Groupe de travail Réseau
Request for Comments : 4738
RFC mise à jour : 3830
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

D. Ignjatic, Polycom
L. Dondeti, QUALCOMM
F. Audet, Nortel
P. Lin, Nortel
novembre 2006

MIKEY-RSA-R : mode supplémentaire de distribution de clés en chiffrement Internet multimédia (MIKEY)

Statut du présent mémoire
Le présent document spécifie un protocole de l'Internet sur la voie de la normalisation pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. Prière de se référer à l'édition en cours des "Protocoles officiels de l'Internet" (STD 1) pour voir l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé
La spécification du chiffrement Internet multimédia (MIKEY, *Multimedia Internet Keying*) décrit plusieurs modes de solution de distribution de clés qui s'adressent à des scénarios multimédia (par exemple, appels SIP et sessions de protocole de flux directs en temps réel (RTSP, *Real Time Streaming Protocol*)) qui utilisent des clés pré-partagées, des clés publiques, et facultativement un échange de clés Diffie-Hellman. Dans le mode de clé publique, l'initiateur chiffre une clé aléatoire avec la clé publique de celui qui répond et l'envoie à celui qui répond. Dans de nombreux scénarios de communication, l'initiateur ne peut pas savoir la clé publique de celui qui répond, ou dans certains cas, l'identifiant de celui qui répond (par exemple, renvoi d'appel) à l'avance. On propose un nouveau mode MIKEY qui fonctionne bien dans ces scénarios. Ce mode améliore aussi la prise en charge de la gestion de clé de groupe dans MIKEY ; il prend en charge le téléchargement de clé de groupe initié par le membre (à la différence du gestionnaire de groupe qui pousse les clés de groupe chez tous les membres). Le présent document met à jour la RFC 3830 avec le mode RSA-R.

Table des matières

1. Introduction

Le protocole MIKEY [RFC3830] a trois méthodes différentes pour le transport ou l'échange de clés : un mode de clé pré-partagée (PSK, *Pre-Shared Key*), un mode de clé publique (RSA) et un mode facultatif d'échange Diffie-Hellman (DHE). En plus, il y a aussi un mode facultatif DH-HMAC [RFC4650], portant le nombre total de modes à quatre. La principale motivation de la conception du protocole MIKEY est une exigence de faible latence des communications en temps réel, et donc tous les échanges se finissent en un demi à un aller retour ; noter que cela n'offre pas de place pour la négociation des paramètres de sécurité du protocole de gestion de clés lui-même. Dans le présent document, on note que les modes de MIKEY définis dans les [RFC3830] et [RFC4650] sont insuffisants pour traiter certains scénarios de déploiement et cas courants d'utilisation, et on propose un nouveau mode appelé MIKEY-RSA en mode inverse, ou simplement MIKEY-RSA-R. Le présent document met à jour la RFC 3830 avec l'ajout de ce nouveau mode à cette spécification.

1.1 Terminologie utilisée 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 la [RFC2119] et indiquent les niveaux d'exigence pour les mises en œuvre conformes.

De plus, le présent document réutilise la terminologie de la spécification MIKEY [RFC3830].

2. Motivation

Comme noté dans l'introduction, la spécification de MIKEY et les autres propositions définissent quatre différents modes de gestion de clé efficaces pour les applications en temps réel. Ces modes diffèrent les uns des autres par la méthode d'authentification choisie (clé publique, ou clé partagée symétrique) ou par la méthode d'établissement de clé (téléchargement de clé ou accord de clé en utilisant l'échange Diffie-Hellman). On résume ces modes ci-dessous, en incluant leurs avantages et inconvénients. On discute ensuite les cas d'utilisation où ces modes sont inutilisables ou inefficaces.

2.1 Description des modes de MIKEY

Le mode PSK exige que l'initiateur et celui qui répond aient une clé secrète commune établie hors ligne. Dans ce mode, l'initiateur choisit une clé de génération de clé de chiffrement du trafic (TGK, *TEK Generation Key*) la chiffre avec une clé déduite de la PSK, et l'envoie à celui qui répond au titre du premier message, à savoir, I_MESSAGE. Le I_MESSAGE est protégé contre la répétition par son horodatage, et protégé en intégrité par une autre clé déduite de la PSK. Un message de vérification facultatif de celui qui répond à l'initiateur assure l'authentification mutuelle. Ce mode ne s'adapte pas bien car il exige l'établissement préalable d'une clé partagée entre les parties communiquantes ; par exemple, si on considère les cas d'utilisation où tout utilisateur peut vouloir communiquer avec tout autre utilisateur dans une entreprise ou dans l'Internet au sens large. Le mode RSA pourrait mieux convenir pour de telles applications.

Dans le mode RSA, l'initiateur choisit une TGK, la chiffre et l'authentifie avec une clé d'enveloppe, et l'envoie à celui qui répond au titre du I_MESSAGE. L'initiateur inclut la clé d'enveloppe, chiffrée avec la clé publique de celui qui répond, dans le I_MESSAGE. Le I_MESSAGE est protégé contre la répétition par des horodatages, et signé par la clé publique de l'initiateur. L'identifiant de l'initiateur, le certificat (CERT), et l'identifiant de celui qui répond peuvent être inclus dans le I_MESSAGE. Si l'initiateur connaît plusieurs clés publiques de celui qui répond, il peut indiquer la clé utilisée dans la charge utile CHASH facultative. Un message Vérification facultatif de celui qui répond à l'initiateur assure l'authentification mutuelle. Le mode RSA fonctionne bien si l'initiateur connaît l'identifiant de celui qui répond et le CERT correspondant (ou peut obtenir le CERT indépendamment du protocole MIKEY). La RFC 3830 suggère qu'un iInitiateur, au cas où il n'aurait pas le certificat de celui qui répond, puisse obtenir le certificat d'un agent de répertoire en utilisant un ou plusieurs allers-retours. Cependant, dans certains cas, l'initiateur ne peut même pas connaître à l'avance l'identifiant de celui qui répond, et à cause de cela ou pour d'autres raisons ne peut pas obtenir le certificat de celui qui répond.

En plus du cas où celui qui répond peut avoir plusieur identifiants, certaines applications peuvent permettre que l'identifiant

de celui qui répond change unilatéralement, comme c'est typique en téléphonie (par exemple, le renvoi d'appel). Dans ces cas et dans d'autres, l'initiateur pourrait vouloir laisser l'autre partie établir son identité et la prouver via un tiers qui a la confiance de l'initiateur (par exemple, une autorité de certification (CA, *Certification Authority*)).

Le mode DH ou DH-HMAC de MIKEY pourrait être utile dans des cas où l'initiateur n'a pas accès à l'identité exacte et/ou CERT de celui qui répond. Dans ces deux modes, les deux parties s'engagent dans un échange DH authentifié pour déduire la TGK. L'inconvénient est que les modes DH ont des frais généraux de calcul et de communication plus élevés que les modes RSA et PSK. PLus important, ces modes ne conviennent pas pour la distribution de clé de groupe. Le mode DH-HMAC exige aussi l'établissement de PSK entre toutes les entités communicantes possibles et donc a des problèmes d'adaptabilité similaires à ceux des protocole de gestion de clé fondés sur PSK.

En résumé, dans certains scénarios de communication -- où l'initiateur pourrait n'avoir pas l'identifiant correct et/ou le certificat de celui qui répond – aucun des modes MIKEY décrits dans la[RFC3830] ou la [RFC4650] ne convient et n'est efficace pour l'établissement de clé de session multimédia.

2.2 Cas d'utilisation qui motivent le mode proposé

En plus des problèmes mentionnés ci-dessus, il y a des types d'applications qui motivent la nouvelle conception de mode MIKEY proposée dans le présent document.

Noter que dans le mode MIKEY-RSA (comme dans cas du mode PSK) l'initiateur propose la politique de sécurité de la session et choisit la TGK. Cependant, il est aussi possible que l'initiateur veuille permettre à celui qui répond de spécifier la politique de sécurité et d'envoyer la TGK. Considérons par exemple le cas d'un scénario de conférence où l'organisateur envoie à un groupe de gens une invitation à participer à une réunion. La procédure pourrait alors être que les invités demandent le matériel de chiffrement de groupe à l'organisateur en envoyant un I_MESSAGE MIKEY. Donc, dans la définition de MIKEY des initiateurs et des répondants, l'initiateur demande à celui qui répond le matériel de chiffrement. Noter que ce mode de fonctionnement est en ligne avec l'architecture de gestion de clé de groupe MSEC [RFC4046].

3. Nouveau mode MIKEY-RSA : MIKEY-RSA-R

3.1 Généralités

Le mode MIKEY proposé exige un aller retour complet. L'initiateur envoie un I_MESSAGE signé au répondant prévu en demandant à celui qui répond d'envoyer le matériel de chiffrement du trafic. Le I_MESSAGE PEUT contenir le certificat de l'initiateur ou un lien (URL) au certificat, et de même, la réplique de celui qui répond, le R_MESSAGE, PEUT contenir le certificat de celui qui répond ou un lien pour lui. Le répondant peut utiliser la clé publique de l'initiateur provenant du certificat contenu dans le I_MESSAGE pour envoyer la TGK chiffrée dans le R_MESSAGE. À réception du R_MESSAGE, l'initiateur peut utiliser le certificat dans le R_MESSAGE pour vérifier si celui qui répond est en fait la partie avec qui il veut communiquer, et accepter la TGK. On se réfère à ce protocole comme MIKEY-RSA en mode inverse, ou simplement MIKEY-RSA-R.

L'échange de mode MIKEY-RSA-R est défini comme suit :

Initiateur **Répondant**

I_MESSAGE = HDR, T, [RAND], [IDi|CERTi], [IDr], {SP}, SIGNi-->

<--R_MESSAGE = HDR, [GenExt(CSB_ID)], T, [RAND], [IDr|CERTr], [SP], KEMAC, PKE, SIGNr

Figure 1 : MIKEY-RSA-R en mode envoi individuel

3.2 Communication de groupe utilisant le mode MIKEY RSA-R

Pour une conférence de groupe utilisant le mode MIKEY RSA-R, les membres qui reçoivent une invitation à initier MIKEY avec le serveur de clé de groupe téléchargent les informations de session sécurisée. Dans ce cas, celui qui répond est soit l'envoyeur du groupe, soit le serveur de clé de groupe. Les membres du groupe demandent la politique du groupe et le matériel de chiffrement comme initiateurs de MIKEY RSA-R. Les initiateurs NE DOIVENT PAS envoyer la charge utile SP. Le répondant envoie toutes les charges utiles nécessaires pour distribuer la politique de groupe sécurisé ainsi que les charges utiles utilisées dans la déduction de clé de groupe : précisément, la charge utile SP est utilisée pour porter la politique de session, et les charges utiles GenExt(CSB-ID), TGK, et RAND choisies par celui qui répond et incluses dans le

R_Message sont utilisées pour calculer les clés de session du protocole sûr de transport en temps réel (SRTP, *Secure Realtime Transport Protocol*).

MIKEY RSA-R pour communication de groupe :

Initiateur **Répondant**
I_MESSAGE = HDR, T, [RAND], [IDi|CERTi], [IDr], SIGNi-->

<--R_MESSAGE = HDR, GenExt(CSB_ID), T, RAND, [IDr|CERTr], SP, KEMAC, PKE, SIGNr

Figure 2 : MIKEY-RSA-R en mode groupe

Noter que la charge utile SP dans le I_MESSAGE n'est pas présente. Dans le R_MESSAGE, les charges utiles CSB_ID, RAND, et SP ne sont pas facultatives.

3.3 Préparation des messages RSA-R

La préparation et l'analyse des messages RSA-R sont décrites aux paragraphes 5.2 et 5.3 de la RFC 3830. Le traitement des erreurs est décrit au paragraphe 5.1.2 et les lignes directrices pour la protection contre la répétition sont au paragraphe 5.4 de la RFC 3830. Dans ce qui suit, on décrit les composants des messages RSA-R et on spécifie le traitement des messages et les règles d'analyse en plus de celles de la RFC 3830.

3.4 Composants du I_MESSAGE

MIKEY-RSA-R exige un aller-retour complet pour télécharger les TGK. Le I_MESSAGE DOIT avoir l'en-tête MIKEY et la charge utile d'horodatage pour la protection contre la répétition. Le champ HDR contient un identifiant de faisceau de session chiffrée (CSB, *Crypto Session Bundle ID*) choisi au hasard par l'initiateur. Le bit V DOIT être réglé à '1' et ignoré par celui qui répond, car une réponse est obligatoire dans ce mode. L'initiateur DEVRAIT indiquer le nombre de sessions de chiffrement (CS, *Crypto Session)* pris en charge, et DEVRAIT remplir les champs Type de transposition d'identifiant de session de chiffrement et Informations d'identifiant de session de chiffrement pour les flux RTP/RTCP qu'il génère. C'est parce que l'envoyeur des flux choisit la source de synchronisation (SSRC) qui est portée dans le champ Informations d'identifiant de session de chiffrement ; voir le paragraphe 6.1.1 de la RFC 3830. L'exception à ce que les initiateurs ne spécifient pas les valeurs de SSRC est pour permettre à celui qui répond de les prendre pour éviter les collisions de SSRC. Les initiateurs de messages MIKEYqui ne génèrent pas de flux RTP DOIVENT spécifier '0' comme nombre de CS prises en charge. Ceci s'applique normalement à la communication de groupe et aux entités dans le mode écoute seule.

Le I_MESSAGE DOIT être signé par l'initiateur suivant la procédure de signature des messages MIKEY spécifiée dans la RFC 3830. La charge utile SIGNi contient cette signature. Donc, le I_MESSAGE est protégé en intégrité et contre la répétition.

La charge utile RAND DEVRAIT être incluse dans le I_MESSAGE quand le mode MIKEY-RSA-R est utilisé pour une communication en envoi individuel. La raison de la recommandation de l'inclusion de la charge utile RAND dans le I_MESSAGE pour la communication en envoi individuel est de permettre à l'initiateur de contribuer à l'entropie du processus de déduction de clé (en plus du CSB_ID). Quand la charge utile RAND n'est pas incluse, l'initiateur va s'appuyer sur celui qui répond pour fournir toute l'entropie pour la génération de clé SRTP, qui est en fait similaire (mais avec l'inversion des rôles) au mode MIKEY-RSA, où celui qui répond fournit toute l'entropie.

La charge utile RAND PEUT être incluse quand MIKEY-RSA-R est utilisé pour établir des clés de groupe. Cependant, la charge utile RAND dans le I_MESSAGE NE DOIT PAS être utilisée pour la génération de clé MIKEY, en cas de communication de groupe. Le répondant DOIT inclure une charge utile RAND dans le R_MESSAGE pour la génération de TEK à partir d'une TGK quand MIKEY-RSA-R est utilisé pour la communication de groupe.

IDi et CERTi DEVRAIENT être inclus, mais ils PEUVENT être laissés en dehors quand il est attendu que l'homologue sache déjà l'identifiant de la partie initiatrice (ou qu'il peut obtenir le certificat d'une autre manière). Par exemple, ce pourrait être le cas si l'identifiant est extrait de SIP. Pour le traitement du certificat, de l'autorisation, et des politiques, voir les paragraphes 4.3 et 6.7 de la RFC 3830. Si CERTi est inclus, il DOIT correspondre à la clé privée utilisée pour signer le I_MESSAGE.

Si celui qui répond a plusieurs identités, l'initiateur PEUT aussi inclure l'identité spécifique, IDr, du répondant avec qui la

communication est désirée. Si la politique de l'initiateur ne permet pas d'accepter un R_MESSAGE de toute autre entité que celle qui peut attester d'une identité spécifique, l'initiateur DOIT inclure cette identité spécifique dans une charge utile IDr dans le I_MESSAGE.

L'initiateur PEUT aussi envoyer des charges utiles Politique de sécurité (SP, *security policy*) contenant toutes les politiques de sécurité qu'il prend en charge. Si celui qui répond ne prend en charge aucune des politiques incluses, il DEVRAIT répondre avec un message d'erreur de type "Sppar invalide" (erreur n° 10). Le répondant a l'option de ne pas envoyer le message d'erreur dans MIKEY si une indication générique de défaillance d'établissement de session semble appropriée et si elle est communiquée via d'autres moyens (voir le paragraphe 4.1.2 de la [RFC4567] pour des lignes directrices supplémentaires).

SIGNi est une signature qui couvre le message MIKEY de l'initiateur, I_MESSAGE, en utilisant la clé de signature de l'initiateur (voir au paragraphe 5.2 de la RFC 3830 la définition exacte). La signature assure à celui qui répond que l'initiateur prétendu a bien généré le message. Cela fournit aussi automatiquement l'intégrité du message.

3.5 Traitement du I_MESSAGE

À réception d'un I_MESSAGE au format RSA-R, celui qui répond DOIT répondre avec un des messages suivants :

- Il DEVRAIT envoyer un message d'erreur "Type de message non pris en charge" (Erreur n° 13) si il ne peut pas correctement analyser le message MIKEY reçu. Le format du message d'erreur est comme spécifé au paragraphe 5.1.2 de la RFC 3830. L'erreur n° 13 n'est pas définie dans la RFC 3830, et donc les mises en œuvre conformes à la RFC 3830 PEUVENT retourner une "erreur non spécifiée" (Erreur n° 12).

- Il DOIT envoyer un R_MESSAGE, si SIGNi peut être correctement vérifié et si l'horodatage est actuel ; si une charge utile SP est présente dans le I_MESSAGE, celui qui répond DOIT retourner une des politiques de sécurité proposées qui correspond à la politique locale de celui qui répond.

- Si une charge utile RAND est présente dans le I_MESSAGE, les deux côtés utilisent cette charge utile RAND comme valeur de RAND dans le calcul de clé de MIKEY. En cas de diffusion groupée, si une charge utile RAND est présente dans le I_MESSAGE, celui qui répond DEVRAIT ignorer la charge utile. Dans tous les cas, le R_MESSAGE pour la communication en diffusion groupée DOIT contenir une charge utile RAND et cette charge utile RAND est utilisée pour le calcul de clé.

- Le reste des règles de message d'errreur est comme décrit au paragraphe 5.1.2 de la RFC 3830, et les règles de traitement de message sont comme décrit au paragraphe 5.3 de la RFC 3830.

3.6 Composants du R_MESSAGE

La charge utile HDR dans le R_MESSAGE est formée suivant la procédure décrite dans la RFC 3830. Spécifiquement, le CSB_ID dans la charge utile HDR DOIT être le même que celui du HDR du I_MESSAGE. Le répondant DOIT remplir le nombre de CS et les champs Type de transposition d'identifiant de CS et Identifiant de CS de la charge utile HDR.

Pour la communication de groupe, tous les membres DOIVENT utiliser les mêmes CSB_ID et CS_ID dans le calcul du matériel de chiffrement du trafic. Donc, pour l'établissement de la clé de groupe, celui qui répond DOIT inclure une charge utile Extension générale contenant un nouveau CSB_ID dans le R_MESSAGE. Si un nouveau CSB_ID est présent dans le R_MESSAGE, l'initiateur et celui qui répond DOIVENT utiliser cette valeur dans le calcul du matériel de clé. De plus, le type de transposition de CS_ID et les informations de transposition de CS_ID DOIVENT être remplis par celui qui répond. La charge utile Extension générale qui porte un CSB_ID NE DOIT PAS être présente en cas de communication en envoi individuel.

La charge utile T est exactement la même que celle reçue dans le I_MESSAGE.

Si le I_MESSAGE n'incluait pas de charge utile RAND, elle DOIT être présente dans le R_MESSAGE. Au cas où elle a été incluse dans le I_MESSAGE, elle NE DOIT PAS être présente dans le R_MESSAGE. Dans une communication de groupe, celui qui répond envoie toujours la charge utile RAND et dans une communication en envoi individuel, l'initiateur ou celui qui répond (mais pas les deux) génère et envoie la charge utile RAND.

Le IDr et le CERTr DEVRAIENT être inclus, mais ils PEUVENT être laissés de côté quand on peut être s'attendre à ce que

l'homologue sache déjà l'identifiant de l'autre partie (ou peut obtenir le certificat d'une autre manière).Par exemple, ce pourrait être le cas si l'identifiant est extrait de SIP. Pour le traitement du certificat, de l'autorisation, et des politiques, voir le paragraphe 4.3 de la RFC 3830. Si CERTr est inclus, il DOIT correspondre à la clé privée utilisée pour signer le R_MESSAGE.

Une charge utile SP PEUT être incluse dans le R_MESSAGE. Si une charge utile SP était dans le I_MESSAGE, alors le R_MESSAGE DOIT contenir une charge utile SP spécifiant les politiques de sécurité de la session RTP sécurisée négociée. Plus précisément, l'initiateur peut avoir fourni plusieurs options, mais celui qui répond DOIT choisir une option par paramètre de politique de sécurité.

La charge utile KEMAC contient un ensemble de sous charges utiles chiffrées et un MAC : KEMAC = E(encr_key, IDr || {TGK}) || MAC. La première charge utile (IDr) dans KEMAC est l'identité de celui qui répond (pas un certificat, mais généralement le même identifiant que celui spécifié dans le certificat). Chacune des charges utiles suivantes (TGK) inclut une TGK choisie au hasard et indépendamment par celui qui répond (et éventuellement d'autres paramètres en rapport, par exemple, la durée de vie de la clé). La partie chiffrée est alors suivie par un MAC, qui est calculé sur la charge utile KEMAC. La encr_key et la auth_key sont déduites de la clé d'enveloppe, env_key, comme spécifé au paragraphe 4.1.4. de la RFC 3830. Les définitions de charge utile sont spécifiées au paragraphe 6.2 de la RFC 3830.

Le répondant chiffre et protège l'intégrité de la TGK avec des clés déduites d'une clé d'enveloppe choisie de façon aléatoire ou pseudo aléatoire, et il chiffre la clé d'enveloppe elle-même avec la clé publique de l'initiateur. La charge utile PKE contient la clé d'enveloppe chiffrée, env_key : PKE = E(PKi, env_key). PKi note la clé publique de l'initiateur. Noter que, comme suggéré dans la RFC 3830, la clé d'enveloppe PEUT être mise en antémémoire et utilisée comme PSK pour le changement de clé.

Pour calculer la signature qui va dans la charge utile SIGNr, celui qui répond DOIT signer :

R_MESSAGE (excluant la charge utile SIGNr elle-même) || IDi || IDr || T.

Noter que les identités et l'horodatage ajoutés sont identiques à ceux transportés dans les charges utiles ID et T.

3.7 Traitement du R_MESSAGE

En plus des règles de traitement de la RFC 3830, les règles suivantes s'appliquent au traitement du R_MESSAGE de mode MIKEY RSA-R.

Si le I_MESSAGE contenait une charge utile RAND, l'initiateur DOIT éliminer en silence un R_MESSAGE qui contient une charge utile RAND. De même, si le I_MESSAGE ne contenait pas de charge utile RAND, l'initiateur DOIT éliminer en silence un R_MESSAGE qui ne contient pas de charge utile RAND.

Si la charge utile SP contient une politique non spécifiée dans le message SP, si il est présent, dans le I_MESSAGE, un tel R_MESSAGE DOIT être éliminé en silence.

3.8 Traitement du certificat

Si une charge utile Certificat est présente, le type Cert d'URL X.509v3 du Tableau 6.7.b de la [RFC3830] est la méthode par défaut dans le mode RSA-R et DOIT être mis en œuvre. L'URL HTTP pour aller chercher un certificat, comme spécifié dans la [RFC2585] DOIT être pris en charge. Les appareils ne sont pas obligés de prendre en charge les URL FTP. Quand on récupère des données de l'URL, le type MIME application/pkix-cert avec les certificats X.509 codés en DER DOIT être pris en charge.

La façon RECOMMANDÉE de faire la validation de certificat est d'utiliser OCSP comme spécifié par la [RFC2560]. Quand OCSP est utilisé et que l'heure de nextUpdate est présentée dans la réponse, elle définit pendant combien de temps le certificat peut être considéré comme valide et conservé en antémémoire. Si OCSP n'est pas accepté ou si nextUpdate n'est pas présent dans la réponse, la temporisation de la mise en antémémoire du certificat est une affaire de politique locale.

Les homologues communicants (comme des agents d'utilisateur SIP par exemple) PEUVENT choisir de créer un URL pointant sur des fichiers de certificats résidant sur eux-mêmes ou en ajoutant leur identifiant et une extension ".cer" à un chemin de racine provisionné vers le certificat. D'autres méthodes PEUVENT aussi être utilisées, sous le contrôle de la

politique locale.

3.9 Ajouts aux types de message et autres valeurs de la RFC 3830

Le présent document introduit deux nouveaux types de message (Tableau 6.1a de la RFC 3830) un numéro d'erreur (Tableau 6.12 de la RFC 3830) et une charge utile d'extension générale (Tableau 6.15 de la RFC 3830). Ce paragraphe spécifie ces ajouts.

3.9.1 Modification du Tableau 6.1a de la RFC 3830

Tableau 6.1a modifié de la RFC 3830 :

Type de données	Valeur	Commentaire
Prépartagé	0	Message de clé prépartagée de l'initiateur
Mess vérif PSK	1	Message de vérification d'un message de clé prépartagée
Clé publique	2	Message de transport de clé publique de l'initiateur
Mess vérif PK	3	Message de vérification d'un message de clé publique
Init D-H	4	Message d'échange DH de l'initiateur
Rép D-H	5	Message d'échange DH du répondeur
Erreur	6	Message d'erreur
Init DHHMAC	7	Message DH HMAC 1
Rép DHHMAC	8	Message DH HMAC 2
RSA-R I_MSG	9	Message de l'initiateur de la clé publique RSA-R (Nouveau)
RSA-R R_MSG	10	Message du répondeur de la clé publique RSA-R (Nouveau)

Figure 3 : Tableau 6.1a de la RFC 3830 (révisé)

3.9.2 Modification du Tableau 6.12 de la RFC 3830

Tableau 6.12 modifié de la RFC 3830 :

Nom d'erreur	Valeur	Commentaire
Échec d'auth	0	Échec d'authentification
TS invalide	1	Horodatage invalide
PRF invalide	2	Fonction PRF non acceptée
MAC invalide	3	Algorithme de MAC non accepté
EA invalide	4	Algorithme de chiffrement non accepté
HA invalide	5	Fonction de hachage non acceptée
DH invalide	6	Groupe DH non accepté
ID invalide	7	Identifiant non accepté
Cert invalide	8	Certificat non accepté
SP invalide	9	Type SP non accepté
Sppar invalide	10	Paramètres SP non acceptés
DT invalide	11	Type de données non accepté
Non spécifié	12	Une erreur non spécifié est survenue
Type de message non pris en charge	13	Message MIKEY non analysable (Nouveau)

Figure 4 : Tableau 6.12 de la RFC 3830 (révisé)

3.9.3 Modification du Tableau 6.15 de la RFC 3830

Tableau 6.15 modifié de la RFC 3830 :

Type	Valeur	Commentaires
Vendor ID	0	Chaîne d'octets spécifique du fabricant
Identifiants SDP	1	Liste d'identifiants de gestion de clé SDP (utilisation allouée dans la [RFC4567])
I-Key TESLA	2	[RFC4442]
Key ID	3	Informations sur le type et l'identité des clés [RFC4563])
CSB_ID	4	CSB_ID modifié du répondant (mode groupe)

Figure 5 : Tableau 6.15 de la RFC 3830 (révisé)

4. Applicabilité des modes RSA-R et RSA

Les modes MIKEY-RSA-R et RSA sont tous deux très utiles : la décision du mode à utiliser dépend de l'application.

Le mode RSA-R est utile quand on a des raisons de croire que celui qui répond peut être une personne différente de celle à qui le I_MESSAGE MIKEY a été envoyé. C'est assez courant dans les applications de téléphonie et de multimédia où la session ou l'appel peut être reciblé ou transmis. Quand la politique de sécurité le permet, laisser un peu de souplesse à l'initiateur pour voir qui peut être celui qui répond avant de prendre la décision de continuer ou interrompre la session, peut être approprié. Dans de tels cas, le principal objectif du message RSA-R de l'initiateur est de présenter sa clé publique/certificat à celui qui répond, et d'attendre qu'un répondant présente son identité.

Le second scénario est quand l'initiateur a déjà le certificat de celui qui répond, mais veut lui permettre de venir avec tout le matériel de chiffrement. Ceci est applicable dans les conférences où celui qui répond est le distributeur de clés et où les initiateurs contactent celui qui répond pour initier le téléchargement de clé. Remarquer que ceci est assez similaire au modèle de téléchargement de clé de groupe comme spécifé dans les protocoles GDOI [RFC3547], GSAKMP [RFC4535], et GKDP [GKDP] (voir aussi la [RFC4046]). Le point central est cependant que les entités participantes doivent savoir qu'elle doivent contacter une adresse bien connue pour ce qui concerne le groupe de conférence. Noter qu'elles ont seulement besoin de l'adresse de celui qui répond, pas nécessairement de son certificat. Si les membres du groupe ont le certificat de celui qui répond, il n'y a pas de dommage ; il n'ont simplement pas besoin du certificat pour composer le I_MESSAGE.

Le mode RSA est utile quand l'initiateur connaît l'identité et le certificat de celui qui répond. Ce mode est aussi utile quand l'échange de clé arrive dans une session établie avec un répondant (par exemple, quand on passe d'un mode non sûr à un mode sûr) et quand la politique est telle qu'il est seulement approprié d'établir une session MIKEY avec le répondant qui est ciblé par l'initiateur.

4.1 Limitations

Le mode RSA-R ne peut pas prendre en charge facilement l'appel à trois, sous les hypothèses qui ont motivé la conception. Un message supplémentaire peut être nécessaire comparé au mode MIKEY-RSA spécifié dans la RFC 3830. Considérons que A veut parler à B et C, mais n'a pas le certificat de B ou de C. A pourrait contacter B et demander que B fournisse une clé pour un appel à trois. Maintenant, si B connaît le certificat de C, il peut simplement utiliser le mode MIKEY-RSA (comme défini dans la RFC 3830) pour envoyer la TGK à C. Sinon, la solution n'est pas directe. Par exemple, A pourrait demander à C de contacter B ou lui-même d'obtenir la TGK, initiant en effet un échange à trois. On devrait noter que l'appel à trois est normalement mis en œuvre en utilisant un pont, cas dans lequel il n'y a pas de problème (cela ressemble aux sessions en point à point à trois, où une extrémité de chaque session est un pont mixant le trafic en un seul flux).

5. Considérations sur la sécurité

On présente un bref survol des propriétés de sécurité de l'échange. Il y a deux messages : I_MESSAGE et R_MESSAGE. Le I_MESSAGE est une demande signée par un initiateur qui demande à celui qui répond de choisir une TGK à utiliser pour protéger les sessions multimédia (par exemple, des sessions SRTP [RFC3711]).

Le message est signé, ce qui assure à celui qui répond que l'initiateur prétendu a bien généré le message. Cela fournit automatiquement aussi l'intégrité de message.

Il y a un horodatage dans le I_MESSAGE, qui quand il est généré et interprété dans le contexte de la spécification MIKEY assure à celui qui répond que la demande est vivante et n'est pas une répétition. Indirectement, cela fournit aussi une protection contre une attaque de déni de service (DoS) en ce que le I_MESSAGE doit lui-même être signé. Le répondantva cependant devoir vérifier la signature et l'horodatage de l'initiateur, et donc va dépenser des ressources significatives de calcul. Il est possible d'atténuer cela en mettant en antémémoire les demandes récemment reçues et vérifiées.

Noter que le I_MESSAGE dans cette méthode égale en gros les propriétés de protection contre le DoS de la méthode DH et non de la méthode de la clé publique car il n'y a pas de charge utile chiffrée par la clé publique de celui qui répond dans le I_MESSAGE. Si IDr n'est pas inclus dans le I_MESSAGE, celui qui répond va accepter le message et une réponse (et l'état) va être créée pour la demande malveillante.

Le R_MESSAGE est assez similaire au I_MESSAGE dans le mode MIKEY-RSA et a les mêmes propriétés de sécurité.

Quand on utilise le mode RSA-R, celui qui répond peut être une personne différente de celle à qui le I_MESSAGE MIKEY a été envoyé. Il est de la responsabilité de l'initiateur de vérifier que l'identité de celui qui répond est acceptable (sur la base de sa politique locale) si elle change par rapport à la partie à laquelle le I_MESSAGE MIKEY a été envoyé, et pour prendre l'action appropriée selon le résultat. Dans certains cas, il pourrait être approprié d'accepter une identité de répondant si elle peut être authentifiée de façon forte ; dans d'autres cas, une liste noire ou blanche peut être approprié.

Quand les deux flux d'envoi individuel et de diffusion groupée doivent être négociés, il est RECOMMANDÉ d'utiliser plusieurs instances de MIKEY-RSA-R plutôt qu'une seule instance en mode groupe. C'est pour éviter de potentielles réutilisations de clé avec le mode compteur.

5.1 Impact du choix du répondant du TGK

Dans les modes MIKEY-RSA ou PSK, l'initiateur choisit la TGK, et celui qui répond a l'option d'accepter ou non la clé. Dans le mode RSA-R pour la communication en envoi individuel, le mode RECOMMANDÉ de fonctionnement est que l'initiateur et celui qui répond contribuent aux informations aléatoires en générant la TEK (RAND de l'initiateur et TGK de celui qui répond). Pour la communication de groupe, l'envoyeur (répondant MIKEY) va choisir la TGK et le RAND ; noter qu'il est de l'intérêt de l'envoyeur de fournir une entropie suffisante à la génération de TEK car elle protège les données envoyées par celui qui répond.

Donc, en cas de communication en envoi individuel, le mode RSA-R est légèrement meilleur que le mode RSA en ce qu'il permet à l'initiateur ainsi qu'à celui qui répond de contribuer à l'entropie du processus de génération de TEK. Cela se fait au prix d'un message supplémentaire. Cependant, comme on l'a noté précédemment, le nouveau mode a besoin que le message supplémentaire permette un provisionnement plus simple.

5.2 Mises à jour des considérations sur la sécurité de la RFC 3830

MIKEY exige la synchronisation des horloges, et un protocole sûr de synchronisation des horloges du réseau DEVRAIT être utilisé, par exemple, [ISO3] ou NTP sécurisé [RFC5905].

La RFC 3830 a des notes supplémentaire sur les propriétés de sécurité du protocole MIKEY, les fonctions de déduction de clé, et les autres composants.

6. Considérations relatives à l'IANA

Les allocations suivantes de l'IANA ont été ajoutées au registre MIKEY :

Ajout à l'espace de noms de charge utile "Erreur" :
Type de message non pris en charge : 13

Ajout à l'espace de nom de charge utile "En-tête commun" :
RSA-R I_MSG : 9
RSA-R R_MSG : 10

Ajout à l'espace de nom de charge utile "Extensions générales" :
CSB_ID : 4

7. Remerciements

Tous nos remerciements à Mark Baugher, Steffen Fries, Russ Housley, Cullen Jennings, et Vesa Lehtovirta pour leur relecture des versions antérieures de ce document.

8. Références

8.1 Références normatives

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

[RFC2560] M. Myers, R. Ankney, A. Malpani, S. Galperin et C. Adams, "Protocole d'état de certificat en ligne d'infrastructure de clé publique X.509 pour l'Internet - OCSP", juin 1999. *(P.S.) (Remplacée par* RFC6960)

[RFC2585] R. Housley et P. Hoffman, "Protocoles de fonctionnement de l'infrastructure de clé publique X.509 pour l'Internet : FTP et HTTP", mai 1999. *(P.S.)*

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

8.2 Références pour information

[GKDP] Dondeti, L., "GKDP: Group Key Distribution Protocol", Travail dn cours, mars 2006.

[RFC3547] M. Baugher, B. Weis, T. Hardjono et H. Harney, "Le domaine d'interprétation de groupe", juillet 2003. *(Obsolète, voir la* RFC6407)

[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.)*

[RFC4442] S. Fries, H. Tschofenig, "Amorçage de l'authentification tolérante aux pertes de flux à synchronisation efficace (TESLA)", mars 2006. *(P.S.)*

[RFC4535] H. Harney et autres, "GSAKMP : protocole de gestion de clés d'association de groupe sécurisé", juin 2006. *(P.S.)*

[RFC4563] E. Carrara et autres, "Type d'information Identifiant de clé pour la charge utile d'extension générale dans le protocole de chiffrement Internet multimédia (MIKEY)", juin 2006. *(P.S.)*

[RFC4567] J. Arkko et autres, "Extensions de gestion de clés pour le protocole de description de session (SDP) et le protocole d'écoulement en temps réel (RTSP)", juillet 2006. *(P.S.)*

[RFC4650] M. Euchner, "Diffie-Hellman authentifié en HMAC pour le protocole de chiffrement Internet multimédia (MIKEY)", septembre 2006. *(P.S.)*

[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* RFC1305, RFC4330) *(P. S ; MàJ par* RFC7822, RFC8573)

[ISO3] ISO/CEI 18014, "Technologie de l'information – techniques de sécurité – services d'horodatage, Partie 1-3", 2002.

Adresse des auteurs

Dragan Ignjatic
Polycom
1000 W. 14th Street
North Vancouver, BC V7P 3P3
Canada
téléphone: +1 604 982 3424
mél : dignjatic@polycom.com

Lakshminath Dondeti
QUALCOMM
5775 Morehouse drive
San Diego, CA 92121
US
téléphone : +1 858 845 1267
mél: ldondeti@qualcomm.com

Francois Audet
Nortel
4655 Great America Parkway
Santa Clara, CA 95054
US
téléphone : +1 408 495 3756
mél : audet@nortel.com

Ping Lin
Nortel
250 Sidney St.
Belleville, Ontario K8P3Z3
Canada
téléphone : +1 613 967 5343
mél : linping@nortel.com

Déclaration complète de droits de reproduction

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