Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

H.235.1

(09/2005)

SÉRIE H: SYSTÈMES AUDIOVISUELS ET MULTIMÉDIAS

Infrastructure des services audiovisuels – Aspects système

Cadre de sécurité H.323: profil de sécurité de base

Recommandation UIT-T H.235.1

RECOMMANDATIONS UIT-T DE LA SÉRIE H

SYSTÈMES AUDIOVISUELS ET MULTIMÉDIAS

CARACTÉRISTIQUES DES SYSTÈMES VISIOPHONIQUES	H.100–H.199
INFRASTRUCTURE DES SERVICES AUDIOVISUELS	
Généralités	H.200–H.219
Multiplexage et synchronisation en transmission	H.220–H.229
Aspects système	**H.230–H.239**
Procédures de communication	H.240–H.259
Codage des images vidéo animées	H.260–H.279
Aspects liés aux systèmes	H.280–H.299
Systèmes et équipements terminaux pour les services audiovisuels	H.300–H.349
Architecture des services d'annuaire pour les services audiovisuels et multimédias	H.350–H.359
Architecture de la qualité de service pour les services audiovisuels et multimédias	H.360–H.369
Services complémentaires en multimédia	H.450–H.499
PROCÉDURES DE MOBILITÉ ET DE COLLABORATION	
Aperçu général de la mobilité et de la collaboration, définitions, protocoles et procédures	H.500–H.509
Mobilité pour les systèmes et services multimédias de la série H	H.510–H.519
Applications et services de collaboration multimédia mobile	H.520–H.529
Sécurité pour les systèmes et services multimédias mobiles	H.530–H.539
Sécurité pour les applications et services de collaboration multimédia mobile	H.540–H.549
Procédures d'interfonctionnement de la mobilité	H.550–H.559
Procédures d'interfonctionnement de collaboration multimédia mobile	H.560–H.569
SERVICES À LARGE BANDE ET MULTIMÉDIAS TRI-SERVICES	
Services multimédias à large bande sur VDSL	H.610–H.619

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T H.235.1

Cadre de sécurité H.323: profil de sécurité de base

Résumé

La présente Recommandation définit un profil permettant d'assurer l'authentification et la protection de l'intégrité, ou l'authentification seulement, pour les messages RAS et les messages de signalisation d'appel H.225.0 ainsi que pour les messages H.245 tunnellisés dans des messages H.225.0, la protection des messages RAS et des messages de signalisation d'appel H.225.0 étant assurée par une valeur de hachage HMAC-SHA1-96 fondée sur un mot de passe et des techniques de chiffrement à mot de passe sécurisé étant utilisées. Ce profil de sécurité est applicable entre un terminal H.323 et un portier, entre deux portiers, entre une passerelle H.323 et un portier ainsi qu'à d'autres entités H.323 dans des environnements administrés avec des clés/mots de passe attribués de façon symétrique.

Dans les anciennes versions de la sous-série H.235, ce profil était défini dans l'Annexe D/H.235. Les Appendices IV, V et VI/H.235.0 donnent le mappage entre tous les paragraphes, toutes les figures et tous les tableaux de la version 3 et tous ceux de la version 4 de la Rec. UIT-T H.235.

Source

La Recommandation UIT-T H.235.1 a été approuvée le 13 septembre 2005 par la Commission d'études 16 (2005-2008) de l'UIT-T selon la procédure définie dans la Recommandation UIT-T A.8.

Mots clés

Authentification, certificat, chiffrement, gestion de clés, intégrité, profil de sécurité, sécurité multimédia, signature numérique.

AVANT-PROPOS

L'UIT (Union internationale des télécommunications) est une institution spécialisée des Nations Unies dans le domaine des télécommunications. L'UIT-T (Secteur de la normalisation des télécommunications) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un Membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux responsables de la mise en œuvre de consulter la base de données des brevets du TSB.

TABLE DES MATIÈRES

Recommandation UIT-T H.235.1

Cadre de sécurité H.323: profil de sécurité de base

1 Domaine d'application

La présente Recommandation définit un profil permettant d'assurer l'authentification et la protection de l'intégrité, ou l'authentification seulement, pour les messages RAS et les messages de signalisation d'appel H.225.0 ainsi que pour les messages H.245 tunnellisés dans des messages H.225.0, la protection des messages RAS et des messages de signalisation d'appel H.225.0 étant assurée par une valeur de hachage HMAC-SHA1-96 fondée sur un mot de passe et des techniques de chiffrement à mot de passe sécurisé étant utilisées. Ce profil de sécurité est applicable entre un terminal H.323 et un portier, entre deux portiers, entre une passerelle H.323 et un portier ainsi qu'à d'autres entités H.323.

2 Références

2.1 Références normatives

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

– Recommandation UIT-T H.225.0 (2003), *Protocoles de signalisation d'appel et paquétisation des flux monomédias pour les systèmes de communication multimédias en mode paquet*.

– Recommandation UIT-T H.235 version 1 (1998), *Sécurité et cryptage des terminaux multimédias de la série H (terminaux H.323 et autres terminaux de type H.245).*

– Recommandation UIT-T H.235 version 2 (2000), *Sécurité et cryptage des terminaux multimédias de la série H (terminaux H.323 et autres terminaux de type H.245).*

– Recommandation UIT-T H.235.0 (2005), *Cadre de sécurité H.323: cadre de sécurité pour les systèmes multimédias de la série H (systèmes H.323 et autres systèmes de type H.245).*

– Recommandation UIT-T H.235.2 (2005), *Cadre de sécurité H.323: profil de sécurité avec signature.*

– Recommandation UIT-T H.235.4 (2005), *Cadre de sécurité H.323: sécurité des appels à routage direct et des appels à routage sélectif.*

– Recommandation UIT-T H.235.6 (2005), *Cadre de sécurité H.323: profil pour le chiffrement vocal avec gestion de clés H.235/H.245 native*.

– Recommandation UIT-T H.245 version 10 (2003), *Protocole de commande pour communications multimédias*.

– Recommandation UIT-T H.323 (2003), *Systèmes de communication multimédia en mode paquet*.

– Recommandation UIT-T H.323 Annexe F (1999), *Dispositifs d'extrémité simples*.

– Recommandation UIT-T Q.931 (1998), *Spécification de la couche 3 de l'interface utilisateur-réseau RNIS pour la commande de l'appel de base*.

– Recommandation UIT-T X.800 (1991), *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT*.

ISO/CEI 7498-2:1989, *Systèmes de traitement de l'information – Interconnexion de systèmes ouverts – Modèle de référence de base – Partie 2: Architecture de sécurité*.

– Recommandation UIT-T X.803 (1994) | ISO/CEI 10745:1995, *Technologies de l'information – Interconnexion des systèmes ouverts – Modèle de sécurité pour les couches supérieure*s.

– Recommandation UIT-T X.810 (1995) | ISO/CEI 10181-1:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: aperçu général*.

– Recommandation UIT-T X.811 (1995) | ISO/CEI 10181-2:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: cadre d'authentification*.

ISO/CEI 10118-3:2004, *Technologies de l'information – Techniques de sécurité – Fonctions de brouillage – Partie 3: Fonctions de brouillage dédiées*.

2.2 Références informatives

[FIPSPUB180-2] Federal Information Processing Standard FIPS PUB 180-2, Secure Hash Standard, U. S. Department of Commerce, Technology Administration, National Institute of Standards and Technology, 1 August 2002.

[OIW] Stable Implementation – Agreements for Open Systems Interconnection Protocols: Part 12 – OS Security; Output from the December 1994 Open Systems Environment Implementors' Workshop (OIW); http://nemo.ncsl.nist.gov/oiw/agreements/stable/OSI/12s_9412.txt.

[RFC2104] IETF RFC 2104 (1997), *HMAC: Keyed-Hashing for Message Authentication*.

[WEBOIDs] http://www.alvestrand.no/objectid/top.html.

3 Termes et définitions

Dans la présente Recommandation, les définitions figurant au § 3/H.323, au § 3/H.225.0 et au § 3/H.245 s'appliquent, en plus de celles du présent paragraphe. Certains des termes suivants sont utilisés selon la définition donnée dans les Recommandations UIT-T X.800 | ISO/CEI 7498-2, UIT-T X.803 | ISO/CEI 10745, X.810 | ISO/CEI 10181-1 et X.811 | ISO/CEI 10181-2.

La présente Recommandation utilise les termes suivants dans le contexte des services de sécurité:

3.1 authentification et intégrité: double service de sécurité faisant partie du profil de base, assurant aussi bien l'intégrité des messages que l'authentification des utilisateurs. Pour s'authentifier, un utilisateur peut appliquer correctement une procédure à clé secrète partagée. Les deux services de sécurité sont assurés par le même mécanisme de sécurité.

3.2 authentification seulement: service de sécurité offert en option par le profil de sécurité de base, assurant l'authentification seulement de certains champs mais pas l'intégrité totale des messages. Le profil de sécurité par authentification seulement s'applique aux messages de signalisation franchissant des dispositifs NAT/pare-feu. Pour s'authentifier, un utilisateur peut appliquer correctement une procédure à clé secrète partagée.

Lorsqu'on utilise des techniques à clé symétrique, les services de sécurité d'authentification/intégrité s'appliquent uniquement bond par bond.

4 Symboles et abréviations

La présente Recommandation utilise les abréviations suivantes:

ASN.1 notation de syntaxe abstraite numéro un (*abstract syntax notation one*)

EP point d'extrémité (*endpoint*)

EPID identificateur de point d'extrémité (*endpoint identifier*)

GK portier (*gatekeeper*)

GKID identificateur de portier (*gatekeeper identifier*)

GRQ demande de portier (*gatekeeper request*)

HMAC code d'authentification de message haché (*hash message authentication code*)

ICV valeur de contrôle d'intégrité (*integrity check value*)

LRQ demande de localisation (*location request*)

MAC code d'authentification de message (*message authentication code*)

NAT traduction d'adresse de réseau (*network address translation*)

OID identificateur d'objet (*object identifier*)

RAS enregistrement, admission et statut (*registration, admission and status*)

RTP protocole de transport en temps réel (*real-time protocol*)

SHA algorithme de hachage sécurisé (*secure hash algorithm*)

TCP protocole de commande de transmission (*transmission control protocol*)

UIT Union internationale des télécommunications

UTC horloge universelle (*universal time clock*)

VoIP téléphonie utilisant le protocole Internet (*voice over Internet protocol*)

5 Conventions

Dans la présente Recommandation, les conventions suivantes s'appliquent:

– la forme "doit/doivent" indique une disposition obligatoire;

– la forme "devrait/devraient" indique une mesure suggérée mais facultative;

– la forme "peut/peuvent" indique une action possible plutôt qu'une action recommandée.

La présente Recommandation définit un **profil de sécurité de base**, qui fournit la sécurité de base par des moyens simples utilisant des techniques cryptographiques de type à mot de passe sécurisé. Ce profil de sécurité de base peut être utilisé conjointement avec d'autres profils de sécurité (par exemple H.235.3, H.235.4, H.235.5, H.235.6 ou H.235.7).

La présente Recommandation utilise des champs H.235 pour fournir des services de sécurité de type authentification/intégrité au moyen de messages de signalisation H.323. Divers identificateurs d'objet (voir § 15) déterminent le service de sécurité qui est effectivement choisi et la version de protocole de la présente Recommandation qui est utilisée. La procédure I spécifie la manière d'implémenter les services de sécurité au moyen de certains mécanismes de sécurité tels que les techniques symétriques (hachage avec clé). Les identificateurs d'objet sont désignés par un symbole dans le texte (par exemple "A"). Voir également le § 5/H.235.0.

Si le service d'intégrité des messages fournit toujours l'authentification des messages, l'inverse n'est pas nécessairement vrai. Dans la pratique, le double service d'authentification et d'intégrité exploite les mêmes données de clé sans introduire de faiblesse au niveau de la sécurité.

De plus, toutes les informations de sécurité relatives à chaque bond sont mises dans l'élément **CryptoHashedToken**. Ces informations sont recalculées à chaque bond.

Dans la présente Recommandation, certaines techniques cryptographiques symétriques sont appliquées pour l'authentification et l'intégrité et on emploie alors les termes de mot de passe et de secret partagé.

Généralement, le mot de passe, la clé de session et le secret partagé ont en commun qu'ils sont utilisés en cryptographie symétrique entre deux entités (ou plus). La différence entre un mot de passe et une clé de session/secret partagé est la manière dont les clés sont effectivement appliquées, par exemple les mots de passe pour l'authentification et l'autorisation, les clés de session pour le chiffrement. Le terme secret partagé est relativement neutre étant donné qu'il ne se réfère pas à un usage spécifique.

Le **mot de passe** (que l'on peut assimiler à un secret partagé) est utilisé pour l'authentification/intégrité des messages RAS et H.225.0 étant donné que cet élément peut être introduit par l'utilisateur. Il s'agit généralement d'une chaîne de caractères alphanumériques que les utilisateurs peuvent mémoriser. En principe, le mot de passe a une durée de vie relativement longue. Il est connu a priori et peut-être défini dans le contexte du processus global d'abonnement de l'utilisateur. Certains algorithmes (par exemple, le passage des mots de passe dans un algorithme de hachage) peuvent transformer le mot de passe en un élément de longueur fixe afin d'en faciliter le traitement dans les protocoles.

Evidemment, l'utilisation des mots de passe ne va pas sans certaines précautions: pour offrir des garanties de sécurité suffisantes, les mots de passe doivent être choisis aléatoirement dans un grand espace, ils doivent présenter une entropie suffisante de manière à ne pas pouvoir être découverts et, enfin, ils doivent être régulièrement modifiés. Les règles de création et de mise à jour des mots de passe n'entrent pas dans le cadre de la présente Recommandation.

Une méthode efficace pour tirer parti des mots de passe et des secrets partagés consiste à transformer la chaîne du mot de passe de l'utilisateur en une chaîne binaire de longueur fixe qui devient ainsi le secret partagé, au moyen d'une fonction de hachage unilatéral robuste sur le plan cryptographique.

A titre d'exemple, dans le cas du profil de sécurité visé dans la présente Recommandation, la fonction de hachage SHA1 appliquée à la chaîne du mot de passe produit un secret partagé de 20 octets. Le hachage présente l'avantage de non seulement occulter le mot de passe proprement dit mais aussi de définir un format de chaîne binaire de longueur fixe sans réellement réduire l'entropie pour autant.

Par conséquent,

secret partagé: = SHA1 (mot de passe)

Le jeton **ClearToken** H.235 a un champ appelé **random** qui contient un entier de 32 bits. Ce champ est utilisé dans le sens suivant: il s'agit d'un nombre croissant monotone qui commence à n'importe quelle valeur et qui augmente à chaque message sortant. Le champ **random** est utilisé comme une valeur de "randomisation" additionnelle pour l'entrée dans la fonction de hachage avec clé au cas où plusieurs messages sont émis si rapidement les uns après les autres qu'ils comportent des horodates identiques. Cela peut se produire lorsque la résolution de l'horloge UTC est insuffisante. En substance, la valeur de hachage produite ou la valeur de contrôle de l'intégrité se distingue par les changements de la valeur de **random**. Ceci a pour but de contrer les attaques par réexécution. Dans un souci de simplicité d'implémentation, on préfère, dans le cas présent, un compteur croissant à une séquence réellement aléatoire. Le destinataire peut conserver les couples **timestamp/random** reçus au cours de la période définie par une fenêtre temporelle locale. Le même couple **timestamp/random** survenant deux fois signale une attaque par réexécution.

NOTE – La fenêtre temporelle compense les écarts de l'heure synchronisée ainsi que les temps de transit dans le réseau.

Le présent profil consiste à "donner à l'identificateur **generalID** de **ClearToken** la valeur de l'identificateur du destinataire". Cela signifie en fait que pour des messages RAS destinés au portier, il s'agit de l'identificateur du portier; pour les messages RAS destinés au point d'extrémité, il s'agit de l'identificateur du point d'extrémité; pour les messages de signalisation d'appel H.225.0 destinés au portier, il s'agit de l'identificateur du portier et pour les messages de signalisation d'appel H.225.0 destinés au point d'extrémité, il s'agit de l'identificateur du point d'extrémité appelé. Voir aussi le § 14.

L'identificateur **sendersID** doit être mis à la chaîne d'identification de l'expéditeur. Cela signifie en fait que pour des messages RAS destinés au portier, il s'agit de l'identificateur du point d'extrémité; pour les messages RAS destinés au point d'extrémité, il s'agit de l'identificateur du portier; pour les messages de signalisation d'appel H.225.0 destinés au portier, il s'agit de l'identificateur du portier et pour les messages de signalisation d'appel H.225.0 destinés au point d'extrémité, il s'agit de l'identificateur du point d'extrémité appelé. Voir aussi le § 14.

Dans la présente Recommandation, la protection de l'intégrité d'un message peut couvrir la totalité du message. Pour un message RAS H.225.0, la protection de l'intégrité couvre la totalité du message RAS; pour un message de signalisation d'appel, elle couvre la totalité du message de signalisation d'appel H.225.0 y compris les en-têtes Q.931.

La présente Recommandation contient des termes bien connus relatifs à la sécurité tels que clé, gestion de clés et dispositif SET, dont les équivalents en anglais ont des sens différents dans d'autres contextes (par exemple clavier tactile, gestion des touches de fonction Q.931/Q.932 et protocoles de transaction électronique sécurisée).

6 Aperçu général

La présente Recommandation définit un profil permettant d'assurer l'authentification et la protection de l'intégrité, ou l'authentification seulement, pour les messages RAS et les messages de signalisation d'appel H.225.0 ainsi que pour les messages H.245 tunnellisés dans des messages H.225.0, la protection des messages RAS et des messages de signalisation d'appel H.225.0 étant assurée par une valeur de hachage HMAC-SHA1-96 fondée sur un mot de passe et des techniques de chiffrement à mot de passe sécurisé étant utilisées. Ce profil de sécurité est applicable entre un terminal H.323 et un portier, entre deux portiers, entre une passerelle H.323 et un portier ainsi qu'à d'autres entités H.323 dans des environnements administrés avec des clés/mots de passe attribués de façon symétrique.

6.1 Brève description des fonctionnalités de sécurité

Les fonctionnalités offertes par ce profil sont les suivantes:

– pour les messages RAS, H.225.0 et H.245 tunnellisés:

  • l'authentification de l'utilisateur auprès de l'entité voulue, indépendamment du nombre de bonds au niveau application franchis par le message;

    NOTE – Par "bond", on entend dans le cas présent un élément de réseau H.235 de confiance (tel que portier, passerelle, pont MCU, proxy, pare-feu). En conséquence, la sécurité bond par bond au niveau application, lorsqu'elle est utilisée avec des techniques symétriques, n'assure pas une sécurité vraie de bout en bout entre les terminaux.

  • l'intégrité du message de signalisation proprement dit, y compris ses champs critiques, parvenant à une entité, indépendamment du nombre de bonds au niveau application franchis par le message;

- l'authentification et l'intégrité d'un message de signalisation bond par bond au niveau application couvrent la totalité du message.

Plusieurs types d'attaque sont combattus au moyen des services de sécurité ci-dessus, utilisés de manière appropriée. Il s'agit:

- des attaques de type déni de service: une vérification rapide des valeurs de hachage cryptographique peuvent préserver de telles attaques;
- des attaques par intercepteur: l'authentification et l'intégrité des messages bond par bond au niveau application empêchent de telles attaques lorsque l'intercepteur, un routeur hostile par exemple, se trouve entre deux bonds au niveau application;
- des attaques par réexécution: l'emploi d'horodates et de numéros de séquence empêche de telles attaques;
- des mystifications: l'authentification de l'utilisateur empêche de telles attaques;
- du détournement de connexions: l'authentification/intégrité de chaque message de signalisation empêche de telles attaques.

D'autres aspects importants du profil de sécurité simple sont:

- l'emploi d'algorithmes robustes, réputés et largement utilisés, fondés sur les travaux de l'IMTC/ETSI/IETF;
- la capacité de mise en place progressive, en fonction des besoins de sécurité du modèle commercial;
- l'applicabilité à divers scénarios de mise en place, par exemple les groupes fermés, les environnements évolutifs et les conférences multipoints;
- le profil de sécurité par authentification seulement est utilisable lorsqu'on veut disposer d'une certaine sécurité pour le franchissement des dispositifs NAT/pare-feu.

Le Tableau 1 groupe par profil de sécurité toutes les procédures définies dans la présente Recommandation afin de traiter des divers besoins en matière de sécurité. La zone hachurée en diagonale (en bleu dans la version électronique) représente le profil optionnel de sécurité par authentification seulement.

Tableau 1/H.235.1 – Profil de sécurité de base

Services de sécurité	**Fonctions d'appel**			
	RAS	**H.225.0**	**H.245 (Note)**	**RTP**
Authentification	HMAC-SHA1-96 avec mot de passe	HMAC-SHA1-96 avec mot de passe	HMAC-SHA1-96 avec mot de passe	
Authentification seulement	HMAC-SHA1-96 avec mot de passe	HMAC-SHA1-96 avec mot de passe	HMAC-SHA1-96 avec mot de passe	
Non-répudiation				
Intégrité	HMAC-SHA1-96 avec mot de passe	HMAC-SHA1-96 avec mot de passe	HMAC-SHA1-96 avec mot de passe	
Confidentialité				
Contrôle d'accès				
Gestion de clés	Attribution de mot de passe à la prise d'abonnement			
NOTE – Message H.245 tunnellisé ou message H.245 imbriqué dans le cadre de la connexion rapide H.225.0.				

Pour l'authentification, l'utilisateur doit utiliser un système à mot de passe, système fortement recommandé pour l'authentification en raison de sa simplicité et de sa facilité d'implémentation. Le hachage de tous les champs des messages RAS et de signalisation d'appel H.225.0 est la méthode recommandée pour assurer l'intégrité des messages (utilisant également le système à mot de passe).

Les entités H.323 sécurisées au moyen de ce profil de sécurité assurent aussi bien l'authentification que l'intégrité au moyen du même mécanisme de sécurité commun.

Les moyens de contrôle d'accès ne sont pas décrits explicitement; ils peuvent être implémentés localement compte tenu des informations reçues dans les champs de signalisation H.235 (jeton ClearToken, jeton CryptoToken).

La présente Recommandation ne décrit pas les procédures d'attribution des mots de passe/clés secrètes au moment de l'abonnement ni les procédures de gestion et d'administration associées. De telles procédures peuvent être exécutées par des moyens qui ne sont pas traités dans la présente Recommandation.

Les entités de communication concernées ont la possibilité de déterminer implicitement lequel du profil de sécurité de base et du profil de sécurité avec signature est utilisé, en évaluant les identificateurs d'objet de sécurité signalés dans les messages (identificateurs **tokenOID** et **algorithmOID**; voir également § 15).

6.2 Applicabilité du profil de sécurité de base

Le profil de sécurité de base est applicable dans un environnement où des mots de passe/clés symétriques peuvent être attribués, au moment de l'abonnement, aux entités H.323 sécurisées (terminaux, etc.) et aux éléments de réseau (portiers, proxys). Il offre l'authentification et l'intégrité, ou l'authentification seulement, pour les messages RAS et les messages de signalisation d'appel H.225.0 ainsi que les messages H.245 tunnellisés dans des messages H.225.0 au moyen de la valeur de hachage HMAC-SHA1-96 fondée sur un mot de passe, comme spécifié par la procédure I. L'établissement de la communication H.225.0 au moyen de FastStart (portier à portier ou terminal à terminal) englobe la gestion de clés Diffie-Hellman intégrée.

Pour le profil de sécurité de base, la procédure de connexion rapide est obligatoire et il est recommandé d'employer la tunnellisation de messages H.245 dans des messages H.225.0.

6.3 Prescriptions H.323

Les entités H.323 qui implémentent ce profil de sécurité de base sont supposées prendre en charge les caractéristiques H.323 suivantes:

- la connexion rapide;
- le modèle à routage par portier.

6.4 Aperçu général des procédures

Description de la procédure à utiliser dans ce profil.

La procédure I est un mécanisme d'authentification de messages de signalisation de type à clés symétriques simple basé sur un mot de passe connu par deux entités (par exemple, un portier et un point d'extrémité H.323). Cette procédure assure l'authentification et l'intégrité des messages RAS, Q.931 et H.245 (voir § 7).

La procédure IA est un mécanisme d'authentification seulement de type à clés symétriques simple basé sur un mot de passe connu par deux entités (par exemple un portier et un point d'extrémité H.323). Cette procédure assure l'authentification mais pas l'intégrité totale des messages. L'option authentification seulement est applicable aux scénarios dans lesquels les messages de signalisation H.323 franchissent des dispositifs NAT/pare-feu.

Selon la politique de sécurité, l'authentification peut être unilatérale ou bilatérale, l'authentification/intégrité étant alors appliquée dans les deux sens, ce qui accroît la sécurité. Le portier décide s'il y a lieu d'appliquer l'authentification/l'intégrité dans les deux sens.

Lorsque les portiers détectent un échec de validation de l'authentification et/ou de l'intégrité dans un message RAS ou un message de signalisation d'appel provenant d'un point d'extrémité sécurisé ou d'un portier homologue, ils répondent par un message de rejet correspondant indiquant l'absence de sécurité en mettant le motif de rejet à **securityDenial** ou tout autre code d'erreur de sécurité approprié, conformément au § 11.1/H.235.0. En fonction de sa capacité à reconnaître des attaques et de la façon la plus appropriée de réagir à ces attaques, un portier qui reçoit un message **xRQ** sécurisé contenant des identificateurs d'objet non définis (**tokenOID**, **algorithmOID**), peut répondre par un message **xRJ** non sécurisé avec le motif de rejet **securityDenial** ou éliminer le message. L'évènement de sécurité observé devrait être journalisé. Par ailleurs, le point d'extrémité doit éliminer le message non sécurisé reçu, temporiser et peut ensuite procéder à un nouvel essai en envisageant de choisir des identificateurs OID différents. De même, un portier qui reçoit un message SETUP H.225.0 sécurisé contenant des identificateurs d'objet non définis (**tokenOID**, **algorithmOID**), peut répondre par un message RELEASE COMPLETE non sécurisé avec le motif de rejet **securityDenied** ou éliminer le message. L'évènement de sécurité observé devrait aussi être journalisé.

Il existe une signalisation H.235 implicite pour indiquer l'utilisation de la procédure I et du mécanisme de sécurité appliqué, sur la base de la valeur des identificateurs d'objet (voir également § 15) et du contenu des champs de message.

Ce profil n'utilise pas les champs ICV H.235; en effet, les valeurs de contrôle d'intégrité cryptographique sont traitées comme des valeurs de hachage cryptographique et sont mises dans les champs de hachage de **CryptoToken**.

7 Authentification et intégrité des messages de signalisation de type à clés symétriques (procédure I)

Il faudra suivre les procédures ci-après en cas d'emploi de la procédure I:

- l'algorithme HMAC-SHA1-96 génère une valeur de hachage de 12 octets (96 bits) comme authentificateur résultant. Pour produire la clé à partir d'un mot de passe, il *faut* utiliser le mécanisme décrit au § 8.2.4/H.235.0.

  NOTE 1 – Lorsqu'on détermine la clé secrète à partir d'un mot de passe entré par l'utilisateur, il faut veiller à ce qu'ils soient suffisamment aléatoires. Il est recommandé, par exemple, d'utiliser des secrets réellement aléatoires pour la clé secrète ou de s'assurer que les mots de passe aléatoires sont suffisamment longs.

- Le champ **CryptoH323Token** de chaque message H.225.0/RAS doit contenir les champs suivants:

  – **nestedCryptoToken** contenant un **CryptoToken** contenant à son tour **cryptoHashedToken** avec les champs suivants:

    - **tokenOID** mis à "A" pour indiquer que le calcul d'authentification/intégrité porte sur tous les champs du message RAS ou de signalisation d'appel H.225.0.

- **hashedVals** contenant le champ **ClearToken** utilisé avec les champs suivants:
  - **tokenOID** mis à "T" indiquant que le jeton **ClearToken** de base comme montré ci-dessous est en cours d'utilisation pour l'authentification de message et la protection contre les attaques par réexécution et optionnellement aussi pour la gestion de clés Diffie-Hellman décrite au § 8.5/H.235.6. On peut aussi utiliser d'autres jetons **ClearToken** en lieu et place du jeton **ClearToken** de base.
  - **timeStamp** contenant l'horodate.
  - **random** contenant un numéro de séquence croissant monotone. Ce numéro permet de distinguer deux messages ayant la même horodate (dans les limites de la résolution d'horloge).
  - **generalID** contenant l'identificateur du destinataire (uniquement dans le cas de messages à destination unique).
  - **sendersID** contenant l'identificateur de l'expéditeur.
  - **dhkey**, utilisé pour transférer les paramètres Diffie-Hellman comme spécifié dans la présente Recommandation pendant l'intervalle **Setup** à **Connect**.
    - **halfkey** contenant la clé publique aléatoire de l'un des correspondants;
    - **modsize** contenant le nombre premier DH (voir Tableau 4/H.235.6);
    - **generator** contenant le groupe DH (voir Tableau 4/H.235.6).

  NOTE 2 – Lorsque le profil de sécurité de base est utilisé sans le profil de sécurité pour le chiffrement vocal, aucun paramètre Diffie-Hellman ne devrait être envoyé et **dhkey** devrait être absent; **halfkey**, **modsize** et **generator** peuvent être mis à {'0'B,'0'B,'0'B}.

- **token** contenant **HASHED**, avec les champs:
  - **algorithmOID** mis à "U" pour indiquer l'utilisation de l'algorithme HMAC-SHA1-96;
  - **params** mis à NULL;
  - **hash** contenant l'authentificateur calculé au moyen de l'algorithme HMAC-SHA1-96. L'authentificateur peut être calculé:
    - sur l'ensemble des champs du message RAS ou de signalisation d'appel H.225.0 si **tokenOID** de **CryptoHashedToken** est mis à "A" (indiquant l'authentification et l'intégrité).

  tokenOID est mis à "A" pour la protection des unités H323-UU-PDU tunnellisées, y compris tout le contenu du message H.245; le calcul de la valeur de hachage doit porter sur l'ensemble du message de signalisation d'appel **H.225.0** avec tous les champs, conformément à la procédure décrite au § 7.3.

- L'authentificateur est vérifié à la fin du tronçon terminal du canal (EP1 à GK1, GK1 à GK2, GK2 à EP2, EP1 à GK2, GK1 à EP2 ou EP1 à EP2 selon le cas) et recalculé avant l'envoi du message vers le tronçon suivant.

NOTE 3 – L'authentificateur est calculé pour chaque message.

NOTE 4 – Il faut utiliser la méthode de bourrage indiquée dans la norme SHA1 (ISO/CEI 10118-3).

NOTE 5 – En cas d'utilisation de l'authentification/intégrité combinées, l'authentificateur est calculé sur l'ensemble du message.

NOTE 6 – Pour éviter le risque d'attaque par réexécution, il est fortement recommandé de veiller, au niveau de l'implémentation, à changer le mot de passe (clé) avant une rotation complète (soit avant la fin du cycle) du numéro de séquence croissant monotone.

NOTE 7 – Le destinataire a la capacité de détecter l'utilisation de la procédure I en évaluant le **tokenOID** du jeton **EncodedGeneralToken** haché (en détectant la présence de "A").

7.1 Calcul de la valeur de hachage fondée sur un mot de passe

L'expéditeur et le destinataire d'un message protégé au niveau de l'authentification/intégrité calculent une valeur de hachage fondée sur une clé à partir de tous les champs de message codés ASN.1 (avec l'identificateur OID "A"). Pour le profil par authentification seulement, l'expéditeur et le destinataire calculent tous deux une valeur de hachage fondée sur une clé à partir de la totalité du ClearToken codé en ASN.1 (avec l'identificateur OID "B").

7.2 Algorithme HMAC-SHA1-96

La valeur de hachage cryptographique de 96 bits HMAC-SHA1-96 est obtenue par troncature de la valeur de hachage de 160 bits donnée par l'algorithme SHA1. Il faut utiliser comme résultat les 96 bits de gauche de la représentation réseau des octets de la valeur de hachage. La référence RFC 2104 décrit la procédure dans laquelle la clé secrète *K* correspond au secret partagé (= mot de passe haché par l'algorithme SHA1) et *text* correspond au "tampon de message".

7.3 Calcul et vérification de l'authentification et de l'intégrité

La procédure pour l'authentification et l'intégrité des messages (identificateur OID mis à "A") est la suivante:

L'expéditeur d'un message doit calculer la valeur de hachage de la manière suivante:

1) mettre la valeur de hachage à une séquence par défaut spécifique d'une longueur de 96 bits. La séquence binaire exacte importe peu mais il est judicieux de choisir une séquence binaire unique qui ne survient pas dans le reste du message;
2) coder l'ensemble du message en ASN.1; pour un message RAS, cette opération doit porter sur la totalité du message RAS H.225; pour un message de signalisation d'appel, cette opération doit porter sur la totalité du message de signalisation d'appel H.225.0;
3) localiser la séquence par défaut dans le message codé; annuler la séquence binaire trouvée et la remplacer par 96 bits zéro;

   NOTE 1 – Cela peut sous-entendre quelques essais et quelques erreurs au cas, très rare, où la séquence par défaut survient plusieurs fois dans le message.
4) calculer la valeur de hachage cryptographique à partir du message codé en ASN.1 en utilisant l'algorithme HMAC-SHA1-96 (voir § 7.2);
5) substituer, dans le message codé, la séquence par défaut par la valeur de hachage calculée.

Le destinataire recevant le message doit procéder de la manière suivante:

1) décoder le message ASN.1;
2) extraire la valeur de hachage reçue et la conserver dans une variable locale RV;
3) rechercher et localiser la valeur de hachage RV dans le message codé reçu;

   NOTE 2 – Dans le cas rare où la sous-chaîne de la valeur de hachage survient à plusieurs reprises dans l'ensemble du message il convient d'itérer les étapes 3 à 6 avec des points de départ de la recherche différents.
4) annuler la séquence binaire dans le message codé et la remplacer par 96 zéros;
5) calculer la valeur de hachage cryptographique à partir du message codé en utilisant l'algorithme HMAC-SHA1-96 (voir § 7.2);
6) comparer la valeur RV avec la valeur de hachage calculée. On considère que le message est exempt d'erreur seulement si les deux valeurs de hachage sont égales; dans ce cas, l'authentification a abouti et la procédure s'arrête;

7) sinon, répéter les étapes 3) à 7) en recherchant d'autres concordances après avoir mis la variable RV à l'emplacement précédent. Si aucune des concordances ne donne une comparaison satisfaisante des valeurs de hachage, l'authentification échoue et le message a été altéré (accidentellement ou intentionnellement) au cours du transit.

8 Authentification seulement (procédure IA)

Les terminaux peuvent choisir d'implémenter le mode authentification seulement (utilisant l'OID "B", voir § 20/H.235.2). Dans ce cas, l'authentificateur est calculé uniquement sur un sous-ensemble (**ClearToken** dans **CryptoToken**) du message RAS/H.225.0. Le mode authentification seulement peut être utile pour le franchissement des dispositifs NAT/pare-feu qui modifient les adresses/ports IP dans les charges utiles H.323.

Etant donné que l'authentification ne porte que sur une partie très limitée du message, le mode authentification seulement ne garantit pas l'intégrité du message comme c'est le cas de la procédure I. Ainsi, le mode authentification seulement offre moins de sécurité.

Pour le mode authentification seulement, les champs suivants doivent être utilisés dans les messages protégés:

- Le champ **CryptoH323Token** de chaque message RAS/H.225.0 doit contenir les champs suivants:
  - **nestedCryptoToken** contient le champ **CryptoToken** qui lui-même contient le champ **cryptoHashedToken** avec les champs suivants:
    - **tokenOID** mis à
      - "B" (voir § 20/H.235.2) pour indiquer que l'opération d'authentification seulement inclut tous les champs de **ClearToken**.
    - **hashedVals** contenant le champ **ClearToken** utilisé avec les champs suivants:
      - **tokenOID** mis à
        - "T" (exemple de ClearToken de base pour le reste du contenu de ClearToken) ou tout identificateur OID approprié pour tout autre usage.
      - **timeStamp** contient l'horodate.
      - **random** contient un numéro de séquence croissant monotone. Ce numéro permet de distinguer deux messages portant la même horodate (dans les limites de la résolution de l'horloge).
      - **generalID** contient l'identificateur du destinataire (uniquement dans le cas de messages à destination unique).
      - **sendersID** contient l'identificateur de l'expéditeur.
      - **dhkey** utilisé pour transférer les paramètres Diffie-Hellman comme spécifié dans la Rec. UIT-T H.235.0 pendant l'intervalle **Setup** à **Connect**.
        - **halfkey** contient la clé publique aléatoire de l'un des correspondants;
        - **modsize** contient le nombre premier DH (voir Tableau 4/H.235.6);
        - **generator** contient le groupe DH (voir Tableau 4/H.235.6).

        NOTE 1 – Lorsque le profil de sécurité de base est utilisé sans le profil de sécurité pour le chiffrement vocal, aucun paramètre de Diffie-Hellman ne devrait être envoyé et **dhkey** devrait être absent; **halfkey**, **modsize** et **generator** peuvent être mis à {'0'B,'0'B,'0'B}.
  - **token** contenant **HASHED** avec les champs:
    - **algorithmOID** mis à "U" indiquant l'utilisation de l'algorithme HMAC-SHA1-96;

- **params** mis à NULL;
- **hash** contenant l'authentificateur calculé au moyen de l'algorithme HMAC-SHA1-96. L'authentificateur doit être calculé sur
  - tous les champs de **ClearToken**, si **tokenOID** dans **CryptoHashedToken** est mis à "B" (indiquant le mode authentification seulement).

- L'authentificateur est vérifié à la fin du tronçon terminal du canal (EP1-GK1, GK1-GK2, GK2-EP2, EP1-GK2, GK1-EP2 ou EP1-EP2 selon le cas), et recalculé avant l'envoi du message vers le tronçon suivant.

NOTE 2 – L'authentificateur est uniquement calculé sur le jeton **ClearToken**.

NOTE 3 – On doit utiliser la méthode de bourrage décrite dans la norme SHA1 (ISO/CEI 10118-3).

NOTE 4 – Afin d'empêcher les attaques par réexécution, il est fortement recommandé de veiller, au niveau de l'implémentation, à changer le mot de passe (clé) avant une rotation complète (soit avant la fin du cycle) du numéro de séquence croissant monotone.

NOTE 5 – Le destinataire est en mesure de détecter l'utilisation de la procédure IA en évaluant l'identificateur **OID** "B" dans l'élément **tokenOID**.

L'authentificateur doit être calculé uniquement sur l'élément **ClearToken** dans l'élément **CryptoH323Token** (à savoir **ClearToken**) du jeton **token** de **cryptoHashedToken**. La valeur de hachage cryptographique doit être calculée sur la chaîne binaire codée en ASN.1 de **ClearToken**.

Les points d'extrémité H.235 Version 1 et Version 2 peuvent utiliser la procédure d'authentification seulement, auquel cas il faut utiliser l'identificateur OID "B" correspondant. Les points d'extrémité H.235 Version 1 doivent se conformer à la procédure décrite au § 11.

9 Exemple d'utilisation de la procédure I

Les Figures 1 à 3 montrent la présence de clés partagées à l'extrémité des canaux de communication pour les différentes combinaisons de portier et de canaux H.225.0 à routage direct. Indépendamment du modèle d'appel, une clé secrète est toujours présente entre un point d'extrémité et son portier afin de permettre l'authentification/intégrité du message RAS. Lorsqu'un canal RAS et un canal H.225.0 se terminent entre les deux mêmes nœuds, on peut utiliser la même clé pour assurer l'authentification/intégrité des messages RAS et H.225.0.

La Figure 1 représente le scénario le plus évolutif dans lequel les deux points d'extrémité sont situés dans des zones qui appliquent le modèle à routage par portier. Tous les portiers concernés partagent mutuellement des clés. Dans un souci d'évolutivité, il est recommandé d'utiliser le scénario décrit à la Figure 1.

NOTE 1 – Ce scénario ne permet pas d'assurer une vraie sécurité de bout en bout entre les points d'extrémité; toute la sécurité dépend des portiers intermédiaires de confiance.

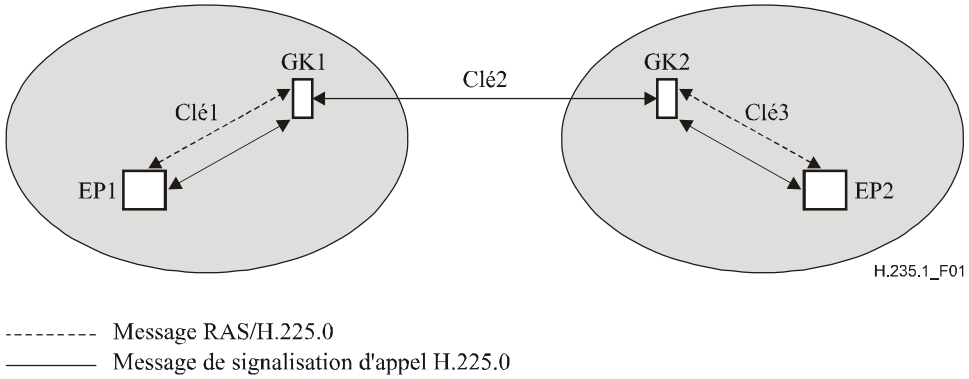

Figure 1/H.235.1 – Exemple d'utilisation de la procédure I dans un scénario portier à portier, les deux points d'extrémité se trouvant dans des zones à routage par portier

La Figure 2 représente un scénario mixte dans lequel un point d'extrémité se trouve dans une zone appliquant le modèle à routage par portier alors que l'autre point d'extrémité se trouve dans une zone appliquant le modèle à routage direct. Ce scénario peut se produire dans des environnements fermés où le nombre de points d'extrémité 2 et de portiers 1 est restreint.

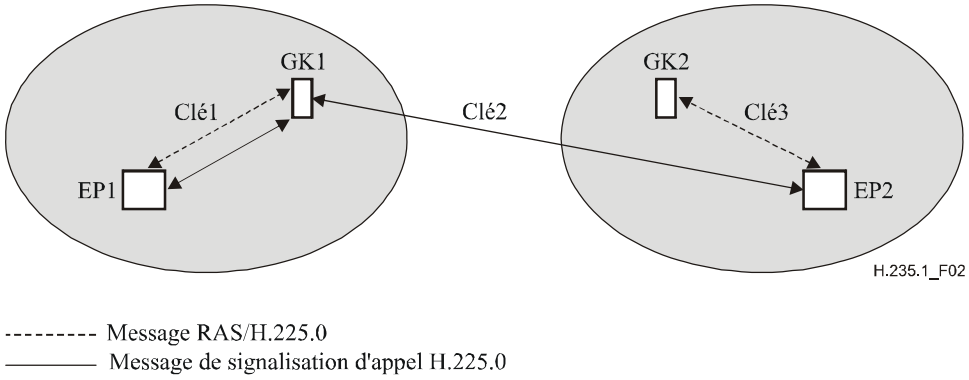

Figure 2/H.235.1 – Exemple d'utilisation de la procédure I dans un scénario mixte avec le point d'extrémité 1 dans une zone à routage par portier et le point d'extrémité 2 dans une zone à routage direct

La Figure 3 représente un scénario dans lequel les deux points d'extrémité se trouvent dans des zones appliquant le modèle à routage direct. Ce scénario n'est pas très évolutif lorsque plusieurs points d'extrémité sont concernés. En principe, on recommande d'utiliser plutôt la Rec. UIT-T H.235.2 avec les procédures II ou III. Pour ce scénario spécifique et les procédures I, II ou III, il faut des mesures de sécurité additionnelles (protection de la fraude et du mauvais usage au moyen d'une autorisation d'appel avec jetons d'accès au niveau des passerelles H.323, par exemple) qui ne sont pas décrites dans la présente Recommandation; un complément d'étude est nécessaire.

NOTE 2 – Ce scénario assure une vraie sécurité de bout en bout entre points d'extrémité sans reposer sur des nœuds intermédiaires de confiance.

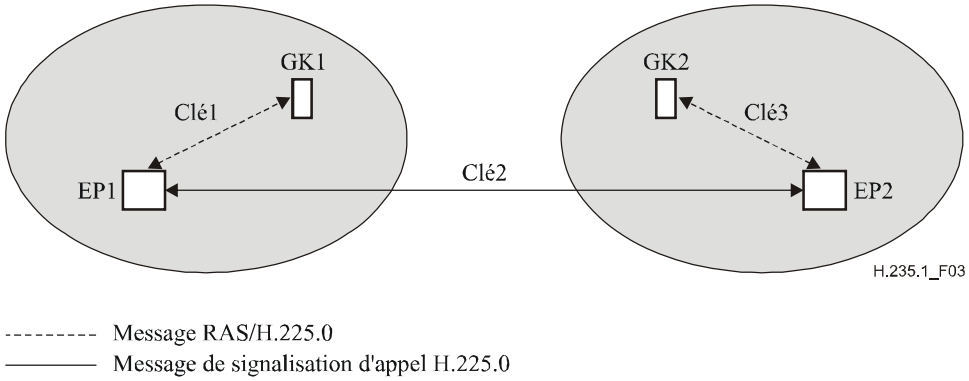

Figure 3/H.235.1 – Exemple d'utilisation de la procédure I pour un scénario dans lequel les deux points d'extrémité sont situés dans des zones à routage direct

Considérons le cas de la Figure 1 dans lequel trois mots de passe sont partagés par paires entre point d'extrémité 1 et portier 1, entre portier 1 et portier 2 et entre portier 2 et point d'extrémité 2. Trois clés de 20 octets – *clé1*, *clé2* et *clé3* – sont produites à partir de ces mots de passe sur la base de la procédure décrite au § 8.2.4/H.235.0. Pour obtenir un maximum de sécurité, il est recommandé de rendre indépendants les trois mots de passe/clés choisis de manière aléatoire.

Les détails des procédures pour l'authentification des messages RAS, H.225.0 et H.245 ainsi que leur intégrité sont présentés ci-après. L'exemple de description illustre les paramètres spécifiques dans un modèle à routage par portier; d'autres combinaisons utiles et valables des identificateurs d'objet dans des scénarios différents sont possibles.

NOTE 3 – Les scénarios présentés sur les Figures 1 à 3 ne sont guère évolutifs lorsque le nombre de clés symétriques (ou mots de passe) utilisés en partage entre les portiers (Figure 1), entre les portiers et les points d'extrémité distants (Figure 2) ou entre les points d'extrémité (Figure 3) est trop élevé.

9.1 Authentification et intégrité des messages RAS

Considérons le cas où le point EP1 souhaite envoyer un message RAS – un message **ARQ**, par exemple – au portier GK1. Le point EP1 produit une horodate et un numéro de séquence et les introduit dans les champs **timeStamp** et **random** respectivement, avec le pseudonyme du portier GK1 dans **generalID** et l'identificateur du point EP dans le champ **sendersID**. Ces champs figurent dans le champ **ClearToken** de **hashedVals**, lui-même faisant partie de **cryptoHashedToken** du champ **CryptoToken** du **cryptoH323Token** du message **ARQ**.

Le champ **tokenOID** de **cryptoHashedToken** est mis à "A", ce qui indique que tous les champs du message **ARQ** sont hachés. Le champ **HASHED** dans **token** de **cryptoHashedToken** a le champ **algorithmOID** mis à "U", ce qui indique l'utilisation de l'algorithme HMAC-SHA1-96 et le champ **params** mis à NULL. Le point EP1 calcule ensuite l'authentificateur sur la base de l'algorithme HMAC-SHA1-96 en utilisant la clé de 20 octets *clé1*. L'authentificateur est calculé sur l'ensemble du message RAS.

Le point EP1 introduit l'authentificateur calculé dans le champ **hash** de **token** du champ **cryptoHashedToken** de **CryptoToken** qui est présent dans le champ **cryptoH323Token** du message **ARQ**. Le message **ARQ** est ensuite envoyé au portier GK1.

Lorsqu'il reçoit le message **ARQ**, le portier GK1 vérifie l'authentificateur sur la base de divers critères, notamment:

- l'actualité de **timeStamp** et l'unicité de **random**;
- l'identité de **generalID** et son propre identificateur;

- la concordance de l'authentificateur du message **ARQ** et de l'authentificateur calculé par le portier GK1.

9.2 Authentification et intégrité des messages H.225.0

Considérons le cas où le point d'extrémité EP1 souhaite envoyer au point d'extrémité EP2 un message H.225.0, un message **Setup** par exemple. Le point EP1 produit une horodate et un numéro de séquence, qu'il introduit respectivement dans les champs **timeStamp** et **random**, avec le pseudonyme du portier GK1 dans **generalID** et l'identificateur du point EP dans le champ **sendersID**. Le point EP1 calcule également une demi-clé Diffie-Hellman et introduit les paramètres Diffie-Hellman **halfkey**, **modsize** et **generator** dans le champ **dhkey** de **ClearToken**. Ces champs se trouvent dans le champ **ClearToken** de **hashedVals**, lui-même se trouvant dans **cryptoHashedToken** du champ **CryptoToken** de **cryptoH323Token** du message **Setup**.

Le champ **tokenOID** de **cryptoHashedToken** est mis à "A" pour indiquer que tous les champs du message de signalisation d'appel H.225.0 sont hachés. Le champ **HASHED** de **token** dans **cryptoHashedToken** a son champ **algorithmOID** mis à "U" pour indiquer l'utilisation de l'algorithme HMAC-SHA1-96 et **params** mis à NULL. Le point EP1 calcule ensuite l'authentificateur sur la base de l'algorithme HMAC-SHA1 au moyen de la clé de 20 octets *clé1*. L'authentificateur est calculé conformément à la méthode de hachage choisie (A) et compte tenu de l'ensemble du message de signalisation d'appel H.225.0.

Le point EP1 introduit l'authentificateur calculé dans **hash** du champ **token** du champ **cryptoHashedToken** de **CryptoToken**, présent dans **cryptoH323Token** du message **Setup**. Le message **Setup** est ensuite envoyé au portier GK1.

Lorsqu'il reçoit le message **Setup**, le portier GK1 vérifie l'authentificateur sur la base de divers critères, notamment:

- l'actualité de **timestamp** et l'unicité de **random**;
- l'identité de **generalID** et son propre identificateur;
- la vérification des paramètres Diffie-Hellman, par exemple vérifier si le nombre premier à 1024 bits et le générateur sont corrects. La vérification des paramètres DH est une opération longue qui n'aura lieu que si la politique locale l'exige;
- la concordance de l'authentificateur du message **Setup** et de l'authentificateur calculé par le portier GK1.

Si la vérification de l'authentificateur est positive, le portier GK1 calcule un nouvel authentificateur qu'il substituera à l'ancien dans le message **Setup** avant de l'envoyer au portier GK2 de la manière qui suit: le portier GK1 remplace les valeurs de **timeStamp**, **random**, **sendersID** et **generalID** du champ **ClearToken** de **hashedVals** par des valeurs qui s'appliquent au tronçon GK1-GK2. Le champ **timestamp** contient l'horodate courante, le champ **random** contient le numéro de séquence croissant monotone du tronçon GK1-GK2, le champ **generalID** contient le pseudonyme du portier GK2 et le champ **sendersID** contient le pseudonyme du portier GK1. Celui-ci introduit également les paramètres Diffie-Hellman reçus, dans le champ **dhkey** de **ClearToken**.

Le portier GK1 calcul ensuite un nouvel authentificateur pour ce message de signalisation d'appel H.225.0 au moyen de la clé *clé2* et de l'algorithme HMAC-SHA1-96 (**algorithmOID**="U"), l'introduit dans le champ **hash** de **token** et transmet le message **Setup** au portier GK2.

Lorsqu'il reçoit le message **Setup**, le portier GK2 vérifie l'authentificateur, calcule un nouvel authentificateur après avoir modifié les champs **ClearToken** de **hashedVals** de manière appropriée, l'introduit dans le champ **hash** et transmet le message **Setup** au point d'extrémité EP2.

9.3 Authentification et intégrité des messages H.245

Considérons le cas où le point EP1 souhaite envoyer un message H.245 – un message **TerminalCapabilitySet** par exemple – au point EP2. Le point EP1 vérifie si un message H.225.0 est en attente d'envoi au portier GK1. Si c'est le cas, le message H.245 est tunnellisé dans ce message H.225.0. Les champs contenus dans le message H.225.0 ont les valeurs indiquées précédemment pour la transmission d'un message H.225.0. Etant donné que le message H.245 est tunnellisé, les champs de **h323-uu-pdu** du message **h323-UserInformation** prennent les valeurs suivantes:

- **h323-message-body** est mis au type de message H.225.0 en cours de transmission;
- **h245Tunnelling** est mis à TRUE;
- **h245Control** contient la chaîne d'octets PDU H.245.

Le point EP1 produit un **CryptoToken** pour le message H.225.0, met **tokenOID** à "A" pour indiquer l'authentification et l'intégrité, met **timeStamp**, **random**, **sendersID**, **generalID** et **tokenOID** à "T" dans **ClearToken** de **hashedVals**, met **algorithmOID** à "U" pour indiquer l'utilisation de l'algorithme HMAC-SHA1-96 et **hash** à l'authentificateur de hachage calculé sur l'ensemble des champs du message de signalisation d'appel H.225.0.

Toutefois, si aucun message H.225.0 n'est en attente d'envoi, le message H.245 sera tunnellisé dans un message **facility** H.225.0 ad hoc. Les champs de **h323-uu-pdu** du message **h323-UserInformation** contiennent les valeurs suivantes:

- **h323-message-body** est mis à **facility** qui contient:
  - **reason** mis à **undefinedReason**;
  - **tokens** et **cryptoTokens** comme pour n'importe quel message H.225.0;
- **h245Tunnelling** est mis à TRUE;
- **h245Control** contient la chaîne d'octets PDU H.245.

Comme indiqué ci-dessus, le point EP1 produit un **CryptoToken** dans le cadre du message **facility** H.225.0. Le message **facility** est ensuite transmis par le point EP1 au portier GK1.

Dans les deux cas (message H.225.0 en attente d'envoi ou utilisation d'un message **facility** H.225.0 ad hoc), le portier GK1 vérifie l'authentificateur à la réception du message. Ensuite, si un message H.225.0 est en attente d'envoi pour le tronçon GK1-GK2, le message H.245 est tunnellisé dans ce message; sinon, il est tunnellisé dans un message **facility** H.225.0 ad hoc. Comme pour toutes les transmissions de message H.225.0, un nouvel authentificateur est calculé pour le message en question avant sa transmission du portier GK1 au portier GK2. Le processus se répète pour le tronçon GK2-EP2.

9.4 Scénario de routage direct

Les entités H.323 sécurisées peuvent communiquer non seulement dans le contexte de routage par portier comme indiqué dans la présente Recommandation mais peuvent également appliquer le modèle à routage direct. Celui-ci nécessite des mesures de sécurité additionnelles (jetons d'accès) qui ne sont pas nécessaires dans les environnements plus simples à routage par portier. La Rec. UIT-T H.235.4 décrit comment sécuriser le modèle à routage direct.

10 Prise en charge de services d'arrière

Les entités H.323 sécurisées peuvent utiliser des services d'arrière conformément à la procédure décrite au § I.1.6/H.235.0.

11 Compatibilité avec le contexte H.235 Version 1

Bien que ces profils de sécurité soient mis au point dans le contexte H.235 Version 2 (Rec. UIT-T H.235 (2000)), il est possible de les appliquer dans un contexte H.235 Version 1 (Rec. UIT-T H.235 (1998)) moyennant quelques modifications mineures. Un destinataire est en mesure de détecter la présence de la version du protocole H.235 de l'expéditeur en évaluant les identificateurs d'objet du profil de sécurité (voir § 15).

Implémentations H.235 Version 1 (Rec. UIT-T H.235 (1998)):

- ne pas attribuer de valeur à ou ne pas évaluer **sendersID** de **ClearToken**;
- ne pas utiliser de services d'arrière comme indiqué au § 10.

12 Comportement pour les messages multidestinataires

Les messages multidestinataires H.225.0 tels que les messages GRQ ou LRQ ne doivent pas comporter le CryptoToken requis par la procédure I, sauf lorsqu'ils sont envoyés à un seul destinataire.

13 Liste des messages de signalisation sécurisés

Le présent paragraphe récapitule les modalités et les moyens décrits dans la présente Recommandation pour sécuriser les divers messages de signalisation H.323.

13.1 Messages RAS H.225.0

Message RAS H.225.0	Champs de signalisation H.235	Authentification et intégrité
Tous	cryptoTokens	Procédure I

13.2 Messages de signalisation d'appel H.225.0

Message de signalisation d'appel H.225.0	Champs de signalisation H.235	Authentification et intégrité
Alerting-UUIE, CallProceeding-UUIE, Connect-UUIE, Setup-UUIE, Facility-UUIE, Progress-UUIE, Information-UUIE, ReleaseComplete-UUIE, Status-UUIE, StatusInquiry-UUIE, SetupAcknowledge-UUIE, Notify-UUIE	cryptoTokens	Procédure I

13.3 Messages de commande d'appel H.245

Les messages H.245 en provenance ou à destination d'entités H.323 sécurisées doivent être portés dans un autre message dans le cadre de la connexion rapide sécurisée ou doivent être tunnellisés dans un message **Facility-UUIE** H.225.0 sécurisé.

14 Utilisation des identificateurs sendersID et generalID

Le paramètre **ClearToken** contient les champs **sendersID** et **generalID**. Lorsque les informations d'identification sont disponibles, le champ **sendersID** doit contenir l'identificateur du portier (GKID, *gatekeeper identifier*) pour les messages provenant du portier et l'identificateur du point d'extrémité (EPID, *endpoint identifier*) pour les messages provenant du point d'extrémité. Lorsque les informations d'identification sont disponibles, le champ **generalID** doit contenir l'identificateur du portier (GKID) pour les messages provenant du point d'extrémité et l'identificateur du point

d'extrémité (EPID) pour les messages provenant du portier. Lorsque les informations d'identification ne sont pas disponibles ou lorsque la diffusion générale multidiffusion est ambiguë, le champ est absent ou contient une chaîne néant. Le Tableau 2 résume la situation.

Tableau 2/H.235.1 – Utilisation des identificateurs sendersID et generalID

Message	sendersID	generalID
GRQ envoyé à un seul destinataire	**EPID** si disponible, autrement **NULL**	**GKID**
GRQ envoyé à plusieurs destinataires	**EPID** si disponible, autrement **NULL**	
GCF, **GRJ**	**GKID**	**EPID** si disponible, autrement **NULL**
RRQ initial	**EPID** si disponible, autrement **NULL**	**GKID**
RCF	**GKID**	**EPID**
RRJ	**GKID**	
URQ, UCF, URJ, BRQ, BCF, BRJ, DRQ, DCF, DRJ, NSM, RIP, SCI, SCR, XRS (EP vers GK)	**EPID**	**GKID**
URQ, UCF, URJ, BRQ, BCF, BRJ, DRQ, DCF, DRJ, NSM, RIP, SCI, SCR, XRS (GK vers EP)	**GKID**	**EPID**
ARQ, IRQ, RAI	**EPID**	**GKID**
ACF, ARJ, BCF, LCF, LRJ, IRR, IRQ, RAC, LCF, LRJ, IACK, INAK	**GKID**	**EPID**
LRQ envoyé à un seul destinataire (EP vers GK)	**EPID**	**GKID**
LRQ envoyé à un seul destinataire (GK vers GK)	**GKID**	**GKID**
LRQ envoyé à plusieurs destinataires	**EPID**	
NOTE – GKID désigne l'identificateur du portier, EPID désigne l'identificateur du point d'extrémité. L'espace vide indique une chaîne d'identification manquante ou nulle.		

15 Liste des identificateurs d'objet

Le Tableau 3 ci-dessous énumère tous les identificateurs OID mentionnés (voir également [OIW] et [WEBOIDS]). Il y a des identificateurs d'objet pour H.235v1 et pour H.235v2.

Tableau 3/H.235.1 – Identificateurs d'objet

Désignation de l'identificateur d'objet	Valeur(s) de l'identificateur d'objet	Description
"A"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 1} {itu-t (0) recommendation (0) h (8) 235 version (0) 1 1}	Utilisé dans la procédure I pour l'identificateur CryptoToken-tokenOID, indiquant que le hachage englobe tous les champs du message RAS ou du message de signalisation d'appel H.225.0 (authentification et intégrité)
"E"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 9} {itu-t (0) recommendation (0) h (8) 235 version (0) 2 9}	ClearToken de bout en bout acheminant l'identificateur sendersID pour vérification du côté destinataire
"T"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 5} {itu-t (0) recommendation (0) h (8) 235 version (0) 1 5}	Utilisé dans les procédures I et IA comme ClearToken de base pour l'authentification de message et la protection contre les attaques par réexécution et optionnellement pour la gestion de clés Diffie-Hellman décrite au § 8.5/H.235.6
"U"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 6} {itu-t (0) recommendation (0) h (8) 235 version (0) 1 6}	Utilisé dans la procédure I pour l'identificateur algorithm OID, indiquant l'utilisation de l'algorithme HMAC-SHAI-96

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	**Systèmes audiovisuels et multimédias**
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	Réseaux de données, communication entre systèmes ouverts et sécurité
Série Y	Infrastructure mondiale de l'information, protocole Internet et réseaux de prochaine génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2006