Groupe de travail Réseau
Request for Comments : 4563
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

E. Carrara, KTH
V. Lehtovirta, Ericsson
K. Norrman, Ericsson
juin 2006

Type d'information Identifiant de clé pour la charge utile d'extension générale dans le protocole de chiffrement Internet multimédia (MIKEY)

Résumé
Le présent mémoire spécifie un nouveau type (le type Informations d'identifiant de clé) pour la charge utile d'extension générale dans le protocole de chiffrement Internet multimédia (MIKEY, *Multimedia Internet KEYing*). Il est utilisé, par exemple, dans le service multimédia de diffusion/diffusion groupée spécifié par le projet en partenariat de troisième génération (3GPP)

Table des matières

1. Introduction....1
1.1 Conventions utilisées dans ce document....2
2. Raisons....2
3. Relations de MIKEY et GKMARCH....2
4. Type d'information Identifiant de clé pour la charge utile d'extension générale....2
5. Définition du type de transposition vide pour le type CS ID Map....3
6. Considérations de transport....4
7. Considérations sur la sécurité....4
8. Considérations relatives à l'IANA....4
9. Remerciements....5
10. Références....5
10.1 Références normatives....5
10.2 Références pour information....5
Adresse des auteurs....5
Déclaration complète de droits de reproduction....6

1. Introduction

Le projet en partenariat de troisième génération (3GPP, *Third Generation Partnership Project*) est actuellement impliqué dans le développement d'un service de diffusion et diffusion groupée, le service multimédia de diffusion/diffusion groupée (MBMS, *Multimedia Broadcast/Multicast Service*) et son architecture de sécurité [MBMS].

[MBMS] requiert l'utilisation du protocole de chiffrement Internet multimédia (MIKEY, *Multimedia Internet KEYing*) [RFC3830] pour convoyer les clés et les paramètres de sécurité en rapport nécessaires pour sécuriser les divers supports qui sont en diffusion ou en diffusion groupée.

Une des exigences que MBMS met à sa sécurité est la capacité à effectuer de fréquentes mises à jour des clés. La raison en est qu'il serait coûteux pour les abonnés de redistribuer les clés de déchiffrement à des non abonnés. Le coût de redistribution des clés en utilisant le canal d'envoi individuel serait plus élevé que le coût d'achat des clés pour que ce

schéma ait un effet. Pour mettre cela en œuvre, MBMS utilise trois niveaux de gestion de clés, pour distribuer les clés de groupe aux clients, et être capable de changer les clés en poussant une nouvelle clé de groupe. Comme illustré dans le paragraphe suivant, MBMS a besoin d'identifier quels types de clés sont impliqués dans le message MIKEY ainsi que leur identité.

Le présent mémoire spécifie un nouveau type pour la charge utile d'extension générale dans MIKEY, pour identifier le type et l'identité des clés impliquées.

1.1 Conventions utilisées dans ce document

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

2. Raisons

Une application qui utilise cette extension est la gestion de clé MBMS. La solution de gestion de clé adoptée par MBMS utilise la gestion de clés à trois niveaux. Les clés sont utilisées de la façon décrite ci-dessous. "Clients" se réfère aux clients qui se sont abonnés à un certain service de diffusion/diffusion groupée.

* Clé d'utilisateur MBMS (MUK, *MBMS User Key*) clé point à point entre le serveur de diffusion groupée et chaque client.

* Clé de service MBMS (MSK, *MBMS Service Key*) clé de groupe entre le serveur de diffusion groupée et tous les clients.

* Clé de trafic MBMS (MTK, *MBMS Traffic Key*) clé de trafic de groupe entre le serveur de diffusion groupée et tous les clients.

Les clés de trafic sont les clés qui sont mises à jour régulièrement.

La MUK point à point (clé de premier niveau) est partagée entre le serveur de diffusion groupée et le client via les moyens définis par [MBMS]. La MUK est utilisée comme clé prépartagée pour faire fonctionner MIKEY avec la méthode de clé prépartagée [RFC3830], et pour livrer (en point à point) la MSK. La même MSK est poussée chez tous les clients, pour être utilisée comme clé de groupe (de second niveau).

Ensuite, la MSK est utilisée pour pousser chez tous les clients une MTK (clé de troisième niveau) la clé de groupe réelle qui est utilisée pour la protection du trafic. Par exemple, la MTK pourrait être la clé maîtresse pour le protocole de transport sécurisé en temps réel (SRTP, *Secure Real-time Transport Protocol*) [RFC3711] dans le cas de flux en direct.

Un identifiant de domaine de clés définit le domaine où les clés de groupe sont valides ou applicables. Par exemple, il peut définir un fournisseur de service spécifique.

Pour permettre la distribution de clés décrite ci-dessus, une indication du type et de l'identité des clés portées dans un message MIKEY est nécessaire. Cette indication est portée dans un nouveau type de la charge utile d'extension générale dans MIKEY.

Il est nécessaire de spécifier quel type de transposition d'identifiant de session de chiffrement (CS ID, *Crypto Session ID*) est associé à une certaine clé. Il y a des cas (par exemple, le cas de téléchargement dans MBMS) où les paramètres requis sont signalés dans la bande (chaque objet en format de contenu de gestion des droits numériques (DRM, *Digital Rights Management*) [DCF] téléchargé contient les paramètres nécessaires pour que le receveur le traite). Comme les paramètres ne sont pas transportés par MIKEY, cela implique qu'un type de transposition de CS ID doit être enregistré comme "transposition vide", comme défini au Tableau 3, qui est à utiliser quand les informations de transposition/politique sont portées en dehors de MIKEY.

3. Relations de MIKEY et GKMARCH

Selon la [RFC3830], MIKEY est un protocole d'enregistrement qui prend en charge le changement de clés pour l'envoi individuel dans les termes de l'architecture de gestion de clé de groupe de MSEC [RFC4046]. MBMS utilise MIKEY à la

fois comme protocole d'enregistrement et comme protocole de changement de clés, et l'extension spécifiée met en œuvre les ajouts nécessaires à la [RFC3830] qui permettent à MIKEY de fonctionner comme protocole de changement de clés à la fois en envoi individuel et en diffusion groupée dans le réglage MBMS.

4. Type d'information Identifiant de clé pour la charge utile d'extension générale

La charge utile Extension générale dans MIKEY est définie au paragraphe 6.15 de la [RFC3830]. Le type de charge utile Extension générale (informations d'identifiant de clé) défini dans le présent document n'est pas restreint à MBMS. Les applications qui utilisent ce type de charge utile Extension générale peuvent définir de nouveaux types d'identifiant de clé, et ces applications DOIVENT définir la sémantique et l'usage des sous charges utiles Type d'identifiant de clé en accord avec la Section 8. L'utilisation par MBMS de sous charges utiles Type d'identifiant de clé, définie au Tableau 2, est spécifiée dans [MBMS].

Les formats de type d'information d'identifiant de clé (Type 3) dans la charge utile Extension générale sont les suivants :

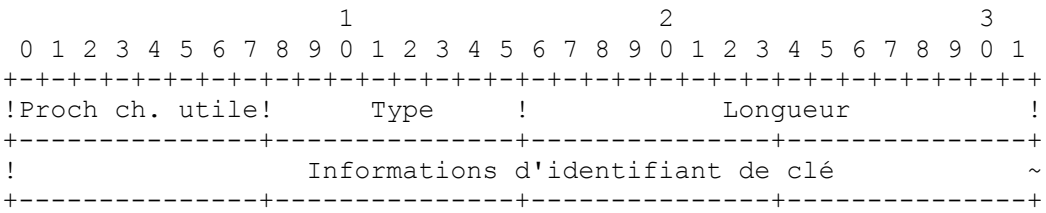

Figure 1. Charge utile d'extension générale Informations d'identifiant de clé

Prochaine charge utile et Longueur sont définis au paragraphe 6.15 de la [RFC3830].

* Type (8 bits) : identifie le type de la charge utile d'extension générale [RFC3830]. Le présent mémoire ajoute le type 3 à ceux déjà définis dans la [RFC3830].

Type	Valeur	Commentaires
Key ID	3	Informations sur le type et l'identité des clés

Tableau 1. Définition de la nouvelle charge utile d'extension générale

* Informations d'identifiant de clé (longueur variable) : donnés de la charge utile générale qui transportent le type et l'identifiant d'une clé. Ce champ est formé par les sous charges utiles Type d'identifiant de clé comme spécifié ci-dessous.

La sous charge utile Type d'identifiant de clé est formatée comme suit :

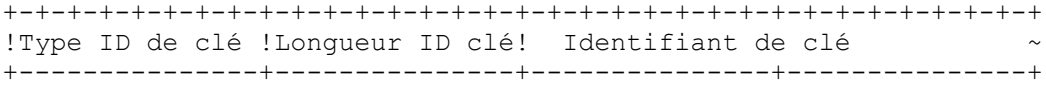

Figure 2. Sous charge utile Type d'identifiant de clé

* Type d'identifiant de clé (8 bits) : décrit le type de l'identifiant de clé. Les types prédéfinis sont donnés au Tableau 2.

Type d'identifiant de clé	Valeur	Commentaire
Identifiant de domaine de clé MBMS	0	Identifiant du domaine de clé de groupe
Identifiant de clé de service MBMS	1	Identifiant de la clé de groupe
Identifiant de clé de trafic MBMS	2	Identifiant de la clé de trafic de groupe

Tableau 2. Définitions de type pour les identifiants de clé

* Longueur d'identifiant de clé (8 bits) : décrit la longueur du champ ID de clé en octets.

* Identifiant de clé (longueur variable) : définit l'identité de la clé.

Noter qu'il peut y avoir plus d'une sous charge utile Type d'identifiant de clé dans une extension, et que la longueur globale (c'est-à-dire, la somme des longueurs de toutes les sous charges utiles de type d'identifiant de clé) du champ Informations d'identifiant de clé ne peut pas excéder 2^16 - 1 octets.

5. Définition du type de transposition vide pour le type Transposition de CS ID

Quand les informations de politique de sécurité sont portées en dehors de MIKEY, le type transposition de CS ID est réglé à une valeur définie au Tableau 3 pour indiquer "transposition vide". Dans ce cas, il NE DOIT PAS y avoir de charge utile Politique de sécurité présente dans le message.

Type de transposition de CS ID	Valeur	Commentaires
Transposition vide	1	Utilisé quand les informations de transposition/politique sont portées hors de MIKEY

Tableau 3. Définition du type Transposition de CS ID

6. Considérations de transport

Comme spécifié à la Section 7 de la [RFC3830], le transport sous-jacent du protocole MIKEY doit être défini pour chaque type de transport. Quand la charge utile Identifiant de clé est utilisée avec MBMS, le transport est UDP, et l'usage de MIKEY sur UDP dans le réglage MBMS est défini dans [MBMS].

7. Considérations sur la sécurité

L'usage de MIKEY pour mettre à jour la clé de chiffrement de trafic (MTK) en diffusion, décrit à la Section 2, dévie de la façon dont MIKEY [RFC3830] a été conçu à l'origine. Deux points principaux se rapportent à la sécurité de l'usage décrit. D'abord, l'origine de la source de livraison de la MTK n'est pas authentifiée, mais plutôt protégée par un MAC de groupe, chiffré par la clé de groupe (MSK). La menace que cela soulève est que les utilisateurs qui font partie du groupe sont capables d'envoyer des messages MTK falsifiés aux autres membres du groupe. L'origine des messages de MTK est un nœud à l'intérieur du réseau cœur, et le modèle de confiance utilisé dans MBMS est que seul l'envoi de trafic de confiance est permis (de l'intérieur du réseau de l'opérateur) sur les supports MBMS. Cependant, il y a toujours le risque que du trafic soit injecté sur l'interface radio entre les stations de base et l'équipement de l'utilisateur. Il est possible aux membres du groupe (c'est-à-dire, avec accès à la MSK) de falsifier les mises à jour de MTK aux autres membres du groupe. Le 3GPP a décidé que les difficultés techniques et les coûts impliqués par la réalisation d'une telle attaque sont assez élevés par rapport aux gains espérés par l'attaquant, et que le risque paraît acceptable. Noter que, dans la mesure où la source d'origine de la livraison de la MTK n'est pas authentifiée, il n'y a rien à gagner en ajoutant l'authentification de la source d'origine aux flux RTP (par exemple, en utilisant SRTP-TESLA [RFC4383]). Donc, l'utilisation actuelle de l'extension spécifiée n'est pas compatible avec SRTP-TESLA, qui exige l'authentification de la source d'origine de la clé d'intégrité.

Noter que dans MBMS, la MSK est protégée de bout en bout, depuis le serveur de diffusion groupée jusqu'aux clients, en utilisant une clé MUK unique par client, mais la MTK est livrée sous la protection de la MSK de clé de groupe, de sorte que l'authentification de la source d'origine n'est pas réalisée.

Ensuite, la livraison de la MTK est séparée de la livraison de la politique de sécurité. La politique de sécurité est livrée avec la MSK. La livraison des MTK est suppposée être fréquente (certains scénarios exigent que la livraison des MTK soit d'une fréquence de quelques secondes). Cela impliquerait que le coût (en termes de bande passante) serait très élevé si la politique de sécurité devait être livrée avec chaque MTK. De plus, les paramètres de politique de sécurité de la session de flux directs ne sont pas prévus pour changer durant la session, même si il va y avoir une mise à jour de la MTK. Il a été décidé dans le 3GPP qu'il n'était pas besoin de mettre à jour la politique durant une session en cours, et que le coût de permettre une telle caractéristique seulement pour se sentir en sécurité, serait trop élevé. Par ailleurs, mettre à jour la politique de sécurité durant une session en cours serait possible en mettant à jour la MSK.

Le type Transposition vide utilisé quand la politique de sécurité est livrée dans la bande s'appuie sur la sécurité fournie par [DCF], et MIKEY est, dans ce cas, seulement utilisé pour fourni la clé maîtresse pour le traitement de DCF.

8. Considérations relatives à l'IANA

Selon la Section 10 de la RFC 3830, le consensus de l'IETF est exigé pour enregistrer des valeurs dans la gamme 0-240 dans l'espace de noms Type de la charge utile d'extension générale MIKEY et l'espace de noms de type d'identifiant de CS de la charge utile d'en-tête commun.

Une nouvelle valeur dans l'espace de noms Type de charge utile d'extension générale MIKEY a été enregistrée à cette fin. La valeur enregistrée pour Key ID est 3 en accord avec la Section 4.

Aussi, la valeur de 1 a été enregistrée pour la transposition vide dans l'espace de noms existant CS ID de la charge utile d'en-tête commun, comme spécifié au Tableau 3 à la Section 5.

Le nouvel espace de noms pour le champ suivant dans la sous charge utile Informations d'identifiant de clé (des Sections 4 et 5) a été établi et sera géré par l'IANA : * Key ID Type

L'IANA a enregistré les types prédéfinis du Tableau 2 pour cet espace de noms. L'IANA va aussi gérer la définition de valeurs supplémentaires à l'avenir. Les valeurs dans la gamme 0-240 pour chaque espace de noms DEVRAIENT être approuvées par le processus de consensus de l'IETF, et les valeurs dans la gamme 241-255 sont réservées pour utilisation privée, en accord avec la [RFC2434].

9. Remerciements

Nous tenons à remercier Fredrik Lindholm.

10. Références

10.1 Références normatives

[MBMS] 3GPP TS 33.246, "Technical Specification 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security; Security of Multimedia Broadcast/Multicast Service".

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

[RFC3830] J. Arkko et autres, "MIKEY : Gestion de clé multimédia pour l'Internet", août 2004. (*MàJ par* RFC4738) *(P.S.)*

10.2 Références pour information

[DCF] Open Mobile Alliance, OMA-DRM-DCF-V2_0-20050329-C, "DRM Content Format V2.0", Candidate Version 2.0 - 29 mars 2005.

[RFC2434] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction d'une section Considérations relatives à l'IANA dans les RFC", BCP 26, octobre 1998. *(Rendue obsolète par la* RFC5226)

[RFC3711] M. Baugher et autres, "Protocole de transport sécurisé en temps réel (SRTP)", mars 2004. *(P.S.)*

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

[RFC4383] M. Baugher, E. Carrara, "Utilisation de l'authentification tolérante aux pertes de flux à synchronisation efficace (TESLA) dans le protocole de transport en temps réel sécurisé (SRTP)", février 2006. *(P.S.)*

Adresse des auteurs

Elisabetta Carrara
Royal Institute of Technology
Stockholm
Sweden
mél : carrara@kth.se

Vesa Lehtovirta
Ericsson Research
02420 Jorvas
Finland
téléphone : +358 9 2993314
mél : vesa.lehtovirta@ericsson.com

Karl Norrman
Ericsson Research
SE-16480 Stockholm
Sweden
téléphone : +46 8 4044502
mél : karl.norrman@ericsson.com

Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d'édition des RFC est fourni par l'activité de soutien administatif (IASA) de l'IETF.