chiffrement de cette taille. Si la définition du chiffrement inclut une longueur fixe de clé (par exemple, KEK_ALG_3DES) le membre du groupe peut prendre sa décision en utilisant seulement l'attribut KEK_ALGORITHM et n'a pas besoin de l'attribut KEK_KEY_LENGTH. L'envoi de l'attribut KEK_KEY_LENGTH dans la charge utile SA est FACULTATIF si le chiffrement de KEK a une longueur de clé fixe. Aussi, noter que la KEK_KEY_LEN inclut seulement la longueur réelle de la clé de chiffrement (la longueur d'IV n'est pas incluse dans cet attribut).

5.3.4 KEK_KEY_LIFETIME

La classe KEK_KEY_LIFETIME spécifie la durée maximale pendant laquelle la KEK est valide. Le GCKS peut rafraîchir la KEK à tout moment avant la fin de la période valide. La valeur est un nombre de 4 octets qui définit une durée de validité en secondes.

5.3.5 SIG_HASH_ALGORITHM

SIG_HASH_ALGORITHM spécifie l'algorithme de hachage de charge utile SIG. Le tableau qui suit définit les algorithmes pour SIG_HASH_ALGORITHM.

Type d'algorithme	Valeur
Réservé	0
SIG_HASH_MD5	1
SIG_HASH_SHA1	2
SIG_HASH_SHA256	3
SIG_HASH_SHA384	4
SIG_HASH_SHA512	5
Non alloué	6-127
Utilisation privée	128-255
Non alloué	256-65535

Les algorithmes de hachage SHA sont définis dans la norme de hachage sûr [FIPS180-3.2008].

Si le SIG_ALGORITHM est SIG_ALG_ECDSA-256, SIG_ALG_ECDSA-384, ou SIG_ALG_ECDSA-521, l'algorithme de hachage est implicite dans la définition, et SIG_HASH_ALGORITHM est FACULTATIF dans une charge utile SAK.

5.3.6 SIG_ALGORITHM

La classe SIG_ALGORITHM spécifie l'algorithme de signature de charge utile SIG. Les valeurs définies sont spécifiées dans le tableau suivant.

Type d'algorithme	Valeur
Réservé	0
SIG_ALG_RSA	1
SIG_ALG_DSS	2
SIG_ALG_ECDSS	3
SIG_ALG_ECDSA-256	4
SIG_ALG_ECDSA-384	5
SIG_ALG_ECDSA-521	6
Non alloué	7-127
Utilisation privée	128-255
Non alloué	256-65535

5.3.6.1 SIG_ALG_RSA

Cet algorithme spécifie l'algorithme de signature numérique RSA qui utilise la méthode de codage EMSA-PKCS1-v1_5, comme décrit dans la [RFC3447].

5.3.6.2 SIG_ALG_DSS

Cet algorithme spécifie l'algorithme de signature numérique DSS comme décrit au paragraphe 4 de [FIPS186-3].

5.3.6.3 SIG_ALG_ECDSS

Cet algorithme spécifie l'algorithme de signature numérique de courbe elliptique comme décrit au paragraphe 5 de [FIPS186-3]. Cette définition est déconseillée en faveur de la famille d'algorithmes SIG_ALG_ECDSA.

5.3.6.4 SIG_ALG_ECDSA-256

Cet algorithme spécifie le groupe ECP aléatoire à 256 bits , comme décrit dans la [RFC5903]. Le format de la signature dans la charge utile SIG DOIT être celui spécifié dans la [RFC4754].

5.3.6.5 SIG_ALG_ECDSA-384

Cet algorithme spécifie le groupe ECP aléatoire à 384 bits, comme décrit dans la [RFC5903]. Le format de la signature dans la charge utile SIG DOIT être celui spécifié dans la [RFC4754].

5.3.6.6 SIG_ALG_ECDSA-521

Cet algorithme spécifie le groupe ECP aléatoire à 521 bits, comme décrit dans la [RFC5903]. Le format de la signature dans la charge utile SIG DOIT être celui spécifié dans la [RFC4754].

5.3.7 SIG_KEY_LENGTH

La classe SIG_KEY_LENGTH spécifie la longueur de la clé de charge utile SIG en bits.

5.4 Politique associée au groupe

Un GCKS peut avoir une politique spécifique de groupe qui n'est pas distribuée dans une SA TEK ou une SA KEK. Certaines de ces politiques ne sont pas pertinentes pour tous les membres du groupe, et certaines sont des politiques spécifiques de l'envoyeur pour un membre particulier du groupe. Les premières peuvent être distribuées dans un échange GROUPKEY-PULL ou un échange GROUPKEY-PUSH, tandis que la dernière DOIT n'être envoyée que dans un échange GROUPKEY-PULL. De plus, un membre du groupe a parfois besoin de faire des demandes de politique pour des ressources du GCKS dans un échange GROUPKEY-PULL. Le GDOI distribue cette politique associée au groupe et les demandes de politique dans la charge utile Politique associée au groupe (GAP, *Group Associated Policy*).

La charge utile GAP peut être distribuée par le GCKS au titre de la charge utile SA. Elle suit toute charge utile SA KEK et est placée avant toute charge utile SA TEK. Dans le cas où la politique du groupe n'inclut pas une SA KEK, le champ d'attribut de SA Prochaine charge utile dans la charge utile SA PEUT indiquer la charge utile GAP.

La charge utile GAP peut être facultativement incluse par un membre du groupe dans le message 3 de l'échange GROUPKEY-PULL afin de faire des demandes de politique.

La charge utile GAP est définie comme suit :

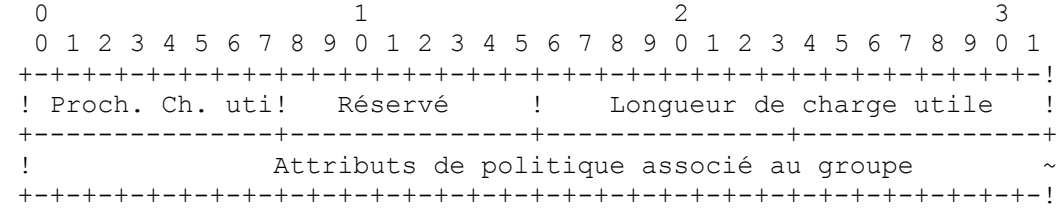


Figure 6 : Charge utile GAP

Les champs de charge utile GAP sont définis comme suit :

- Prochaine charge utile (1 octet) – Identifie la prochaine charge utile présente dans le message GROUPKEY-PULL ou GROUPKEY-PUSH. Le seul type valide de prochaine charge utile pour ce message est une SA TEK ou zéro pour indiquer qu'il n'y a plus d'attribut d'association de sécurité.
- Réservé (1 octet) -- DOIT être zéro.

- o Longueur de charge utile (2 octets) – Longueur de cette charge utile, incluant l'en-tête GAP et les attributs.
- o Attributs de politique associée au groupe (variable) – Contient les attributs suivant le format défini au paragraphe 3.3 de la [RFC2408]. Dans le tableau, les attributs qui sont définis comme TV sont marqués comme basiques (B) ; les attributs qui sont définis comme TLV sont marqués comme variables (V).

Type d'attribut	Valeur	Type
Réservé	0	
ACTIVATION_TIME_DELAY	1	B
DEACTIVATION_TIME_DELAY	2	B
SENDER_ID_REQUEST	3	B
Non alloué	4-127	
Utilisation privée	128-255	
Non alloué	256-32767	

Plusieurs attributs de politique associée au groupe sont définis dans le présent mémoire. Une mise en œuvre de GDOI DOIT l'interrompre si elle rencontre un attribut ou capacité qu'elle ne comprend pas. Les valeurs pour ces attributs sont incluses dans la section Considérations relatives à l'IANA de ce mémoire.

5.4.1 ACTIVATION_TIME_DELAY/DEACTIVATION_TIME_DELAY

Le paragraphe 4.2.1 de la [RFC5374] spécifie une méthode de retour à zéro de clés qui exige que deux valeurs lui soit données par le protocole de gestion de clé de groupe. L'attribut ACTIVATION_TIME_DELAY permet à un GCKS de régler le délai d'heure d'activation (ATD, *Activation Time Delay*) pour les SA générées à partir des TEK. Le ATD définit combien de temps après la réception de nouvelles SA elles doivent être activées par le GM. La valeur de l'ATD est en secondes.

L'attribut DEACTIVATION_TIME_DELAY permet au GCKS de régler le délai d'heure de désactivation (DTD, *Deactivation Time Delay*) pour les SA précédemment distribuées. Le DTD définit combien de temps DEVRAIT s'écouler après avoir reçu de nouvelles SA avant de désactiver les SA qui sont détruites par l'événement de changement de clés. La valeur est en secondes.

Les valeurs de ATD et DTD sont indépendantes. Cependant, la politique la plus efficace aura la valeur de DTD la plus grande, car elle permet que les nouvelles SA soient activées après que les plus anciennes SA sont désactivées. Une telle politique assure que le trafic de groupe protégé va toujours s'écouler sans interruption.

5.4.2 SENDER_ID_REQUEST

L'attribut SENDER_ID_REQUEST est utilisé par un membre du groupe pour demander des SID durant le message GROUPKEY-PULL, et inclut un compte du nombre de valeurs de SID qu'il désire.

5.5 Charge utile SA TEK

La charge utile SA TEK (SAT) contient les attributs de sécurité pour une seule TEK associée à un groupe.

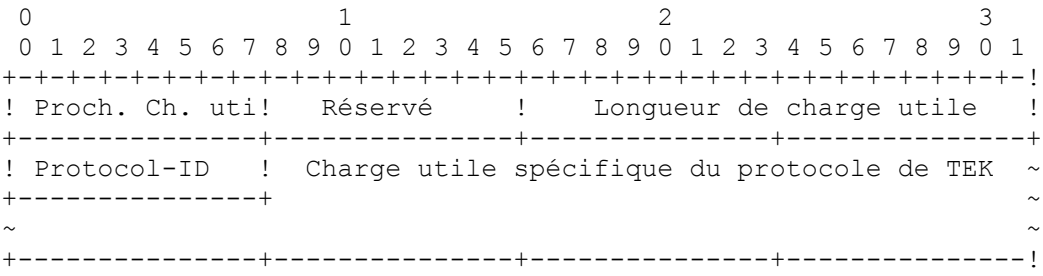


Figure 7 : Charge utile SA TEK

Les champs de la charge utile SAT sont définis comme suit :

- o Prochaine charge utile (1 octet) – Identifie la prochaine charge utile pour le message GROUPKEY-PULL ou GROUPKEY-PUSH. Les seuls types valides de prochaine charge utile pour ce message sont une autre charge utile SAT ou zéro pour indiquer qu'il n'y a plus d'attribut d'association de sécurité.

- Réservé (1 octet) -- DOIT être zéro.

- Longueur de charge utile (2 octets) – Longueur de cette charge utile, incluant la charge utile spécifique du protocole de TEK.

- Protocol-ID (1 octet) -- Valeur qui spécifie le protocole de sécurité. Le tableau suivant définit les valeurs pour le protocole de sécurité.

Identifiant de protocole	Valeur
Réservé	0
GDOI_PROTO_IPSEC_ESP	1
GDOI_PROTO_IPSEC_AH	2
Non alloué	3-127
Utilisation privée	128-255

- Charge utile spécifique du protocole de TEK (variable) – C'est la charge utile qui décrit les attributs spécifiques pour l'identifiant de protocole.

5.5.1 GDOI_PROTO_IPSEC_ESP/GDOI_PROTO_IPSEC_AH

La charge utile spécifique de protocole de TEK pour ESP et AH est comme suit :

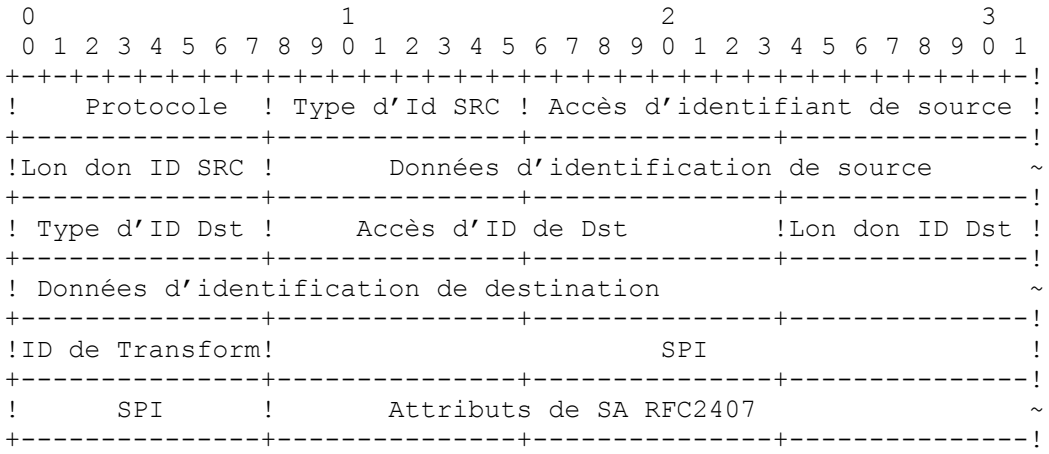


Figure 8 : Charge utile ESP/AH de TEK

Les champs de la charge utile SAT sont définis comme suit :

- Protocole (1 octet) -- Valeur qui décrit un identifiant de protocole IP (par exemple, UDP/TCP) [PROT-REG]. Une valeur de zéro signifie que le champ Protocole DOIT être ignoré.
- Type d'Id SRC (1 octet) -- Valeur qui décrit les informations d'identité trouvées dans le champ Données d'identification de source. Les valeurs définies sont spécifiées par la section Type d'identification IPsec dans le registre ISAKMP de l'IANA [ISAKMP-REG].
- Accès d'identifiant de source (2 octets) -- Valeur qui spécifie un accès associé à l'identifiant de source. Une valeur de zéro signifie que le champ Accès d'identifiant de source DOIT être ignoré.
- Lon don ID SRC (1 octet) -- Valeur qui spécifie la longueur (en octets) du champ Données d'identification de source.
- Données d'identification de source (longueur variable) -- Valeur, comme indiqué par le type d'identifiant de source. Réglé à 3 octets ou zéro pour les groupes de diffusion groupe à sources multiples qui utilisent une TEK commune pour tous les envoyeurs.
- Type d'ID Dst (1 octet) -- Valeur qui décrit les informations d'identité trouvées dans le champ Données d'identification de destination. Les valeurs définies sont spécifiées par la section Type d'identification IPsec dans le registre ISAKMP de l'IANA [ISAKMP-REG].
- Accès d'ID de Dst (2 octets) -- Valeur qui spécifie un accès associé à l'identifiant de destination. Une valeur de zéro signifie que le champ Accès d'ID de Dst DOIT être ignoré.
- Lon don ID Dst (1 octet) -- Valeur qui spécifie la longueur (en octets) du champ Données d'identification de destination.
- Données d'identification de destination (longueur variable) -- Valeur, comme indiquée par le type d'ID Dst.
- ID de Transform (1 octet) -- Valeur qui spécifie quelle transformation ESP ou AH est à utiliser. La liste des valeurs valides est définie dans la section Identifiants de transformation ESP ou AH IPsec du registre ISAKMP de l'IANA

[ISAKMP-REG].

- SPI (4 octets) – Indice de paramètre de sécurité pour ESP.
- Attributs de SA RFC2407 – Attributs ESP et AH selon le paragraphe 4.5 de la [RFC2407]. Le GDOI prend en charge tous les attributs de SA DOI IPsec pour GDOI_PROTO_IPSEC_ESP et GDOI_PROTO_IPSEC_AH, à l'exclusion de la description de groupe (paragraphe 4.5 de la [RFC2407]) qui NE DOIT PAS être envoyé par une mise en œuvre GDOI et est ignoré par une mise en œuvre GDOI si il est reçu. Les attributs suivants DOIVENT être pris en charge par une mise en œuvre qui prend en charge ESP et AH : SA Life Type, SA Life Duration, et Encapsulation Mode. Une mise en œuvre qui prend en charge ESP DOIT aussi prendre en charge l'attribut Algorithme d'authentification si la transformation ESP inclut l'authentification. L'attribut Algorithme d'authentification de IPsec DOI est l'authentification de groupe dans GDOI.

5.5.1.1 Nouveaux attributs d'association de sécurité IPsec

"Extensions de diffusion groupée à l'architecture de sécurité pour le protocole Internet" (RFC5374) introduit de nouvelles exigences pour un système de gestion de clé de groupe qui distribue la politique IPsec. Il définit aussi de nouveaux attributs au titre de la base de données de politique de sécurité de groupe (GSPD, *Group Security Policy Database*). Ces attributs décrivent la politique qu'un système de gestion de clé de groupe doit apporter à un membre du groupe afin de prendre en charge ces extensions. La charge utile GDOI SA TEK distribue la politique IPsec en utilisant les attributs d'association de sécurité IPsec définis dans [ISAKMP-REG]. Ce paragraphe définit comment GDOI peut convoyer les nouveaux attributs comme attributs d'association de sécurité IPsec.

5.5.1.1.1 Préservation d'adresse

Les applications utilisent les extensions de la [RFC5374] pour copier l'adresse IP dans l'en-tête IP externe lors de l'encapsulation d'un paquet IP comme paquet en mode tunnel IPsec. Cela permet qu'un paquet en diffusion groupée IP continue d'être acheminé comme paquet en diffusion groupée IP. Cet attribut fournit aussi la politique nécessaire de sorte que le membre du groupe GDOI puisse établir la GSPD de façon appropriée. Le tableau suivant définit les valeurs pour l'attribut Préservation d'adresse.

Type de préservation d'adresse	Valeur
Réservé	0
Aucune	1
Seulement source	2
Seulement destination	3
Source et destination	4
Non alloué	5-61439
Utilisation privée	61440-65535

Selon la politique du groupe, plusieurs méthodes de préservation d'adresse sont possibles : aucune préservation d'adresse ("Aucune"), préservation des adresse de la source originale ("Seulement source"), préservation de l'adresse de destination originale ("Seulement destination"), ou les deux adresses ("Source et destination"). Si cet attribut n'est pas inclus dans une charge utile GDOI SA TEK fournie par un GCKS, la préservation d'adresse de source et destination a été définie pour la SA TEK.

5.5.1.1.2 Direction de SA

Selon la politique du groupe, une SA IPsec créée à partir d'une charge utile SA TEK est définie comme étant dans la direction d'envoi et/ou de réception. Le tableau suivant définit les valeurs pour l'attribut Direction de SA.

Nom	Valeur
Réservé	0
Envoi seul	1
Réception seule	2
Symétrique	3
Non alloué	4-61439
Utilisation privée	61440-65535

La politique de SA TEK utilisée par plusieurs envoyeurs DOIT être installée dans les deux directions d'envoi et de réception ("Symétrique") tandis qu'une SA TEK pour un seul envoyeur DEVRAIT être installée dans la direction de réception par les receveurs ("Réception seule") et dans la direction d'envoi par l'envoyeur ("Envoi seul").

Une charge utile SA TEK qui ne comporte pas l'attribut Direction de SA est traitée comme une SA IPsec symétrique. Noter que symétrique est la seule valeur qui puisse avoir un sens pour une SA TEK distribuée dans un message GROUPKEY-PUSH. Autrement, Réception seule pourrait être distribué, mais les envoyeurs du groupe auraient besoin d'être configurés à ne pas recevoir les messages GROUPKEY-PUSH afin de conserver leur rôle.

5.5.2 Autres protocoles de sécurité

Au delà de ESP et AH, GDOI devrait servir à établir des SA pour des groupes sûr nécessaires pour d'autres protocoles de sécurité qui fonctionnent aux couches transport, application, et inter-réseau. Ces autres protocoles de sécurité sont cependant en cours de développement ou n'existent pas encore.

Les informations suivantes doivent être fournies au GDOI par un protocole de sécurité.
- o L'identifiant de protocole pour le protocole de sécurité particulier
- o La taille du SPI
- o La méthode de génération du SPI
- o Les transformations, attributs, et clés nécessaires pour le protocole de sécurité

Tous les protocoles de sécurité DOIVENT fournir les informations de la liste ci-dessus pour guider la spécification de GDOI pour ce protocole. Les définitions pour la prise en charge de ces protocoles de sécurité dans GDOI seront spécifiées dans des documents séparés.

Un protocole de sécurité PEUT protéger le trafic à tout niveau de la pile réseau. Cependant, dans tous les cas, les applications du protocole de sécurité DOIVENT protéger le trafic qui PEUT être partagé par plus de deux entités.

5.6 Charge utile de téléchargement de clé

La charge utile Téléchargement de clé contient des clés de groupe pour le groupe spécifié dans la charge utile SA. Ces charges utiles Téléchargement de clé peuvent avoir plusieurs attributs de sécurité qui leur sont appliqués sur la base de la politique de sécurité du groupe comme défini par la charge utile SA associée.

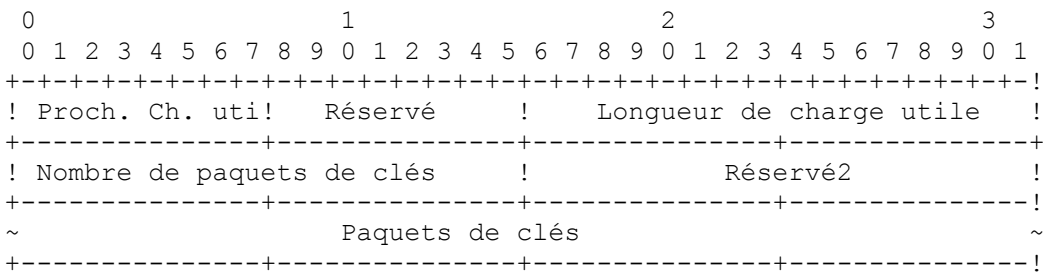


Figure 9 : Charge utile de téléchargement de clé

Les champs de charge utile Téléchargement de clé sont définis comme suit :

- o Proch. Ch. uti (1 octet) – Identifiant pour le type de charge utile de la prochaine charge utile dans le message. Si la charge utile en cours est la dernière du message, ce champ sera alors à zéro.
- o Réservé (1 octet) – Non utilisé; réglé à zéro.
- o Longueur de charge utile (2 octets) -- Longueur en octets de la charge utile en cours, incluant l'en-tête générique de charge utile.
- o Nombre de paquets de clés (l octets) -- Contient le nombre total de paquets de clés qui sont passés dans ce bloc de données.
- o Paquets de clés (variable) –Plusieurs types de paquets de clés sont définis. Chaque paquet de clé a le format suivant.

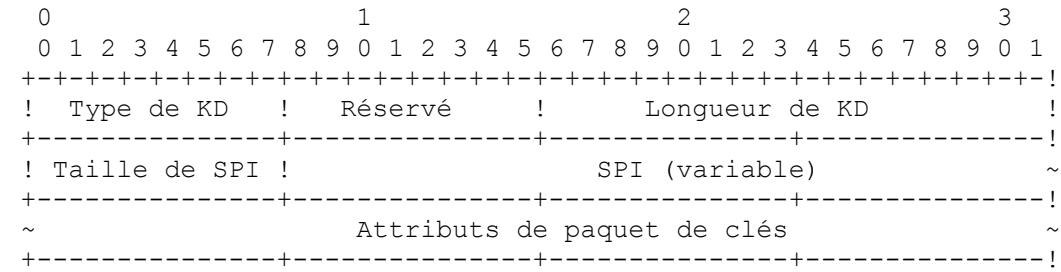


Figure 10 : Paquet de clés

- o Type de téléchargement de clé (KD) (1 octet) – Identifiant pour le champ Données de clé de ce paquet de clés.

Type de téléchargement de clé	Valeur
Réservé	0
TEK	1
KEK	2
LKH	3
SID	4
Non alloué	4-127
Utilisation privée	128-255

"KEK" est une seule clé, tandis que LKH est un dispositif de clés de chiffrement de clés.

- Réservé (1 octet) – Non utilisé; réglé à zéro.
- Longueur de KD (2 octets) -- Longueur en octets des données du paquet de clés, y compris l'en-tête du paquet de clés.
- Taille de SPI (1 octet) -- Valeur qui spécifie la longueur en octets du SPI comme défini par l'identifiant de protocole.
- SPI (longueur variable) – Indice de paramètre de sécurité, qui correspond au SPI précédemment envoyé dans une charge utile SAK ou SAT.
- Attributs de paquets de clés (longueur variable) – Contient les informations de clés. Le format de ce champ est spécifique de la valeur du champ Type de KD. Les paragraphes suivants décrivent le format de chaque type de KD.

5.6.1 Type téléchargement de TEK

Les attributs suivants peuvent être présents dans un type de téléchargement de TEK. Exactement un attribut correspondant à chaque type envoyé dans la charge utile SAT DOIT être présent. Les attributs doivent respecter le format défini dans ISAKMP (paragraphe 3.3 de la [RFC2408]). Dans le tableau, les attributs définis comme TV sont marqués basique (B) ; les attributs définis comme TLV sont marqués variables (V).

Classe de TEK	Valeur	Type
Réservé	0	
TEK_ALGORITHM_KEY	1	V
TEK_INTEGRITY_KEY	2	V
TEK_SOURCE_AUTH_KEY	3	V
Non alloué	4-127	
Utilisation privée	128-255	
Non alloué	256-32767	

Si aucun paquet de clé TEK n'est inclus dans une charge utile Enregistrement KD, le membre du groupe peut s'attendre à recevoir la TEK au titre d'une SA Rekey. Au moins une TEK doit être incluse dans chaque charge utile Rekey KD. Plusieurs TEK peuvent être incluses si plusieurs flux associés à la SA doivent subir un changement de clé.
Lorsque une spécification d'algorithme précise le format du matériel de clés, la valeur transportée dans la charge utile KD pour cette clé est passée conformément à cette spécification. Le matériel de clés peut contenir des informations qui vont au delà de la clé. Par exemple, la [RFC4106] "Utilisation du mode compteur/de Galois (GCM) dans la charge utile de sécurité encapsulée dans IPsec (ESP)" définit une valeur de sel au titre de KEYMAT.

5.6.1.1 TEK_ALGORITHM_KEY

La classe TEK_ALGORITHM_KEY déclare que la clé de chiffrement pour ce SPI est contenue comme l'attribut Paquet de clé. L'algorithme de chiffrement qui va utiliser cette clé a été spécifié dans la charge utile SAT.
Dans le cas où l'algorithme requiert plusieurs clés (par exemple, 3DES) toutes les clés seront incluses dans un attribut.

Les clés DES vont comporter 64 bits (les 56 bits de clé plus les bits de parité). Les clés Triple DES seront spécifiées comme un seul attribut de 192 bits (incluant les bits de parité) dans l'ordre selon lequel les clés doivent être utilisées pour le chiffrement (par exemple, DES_KEY1, DES_KEY2, DES_KEY3).

5.6.1.2 TEK_INTEGRITY_KEY

La classe TEK_INTEGRITY_KEY déclare que la clé d'intégrité pour ce SPI est contenue comme attribut Paquet de clé. L'algorithme d'intégrité qui va utiliser cette clé a été spécifié dans la charge utile SAT. Donc, GDOI suppose que le chiffrement symétrique et les clés d'intégrité sont tous deux poussés au GM. Les clés HMAC-SHA1 vont consister en 160 bits [RFC2404], et les clés HMAC-MD5 vont consister en 128 bits [RFC2403]. Les clés HMAC-SHA2 et AES-GMAC auront une longueur de clé égale à la longueur de sortie des fonctions de hachage [RFC4543], [RFC4868].

5.6.1.3 TEK_SOURCE_AUTH_KEY

La classe TEK_SOURCE_AUTH_KEY déclare que la clé d'authentification de source pour ce SPI est contenue dans l'attribut Paquet de clé. L'algorithme d'authentification de source qui va utiliser cette clé a été spécifié dans la charge utile SAT.

5.6.2 Type Téléchargement de KEK

Les attributs suivants peuvent être présents dans un type Téléchargement de KEK. Exactement un attribut correspondant à chaque type envoyé dans la charge utile SAK DOIT être présent. Les attributs DOIVENT suivre le format défini dans ISAKMP (paragraphe 3.3 de la [RFC2408]). Dans le tableau, les attributs définis comme TV sont marqués basiques (B) ; les attributs définis comme TLV sont marqués variables (V).

Classe de KEK	Valeur	Type
Réservé	0	
KEK_ALGORITHM_KEY	1	V
SIG_ALGORITHM_KEY	2	V
Non alloué	3-127	
Utilisation privée	128-255	
Non alloué	256-32767	

Si le paquet de clé KEK est inclus, il DOIT y en avoir seulement un de présent dans la charge utile KD.

5.6.2.1 KEK_ALGORITHM_KEY

La classe KEK_ALGORITHM_KEY déclare la clé de chiffrement pour ce SPI qui est contenue dans l'attribut Paquet de clé. L'algorithme de chiffrement qui va utiliser cette clé a été spécifié dans la charge utile SAK.
Si le mode de fonctionnement de l'algorithme exige un IV, un IV explicite DOIT être inclus dans le KEK_ALGORITHM_KEY avant la clé réelle.

5.6.2.2 SIG_ALGORITHM_KEY

La classe SIG_ALGORITHM_KEY déclare que la clé publique pour ce SPI est contenue dans l'attribut Paquet de clé, qui peut être utile lorsque aucune infrastructure de clé publique n'est disponible. L'algorithme de signature qui va utiliser cette clé a été spécifié dans la charge utile SAK.

5.6.3 Type de téléchargement de LKH

Le paquet de clés LKH comporte les attributs qui représentent différents nœuds dans l'arborescence de clés LKH.

Les attributs suivants sont utilisés pour passer un dispositif de KEK LKH dans la charge utile KD. Les attributs DOIVENT respecter le format défini dans ISAKMP (paragraphe 3.3 de la [RFC2408]). Dans le tableau, les attributs définis avec un TV sont marqués par basique (B) ; les attributs définis par un TLV sont marqués comme variables (V).

Classe de KEK	Valeur	Type
Réservé	0	
LKH_DOWNLOAD_ARRAY	1	V
LKH_UPDATE_ARRAY	2	V
SIG_ALGORITHM_KEY	3	V
Non alloué	4-127	
Utilisation privée	128-255	
Non alloué	256-32767	

Si un paquet de clés LKH est inclus dans la charge utile KD, il DOIT y en avoir seulement un de présent.

5.6.3.1 LKH_DOWNLOAD_ARRAY

Cet attribut est utilisé pour télécharger un ensemble de clés à un membre du groupe. Il NE DOIT PAS être inclus dans une charge utile KD de message GROUPKEY-PUSH si le GROUPKEY-PUSH est envoyé à plus d'un membre du groupe. Si un attribut LKH_DOWNLOAD_ARRAY est inclus dans une charge utile KD, il DOIT seulement y en avoir un de présent. Cet attribut consiste en un bloc d'en-tête, suivi par une ou plusieurs clés LKH.

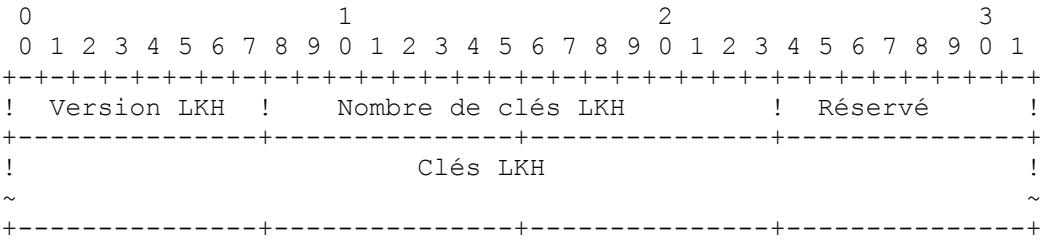


Figure 11 : Dispositif de téléchargement LKH

Les champs de l'attribut KEK_LKH sont définis comme suit :

- Version LKH (1 octet) – C'est la version du format de données LKH. Doit être un.
- Nombre de clés LKH (2 octets) -- Cette valeur est le nombre de clés LKH distinctes dans cette séquence.
- Réservé (1 octet) – Non utilisé ; réglé à zéro.

Chaque clé LKH est définie comme suit :

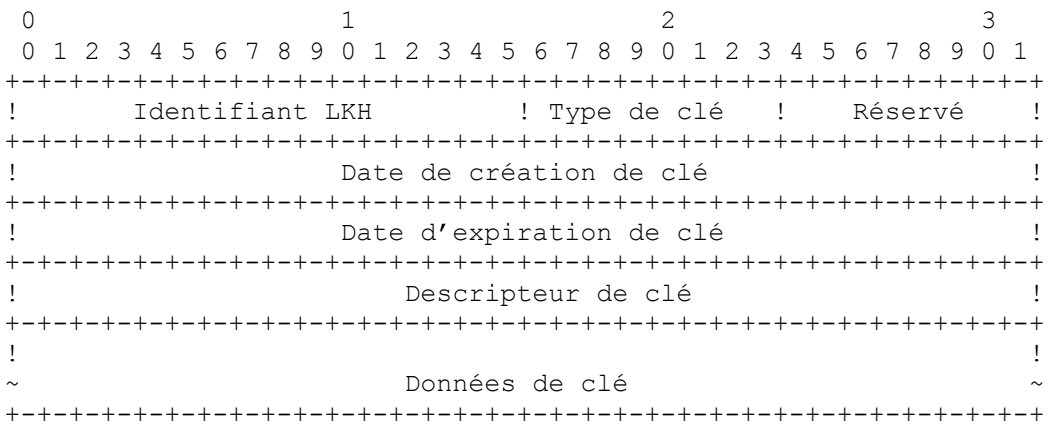


Figure 12 ; Clé LKH

- Identifiant LKH (2 octets) -- Identité du nœud LKH. Un GCKS est libre de choisir l'identifiant d'une manière spécifique de la mise en œuvre (par exemple, la position de cette clé dans une structure arborescente binaire utilisée par LKH).

- Type de clé (1 octet) – Algorithme de chiffrement pour lequel ces données de clé sont à utiliser. Cette valeur est spécifiée au paragraphe 5.3.3.

- Réservé (1 octet) – Non utilisé ; réglé à zéro.

- Date de création de clé (4 octets) – Valeur horaire non signée qui définit une période de validité en secondes représentant le nombre de secondes depuis 0 heure, 0 minute, 0 seconde, du 1er janvier 1970, en temps universel coordonné (UTC), sans inclure de saut de secondes [RFC5905]. C'est l'heure à laquelle les données de clé ont été générées à l'origine. Une valeur horaire de zéro indique qu'il n'y a pas de temps avant que cette clé ne soit pas valide.

- Date d'expiration de clé (4 octets) -- Valeur horaire non signée qui définit une période de validité en secondes représentant le nombre de secondes depuis 0 heure, 0 minute, 0 seconde, du 1er janvier 1970, en temps universel coordonné (UTC), sans inclure de saut de secondes [RFC5905]. C'est l'heure à laquelle l'utilisation de la clé ne sera plus valide. Une valeur horaire de zéro indique que cette clé n'a pas d'heure d'expiration.

- Descripteur de clé (4 octets) -- Valeur allouée par le GCKS pour identifier de façon univoque une clé au sein d'un identifiant de LKH. Chaque nouvelle clé distribuée par le GCKS pour ce nœud aura une identité de descripteur de clé distincte des descripteurs de clé précédents ou suivants spécifiés pour ce nœud.

- Données de clé (longueur variable) – Données de clé, qui dépendent de l'algorithme de type de clé pour son format. Si le mode de fonctionnement pour l'algorithme exige un IV, un IV explicite DOIT être inclus dans le champ Données de clé ajouté devant la clé réelle.

Les dates de création de clé et d'expiration de clé PEUVENT être zéro. Cela est nécessaire dans le cas où la synchronisation n'est pas possible au sein du groupe.

La première structure de clé LKH dans un attribut LKH_DOWNLOAD_ARRAY contient l'identifiant de feuille et la clé pour le membre du groupe. Le reste de la structure de clé LKH contient des clés le long du chemin de l'arborescence de clés dans l'ordre des feuilles, culminant à la KEK de groupe.

5.6.3.2 LKH_UPDATE_ARRAY

Cet attribut est utilisé pour mettre à jour les clés pour un groupe. Il est très vraisemblablement à inclure dans une charge utile de message GROUPKEY-PUSH KD pour changer les clés du groupe entier. Cet attribut consiste en un bloc d'en-tête, suivi par une ou plusieurs clés LKH, comme défini au paragraphe précédent.

Il peut y avoir n'importe quel nombre d'attributs UPDATE_ARRAY inclus dans une charge utile KD.

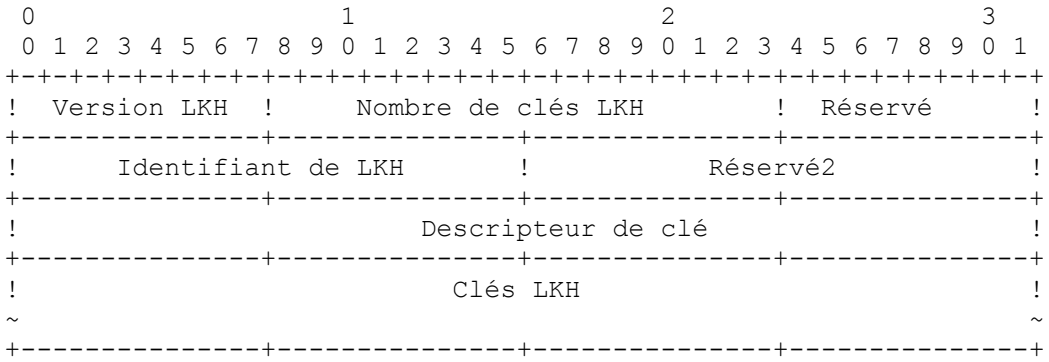


Figure 13 : Dispositif de mise à jour de LKH

- Version LKH (1 octet) -- Version du format de données de LKH. Doit être un.
- Nombre de clés de LKH (2 octets) -- Nombre de clé LKH distinctes dans cette séquence.
- Réservé (1 octet) – Non utilisé; réglé à zéro.
- Identifiant de LKH (2 octets) – Identifiant de nœud associé à la clé utilisée pour chiffrer la première clé de LKH.
- Réservé2 (2 octets) -- Non utilisé; réglé à zéro.
- Descripteur de clé (4 octets) -- Valeur allouée par le GCKS pour identifier de façon univoque la clé au sein de l'identifiant de LKH utilisé pour chiffrer la première clé LKH.

Les clés LKH sont comme défini au paragraphe précédent. Les structures de clé LKH contiennent des clés le long du chemin de l'arborescence de clés dans l'ordre depuis l'identifiant LKH trouvé dans l'en-tête LKH_UPDATE_ARRAY, culminant dans la KEK de groupe. Le champ Données de clé de chaque clé LKH est chiffré avec la clé LKH qui la précède dans l'attribut LKH_UPDATE_ARRAY. La première clé LKH est chiffrée avec la clé définie par l'identifiant LKH et le descripteur de clé trouvé dans l'en-tête LKH_UPDATE_ARRAY.

5.6.3.3 SIG_ALGORITHM_KEY

La classe SIG_ALGORITHM_KEY déclare que la clé publique pour ce SPI est contenue dans l'attribut Paquet de clé, qui peut être utile lorsque aucune infrastructure de clé publique n'est disponible. L'algorithme de signature qui va utiliser cette clé a été spécifiée dans la charge utile SAK.

5.6.4 Type de téléchargement SID

Cet attribut est utilisé pour télécharger une ou plusieurs valeurs d'identifiant d'envoyeur (SID, *Sender-ID*) pour l'utilisation exclusive d'un membre du groupe.

Le type Téléchargement SID n'exige pas de SPI. Lorsque le type de KD est SID, le champ Taille de SPI DOIT être zéro, et le champ SPI est omis.

Classe de SID	Valeur	Type
Réservé	0	
NUMBER_OF_SID_BITS	1	B
SID_VALUE	2	V
Non alloué	3-128	
Utilisation privée	129-255	
Non alloué	256-32767	

Comme une valeur de SID est destinée à un seul membre du groupe, le type Téléchargement de SID NE DOIT PAS être distribué dans un message GROUPKEY-PUSH distribué à plusieurs membres du groupe.

5.6.4.1 NUMBER_OF_SID_BITS

La classe NUMBER_OF_SID_BITS déclare combien de bits du nom occasionnel de chiffrement vont représenter une valeur de SID. Cette valeur est appliquée à chaque valeur de SID distribuée dans le téléchargement de SID.

5.6.4.2 SID_VALUE

La classe SID_VALUE déclare une seule valeur de SID pour l'usage exclusif du membre du groupe. Plusieurs attributs

SID_VALUE PEUVENT être incluses dans un téléchargement de SID.

5.6.4.3 Sémantique du membre du groupe

La valeur de l'attribut SID_VALUE distribuée à un membre du groupe DOIT être utilisée par ce membre du groupe comme la portion du champ SID de l'IV pour toutes les SA de sécurité des données incluant un mode de fonctionnement fondé sur le compteur distribuées par le GCKS au titre de ce groupe.

Lorsque le champ IV spécifique de l'envoyeur (SSIV, *Sender-Specific IV*) pour toute SA de sécurité des données est épuisé, le membre du groupe NE DOIT PAS agir plus longtemps comme envoyeur sur cette SA en utilisant son SID actif. Le membre du groupe DEVRAIT se réenregistrer, et à ce moment le GCKS va produire un nouveau SID au membre du groupe, ainsi que soit les mêmes SA de sécurité des données, soit des SA de remplacement. Le nouveau SID remplace le SID existant utilisé par ce membre du groupe et aussi remet la valeur de SSIV à sa valeur de départ. Un membre du groupe PEUT se réenregistrer avant l'épuisement réel du champ SSIV pour éviter d'abandonner des paquets de données à cause de l'épuisement des valeurs de SSIV disponibles combiné à une valeur de SID particulière.

Le message GROUPKEY-PUSH peut inclure des SA de sécurité des données qui sont distribuées au membre du groupe pour la première fois. Un SID produit précédemment au membre du groupe receveur est utilisé avec les SA de sécurité des données en mode de fonctionnement fondé sur le compteur sur lesquelles le membre du groupe agit comme envoyeur. Comme cette SA de sécurité des données n'a pas été précédemment utilisée pour la transmission, le champ SSIV devrait être réglé à sa valeur de départ.

5.6.4.4 Sémantique du GCKS

Si une charge utile KD comporte du matériel de clés qui est associé à un mode de fonctionnement de compteur, une charge utile KD de type Téléchargement de SID contenant au moins un attribut SID_VALUE DOIT être incluse.

Le GCKS NE DOIT PAS envoyer la charge utile KD de type Téléchargement de SID au titre d'un message GROUPKEY-PUSH parce que distribuer la même politique spécifique de l'envoyeur à plus d'un membre du groupe réduirait la sécurité du groupe.

5.7 Charge utile Numéro de séquence

La charge utile Numéro de séquence (SEQ) fournit une protection anti répétition pour le message GROUPKEY-PUSH. Son utilisation est similaire à celle du champ Numéro de séquence défini dans le protocole ESP d'IPsec [RFC4303].

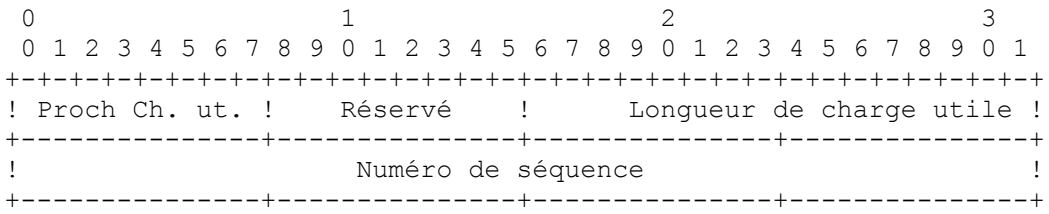


Figure 14 : Charge utile Numéro de séquence

Les champs de la charge utile Numéro de séquence sont définis comme suit :

- Proch Ch. ut. (1 octet) – Identifiant pour le type de charge utile de la prochaine charge utile dans le message. Si la charge utile en cours est la dernière du message, ce champ sera alors à zéro.

- Réservé (1 octet) – Non utilisé; réglé à zéro.

- Longueur de charge utile (2 octets) – Longueur en octets de la charge utile actuelle, y compris l'en-tête de charge utile générique. DOIT avoir la valeur 8.

- Numéro de séquence (4 octets) – Ce champ contient une valeur de compteur à accroissement monotone pour le groupe. Il est initialisé à zéro par le GCKS et incrémenté à chaque message transmis ultérieurement. Donc, le premier paquet envoyé pour une certaine SA Rekey aura un numéro de séquence de 1. La mise en œuvre de GDOI tient un compteur de séquences comme un attribut de la SA Rekey et incrémente le compteur à réception d'un message GROUPKEY-PUSH. La valeur actuelle du numéro de séquence DOIT être transmise aux membres du groupe au titre de l'enregistrement de la charge utile SA.

5.8 Nom occasionnel

La portion données de la charge utile Nom occasionnel (c'est-à-dire, Ni_b et Nr_b inclus dans les HASH) DOIT être une valeur entre 8 et 128 octets.

5.9 Charge utile Supprimer

Le GCKS peut parfois vouloir signaler aux receveurs de supprimer des SA, par exemple, à la fin d'une diffusion. La suppression des clés peut être accomplie par l'envoi d'une charge utile Supprimer ISAKMP (paragraphe 3.15 de la [RFC2408]) au titre d'un message GDOI GROUPKEY-PUSH.

Une ou plusieurs charges utiles Supprimer PEUVENT être placées à la suite de la charge utile SEQ dans un message GROUPKEY-PUSH. Si un GCKS n'a pas d'autre SA à envoyer aux membres du groupe, les charges utiles SA et KD DOIVENT être omises du message.

Les champs suivants de la charge utile Supprimer sont définis comme suit :

- Le champ Domaine d'interprétation contient le DOI GDOI.

- Le champ Identifiant de protocole contient les valeurs d'identifiant de protocole de TEK définies au paragraphe 5.5. Pour supprimer une SA de KEK, la valeur de zéro DOIT être utilisée comme identifiant de protocole. Noter qu'une seule valeur d'identifiant de protocole peut être définie dans une charge utile Supprimer. Donc, si une SA TEK et une SA KEK sont à supprimer, leurs valeurs de SPI DOIVENT être envoyées dans des charges utiles Supprimer différentes.

Il peut y avoir des circonstances où le GCKS peut vouloir démarrer avec une "ardoise propre". Si l'administrateur n'a plus confiance dans l'intégrité du groupe, le GCKS peut signaler la suppression de toutes les politiques d'un protocole de TEK particulier en envoyant une TEK avec une valeur de SPI égale à zéro dans la charge utile Supprimer. Par exemple, si le GCKS souhaite retirer toutes les KEK et toutes les TEK du groupe, le GCKS DEVRAIT envoyer une charge utile Supprimer avec un SPI de zéro et un Identifiant de protocole d'une valeur de Identifiant de protocole de TEK, suivie par une autre charge utile Supprimer avec une valeur de SPI de zéro et un identifiant de protocole de zéro, indiquant que la SA KEK devrait être supprimée.

6. Choix de l'algorithme

Pour que les mises en œuvre de GDOI interopèrent, elles doivent prendre en charge en commun un ou plusieurs algorithmes de sécurité. Cette section spécifie les exigences de mise en œuvre d'algorithme de sécurité pour les mises en œuvre de GDOI conformes à la norme. Dans tous les cas, les choix sont destinés à entretenir au moins 112 bits de sécurité [SP.800-131].

Des algorithmes non référencés dans cette section PEUVENT être utilisés.

6.1 KEK

Ces tableaux font la liste de la sélection d'algorithmes pour les valeurs qui se rapportent à la KEK.

Exigence	Algorithme de gestion de KEK
DEVRAIT	LKH

Exigence	Algorithme KEK (notes)
DOIT	KEK_ALG_AES avec clés de 128 bits
NE DEVRAIT PAS	KEK_ALG_DES (1)

Exigence	Algorithme de hachage de signature de KEK (notes)
DOIT	SIG_HASH_SHA256
DEVRAIT	SIG_HASH_SHA1 (2)
NE DEVRAIT PAS	SIG_HASH_MD5 (3)

Exigence	Algorithme de signature de KEK (notes)
DOIT	SIG_ALG_RSA avec clés de 2048 bits

Notes :
(1) DES, avec sa petite taille de clé et la force de sécurité correspondante, est d'une sécurité discutable pour une utilisation générale
(2) l'utilisation de SIG_HASH_SHA1 comme algorithme de hachage de signature utilisé avec des messages GROUPKEY-PUSH reste sûr au moment de la rédaction, et il est largement déployé.
(3) Bien qu'il n'ait pas été trouvé de réelle faiblesse de résistance de seconde préimage avec MD5 au moment de cette rédaction, il a été révélé que la force de la sécurité de MD5 décline rapidement au fil du temps, et son utilisation devrait être soigneusement comprise et soupesée.

6.2 TEK

Le tableau suivant fait la liste des exigences pour la prise en charge de protocole de sécurité par une mise en œuvre.

Exigence	Algorithme de gestion de KEK
DOIT	GDOI_PROTO_IPSEC_ESP

7. Considérations pour la sécurité

GDOI est un protocole de gestion d'association de sécurité (SA) pour des groupes d'envoyeurs et receveurs. Ce protocole effectue l'authentification des participants au protocole qui communiquent (Membre du groupe, Contrôleur de groupe/Serveur de clés). Il assure la confidentialité des messages de gestion de clés, et il assure l'authentification de la source de ces messages. GDOI comporte des défenses contre les attaques par interposition, de capture de connexion, de répétition, de réflexion, et de déni de service (DoS) sur les réseaux non sûrs. GDOI suppose que le réseau n'est pas sûr et peut être sous le contrôle complet d'un agresseur.

GDOI suppose que les membres du groupe et le GCKS sont sûrs même si le réseau n'est pas sûr. GDOI établit en fin de compte des clés entre les membres d'un groupe, qui DOIVENT être de confiance pour utiliser ces clés d'une manière autorisée conformément à la politique du groupe. Une entité GDOI compromise par un agresseur peut révéler les secrets nécessaires pour espionner le trafic du groupe et/ou prendre l'identité d'un envoyeur du groupe, de sorte que les mesures de sécurité des hôtes qui limitent l'accès non autorisé sont de la plus haute importance. Cette dernière menace pourrait être atténuée en utilisant l'authentification de la source d'origine dans les SA de sécurité des données (par exemple, l'utilisation de signatures RSA [RFC4359] ou TESLA [RFC4082]). Le choix des SA de sécurité des données est une affaire de politique du groupe et sort du domaine d'application du présent mémoire.

Il y a trois phases de GDOI, comme décrit dans ce document : un protocole de phase 1 ISAKMP, l'échange GROUPKEY-PULL protégé par le protocole ISAKMP de phase 1, et le message GROUPKEY-PUSH. Chaque phase est considérée séparément ci-dessous.

7.1 ISAKMP phase 1

GDOI utilise l'échange de phase 1 défini dans la [RFC2409] pour protéger l'échange GROUPKEY-PULL. Donc, toutes les propriétés de sécurité et les considérations sur ces échanges (comme noté dans la [RFC2409]) sont pertinentes pour GDOI.

GDOI peut hériter des problèmes de ses protocoles antérieurs, tels que l'exposition de l'identité, l'absence d'authentification unidirectionnelle, ou de mouchards à états pleins [PK01].

7.1.1 Authentification

L'authentification est fournie via les mécanismes définis dans la [RFC2409], à savoir le chiffrement par des clés prépartagées ou par des clés publiques.

7.1.2 Confidentialité

La confidentialité est réalisée en phase 1 par un échange Diffie-Hellman qui fournit le matériel de clés et par la négociation de transformations de chiffrement.

Le protocole de phase 1 protègera les clés de chiffrement et d'intégrité envoyées dans le protocole GROUPKEY-PULL.

La force du chiffrement utilisé pour la phase 1 DEVRAIT excéder celle des clés envoyées dans le protocole GROUPKEY-PULL.

7.1.3 Protection contre l'attaque par interposition

Une attaque par interposition ou de capture de connexion réussie déjoue l'authentification d'entité d'une ou plusieurs entités en communication durant l'établissement des clés. GDOI s'appuie sur l'authentification de phase 1 pour combattre les attaques par interposition.

7.1.4 Protection contre l'attaque par répétition/réflexion

Dans une attaque en répétition/réflexion, un attaquant capture des messages entre les entités GDOI et les transmet ensuite à une entité GDOI. Les attaques en répétition et réflexion cherchent à obtenir des informations à partir d'un message de réponse GDOI suivant ou cherchent à interrompre le fonctionnement d'un membre GDOI ou d'une entité GCKS. GDOI s'appuie sur le mécanisme de nom occasionnel de phase 1 en combinaison avec un code d'authentification de message fondé sur le hachage pour protéger contre la répétition ou la réflexion de messages précédents de gestion de clés.

7.1.5 Protection contre l'attaque par déni de service

Une attaque de DoS envoie des messages à une entité GDOI pour amener cette entité à effectuer des opérations d'authentification de message inutiles. GDOI utilise le mécanisme de mouchard de phase 1 pour identifier les messages parasites avant de traiter le hachage cryptographique. C'est une forme "faible" de protection contre le déni de service en ce que l'entité GDOI doit vérifier que ce sont de bons mouchards, qui peuvent être imités avec succès par un attaquant sophistiqué. Le mécanisme de mouchard de phase 1 est à états pleins et engage des ressources de mémoire pour les mouchards.

7.2 Échange GROUPKEY-PULL

L'échange GROUPKEY-PULL permet à un membre du groupe de demander des SA et des clés à un GCKS. Il fonctionne comme un protocole de phase 2 sous la protection de l'association de sécurité de phase 1.

7.2.1 Authentification

L'authentification de l'homologue n'est pas exigée dans le protocole GROUPKEY-PULL. Elle fonctionne dans le contexte du protocole de phase 1, qui a précédemment authentifié l'identité de l'homologue.

L'authentification de message est fournie par les charges utiles HASH dans chaque message, où le HASH est défini comme étant sur SKEYID_a (déduit de l'échange de phase 1) l'identifiant de message ISAKMP, et toutes les charges utiles dans le message. Comme seulement deux points d'extrémité de l'échange connaissent la valeur du SKEYID_a, cela assure que c'est l'homologue qui a envoyé le message.

7.2.2 Confidentialité

La confidentialité est fournie par l'association de sécurité de phase 1, selon les modalités décrites dans la [RFC2409].

7.2.3 Protection contre l'attaque par interposition

L'authentification de message (décrite ci-dessus) comporte un secret connu seulement du membre du groupe et du GCKS lors de la construction d'une charge utile HASH. Cela empêche les attaques par interposition et par capture de connexion parce qu'un attaquant ne sera pas capable de changer le message sans être détecté.

7.2.4 Protection contre la répétition

Un message GROUPKEY-PULL identifie ses messages en utilisant une paire de mouchards provenant de l'échange de phase 1 qui le précède. Un message GROUPKEY-PULL avec des mouchards invalides sera éliminé. Donc, les messages GDOI qui ne sont pas associés à une session GDOI en cours seront éliminés sans autre traitement.

Les messages GDOI répétés qui sont associés à une session GDOI en cours seront déchiffrés et authentifiés. Le M-ID dans le HDR identifie une session. Les paquets répétés seront traités conformément à l'automate à états de cette session. Les

paquets qui ne correspondent pas à cet automate à états seront éliminés sans traitement.

7.2.5 Protection contre le déni de service

Les mises en œuvre de GCKS DEVRAIENT garder un enregistrement des messages GROUPKEY-PULL récemment reçus (par exemple, un hachage du paquet) et rejeter les messages qui ont déjà été traités. Cela assure la protection contre le DoS et la répétition des messages envoyés précédemment. Une mise en œuvre PEUT choisir de limiter le débit de réception des messages GDOI afin d'atténuer la surcharge de ses ressources de calcul.

Le GCKS NE DEVRAIT PAS effectuer de tâches coûteuses en calcul avant de recevoir un HASH avec son propre nom occasionnel inclus. Le GCKS NE DOIT PAS mettre à jour l'état de gestion de groupe (par exemple, l'arborescence de clés LKH, le compteur de SID) jusqu'à ce qu'il reçoive le troisième message de l'échange avec une charge utile HASH valide incluant son propre nom occasionnel.

7.2.6 Autorisation

Une mise en œuvre de GCKS DEVRAIT tenir une liste d'autorisations des membres autorisés du groupe. Un membre du groupe DOIT spécifiquement énumérer chaque GCKS autorisé dans sa base de données d'autorisation d'homologues du groupe (GPAD, *Group Peer Authorization Database*) [RFC5374].

7.3 Échange GROUPKEY-PUSH

L'échange GROUPKEY-PUSH est un seul message qui permet à un GCKS d'envoyer des SA et des clés aux membres du groupe. C'est vraisemblablement pour être envoyé à tous les membres en utilisant un groupe de diffusion groupée IP. Ce message fournit un changement de clés efficace et une capacité d'ajustement des membres du groupe.

7.3.1 Authentification

L'échange GROUPKEY-PULL distribue une clé publique qui est utilisé pour l'authentification de message. Le message GROUPKEY-PUSH est signé numériquement en utilisant la clé privée correspondante détenue par le GCKS. Cette signature numérique assure l'authentification de source pour le message. Donc, GDOI protège le GCKS d'une usurpation d'identité dans un environnement de groupe.

7.3.2 Confidentialité

Le GCKS chiffre le message GROUPKEY-PUSH avec une clé de chiffrement qui a été distribuée dans l'échange GROUPKEY-PULL ou dans un précédent échange GROUPKEY-PUSH. La clé de chiffrement peut être une simple KEK ou le résultat du calcul d'une méthode de gestion de groupe (par exemple, LKH).

7.3.3 Protection contre l'attaque par interposition

Cette combinaison de services de confidentialité et d'authentification de message protège le message GROUPKEY-PUSH des attaques par interposition et de capture de connexion.

7.3.4 Protection contre l'attaque par répétition/réflexion

Le message GROUPKEY-PUSH comporte un numéro de séquence à accroissement monotone pour protéger contre les attaques de répétition et de réflexion. Un membre du groupe va éliminer les numéros de séquence associés au SPI de KEK en cours qui ont la même valeur ou une valeur inférieure au numéro répété le plus récemment reçu.

Les mises en œuvre DEVRAIENT garder un enregistrement (par exemple, une valeur de hachage) des messages GROUPKEY-PUSH récemment reçus et rejeter les messages dupliqués avant d'effectuer des opérations cryptographiques. Cela permet une élimination précoce des messages répétés.

7.3.5 Protection contre l'attaque de déni de service

Une paire de mouchards identifie l'association de sécurité pour le message GROUPKEY-PUSH. Les mouchards servent donc de forme faible de protection contre le déni de service pour le message GROUPKEY-PUSH.

La signature numérique utilisée pour l'authentification de message a un coût de calcul bien plus important qu'un code d'authentification de message et pourrait amplifier les effets d'une attaque de DoS sur un membre GDOI qui traite les messages GROUPKEY-PUSH. Le coût supplémentaire des signatures numériques est justifié par le besoin d'empêcher l'usurpation d'identité du GCKS: Si une clé symétrique partagée était utilisée pour l'authentification du message GROUPKEY-PUSH, l'authentification de source du GCKS serait alors impossible, et tout membre serait capable de se faire passer pour le GCKS.

Le potentiel d'amplification d'une attaque de DoS par une signature numérique est atténué par l'ordre des opérations effectuées par le membre du groupe, où l'opération cryptographique la moins coûteuse est effectuée en premier. Le membre du groupe commence par déchiffrer le message en utilisant un chiffrement symétrique. Si la forme de ce message est valide, le numéro de séquence est alors comparé au numéro de séquence le plus récent reçu. C'est seulement quand le numéro de séquence est valide (c'est-à-dire, quand il a une valeur supérieure à celle reçue précédemment) que la signature numérique est vérifiée et que le message continue son traitement. Donc, afin qu'une attaque de DoS soit montée, un attaquant aura besoin de savoir la clé de chiffrement symétrique utilisée pour la confidentialité, et un numéro de séquence valide. Généralement parlant, cela signifie que seuls les membres actuels du groupe peuvent effectivement déployer une attaque de DoS.

7.4 Contrôle d'accès vers l'avant et vers l'arrière

Grâce à GROUPKEY-PUSH, le GDOI prend en charge des méthodes de gestion de clé telles que LKH (paragraphe 5.4 de la [RFC2627]) qui ont la propriété de refuser l'accès à une nouvelle clé de groupe à un membre retiré du groupe (contrôle d'accès vers l'avant) et à une ancienne clé du groupe à un membre ajouté au groupe (contrôle d'accès vers l'arrière). Les concepts de "contrôle d'accès vers l'avant" et de "contrôle d'accès vers l'arrière" ont aussi été décrits respectivement comme "sécurité parfaite vers l'avant" et "sécurité parfaite vers l'arrière", dans la littérature [RFC2412].

Des algorithmes de gestion de groupe qui assurent le contrôle d'accès vers l'avant et vers l'arrière autres que LKH ont été proposés dans la littérature, incluant des arborescences de fonction unidirectionnelle [OFT] et une différence de sous-ensemble [NNL]. Ces algorithmes pourraient être utilisés avec GDOI, mais ne sont pas spécifiés au titre de ce document.

7.4.1 Exigences du contrôle d'accès vers l'avant

Lorsque la composition du groupe est altérée en utilisant un algorithme de gestion de groupe, de nouvelles SA de sécurité des données sont normalement aussi nécessaires. De nouvelles SA assurent que les membres qui se sont vu refuser l'accès ne peuvent plus participer au groupe.

Si le contrôle d'accès vers l'avant est une propriété désirée pour le groupe, les nouvelles SA de sécurité des données NE DOIVENT PAS être incluses dans un message GROUPKEY-PUSH qui change la composition du groupe. Cela est nécessaire parce que les nouvelles SA de sécurité des données ne sont pas protégées par la nouvelle KEK. Deux messages GROUPKEY-PUSH en séquence doivent plutôt être envoyés par le GCKS ; le premier va changer la KEK, et le second (protégé par la nouvelle KEK) distribuant les nouvelles SA de sécurité des données.

Noter que dans la séquence ci-dessus, bien que la nouvelle KEK puisse effectivement refuser l'accès au groupe à certains membres du groupe, ils seront capables de voir la nouvelle politique de KEK. Si la politique de contrôle d'accès vers l'avant pour le groupe comporte de garder secrète la politique de KEK ainsi que la KEK elle-même, deux messages GROUPKEY-PUSH changeant la KEK doivent alors survenir avant que soient transmises les nouvelles SA de sécurité des données.

Si d'autres méthodes d'utilisation de LKH ou d'autres algorithmes de gestion de groupe sont ajoutés à GDOI, ces méthodes PEUVENT lever les restrictions ci-dessus qui exigent plusieurs messages GROUPKEY-PUSH, pourvu que ces méthodes spécifient comment la politique de contrôle d'accès est conservée au sein d'un seul message GROUPKEY-PUSH.

7.4.2 Exigences du contrôle d'accès vers l'arrière

Si le contrôle d'accès vers l'arrière est une propriété désirée pour le groupe, un nouveau membre NE DOIT PAS recevoir les SA de sécurité des données qui ont été utilisées avant son adhésion au groupe. Cela peut être accomplis si le GCKS ne donne la SA Rekey qu'aux nouveaux membres dans un échange GROUPKEY-PULL, suivi par un message GROUPKEY-PUSH qui à la fois supprime les SA de sécurité des données actuelles et fournit de nouvelles SA de sécurité des données de remplacement. Le nouveau membre du groupe va effectivement rejoindre le groupe au moment où les membres existants commencent à envoyer sur les SA de sécurité des données.

Si il y a une possibilité que le nouveau membre du groupe ait mémorisé les messages GROUPKEY-PUSH délivrés avant

son adhésion au groupe, la procédure ci-dessus n'est alors pas suffisante. Dans ce cas, pour réaliser le contrôle d'accès vers l'arrière, le GCKS a besoin de retourner une nouvelle SA Rekey au membre du groupe dans un échange GROUPKEY-PULL plutôt que celui existant. Le GCKS va ensuite délivrer deux messages GROUPKEY-PUSH. Le premier, destiné aux membres existants du groupe, distribue la nouvelle SA Rekey aux membres existants. Le GCKS va alors délivrer le second message GROUPKEY-PUSH en utilisant la nouvelle SA Rekey qui à la fois supprime les SA de sécurité des données actuelles et fournit de nouvelles SA de sécurité des données de remplacement. Les membres préexistants et les nouveaux membres vont tous deux traiter le second message GROUPKEY-PUSH, et tous seront capables de communiquer en utilisant les nouvelles SA de sécurité des données.

7.5 Déduction du matériel de clé

Un GCKS distribue le matériel de clés associé à des SA de sécurité des données et à la SA Rekey. Comme ces associations de sécurité sont utilisées par un ensemble de membres du groupe, ce matériel de clés n'est en relation avec aucune connexion par paire, et il n'y a pas d'exigence dans "l'architecture de sécurité de groupe de diffusion groupée" [RFC3740] que les membres du groupe permettent le matériel de clés de groupe. Comme le GCKS est seul responsable de la génération du matériel de clés, le GCKS DOIT déduire le matériel de clés en utilisant un générateur de nombres aléatoires fort. Comme il n'y a pas de souci d'interopérabilité avec la génération des clés, aucune méthode n'est prescrite dans GDOI.

8. Considérations relatives à l'IANA

8.1 Ajouts aux registres actuels

Il a été alloué à l'attribut de KEK GDOI appelé SIG_HASH_ALGORITHM [GDOI-REG] plusieurs nouvelles valeurs de type d'algorithme à partir de l'espace Réservé pour représenter les algorithmes de hachage SHA-256, SHA-384, et SHA-512, comme défini dans [FIPS180-3.2008]. Les noms des nouveaux algorithmes sont respectivement SIG_HASH_SHA256, SIG_HASH_SHA384, et SIG_HASH_SHA512, et ils ont respectivement les valeurs 3, 4, et 5.

Il a été alloué à l'attribut KEK GDOI appelé SIG_ALGORITHM [GDOI-REG] plusieurs nouvelles valeurs de type d'algorithme à partir de l'espace Réservé pour représenter les algorithmes de signature SIG_ALG_ECDSA-256, SIG_ALG_ECDSA-384, et SIG_ALG_ECDSA-521. Les valeurs de type d'algorithme sont respectivement 4, 5, et 6.

Un nouveau type d'identifiant de protocole de type de TEK de SA GDOI [GDOI-REG] a été alloué à partir de l'espace Réservé. Le nouvel identifiant d'algorithme est appelé GDOI_PROTO_IPSEC_AH, il se réfère à l'encapsulation AH d'IPsec, et a une valeur de 2.

Un nouveau type de Prochaine charge utile [ISAKMP-REG] a été alloué. Le nouveau type est appelé "SA de politique associée au groupe (GAP, *Group Associated Policy*)" et a une valeur de 22.

Un nouveau type de téléchargement de clé (paragraphe 5.6) a été alloué. Le nouveau type est appelé "SID" et a une valeur de 4.

8.2. Nouveaux registres

Un nouveau registre identifiant les valeurs possibles des attributs de politique de charge utile GAP (de la forme décrite au paragraphe 3.3 de la [RFC2408]) a été créé dans le registre Charges utiles GDOI [GDOI-REG]. Le présent mémoire définit les valeurs suivantes pour ce registre :

Type d'attribut	Valeur	Type
Réservé	0	
ACTIVATION_TIME_DELAY	1	B
DEACTIVATION_TIME_DELAY	2	B
SENDER_ID_REQUEST	3	B
Non alloué	4-127	
Utilisation privée	128-255	
Non alloué	256-32767	

La procédure d'enregistrement est l'action de normalisation. Les termes Action de normalisation et Utilisation privée sont à appliquer comme défini dans la [RFC5226].

Un nouvel attribut d'association de sécurité IPsec [ISAKMP-REG] définissant la préservation des adresses IP a été enregistré. La classe d'attribut est appelée "Préservation d'adresse", et est un type de base. Les règles suivantes s'appliquent pour définir les valeurs de l'attribut :

Nom	Valeur
Réservé	0
Aucune	1
Source-seule	2
Destination-seule	3
Source-et-Destination	4
Non alloué	5-61439
Utilisation privée	61440-65535

La procédure d'enregistrement est l'Action de normalisation. Les termes Action de normalisation et Utilisation privée sont à appliquer comme défini dans la [RFC5226].

Un nouvel attribut d'association de sécurité IPsec [ISAKMP-REG] définissant la direction de la SA a été créé. La classe d'attribut est appelée "SA Direction", et est un type de base. Les règles suivantes s'appliquent pour définir les valeurs de l'attribut :

Nom	Valeur
Réservé	0
Envoyeur-seul	1
Receveur-seul	2
Symétrique	3
Non alloué	4-61439
Utilisation privée	61440-65535

La procédure d'enregistrement est l'Action de normalisation. Les termes Action de normalisation et Utilisation privée sont à appliquer comme défini dans la [RFC5226].

Lorsque le SID "Type de téléchargement de clé" (décrit au paragraphe précédent) a un ensemble d'attributs, les attributs doivent suivre le format défini dans ISAKMP (paragraphe 3.3 de la [RFC2408]). Dans le tableau, les attributs définis comme TV sont marqués comme basiques (B) ; les attributs définis comme des TLV sont marqués variables (V).

Classse de SID	Valeur	Type
Réservé	0	
NUMBER_OF_SID_BITS	1	B
SID_VALUE	2	V
Non alloué	3-128	
Utilisation privée	129-255	
Non alloué	256-32767	

La procédure d'enregistrement est l'Action de normalisation. Les termes Action de normalisation et Utilisation privée sont à appliquer comme défini dans la [RFC5226].

8.3 Nettoyage des registres existants

Plusieurs registres existants de charge utile GDOI n'utilisent pas les termes de la RFC5226 et/ou ne décrivent par la gamme entière des valeurs possibles. Les paragraphes qui suivent corrigent ces registres. Les termes Action de normalisation , Non alloué, et Utilisation privée sont à appliquer comme défini dans la [RFC5226].

8.3.1. Algorithme Pop

La procédure d'enregistrement est l'Action de normalisation. Les valeurs 4 à 27 sont désignées comme Non allouées. Les valeurs 256 à 32767 ont été ajoutées et sont désignées comme Non allouées.

8.3.2 Attributs de KEK

La procédure d'enregistrement est l'Action de normalisation. Les valeurs 9 à 127 ont été ajoutées et sont désignées comme Non allouées. Les valeurs 128 à 255 ont été ajoutées et sont désignées comme d'utilisation privée. Les valeurs 256 à 32 767 ont été ajoutées et sont désignées comme Non allouées.

8.3.3 KEK_MANAGEMENT_ALGORITHM

La procédure d'enregistrement est l'Action de normalisation. Les valeurs 2 à 127 sont désignées comme non allouées. Les valeurs 128 à 255 ont été ajoutées et sont désignées comme d'utilisation privée. Les valeurs 256 à 65 535 ont été ajoutées et sont désignées comme non allouées.

8.3.4 KEK_ALGORITHM

La procédure d'enregistrement est l'Action de normalisation. Les valeurs 4 à 127 sont désignées comme non allouées. Les valeurs 256 à 65 535 ont été ajoutées et sont désignées comme non allouées.

8.3.5 SIG_HASH_ALGORITHM

La procédure d'enregistrement est l'Action de normalisation. Les valeurs 6 à 127 sont désignées comme non allouées. Les valeurs 256 à 65 535 ont été ajoutées et sont désignées comme non allouées.

8.3.6 SIG_ALGORITHM

La procédure d'enregistrement est l'Action de normalisation. Les valeurs 7 à 127 sont désignées comme non allouées. Les valeurs 256 à 65 535 ont été ajoutées et sont désignées comme non allouées.

8.3.7 Valeurs de charge utile de SA TEK

La procédure d'enregistrement est l'Action de normalisation. Les valeurs 3 à 127 sont désignées comme non allouées.

8.3.8 Types de téléchargement de clé

La procédure d'enregistrement est l'Action de normalisation. Les valeurs 5 à 127 sont désignées comme non allouées.

8.3.9 Types de téléchargement de TEK

La procédure d'enregistrement est l'Action de normalisation. Les valeurs 4 à 127 ont été ajoutées et sont désignées comme non allouées. Les valeurs 128 à 255 ont été ajoutées et sont désignées comme d'utilisation privée. Les valeurs 256 à 32 767 ont été ajoutées et sont désignées comme non allouées.

8.3.10 Types de téléchargement de KEK

La procédure d'enregistrement est l'Action de normalisation. Les valeurs 4 à 127 ont été ajoutées et sont désignées comme non allouées. Les valeurs 128 à 255 ont été ajoutées et sont désignées comme d'utilisation privée. Les valeurs 256 à 32 767 ont été ajoutées et sont désignées comme non allouées.

8.3.11 Types de téléchargement de LKH

La procédure d'enregistrement est l'Action de normalisation. Les valeurs 4 à 127 sont désignées comme non allouées. Les valeurs 256 à 32767 ont été ajoutées et sont désignées comme non allouées.

9. Remerciements

Le présent mémoire remplace la RFC 3547, et les auteurs souhaitent remercier Mark Baugher et Hugh Harney pour leurs importantes contributions qui ont conduit à cette nouvelle spécification de GDOI.

Les auteurs remercient Catherine Meadows pour sa relecture attentive et ses suggestions pour atténuer les attaques par interposition qu'elle avait précédemment identifiées. Yoav Nir, Vincent Roca, Sean Turner, et Elwyn Davies ont fourni de nombreux commentaires techniques et rédactionnels utiles et des suggestions d'amélioration.

10. Références

10.1 Références normatives

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

[RFC2403] C. Madson, R. Glenn, "Utilisation de HMAC-MD5-96 au sein d'ESP et d'AH", novembre 1998. *(P.S.)*

[RFC2404] C. Madson, R. Glenn, "Utilisation de HMAC-SHA-1-96 au sein d'ESP et d'AH", novembre 1998. *(P.S.)*

[RFC2407] D. Piper, "Le domaine d'interprétation de sécurité IP de l'Internet pour ISAKMP", novembre 1998. *(Obsolète, voir* RFC4306)

[RFC2408] D. Maughan, M. Schertler, M. Schneider et J. Turner, "Association de sécurité Internet et protocole de gestion de clés (ISAKMP)", novembre 1998. *(Obsolète, voir la* RFC4306)

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

[RFC2627] D. Wallner, E. Harder, R. Agee,"Gestion de clés en diffusion groupé : problèmes et architectures", juin 1999. *(Info.)*

[RFC3447] J. Jonsson et B. Kaliski, "Normes de cryptographie à clés publiques (PKCS) n° 1 : Spécifications de la cryptographie RSA version 2.1", février 2003.

[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.)*

[RFC4754] D. Fu, J. Solinas, "Authentification IKE et IKEv2 avec l'algorithme de signature numérique à courbe elliptique (ECDSA)", janvier 2007. *(P.S.)*

[RFC4868] S. Kelly, S. Frankel, "Utilisation de HMAC-SHA-256, HMAC-SHA-384, et HMAC-SHA-512 avec IPsec", mai 2007. *(P.S.)*

[RFC5374] B. Weis et autres, "Extensions de diffusion groupée à l'architecture de sécurité du protocole Internet", novembre 2008. *PS*

[RFC5903] D. Fu, J. Solinas, "Groupes de courbes elliptiques modulo un nombre premier (groupes ECP) pour IKE et IKEv2", juin 2010. (*Remplace* RFC4753) *(Information)*

[RFC6054] D. McGrew, B. Weis, "Utilisation des modes de compteur avec l'encapsulation de charge utile de sécurité (ESP) et l'en-tête d'authentification (AH) pour protéger le trafic de groupe", novembre 2010. *(P.S.)*

10.2 Références pour information

[FIPS180-3.2008] National Institute of Standards and Technology, "Secure Hash Standard", FIPS PUB 180-3, octobre 2008, < http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf >.

[FIPS186-3] "Digital Signature Standard (DSS)", United States of America, National Institute of Science and Technology, Federal Information Processing Standard (FIPS) 186-2, juin 2009.

[FIPS197] "Advanced Encryption Standard (AES)", United States of America, National Institute of Science and Technology, Federal Information Processing Standard (FIPS) 197, novembre 2001.

[FIPS46-3] "Data Encryption Standard (DES)", United States of America, National Institute of Science and Technology, Federal Information Processing Standard (FIPS) 46-3, octobre 1999.

[FIPS81] "DES Modes of Operation", United States of America, National Institute of Science and Technology, Federal Information Processing Standard (FIPS) 81, décembre 1980.

[GDOI-REG] Internet Assigned Numbers Authority, "Group Domain of Interpretation (GDOI) Payload Type Values", IANA Registry, décembre 2004, < http://www.iana.org/assignments/gdoi-payloads >.

[HD03] Hardjono, T. et L. Dondeti, "Multicast and Group Security", Artech House Computer Security Series, ISBN 1-58053-342-6, 2003.

[ISAKMP-REG] "'Magic Numbers' for ISAKMP Protocol", < http://www.iana.org/assignments/isakmp-registry >.

[MP04] Meadows, C. et D. Pavlovic, "Deriving, Attacking, and Defending the GDOI Protocol", European Symposium on Research in Computer Security (ESORICS) 2004, pp. 53-72, septembre 2004.

[NNL] Naor, D., Noal, M., et J. Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers", Advances in Cryptology, Crypto '01, Springer-Verlag LNCS 2139, 2001, pp. 41-62, 2001, < http://www.iacr.org/archive/crypto2001/21390040.pdf >.

[OFT] Sherman, A. et D. McGrew, "Key Establishment in Large Dynamic Groups Using One-Way Function Trees", IEEE Transactions on Software Engineering, Vol. 29, Issue 5, pp. 444-458, mai 2003, < http://ieeexplore.ieee.org/search/freesrchabstract.jsp?tp=&arnumber=1199073 >.

[PK01] Perlman, R. et C. Kaufman, "Analysis of the IPsec Key Exchange Standard", Enabling Technologies: Infrastructure for Collaborative Enterprises, WET ICE 2001, Proceedings. Tenth IEEE International Workshops on IEEE Transactions on Software Engineering, pp. 150-156, juin 2001, <http://ieeexplore.ieee.org/search/freesrchabstract.jsp?tp=&arnumber=953405>.

[PROT-REG] "Assigned Internet Protocol Numbers", < http://www.iana.org/assignments/protocol-numbers/ >.

[RFC2412] H. Orman, "Protocole OAKLEY de détermination de clés", novembre 1998. *(Information)*

[RFC3686] R. Housley, "Utilisation du mode Compteur de la norme de chiffrement évolué (AES) avec l'encapsulation de la charge utile de sécurité (ESP) dans IPsec", janvier 2004. *(P.S.)*

[RFC3740] T. Hardjono et B. Weis, "Architecture de sécurité de groupe de diffusion groupée", mars 2004.

[RFC3947] T. Kivinen et autres, "Négociation de traversée de NAT dans IKE", janvier 2005. *(P.S.)*

[RFC4046] M. Baugher et autres, "Architecture de gestion de clé de groupe de diffusion groupée sécurisée (MSEC)", avril 2005. *(Info.)*

[RFC4082] A. Perrig et autres, "Authentification de flux tolérante aux pertes en temps efficace (TESLA) : Introduction à la transformation d'authentification de source de diffusion groupée", juin 2005.

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

[RFC4301] S. Kent et K. Seo, "Architecture de sécurité pour le protocole Internet", décembre 2005. *(P.S.)*

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

[RFC4359] B. Weis, "Utilisation des signatures RSA/SHA-1 au sein d'une charge utile de sécurité par encapsulation (ESP) et d'un en-tête d'authentification (AH)", janvier 2006. *(P.S.)*

[RFC4543] D. McGrew, J. Viega, "Utilisation du code d'authentification de message de Galois (GMAC) dans les ESP et AH d'IPsec", mai 2006. *(P.S.)*

[RFC5226] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction d'une section Considérations relatives à l'IANA dans les RFC", BCP 26, mai 2008. (*Remplace la* RFC2434)

[RFC5905] D. Mills, J. Martin, J. Burbank, W. Kasch, "Protocole de l'heure du réseau version 4 (NTPv4) : Spécification du protocole et des algorithmes ", juin 2010. (*Remplace les* RFC1305, RFC4330). *(P. S.)*

[RFC5996] C. Kaufman, P. Hoffman, Y. Nir, P. Eronen, "Protocole d'échange de clés sur Internet, version 2 (IKEv2)", septembre 2010 (*Remplace les* RFC4306, RFC4718) (*MàJ par* RFC5998) *(P.S.)*

[SP.800-131] Barker, E. et A. Roginsky, "Recommendation for the Transitioning of Cryptographic Algorithms and Key Lengths", United States of America, National Institute of Science and Technology, DRAFT NIST Special Publication 800-131, juin 2010.

[SP.800-38A] Dworkin, M., "Recommendation for Block Cipher Modes of Operation", United States of America, National Institute of Science and Technology, NIST Special Publication 800-38A 2001 éd, décembre 2001.

Appendice A. Applications GDOI

GDOI peut être utilisé pour distribuer des clés pour plusieurs applications sûres de diffusion groupée, où différentes applications ont des exigences de gestion de clé différentes. La présente section souligne deux exemples de façons dont GDOI peut être utilisé. D'autres exemples se trouvent à la Section 10 de [HD03].

Une application simple est la livraison sûre de contenu périodique en diffusion groupée sur le réseau IP d'une organisation, peut-être une diffusion vidéo en diffusion groupée. En supposant que la trame de livraison du contenu est limitée dans le temps et que les membres du groupe ne sont pas supposés changer avec le temps, il n'est pas nécessaire que la politique du groupe comporte un échange GROUPKEY-PUSH, et il n'est pas nécessaire que le GCKS distribue une SA Rekey. Donc, le GCKS GDOI peut avoir seulement besoin de distribuer un seul ensemble de SA de sécurité des données pour protéger la diffusion limitée dans le temps.

À l'opposé, une application persistante de diffusion groupée IP (par exemple, un service de livraison de bulletins de stock) peut avoir de nombreux membres du groupe, où les membres du groupe changent au fil du temps. Un changement périodique de SA de sécurité des donnéess peut être souhaitable, et le potentiel de changement des membres du groupe exige l'utilisation d'une méthode de gestion de groupe qui permette de mettre fin à l'autorisation de membres du groupe. Le GCKS GDOI va distribuer l'ensemble actuel de SA de sécurité des données et une SA Rekey pour enregistrer les membres du groupe. Il va alors utiliser régulièrement des échanges GROUPKEY-PUSH programmés pour livrer les nouvelles SA pour le groupe. De plus, les membres du groupe sur le GCKS peuvent être fréquemment ajustés, d'où résultera un échange GROUPKEY-PUSH qui délivre les nouvelles SA Rekey protégées par une méthode de gestion de groupe. Chaque GROUPKEY-PUSH peut inclure des SA de sécurité des données et/ou une SA Rekey.

Dans chaque exemple, la politique pertinente est définie sur le GCKS et relayée aux membres du groupe en utilisant les protocoles GROUPKEY-PULL et/ou GROUPKEY-PUSH. Les choix spécifiques de politique configurés par l'administrateur du GCKS dépendent de chaque application.

Appendice B. Changements significatifs par rapport à la RFC 3547

Les changements significatifs suivants ont été faits par rapport à la RFC 3547.

- La charge utile Preuve de possession (POP) a été retirée de l'échange GROUPKEY-PULL. Elle fournissait une forme d'autorisation de remplacement, mais son utilisation était sous spécifiée. De plus, Meadows et Pavlovic [MP04] ont exposé une attaque par interposition sur la méthode d'autorisation POP, qui aurait exigé des changements de sa sémantique. Aucune mise en œuvre connue de la RFC 3547 ne prenait en charge la charge utile POP, de sorte qu'elle a été retirée. Le retrait de la charge utile POP supprimait le besoin de la charge utile CERT dans cet échange, et il a été lui aussi supprimé.
- Les charges utiles Échange de clé (KE_I, KE_R) ont été retirées de l'échange GROUPKEY-PULL. Cependant, la spécification pour le calcul du matériel de clé pour la fonction de chiffrement supplémentaire dans la RFC 3547 est erronée. De plus, il a été observé que parce que le message d'enregistrement GDOI utilise des chiffrements forts et fournit un chiffrement authentifié, le chiffrement supplémentaire du matériel de clé dans un message d'enregistrement GDOI ne fournit qu'une valeur ajoutée négligeable. Donc, l'utilisation des charges utiles KE est déconseillée dans ce mémoire.

- La charge utile de certificat (CERT) a été retirée de l'échange GROUPKEY-PUSH. L'utilisation de cette charge utile était sous spécifiée. Dans tous les cas d'utilisation connus, la clé publique utilisée pour vérifier la charge utile GROUPKEY-PUSH est distribuée directement à partir du serveur de clés au titre de l'échange GROUPKEY-PULL.

- Les algorithmes de chiffrement pris en charge ont été changés pour suivre les lignes directrices actuelles. Il est demandé aux mises en œuvre de prendre en charge AES avec des clés de 128 bits pour chiffrer le message Rekey et de prendre en

charge SHA-256 pour les signatures cryptographiques. L'utilisation de DES est déconseillée.

- Un nouveau protocole de prise en charge pour AH.

- De nouvelles définitions du protocole ont été ajoutées pour se conformer à la plus récente "Architecture de sécurité pour le protocole Internet" [RFC4301] et aux "Extensions de diffusion groupée à l'architecture de sécurité pour le protocole Internet" [RFC5374]. Cela inclut l'ajout de la charge utile GAP.

- De nouvelles définitions du protocole et de la sémantique ont été ajoutées pour la prise en charge de "Utilisation des modes de compteur avec l'encapsulation de charge utile de sécurité (ESP) et l'en-tête d'authentification (AH) pour protéger le trafic de groupe" [RFC6054].

- La spécification pour l'IANA a été ajoutée pour mieux préciser l'utilisation du registre des charges utiles GDOI.

Adresse des auteurs

Brian Weis
Cisco Systems
170 W. Tasman Drive
San Jose, California 95134-1706
USA
téléphone : +1-408-526-4796
mél : bew@cisco.com

Sheela Rowles
Cisco Systems
170 W. Tasman Drive
San Jose, California 95134-1706
USA
téléphone : +1-408-527-7677
mél : sheela@cisco.com

Thomas Hardjono
MIT
77 Massachusetts Ave.
Cambridge, Massachusetts 02139
USA
téléphone : +1-781-729-9559
mél : hardjono@mit.edu