Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

H.235.3

(09/2005)

SÉRIE H: SYSTÈMES AUDIOVISUELS ET MULTIMÉDIAS

Infrastructure des services audiovisuels – Aspects système

Cadre de sécurité H.323: profil de sécurité hybride

Recommandation UIT-T H.235.3

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.235.3

Cadre de sécurité H.323: profil de sécurité hybride

Résumé

La présente Recommandation a pour objet de décrire un profil de sécurité hybride, efficace et adaptable, fondé sur l'infrastructure à clé publique PKI, pour la version 2 de la Rec. UIT-T H.235.0 ou pour une version supérieure. Le profil présenté ici tire parti des profils de sécurité décrits dans les Recommandations UIT-T H.235.1 et H.235.2 par la mise en œuvre des signatures numériques H.235.2 et du profil de sécurité de base de la Rec. UIT-T H.235.1.

Dans les anciennes versions de la sous-série H.235, ce profil était défini dans l'Annexe F/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.235.3 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 avait 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.235.3

Cadre de sécurité H.323: profil de sécurité hybride

1 Domaine d'application

La présente Recommandation a pour objet de décrire un profil de sécurité hybride, efficace et adaptable, fondé sur l'infrastructure à clé publique PKI, pour la version 2 de la Rec. UIT-T H.235.0 ou pour une version supérieure. Le profil présenté ici tire parti des profils de sécurité décrits dans les Recommandations UIT-T H.235.1 et H.235.2 par la mise en œuvre des signatures numériques H.235.2 et du profil de sécurité de base H.235.1.

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.235.1 (2005), *Cadre de sécurité H.323: profil de sécurité de base*.

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

– 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 (2005), *Protocole de commande pour communications multimédias*.

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

– 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.509 (2005) | ISO/CEI 9594-8:2005, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre général des certificats de clé publique et d'attribut*.

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

  ISO 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*.

– IETF RFC 3280 (2002), *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.

2.2 Références informatives

[ISO | CEI 14888-3] ISO/CEI 14888-3:1998, *Technologies de l'information – Techniques de sécurité – Signatures digitales avec appendice – Partie 3: Mécanismes fondés sur certificat*.

[PKCS] PKCS #1 v2.0: *RSA Cryptography Standard;* RSA Laboratories; 1er octobre 1998; http://www.rsa.com/rsalabs/pubs/PKCS/index.html.

[PKCS] PKCS #7: *Cryptographic Message Syntax Standard*, An RSA Laboratories Technical Note, version 1.5, Revised 1er novembre 1993; http://www.rsa.com/rsalabs/pubs/PKCS/index.html.

[RFC1321] IETF RFC 1321 (1992), *The MD5 Message-Digest Algorithm*.

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 la Rec. UIT-T X.800 | ISO 7498-2, X.803 | ISO/CEI 10745, X.810 | ISO/CEI 10181-1, X.811 | ISO/CEI 10181-2 et H.235.0.

4 Symboles et abréviations

La présente Recommandation utilise les abréviations suivantes:

ALG passerelle au niveau application (*application level gateway*)

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

BRJ rejet de largeur de bande (*bandwidth reject*)

BRQ demande de largeur de bande (*bandwidth request*)

CA autorité de certification (*certification authority*)

CRL liste de révocation de certificats (*certificate revocation list*)

DB base de données (*database*)

DH Diffie-Hellman

DN nom distinctif (*distinguished name*)

EP point d'extrémité (*endpoint*)

GCF confirmation de portier (*gatekeeper confirm*)

GK portier (*gatekeeper*)

GKID identificateur de portier (*gatekeeper identifier*)

GKSP processeur de sécurité de portier (*gatekeeper security processor*)

GRJ rejet de portier (*gatekeeper reject*)

GRQ demande de portier (*gatekeeper request*)

HMAC code d'authentification de message "d'après les signaux parasites" (*hashed message authentication code*)

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

ID identificateur

IP protocole Internet (*Internet protocol*)

LDAP protocole rapide d'accès à l'annuaire (*lightweight directory access protocol*)

LRQ demande de localisation (*location request*)

MCU unité de commande multidiffusion, pont de conférence (*multipoint control unit*)

MD5 résumé de message numéro 5 (*message digest 5*)

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

OID identificateur d'objet (*object identifier*)

PDU unité de données protocolaire (*protocol data unit*)

PKI infrastructure à clé publique (*public key infrastructure*)

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

RCF confirmation d'enregistrement (*registration confirm*)

RRJ rejet d'enregistrement (*registration reject*)

RRQ demande d'enregistrement (*registration request*)

RSA algorithme à clé publique de Rivest, Shamir et Adleman (*Rivest, Shamir and Adleman encryption algorithm*)

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

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

UDP protocole datagramme d'utilisateur (*user datagram protocol*)

URQ demande de désenregistrement (*unregistration request*)

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 description du profil de sécurité hybride utilise les termes et définitions des Recommandations UIT-T H.235.1 et H.235.2.

Si le service d'intégrité des messages fournit toujours l'authentification des messages, l'inverse n'est pas toujours vrai. En mode d'authentification seulement, l'intégrité assurée porte uniquement sur un sous-ensemble donné de champs de message. Cela s'applique aux services d'intégrité assurés par des moyens asymétriques (par exemple des signatures numériques). Donc, en pratique, le double service d'authentification et d'intégrité exploite les mêmes données de clé sans introduire de faiblesse au niveau de la sécurité.

Ce profil de sécurité est applicable dans les environnements pouvant comporter de nombreux terminaux, dans lesquels l'attribution d'un mot de passe statique ou d'une clé symétrique n'est pas possible, par exemple les scénarios à grande échelle, voire à l'échelle mondiale. Il repose sur la disponibilité d'une infrastructure à clé publique avec des certificats attribués et des clés privées ou publiques, des répertoires, etc. Par ailleurs, ce profil de sécurité utilise, dans la mesure du possible, les techniques cryptographiques symétriques.

Pour ce profil de sécurité, on introduit les termes de "premier message" et "dernier message" envoyés. La protection de sécurité du premier message (et probablement aussi du dernier) est différente de celle des autres messages.

Le "premier message" envoyé est considéré comme un message qui circule entre deux entités H.323 et qui établit un contexte de sécurité. Il met à la disposition de ces deux entités les données de clé symétrique et marque par exemple le début d'un appel. Dans le cas des messages RAS H.225.0, le premier message correspond au message RRQ et au message de réponse correspondant. Dans le cas de la signalisation d'appel H.225.0 utilisant le démarrage rapide, le premier message correspond aux messages SETUP et CONNECT.

Le "dernier message" met fin au contexte de sécurité qui a été établi. Les données de clé qui ont été établies sont détruites. Dans le cas des messages RAS H.225.0, le dernier message correspond au message URQ et au message de réponse correspondant, alors que pour la signalisation d'appel H.225.0, le dernier message correspond à RELEASE-COMPLETE.

6 Aperçu général

La présente Recommandation décrit un profil de sécurité hybride, efficace et adaptable, fondé sur l'infrastructure à clé publique (PKI), utilisant les signatures numériques de la Rec. UIT-T H.235.2 et le profil de sécurité de base de la Rec. UIT-T H.235.1. La présente Recommandation est proposée à titre d'option. Les entités de sécurité H.323 (terminaux, portiers, passerelles, ponts MCU, etc.) peuvent implémenter ce profil de sécurité hybride pour améliorer la sécurité ou chaque fois que c'est nécessaire.

Dans le présent contexte, "hybride" signifie que les procédures de sécurité du profil avec signature de la Rec. UIT-T H.235.2 sont en fait appliquées avec une certaine souplesse et que les signatures numériques restent conformes aux procédures RSA. Les signatures numériques ne sont cependant utilisées qu'en cas de nécessité absolue; en conditions normales, ce sont les techniques de sécurité symétriques hautement efficaces du profil de sécurité de base de la Rec. UIT-T H.235.1 qui sont employées.

Ce profil de sécurité hybride est applicable à la téléphonie IP "mondiale" évolutive; il n'est pas exposé aux limitations du profil de sécurité de base, simple, de la Rec. UIT-T H.235.1, lorsqu'il est appliqué de manière stricte. De plus, il n'est pas exposé à certains inconvénients du profil de la Rec. UIT-T H.235.2, tels qu'un plus grand besoin de largeur de bande et de performance, lorsqu'il est appliqué de manière stricte. Par exemple, le profil de sécurité hybride ne dépend pas de l'administration (statique) de secrets mutuellement partagés pour les bonds dans des domaines différents. Les utilisateurs peuvent donc très facilement choisir leur fournisseur de téléphonie IP.

Par conséquent, ce profil de sécurité accepte aussi une certaine mobilité de l'utilisateur. Par ailleurs, il n'applique la cryptographie asymétrique avec signatures et certificats qu'en cas de nécessité, se limitant dans les autres cas aux techniques symétriques, plus simples et plus efficaces. Il assure la tunnellisation des messages H.245 pour l'intégrité de ceux-ci. Il implémente également certaines dispositions pour la non-répudiation des messages.

Ce profil de sécurité hybride, pour lequel le modèle à routage par portier est obligatoire, est fondé sur les techniques de tunnellisation H.245. La prise en charge de modèles autres que le modèle à routage par portier nécessite un complément d'étude.

Les fonctionnalités offertes par ce profil sont les suivantes:

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

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

  NOTE 1 – Par "bond", on entend dans le cas présent un élément de réseau H.235 de confiance (tel que portier, passerelle, pont MCU, proxy ou pare-feu). En conséquence, la sécurité bond par bond au niveau applicatif, lorsqu'elle est utilisée avec des techniques symétriques, n'assure pas une sécurité vraie de bout en bout entre les terminaux;

– l'intégrité de tous les champs ou des champs critiques d'un message arrivant à une entité, indépendamment du nombre de bonds au niveau applicatif franchis par le message. L'intégrité du message assurée au moyen d'un nombre aléatoire fort est proposée en option;

– l'authentification, l'intégrité et la non-répudiation (dans une certaine mesure) d'un message bond par bond au niveau applicatif couvrent la totalité du message;

– grâce à l'infrastructure à clé publique, les utilisateurs peuvent choisir le fournisseur du service. La gestion des clés pour la distribution des clés de session est judicieusement intégrée dans le profil de sécurité hybride.

Les services de sécurité décrits ci-dessus permettent de combattre de façon satisfaisante diverses attaques telles que les suivantes:

– *attaques par intercepteur*: l'authentification et l'intégrité des messages bond par bond au niveau applicatif protègent contre de telles attaques lorsque l'intercepteur, un routeur hostile par exemple, se trouve entre deux bonds au niveau applicatif;

– *attaques par réexécution*: l'emploi d'horodates et de numéros de séquence protège contre de telles attaques;

– *mystifications*: l'authentification de l'utilisateur protège contre de telles attaques;

– *détournement de connexions*: l'utilisation de l'authentification/intégrité pour chaque message de signalisation empêche de telles attaques.

Ce profil de sécurité repose sur le modèle d'appel à routage par portier, dans lequel est appliquée la méthode de signalisation d'appel à connexion rapide. Les messages de commande d'appel H.245 sont tunnellisés en toute sécurité dans des messages de signalisation d'appel H.225.0 et bénéficient en conséquence du système de protection de sécurité H.225.0.

Le profil de sécurité avec signature permet de tunnelliser en toute sécurité les unités PDU de commande d'appel H.245 dans des messages facility H.225.0. Les mécanismes de mise à jour et de synchronisation des clés H.245, qui sont par exemple utiles pour les très longues communications, nécessitent une tunnellisation pour pouvoir signaler le message FACILITY de mise à jour de clé.

La zone hachurée en diagonale du Tableau 1 représente les mécanismes de sécurité qui sont utilisés par le profil de sécurité hybride.

NOTE 2 – Les certificats RSA avec hachage MD5 ([RFC 1321]) ne font pas partie de ce profil de sécurité.

Le profil de sécurité pour le chiffrement vocal de la Rec. UIT-T H.235.6 (voir § 6.1/H.235.6) peut facultativement être utilisé en association avec le profil de sécurité hybride. Son utilisation est négociée dans le contexte de la signalisation d'établissement de l'appel.

Tableau 1/H.235.3 – Aperçu général du profil de sécurité hybride

Services de sécurité	Fonctions d'appel			
	RAS	**H.225.0**	**H.245 (Note 3)**	**RTP**
Authentification	Signature numérique RSA (SHA1) HMAC-SHA1-96	Signature numérique RSA (SHA1) HMAC-SHA1-96	Signature numérique RSA (SHA1) HMAC-SHA1-96	
Non-répudiation	(Possible sur premier message seulement)	(Possible sur premier message seulement)		
Intégrité	Signature numérique RSA (SHA1) HMAC-SHA1-96	Signature numérique RSA (SHA1) HMAC-SHA1-96	Signature numérique RSA (SHA1) HMAC-SHA1-96	
Confidentialité				
Commande d'accès				
Gestion de clés	attribution d'un certificat Echange de clés Diffie-Hellmann authentifiées	attribution d'un certificat Echange de clés Diffie-Hellmann authentifiées		

NOTE 1 – Le profil de sécurité hybride doit également être pris en charge par d'autres entités H.235 (telles que les portiers, les passerelles et les proxys H.235).

NOTE 2 – Les bits d'utilisation de clé disponible dans le certificat peuvent également déterminer le service de sécurité assuré par un terminal (par exemple, la non-répudiation déclarée par assertion).

NOTE 3 – Message H.245 tunnellisé ou message H.245 imbriqué dans le cadre de la connexion rapide H.225.0.

La présente Recommandation permet d'assurer une protection de l'intégrité couvrant la totalité de chaque 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.

Pour l'authentification, l'utilisateur devrait utiliser un système de signature à clé publique ou privée. Un tel système offre généralement une meilleure intégrité.

La présente Recommandation ne définit pas de procédures pour l'enregistrement, la certification et l'attribution d'un certificat depuis un centre de confiance, ni pour l'attribution de clés privées ou publiques, pour les services d'annuaire, les paramètres CA spécifiques, la révocation de certificats, la mise à jour ou la récupération de paires de clés. Elle ne définit pas non plus d'autres procédures d'exploitation ou de gestion des certificats, par exemple la remise de certificats ou de clés publiques/privées et de certificats ainsi que l'installation dans les terminaux. De telles procédures peuvent être exécutées par des moyens qui ne font pas partie de la présente Recommandation.

Les entités de communication concernées ont la capacité de déterminer implicitement l'utilisation du profil de sécurité de base H.235.1, du profil avec signature H.235.2 ou de ce profil de sécurité hybride en évaluant les identificateurs d'objet de sécurité signalés dans les messages (**tokenOID** et **algorithmOID**; voir également § 10/H.235.2).

6.1 Prescriptions H.323

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

– la connexion rapide;

– la tunnellisation H.245;

– le modèle à routage par portier.

6.2 Authentification et intégrité

La présente Recommandation utilise les termes suivants dans le contexte de la fourniture de services de sécurité.

Authentification et intégrité: double service de sécurité prenant en charge l'intégrité de message en plus de l'authentification de l'utilisateur. L'utilisateur s'authentifie par la signature numérique correcte de données au moyen de la clé privée ou par l'application correcte d'un secret partagé correspondant. En outre, le message est protégé contre les altérations. Les deux services de sécurité sont fournis par le même mécanisme de sécurité. L'authentification et l'intégrité combinées ne sont possibles que dans le cas bond par bond.

NOTE – L'utilisation de signatures numériques permet de prendre en charge un service de sécurité de non-répudiation; cela dépend aussi de la valeur des bits d'utilisation de la clé de signature dans le certificat (voir également RFC 3280).

Les procédures destinées à être utilisées dans ce profil sont les suivantes.

La procédure IV est fondée sur des signatures numériques au moyen d'une paire de clés privée/publique et de techniques cryptographiques symétriques pour assurer l'authentification et l'intégrité des messages RAS, Q.931 et H.245. Les terminaux peuvent utiliser cette méthode si une sécurité efficace et adaptable est requise.

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 mode préféré est celui de l'authentification bilatérale.

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 reçu d'un terminal 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 la capacité à reconnaître des attaques et de la manière 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**) devrait répondre par un message **xRJ** non sécurisé avec le motif de rejet **securityDenial** ou peut ignorer ce message. 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 de signalisation d'appel H.225.0 sécurisé contenant des identificateurs d'objet non définis (**tokenOID**, **algorithmOID**) devrait répondre par un message RELEASE COMPLETE non sécurisé avec le motif de rejet **securityDenied** ou peut ignorer ce message, tandis qu'un portier qui reçoit un message FACILITY H.225.0 sécurisé contenant des identificateurs d'objet non définis (**tokenOID**, **algorithmOID**) devrait répondre par un message FACILITY non sécurisé avec le motif **undefinedReason** ou peut ignorer ce message. De manière analogue, l'événement de sécurité rencontré devrait être journalisé. Dans sa réponse, l'expéditeur peut donner une liste de certificats acceptables dans des jetons distincts afin de faciliter le choix de l'un d'eux par le destinataire.

Une signalisation H.235 implicite permet d'indiquer l'utilisation de la procédure IV et du mécanisme de sécurité appliqué, sur la base de la valeur des identificateurs d'objet (voir

également § 13) et du contenu des champs de message. Les identificateurs d'objet sont désignés symboliquement par des lettres (par exemple "A") dans la présente Recommandation.

Ce profil n'utilise pas les champs ICV H.235; en effet, les valeurs de contrôle d'intégrité cryptographique sont placées dans le champ **signature** du jeton **token** du **cryptoSignedToken**, lorsque le profil renvoie à la Rec. UIT-T H.235.2, ou bien les valeurs de contrôle d'intégrité sont placées dans les champs de hachage de **CryptoToken** lorsque le profil renvoie à la Rec. UIT-T H.235.1.

7 Procédure IV

Si on utilise la procédure IV pour la sécurité bond par bond, il est nécessaire de se conformer aux dispositions ci-après. Cette procédure réunit la procédure I du § 7/H.235.1 et la procédure II du § 7/H.235.2.

Pour le premier message, comportant la réponse correspondante, envoyé dans chaque sens, on utilise la procédure II/H.235.2 (authentification et intégrité bond par bond, voir § 7/H.235.2) avec les valeurs suivantes:

– l'identificateur OID "A1" au lieu de "A" et l'identificateur OID "S1" au lieu de "S". L'emploi de ces identificateurs OID permet d'identifier le profil de sécurité hybride;
– l'identificateur **algorithmOID** de **tokenOID** est mis à "W" pour indiquer l'utilisation de la signature RSA-SHA1;
– le champ **signature** contient une signature RSA codée en ASN.1 (voir § 12/H.235.2);
– le champ **certificate** devrait contenir le certificat d'utilisateur de l'expéditeur s'il n'est pas autrement accessible par le destinataire; le champ **type** contient l'identificateur OID "W" pour indiquer qu'un certificat RSA-SHA1 est contenu ou l'identificateur OID "P" (voir § 20/H.235.2) pour indiquer que le champ **certificate** contient une adresse URL.

Dans un scénario à un seul domaine administratif, le "premier message/réponse" est défini comme étant le message/réponse RAS H.225.0 initial; il correspond généralement aux messages GRQ/GCF ou RRQ/RCF. Dans un scénario à plusieurs domaines administratifs, le premier message/réponse à l'intérieur de chaque domaine est défini comme indiqué ci-dessus; le premier message entre domaines est défini comme étant le message SETUP.

Lorsqu'un certificat numérique est acheminé dans un message, l'entité le recevant compare l'identité de l'expéditeur avec l'identité du certificat conformément à la procédure du § 14/H.235.2, afin d'éviter les attaques par intercepteur.

L'expéditeur et le destinataire échangent et calculent une chaîne binaire secrète de Diffie-Hellman authentifiée. Le Tableau 4/H.235.6 donne un exemple de paramètres de groupe de Diffie-Hellman et recommande de choisir si possible, pour des raisons de sécurité, le nombre premier à 1024 bits. Le secret Diffie-Hellman est calculé pour chaque tronçon, indépendamment de l'utilisation ou non du profil pour le chiffrement vocal.

A partir de la chaîne binaire commune qu'elles calculent, les deux parties déduisent un secret de 160 bits en prenant les 160 bits les moins significatifs. Ce secret sert de mot de passe/secret partagé utilisé dans la Rec. UIT-T H.235.1.

Dans un scénario où les portiers se trouvent dans des domaines administratifs distincts, l'expéditeur et le destinataire utilisent deux jetons dans chaque sens pour la signalisation d'appel H.225.0:

– un jeton **ClearToken** dans le **CryptoToken,** utilisé pour calculer la clé de média qui est partagée entre les terminaux (voir § 8.5/H.235.6). Cela est uniquement nécessaire en cas d'utilisation du chiffrement vocal;

– un jeton **ClearToken** distinct est utilisé pour calculer une clé de liaison qui est partagée entre l'expéditeur et le destinataire pour la protection de la liaison de signalisation. Cette clé de liaison remplace le mot de passe partagé entre les portiers dans la Rec. UIT-T H.235.1. L'identificateur **tokenOID** de ce **ClearToken** est mis à "Q" pour indiquer l'utilisation d'un échange Diffie-Hellman et du profil de sécurité hybride. Le calcul de la clé de liaison se déroule de la même manière que celui de la clé de média (voir § 8.5/H.235.6).

NOTE 1 – Dans les environnements à routage direct, les entités et terminaux expéditeur/destinataire correspondent. Dans les environnements à routage par portier, la clé de liaison est partagée bond par bond par chaque paire de portiers homologues alors que la clé de média est partagée de bout en bout.

Dans les environnements à routage par portier, celui-ci renvoie au bond suivant le jeton de Diffie-Hellman reçu du point d'extrémité.

Pour tous les messages/réponses envoyés dans chaque sens, sauf le premier, c'est la procédure I/H.235.1 (voir § 7/H.235.1) qui est utilisée. Cela s'applique également dans un scénario dans lequel plusieurs portiers se trouvent dans un même domaine administratif. Dans ce cas, la gestion de clé asymétriques n'est pas requise, les moyens de la Rec. UIT-T H.235.1 étant suffisants.

La présente Recommandation peut être utilisée avec des systèmes H.235 version 1 si l'on tient compte de l'utilisation restreinte des identificateurs senders ID et generalID, comme indiqué dans le § 19/H.235.2.

Il est prévu qu'un portier ne devrait recevoir qu'un seul message **RRQ**, comprenant un jeton DH avec une signature numérique en provenance d'un point d'extrémité fixe particulier. Toutefois, les messages **RCF/RRJ** perdus ou retardés peuvent conduire à la retransmission d'un autre message **RRQ** signé.

Si une réponse d'enregistrement correspondante n'arrive pas en temps voulu au point d'extrémité, celui-ci peut tenter un nouvel essai. A cette fin, il emploie le jeton DH le plus récent, mais emploie un nouveau numéro de séquence et une nouvelle horodate.

Pour un point d'extrémité fixe particulier, le portier emploie le message **RRQ** signé reçu le plus récent et déduit le secret partagé à partir de ce jeton DH, même s'il dispose déjà d'un secret partagé. Donc, il annule tout secret partagé existant et le remplace par le secret nouvellement déduit. Il répond par un message **RCF** signé qui contient le jeton DH de réponse. Il est préférable que ce jeton DH de réponse soit de nouveau produit.

NOTE 2 – La méthode recommandée et préférée pour la mise à jour des clés est celle qui emploie le message FACILITY tel qu'il est défini dans le § 9. Toutefois, il est admis que la mise à jour des clés peut se faire en employant un autre message RRQ signé supplémentaire avec un nouveau jeton DH.

NOTE 3 – Un portier en possession d'un secret partagé répond à un message **RRQ** protégé HMAC (conformément à la Rec. UIT-T H.235.1) par un message de réponse protégé HMAC.

8 Association de sécurité pour appels simultanés

Une optimisation a été prévue pour les cas dans lesquels une paire fixe d'entités traiterait plusieurs appels indépendants en parallèle au moyen d'une seule voie de signalisation d'appel. Au lieu d'établir plusieurs clés de liaison avec l'échange de Diffie-Hellman pour chaque appel, on a défini une association de sécurité qui s'applique à plusieurs appels simultanés.

Plus précisément, l'association de sécurité couvre tous les appels entre deux entités fixes tant que la voie de signalisation d'appel existe. Les entités utilisent le fanion **multipleCalls** dans le message Setup pour indiquer la capacité de signalisation d'appels multiples sur une seule connexion de signalisation d'appel (voir § 7.3/H.323).

Si l'on utilise une seule connexion de signalisation d'appel, il ne faut établir qu'une seule clé de liaison commune (voir Figure 1).

Par ailleurs, si le fanion **multipleCalls** du message SETUP est mis à zéro, une clé de liaison est calculée individuellement pour chaque nouvel appel.

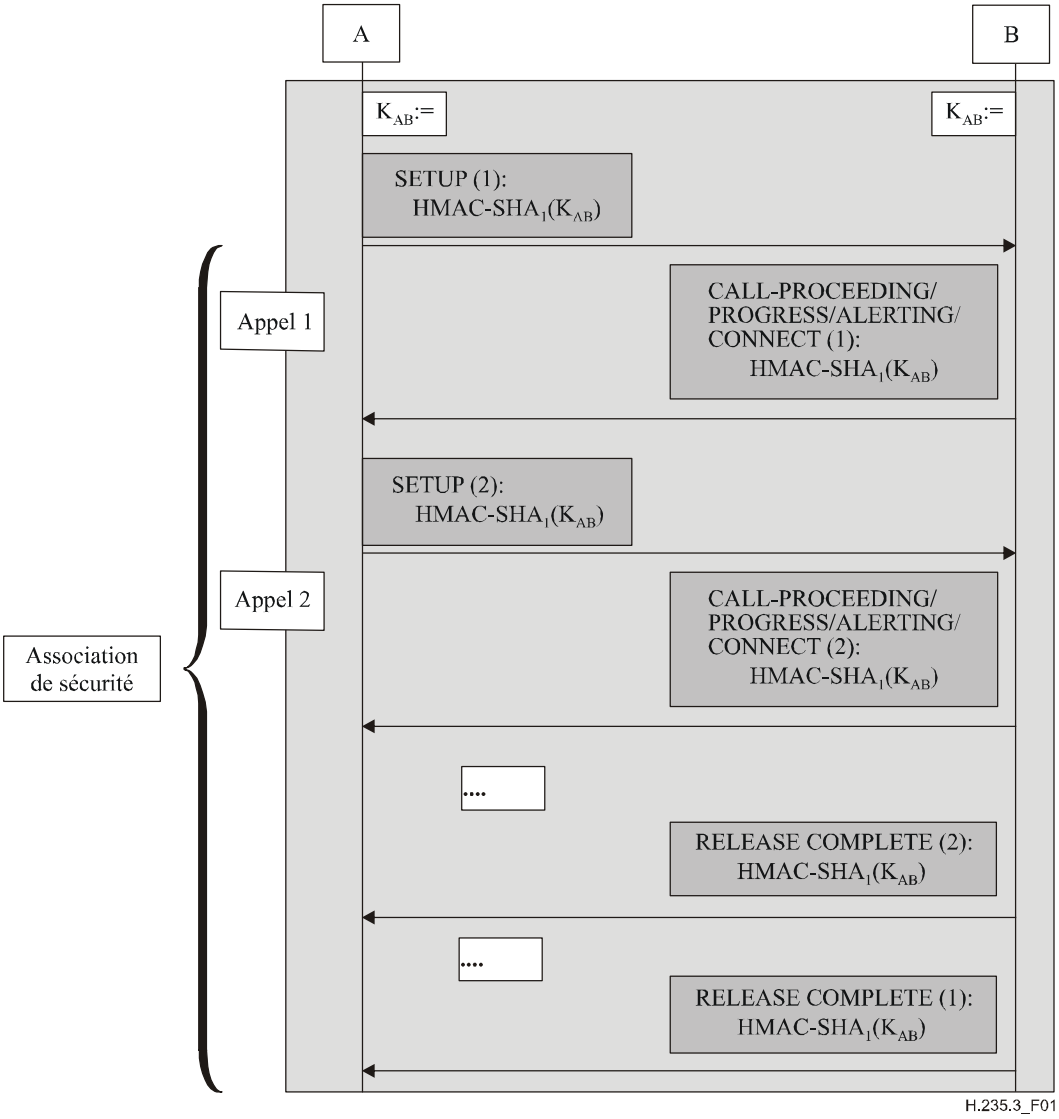


Figure 1/H.235.3 – Association de sécurité pour appels simultanés

9 Mise à jour de la clé

Une procédure facultative de mise à jour de la clé permet à chacune des entités de communication (portier ou terminal) de rafraîchir la clé de session en vigueur en la remplaçant par une nouvelle clé. Une telle mise à jour de la clé devrait être lancée par celle des deux entités qui en ressent la nécessité. Une mise à jour de clé peut être motivée par une clé de session compromise, par le sentiment que la clé de session n'assure ou n'assurera plus la sécurité ou pour d'autres critères liés à la politique de sécurité. Tous ces aspects ne relèvent pas du domaine de la présente Recommandation.

L'entité qui invoque la mise à jour de la clé utilise un message FACILITY, contenant un nouveau jeton de Diffie-Hellman, un certificat numérique facultatif et sa propre signature numérique. Lorsqu'il reçoit le message FACILITY, le destinataire répond par un message FACILITY analogue, acheminant son jeton de Diffie-Hellman, un certificat numérique facultatif et sa propre signature numérique. Dès que la procédure de mise à jour de la clé est terminée, les deux entités utilisent la nouvelle clé de liaison calculée.

– le champ **tokenOID** de **ClearToken** dans le message FACILITY est mis à "Q", pour indiquer l'utilisation de l'échange de Diffie-Hellman et du profil de sécurité hybride. Le calcul de la clé de liaison se déroule de la même manière que celui de la clé de session de media (voir § 8.5/H.235.6).

Le message FACILITY pour la mise à jour de la clé est protégé conformément à la procédure II/H.235.2. Tout autre message FACILITY sans jeton de Diffie-Hellman n'est pas utilisé pour la mise à jour de la clé et est protégé conformément à la procédure I du § 7/H.235.1.

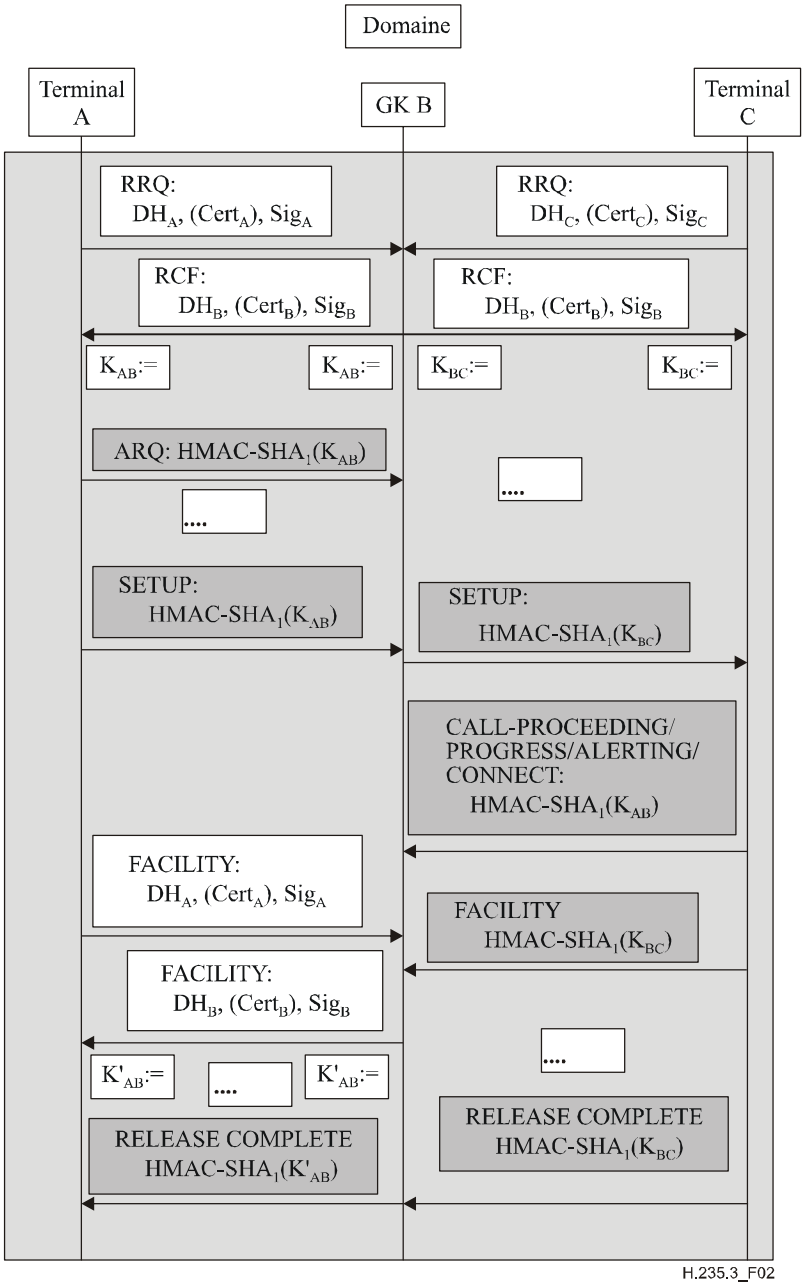
10 Utilisation de techniques à courbe elliptique

A étudier.

11 Exemples d'illustration

Les diagrammes des Figures 2 et 3 illustrent l'utilisation du profil de la présente Recommandation dans un flux de messages de base. On notera que ces diagrammes ne montrent pas le flux de messages complet et que plusieurs messages sont omis par souci de simplicité. Les messages ombrés de gris clair se rapportent au profil avec signature H.235.2 et les messages ombrés de gris foncé au profil de base H.235.1. Sur les figures, l'accent est mis sur les parties touchant à la sécurité (les plus importantes) de chaque message (CryptoTokens H.235, jetons) et les détails sont omis.

Le diagramme de la Figure 2 montre un flux de messages de base dans un scénario avec un portier dans un seul domaine administratif. Si l'on suppose que le certificat du portier est connu de tous les terminaux concernés et que les terminaux connaissent également le certificat du portier, il n'est pas nécessaire de transmettre les certificats dans la bande pendant la procédure d'enregistrement.



Cert	certificat d'utilisateur	K, K'	clé de liaison symétrique
DH_A	jeton Diffie-Hellman g^a mod p	Sig	signature numérique
DH_B	jeton Diffie-Hellman g^b mod p		
EP	point d'extrémité (terminal)		
GK	portier		

Figure 2/H.235.3 – Flux de messages dans un scénario avec un seul domaine administratif

NOTE 1 – Les Figures 2 et 3 englobent aussi la procédure de démarrage rapide lorsque les messages de signalisation d'appel SETUP et CALL PROCEEDING/PROGRESS/ALERTING/CONNECT comportent le jeton de démarrage rapide (voir § 8.1.7/H.323). Sinon, le mode supposé est le mode de démarrage non rapide conformément au § 7.3.1/H.323. La Figure 2 montre également la procédure de mise à jour de la clé entre le terminal A et le portier B au moyen du message FACILITY.

La Figure 3 présente un exemple de flux de messages dans un scénario avec plusieurs domaines administratifs. Alors que le profil de sécurité hybride est appliqué dans chaque domaine entre le

terminal et le portier comme indiqué sur la Figure 2, le profil de sécurité hybride peut également être appliqué entre deux domaines pendant la phase d'établissement de l'appel.

NOTE 2 – Sur la Figure 3, toutes les communications entre éléments frontières (BE, *border element*) et toutes les communications entre un portier et un élément frontière sont omises. Par ailleurs, la Figure 3 montre la procédure de mise à jour de la clé entre les deux domaines au moyen du message FACILITY.

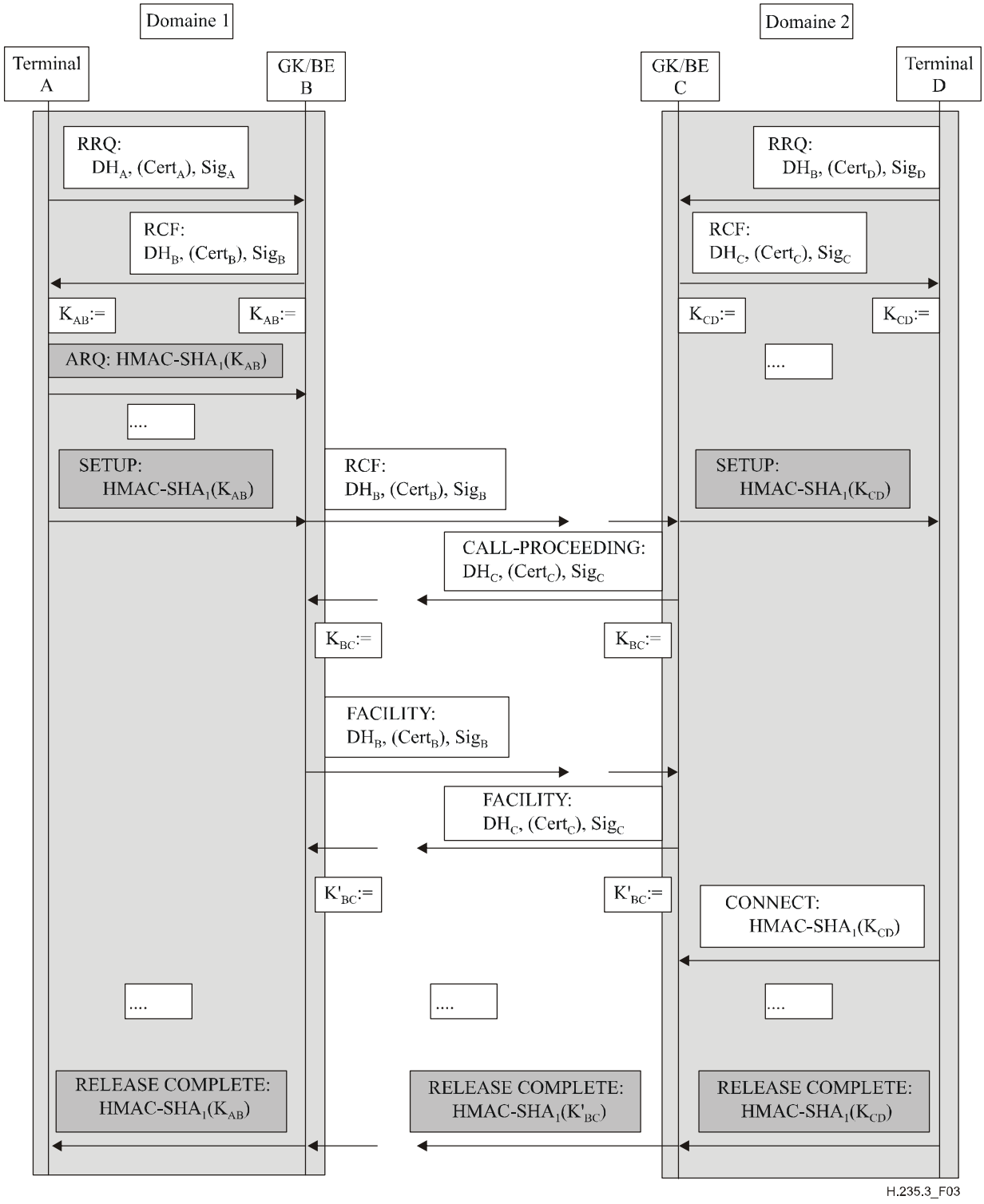


Figure 3/H.235.3 – Flux de messages dans un scénario avec plusieurs domaines administratifs

12 Comportement pour les messages multidestinataires

Les messages H.225.0 multidestinataires tels que **GRQ** et **LRQ** doivent comporter un champ **CryptoToken** conformément à la procédure II lorsque l'identificateur **generalID** n'est pas défini. Si de tels messages sont envoyés à un seul destinataire, ils doivent comporter un champ **CryptoToken** ayant un identificateur **generalID** défini.

13 Liste des messages de signalisation sécurisés

La procédure IV utilise la procédure I/H.235.1 ou la procédure II/H.235.2, selon le scénario et le message proprement dit, comme indiqué ci-dessous.

13.1 Messages RAS H.225.0

Message RAS H.225.0	Champs de signalisation H.235	Authentification et intégrité	Non-répudiation
GatekeeperRequest, GatekeeperConfirm, GatekeeperReject si la découverte de portier est appliquée RegistrationRequest, RegistrationConfirm, RegistrationReject si la découverte de portier n'est pas appliquée	CryptoToken, ClearToken	Procédure II	Procédure II
Tout autre message RAS (Note 2)	CryptoToken	Procédure I	
NOTE 1 – Pour les messages à un seul destinataire, la procédure II est appliquée avec les champs de sécurité de CryptoToken définis. NOTE 2 – Les messages de découverte de portier et les messages à plusieurs destinataires ne sont pas envoyés.			

13.2 Messages de signalisation d'appel H.225.0 (domaine administratif unique)

Message de signalisation d'appel H.225.0	Champs de signalisation H.235	Authentification et intégrité	Non-répudiation
Setup-UUIE, Connect-UUIE (Note 1), Facility-UUIE (Note 2), Alerting-UUIE, CallProceeding-UUIE, Facility-UUIE, Progress-UUIE, Information-UUIE, ReleaseComplete-UUIE, Status-UUIE, StatusInquiry-UUIE, SetupAcknowledge-UUIE, Notify-UUIE	CryptoToken, ClearToken	Procédure I	
Facility-UUIE (Note 3)	CryptoToken	Procédure II	Procédure II
NOTE 1 – A supposer que chaque message soit le premier dans chaque sens. NOTE 2 – Pas utilisé pour la mise à jour de la clé. NOTE 3 – Utilisé pour la mise à jour de la clé.			

13.3 Messages de signalisation d'appel H.225.0 (plusieurs domaines administratifs)

Message de signalisation d'appel H.225.0	Champs de signalisation H.235	Authentification et intégrité	Non-répudiation
Setup-UUIE, Connect-UUIE (Note 1), Alerting-UUIE (Note 2), CallProceeding-UUIE, Facility-UUIE (Note 3), Progress-UUIE, Information-UUIE, ReleaseComplete-UUIE	CryptoToken, ClearToken	Procédure II	Procédure II
Alerting-UUIE (Note 4), CallProceeding-UUIE, Facility-UUIE (Note 5), Progress-UUIE, Information-UUIE, ReleaseComplete-UUIE, Status-UUIE, StatusInquiry-UUIE, SetupAcknowledge-UUIE, Notify-UUIE	CryptoToken, ClearToken	Procédure I	Procédure I
NOTE 1 – A supposer que chaque message soit le premier dans chaque sens. NOTE 2 – N'importe lequel de ces messages survient comme premier message dans l'un ou l'autre sens. NOTE 3 – Utilisé pour la mise à jour de la clé. NOTE 4 – Aucun de ces messages ne survient comme premier message dans l'un ou l'autre sens. NOTE 5 – Pas utilisé pour la mise à jour de la clé.			

14 Liste des identificateurs d'objet

Le Tableau 2 énumère tous les identificateurs OID mentionnés.

Tableau 2/H.235.3 – Identificateurs d'objet

Désignation de l'identificateur d'objet	Valeur(s) de l'identificateur d'objet	Description
"A1"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 20}	Utilisé en remplacement de l'identificateur OID "A" dans la procédure II de la Rec. UIT-T H.235.2 pour l'identificateur CryptoToken-tokenOID, indiquant que la signature ou le hachage RSA englobe tous les champs du message RAS ou de signalisation d'appel H.225.0 (authentification et intégrité).
"S1"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 21}	Utilisé en remplacement de l'identificateur OID "S" dans la procédure II de Rec. UIT-T H.235.2 pour l'identificateur ClearToken-tokenOID, indiquant que le champ ClearToken est utilisé pour l'authentification et l'intégrité du message. Cet identificateur dans le champ CryptoToken de bout en bout indique aussi implicitement l'utilisation de l'échange de Diffie-Hellman pendant la procédure de démarrage rapide.
"Q"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 22}	Utilisé dans la procédure IV pour indiquer que le champ ClearToken de la liaison bond par bond achemine un jeton de Diffie-Hellman.
"W	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 23}	Utilisé dans la procédure IV pour l'identificateur algorithm OID, indiquant l'utilisation d'une signature numérique fondée sur l'algorithme RSA SHA1.

Appendice I

Processeur de sécurité de portier H.235.3

Le présent appendice donné à titre d'information décrit un exemple d'implémentation d'un processeur de sécurité de portier H.235.3 (GKSP, *gatekeeper security processor*) conjointement avec un portier. Le processeur GKSP a pour objet de transférer certaines tâches de sécurité H.235.3 (exécution d'opérations Diffie-Hellman très longues, calculs et vérifications de signature numérique, traitement de certificat X.509, par exemple) d'un portier monolithique vers une entité fonctionnelle nouvelle et distincte appelée processeur de sécurité de portier (GKSP). Il y a au moins une entité GKSP pour chaque portier, mais un même portier peut aussi desservir plusieurs entités GKSP afin de pouvoir augmenter le nombre de points d'extrémité desservis et d'améliorer la robustesse de l'ensemble du système.

La Figure I.1 illustre une telle architecture de portier décomposé, dans laquelle l'entité GKSP contient les fonctions de sécurité H.235.3.

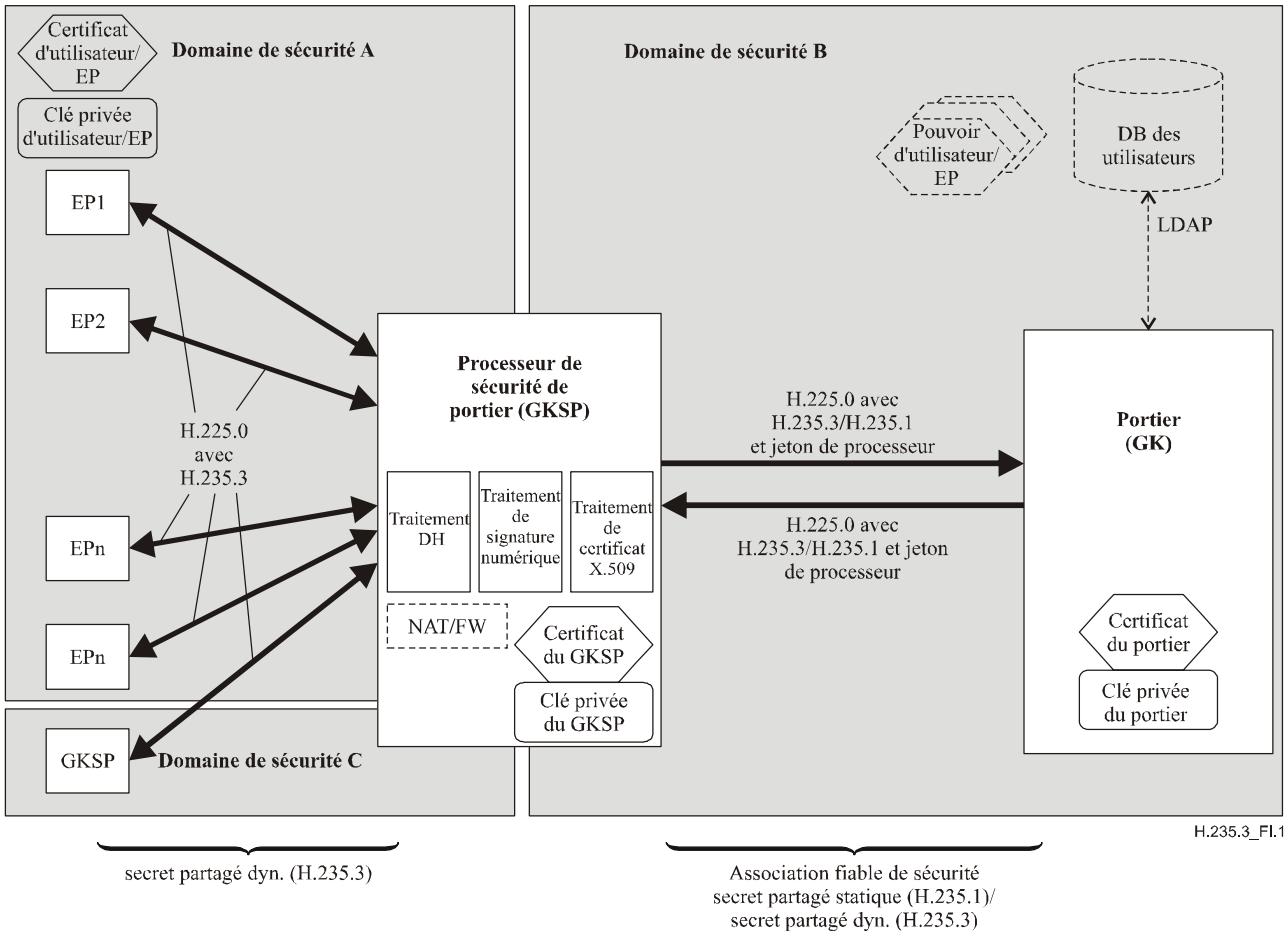


Figure I.1/H.235.3 – Architecture du processeur de sécurité de portier

NOTE 1 – L'entité GKSP peut contenir d'autres fonctions utiles, par exemple une fonction NAT (fonction de traduction d'adresse réseau), un pare-feu, une passerelle de couche Application (ALG, *application level gateway*) etc.; ces fonctions, qui peuvent faire partie du traitement de sécurité ou peuvent être incluses comme des fonctions internes distinctes, ne sont pas décrites ici et nécessitent un complément d'étude.

L'entité GKSP dessert un certain nombre de points d'extrémité dans un domaine administratif de sécurité A. Elle peut aussi communiquer avec une autre entité GKSP appartenant à un autre domaine administratif de sécurité C (ceci n'est pas représenté).

NOTE 2 – Dans la pratique, il n'est pas nécessaire que les trois domaines administratifs de sécurité soient distincts. L'entité GKSP peut être placée entièrement dans le domaine administratif de sécurité B auquel le portier appartient, ou bien elle peut être placée dans le domaine de sécurité A, ou dans un domaine de sécurité propre, distinct (ceci n'est pas représenté).

Grâce à l'entité GKSP, le portier est libéré de l'exécution des opérations de sécurité nécessitant de nombreux calculs. Le portier continue à déterminer l'autorisation et l'admission en comparant un justificatif d'identité approprié (par exemple un pseudonyme/un nom DN/un numéro de série de certificat, un certificat X.509) avec les données qui figurent dans la base de données (interne/externe) des utilisateurs abonnés avec leurs permissions et justificatifs d'identité. Le paragraphe I.3 définit les justificatifs d'identité à utiliser par une entité GKSP H.235.3.

NOTE 3 – La présente Recommandation ne définit pas d'interface LDAP possible entre le portier et la base de données des abonnés/utilisateurs. Par ailleurs, les critères et les justificatifs d'identité (par exemple pseudonyme/nom DN/numéro de série de certificat) à utiliser pour le contrôle d'accès sont à définir dans la politique du portier. Les justificatifs d'identité (pseudonyme/nom DN/numéro de série de certificat) à enregistrer dans une base de données d'utilisateurs dépendent de ladite base de données.

NOTE 4 – L'entité GKSP n'a pas besoin de participer aux opérations relatives à la configuration ou à l'administration des utilisateurs/abonnés et n'a pas besoin d'accéder à une base de données d'utilisateurs.

NOTE 5 – Les points d'extrémité de type H.235.3 et l'entité GKSP possèdent généralement aussi un certificat racine (non représenté sur la Figure I.1). Le certificat racine permet de vérifier le certificat de l'entité considérée (point d'extrémité, entité GKSP).

Les communications entre l'entité GKSP et son portier ou entre deux entités GKSP sont sécurisées. A titre d'exemple, l'application du profil H.235.1 se fait lorsqu'un secret partagé configuré statiquement est utilisé et l'application du profil H.235.3 permet d'établir un secret partagé dynamique. Dans l'un et l'autre cas, le portier et l'entité GKSP sont supposés avoir établi une relation de confiance mutuelle, qu'il s'agisse d'une association de sécurité statique ou dynamique. Lorsque plusieurs entités GKSP interviennent, elles peuvent établir une relation de confiance en chaîne.

Par conséquent, le portier délègue à l'entité GKSP l'exécution des procédures d'authentification de l'extrémité distante et l'exécution correcte des procédures de sécurité. L'entité GKSP signale au portier le résultat de son traitement de sécurité dans une assertion de sécurité simple en utilisant le jeton de processeur.

On suppose que chaque point d'extrémité de type H.235.3 et l'entité GKSP possèdent un certificat X.509 qui relie de façon fiable l'identité du détenteur légitime de la clé publique et une clé privée correspondante pour la signature.

NOTE 6 – La clé publique correspondant à la clé privée n'est pas représentée explicitement sur la Figure I.1; la clé publique certifiée est généralement acheminée dans le certificat X.509 de l'utilisateur/du point d'extrémité.

NOTE 7 – Les certificats/clés privées des points d'extrémité/entité GKSP ne sont pas tous représentés.

NOTE 8 – Le certificat de l'entité GKSP est généralement un certificat de serveur.

Le portier est tenu de posséder un certificat distinct et unique ainsi qu'une clé privée uniquement s'il met en œuvre le profil H.235.3 pour ses communications avec l'entité GKSP.

L'entité GKSP est un proxy à états fonctionnant entre les points d'extrémité et le portier ou entre deux portiers. Il y a au moins une entité GKSP pour chaque portier, mais un même portier peut aussi desservir plusieurs entités GKSP afin de pouvoir augmenter le nombre de points d'extrémité desservis et d'améliorer la robustesse de l'ensemble du système. Des entités GKSP H.235.3 peuvent être disposées en chaîne linéaire comme représenté sur la Figure I.2, ou dans une architecture hiérarchique comme représenté sur la Figure I.3.

Il y a au moins une entité GKSP générique pour chaque portier, mais un même portier peut aussi desservir plusieurs entités GKSP génériques afin de pouvoir augmenter le nombre de points

d'extrémité desservis et d'améliorer la robustesse de l'ensemble du système. Il peut y avoir une ou plusieurs entités GKSP génériques entre un point d'extrémité et un portier; les configurations linéaires ou hiérarchiques avec plusieurs portiers sont donc possibles en principe. Un point d'extrémité établit toujours une relation de confiance avec le portier qui lui est associé par le biais d'une ou de plusieurs entités GKSP. Un même portier peut avoir plusieurs relations de confiance avec plusieurs points d'extrémité.

La Figure I.2 représente une architecture d'entités GKSP en chaîne linéaire.

Figure I.2/H.235.3 – Architecture d'entités GKSP en chaîne

Sur la Figure I.2, l'entité GKSP1 authentifie le message RRQ reçu du point EP1, tandis que le portier GK1 ou GK2 décide de l'autorisation du point EP1. Les entités GKSP1 et GKSP2 (resp. les entités GKSP3 et GKSP4) relaient les messages de signalisation H.323 entre le point EP1 et le portier GK1 (resp. entre les portiers GK1 et GK2).

La Figure I.3 représente une architecture hiérarchique d'entités GKSP en cascade.

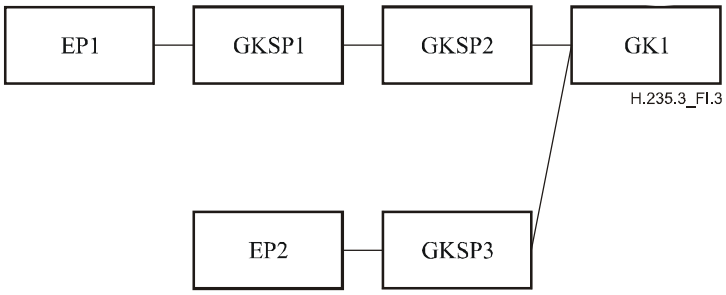


Figure I.3/H.235.3 – Architecture hiérarchique d'entités GKSP

L'entité GKSP a au moins une adresse IP; une entité GKSP est généralement un dispositif de sécurité périphérique qui est situé à la frontière entre deux domaines administratifs de sécurité distincts. Par conséquent, l'entité GKSP peut avoir deux adresses IP, une adresse IP en direction des points d'extrémité H.323/de l'entité GKSP homologue (domaines administratifs de sécurité A et C) et une adresse IP différente en interne en direction du portier (domaine administratif de sécurité B).

I.1 Découverte d'un processeur de sécurité de portier

On suppose qu'un point d'extrémité H.323 n'est pas tenu de connaître la présence d'une entité GKSP. Le point d'extrémité peut avoir configuré l'adresse IP de l'entité GKSP en tant que point de contact de portier. Le point d'extrémité a exactement le même comportement dans un scénario avec entité GKSP que dans un scénario sans entité GKSP. Il peut utiliser la phase de découverte de portier avec le message **GRQ** pour localiser l'entité GKSP qui le dessert.

S'il existe une entité GKSP qui dessert le point d'extrémité demandeur, l'entité GKSP doit déterminer si son portier prend en charge un processeur de sécurité.

Si l'entité GKSP a l'intention d'utiliser le profil H.235.1 en direction du portier mais qu'aucun secret partagé n'a été configuré entre l'entité GKSP et le portier, l'entité GKSP renvoie le message **GRJ** au point d'extrémité avec le motif **reason** mis à **securityDenial/securityDenied**. Dans le cas contraire, l'entité GKSP retransmet le message **GRQ** dans lequel elle inclut un jeton ClearToken de

processeur avec l'élément de profil de type ElementID 0 comme défini dans le Tableau I.1. Comme dans ce cas, le portier prend en charge l'entité GKSP, il renvoie un message **GCF**/**GRJ** dans lequel il inclut un jeton de processeur.

Si l'entité GKSP a l'intention d'utiliser le profil H.235.3 en direction du portier, elle retransmet au portier le message **GRQ** dans lequel elle inclut un jeton ClearToken de processeur avec l'élément de profil de type ElementID 0 comme défini dans le Tableau I.1. Un portier qui prend en charge une entité GKSP et qui est conforme au présent appendice répond par un message **GCF** dans lequel il inclut un jeton ClearToken de processeur.

En principe, un portier qui ne prend pas en charge de processeur de sécurité ou un portier qui n'a pas implémenté le présent appendice ignore le jeton de processeur acheminé et répond par un message **GCF**/**GRJ**. L'entité GKSP est capable de reconnaître cette situation, étant donné que le message **GRQ**/**GRJ** reçu ne contient pas de jeton de processeur. L'entité GKSP envoie alors un message **GRJ** au point d'extrémité avec le motif **reason** mis à **securityDenial**/**securityDenied**.

Un portier qui reçoit un message **GRQ** en provenance directe d'un point d'extrémité sans passer par une entité GKSP et qui connaît une entité GKSP répond par un message **GRJ** avec le motif **reason** mis à **securityDenial**/**securityDenied** (sans inclure de jeton de processeur).

I.2 Opérations du processeur de sécurité de portier

Le processeur de sécurité de portier remplit au minimum les fonctions suivantes:

- termine l'exécution du protocole H.235.3 avec les points d'extrémité H.323 ou avec l'entité GKSP homologue comme défini par la procédure IV;
- exécute le protocole H.235.3 Diffie-Hellman avec les points d'extrémité H.323 ou l'entité GKSP homologue; autrement dit, il exécute les opérations Diffie-Hellman modulaires d'élévation à la puissance;
- vérifie les signatures numériques reçues en provenance des points d'extrémité H.323 ou de l'entité GKSP homologue dans des messages sécurisés H.235.3;
- procède à des contrôle de sécurité des certificats numériques X.509 reçus: vérification de trajet, contrôle de validité, contrôle de liste CRL, etc;
- avant de retransmettre un message au portier ou à une autre entité GKSP, l'entité GKSP produit de nouveaux jetons H.235 (H.235.1 ou H.235.3). Elle insère son identificateur dans le champ **sendersID** et l'identificateur de portier (GKID) dans le champ **generalID** dans le ClearToken H.235 de base;
- concernant les messages reçus en provenance d'un point d'extrémité H.323, l'entité GKSP inclut un jeton de processeur. Pour le message **RRQ**/**GRQ** initial, le jeton de processeur contient un élément de profil de sécurité de type ElementID 0, qui indique la méthode d'authentification rencontrée. L'entité GKSP peut aussi inclure un élément de profil de sécurité avec ElementID 0 dans un autre message RAS et/ou de signalisation d'appel H.225.0.

Le jeton de processeur contient en outre un ou plusieurs éléments de profil de sécurité qui acheminent les justificatifs d'identité.

Les justificatifs d'identité définis dans le présent appendice sont les suivants:

- ElementID 1 pour la fourniture du champ subject trouvé dans un certificat X.509;
- ElementID 2 pour la fourniture du champ subjectAltName trouvé dans un certificat X.509;
- ElementID 3 pour la fourniture du numéro de série trouvé dans un certificat X.509;
- ElementID 4 pour la fourniture du nom d'émetteur trouvé dans un certificat X.509;
- ElementID 5 pour la fourniture de l'identificateur de point d'extrémité du terminal H.323.

NOTE – Le portier peut en outre interpréter l'élément pseudonyme H.323 des messages H.225.0 comme un justificatif d'identité. Comme cet élément est de toute façon présent dans les messages, il n'est pas nécessaire de définir un élément pseudonyme à part dans un élément de profil de sécurité.

Lorsqu'une erreur est rencontrée, l'entité GKSP inclut également un élément de profil de sécurité de type ElementID 6 pour indiquer cette erreur. Si l'authentification entre le point d'extrémité H.323 et l'entité GKSP aboutit, l'entité GKSP peut inclure un élément de profil de sécurité de type ElementID 6 pour indiquer qu'aucune erreur de sécurité n'a été rencontrée.

– Si l'entité GKSP rencontre des erreurs de sécurité (signature numérique erronée, échec de validation de certificat, etc.) dans un message reçu en provenance du point d'extrémité H.323 ou de l'entité GKSP homologue, elle journalise l'erreur et retransmet le message au portier après y avoir inclus un jeton de processeur avec un élément de profil de sécurité de type ElementID 6 indiquant le type d'erreur et laisse le soin au portier de décider et de réagir en conséquence.
– Si l'entité GKSP rencontre des erreurs de sécurité dans un message reçu en provenance du portier ou d'une autre entité GKSP, elle journalise l'erreur et élimine le message.
– Calcule des signatures numériques pour les messages H.235.3 sortants destinés aux points d'extrémité H.323 ou à l'entité GKSP homologue.
– Retransmet tout message H.225.0 entre un point d'extrémité H.323 et un portier ou une entité GKSP dans un sens comme dans l'autre et exécute les opérations suivantes sur les jetons:
  - communique avec son portier au moyen du protocole H.225.0, les jetons H.235.3 reçus en provenance des points d'extrémité H.323 ou de l'entité GKSP homologue dans le premier message de prise de contact étant enlevés;
  - vérifie les jetons H.235.1 imbriqués reçus en provenance des points d'extrémité H.323 ou de l'entité GKSP homologue et les enlève avant de retransmettre les messages au portier;
  - termine l'exécution du protocole H.235.1/H.235.3 avec son portier;
  - inclut des jetons H.235.1/H.235.3 en direction des points d'extrémité H.323 ou de l'entité GKSP homologue pour les messages sortants;
  - laisse quasiment intacts les messages H.225.0 reçus en provenance des points d'extrémité H.323 ou du portier; ne réécrit que les jetons comme défini ci-dessus;
  - l'exécution du protocole H.225.0 entre l'entité GKSP et son portier est sécurisée au moyen du profil de sécurité de base H.235.1 ou du profil de sécurité hybride H.235.3.
– Si l'entité GKSP et le portier ou l'entité GKSP et une autre entité GKSP mettent en œuvre le profil de sécurité hybride H.235.3, l'entité GKSP effectue l'une des deux tâches suivantes:
  a) exécute le protocole H.235.3 avec le portier ou l'entité GKSP pour établir une nouvelle clé dynamique à la réception du premier message en provenance du premier point d'extrémité ou de l'entité GKSP homologue;
  b) lance l'exécution du protocole H.235.3 avec le portier ou l'entité GKSP pour établir une nouvelle clé dynamique avant qu'un autre point d'extrémité H.323 ou que l'entité GKSP homologue ait commencé la communication. Ceci permet d'avoir déjà un secret dynamique partagé en place à utiliser pour la protection des premiers messages de prise de contact reçus en provenance d'un terminal H.323 ou de l'entité GKSP homologue; ceci permet en outre de raccourcir la durée totale d'établissement des associations de sécurité.
– L'entité GKSP ne retransmet pas de message FACILITY H.235.3 pour la mise à jour de clé.

– Si l'entité GKSP et le portier ou l'entité GKSP et une autre entité GKSP mettent en œuvre le profil de sécurité de base H.235.1, l'entité GKSP applique la clé partagée statique pour la protection des messages RAS et/ou de signalisation d'appel H.225.0.

– Garde une trace des associations de sécurité; autrement dit établit le secret partagé DH; conserve les secrets partagés dynamiques. Suivant sa politique de sécurité, l'entité GKSP peut invoquer au moyen de messages FACILITY un recalcul de clé pour le ou les secrets partagés dynamiques conservés. Une fois que le terminal H.323 ou l'entité GKSP homologue s'est désenregistré, l'entité GKSP devrait éliminer la clé partagée dynamique et considérer qu'aucune association de sécurité n'est en place.

– Etablit un mappage biunivoque entre les ports de transport (EP-GKSP et GKSP-GK) pour les protocoles RAS et/ou de signalisation d'appel H.225.0.

I.3 Jeton de processeur

Dès qu'elle reçoit un message RAS et/ou de signalisation d'appel H.225.0 sécurisé H.235.3 contenant un certificat X.509 et une signature numérique, l'entité GKSP supprime les jetons H.235.3 et inclut un jeton de processeur distinct dans le message qu'elle retransmet à son portier ou à l'éventuelle entité GKSP suivante.

Avec le jeton de processeur, l'entité GKSP signale la méthode d'authentification rencontrée, l'identificateur de point d'extrémité rencontré, le nom rencontré dans le certificat (name ou subjectAltName), le numéro de série rencontré dans le certificat X.509, le nom d'émetteur rencontré dans le certificat X.509 ou une indication d'erreur. Le jeton de processeur joue le rôle d'une simple assertion de sécurité déclarant si la relation de sécurité est établie ou non entre l'entité GKSP et les points d'extrémité H.323 en direction du portier.

Le portier est en mesure de détecter la présence d'une entité GKSP en inspectant le message reçu et en reconnaissant qu'il contient un jeton de processeur. Le portier interprète l'absence de tout jeton de processeur comme l'absence de toute entité GKSP.

Le jeton de processeur est un jeton ClearToken avec les champs suivants:

– **tokenOID** contient l'identificateur OID "PT"; voir Tableau I.2.

– **generalID** contient

  • soit l'identificateur du point d'extrémité H.323 dans le cas d'un message sécurisé H.235 reçu en provenance d'un point d'extrémité H.323;

  • soit l'identificateur du portier dans le cas d'un message sécurisé H.235 reçu en provenance du portier.

– **certificate** peut optionnellement contenir le certificat H.235.2/H.235.3 reçu en provenance du point d'extrémité H.323 ou de l'entité GKSP homologue. Si cette option est implémentée, l'entité GKSP retransmet le certificat au portier.

  Il est préférable d'utiliser le champ subject/subjectAltName, ou l'identificateur de point d'extrémité ou le numéro de série de certificat ou un autre justificatif d'identité simple plutôt que d'inclure la totalité du certificat dans le champ **certificate**. En effet, les certificats X.509 ont tendance à contenir des données volumineuses et il existe un problème potentiel de fragmentation de message lorsque les certificats sont inclus dans des messages H.225.0 transportés par le protocole UDP.

– **profileInfo** contient au moins un élément de profil.

  Le jeton de processeur peut contenir plusieurs des éléments de profil spécifiés dans le Tableau I.1:

Les autres champs du ClearToken du processeur de sécurité de portier ne sont pas utilisés.

Tableau I.1/H.235.3 – Spécification des éléments de profil

Valeur de ElementID	Description	Spécification
0	Indique un élément de profil qui achemine la méthode d'authentification. L'utilisation de cet élément de profil est obligatoire pour le message initial de prise de contact (GRQ ou RRQ) et facultatif dans les autres cas.	• **paramS** n'est pas utilisé. • **element** contient un élément dans lequel le champ **integer** prend l'une des valeurs suivantes pour indiquer la méthode d'authentification rencontrée au niveau du point d'extrémité H.323 ou de l'entité GKSP homologue: 1) autre méthode d'authentification, non spécifiée et non normalisée; 2) aucune (autrement dit pas d'authentification); 3) secret partagé H.235.1 (non défini dans le présent appendice); 4) H.235.2; 5) H.235.3; 6) H.235.5, (non défini dans le présent appendice); 7) H.235.4, (non défini dans le présent appendice); 8) H.530, (non défini dans le présent appendice).
1	Indique un élément de profil qui contient le champ **subject** du certificat reçu. L'utilisation de cet élément de profil est facultative.	• **paramS** n'est pas utilisé. • **element** contient un élément dont le champ **name** ou **octets** contient le champ **subject** du certificat reçu. NOTE – Il est possible que l'entité GKSP doive recoder le champ **subject** représenté comme un nom X.509 en une chaîne **octets** ou représenté en un nom **name** BMP.
2	Indique un élément de profil qui contient le champ **subjectAltName** du certificat reçu. L'utilisation de cet élément de profil est facultative.	• **paramS** n'est pas utilisé. • **element** contient un élément dont le champ name ou octets contient le champ **subjectAltName** du certificat reçu. NOTE – Il est possible que l'entité GKSP doive recoder le champ **subjectAltName** représenté comme un nom X.509 en un chaîne **octets** ou représenté en un nom **name** BMP.
3	Indique un élément de profil qui contient le numéro de série du certificat. L'utilisation de cet élément de profil est obligatoire.	• **paramS** n'est pas utilisé. • **element** contient un élément dont le champ **integer** contient le champ **CertificateSerialNumber** du certificat X.509 reçu.
4	Indique un élément de profil qui contient le nom de l'émetteur du certificat. L'utilisation de cet élément de profil est obligatoire.	• **paramS** n'est pas utilisé. • **element** contient un élément dont le champ **name** ou **octets** contient le nom **issuer** du certificat X.509 reçu. NOTE – Il est possible que l'entité GKSP doive recoder le nom **issuer** représenté comme un nom X.509 en une chaîne **octets** ou représenté en un nom **name** BMP.

Tableau I.1/H.235.3 – Spécification des éléments de profil

Valeur de ElementID	Description	Spécification
5	Indique un élément de profil qui contient l'identificateur du point d'extrémité/terminal d'origine. L'utilisation de cet élément de profil est facultative.	• **paramS** n'est pas utilisé. • **element** contient un élément dont le champ **name** contient l'identificateur du point d'extrémité/terminal d'origine.
6	Indique un élément de profil qui contient une indication d'erreur. L'utilisation de cet élément de profil est obligatoire en cas d'erreur (> 0) mais facultatif pour indiquer l'absence d'erreur (0).	• **paramS** n'est pas utilisé. • **element** contient un élément dont le champ **integer** contient l'une des valeurs d'erreur codées suivantes: 0: pas d'erreur 1: securityDenied 2: securityWrongSyncTime 3: securityReplay 4: securityWrongGeneralID 5: securityWrongSendersID 6: securityMessageIntegrityFailed 7: securityWrongOID 8: securityDHmismatch 9: securityCertificateExpired 10: securityCertificateDateInvalid 11: securityCertificateRevoked 12: securityCertificateNotReadable 13: securityCertificateSignatureInvalid 14: securityCertificateMissing 15: securityCertificateIncomplete 16: securityUnsupportedCertificateAlgOID 17: securityUnknownCA 18: erreur de sécurité non spécifiée 19: entité GKSP non prise en charge.

I.4 Exemple d'illustration d'une entité GKSP

Le présent paragraphe donne des exemples de diagrammes de flux de messages (voir les Figures I.4 et I.5) pour un processeur de sécurité de portier (GKSP) fonctionnant dans un domaine administratif de sécurité. Il est à noter que sur les Figures I.4 et I.5, seuls les messages qui sont cruciaux pour le profil H.235.3 sont représentés; en pratique, il peut y avoir beaucoup plus de messages RAS et/ou de signalisation d'appel H.225.0.

Sur les deux Figures, le terminal A H.323 de type H.235.3 et l'entité GKSP mettent en œuvre le profil de sécurité hybride H.235.3; le terminal A et l'entité GKSP B ne partagent donc pas de secret statique. Sur la Figure I.4, l'entité GKSP et le portier mettent en œuvre le profil de sécurité de base H.235.1 pour la protection des messages RAS et de signalisation d'appel H.225.0. K_{BC} représente le secret statique partagé entre l'entité GKSP B et le portier C.

La Figure I.4 illustre la totalité d'un appel provenant du terminal A et passant par l'entité GKSP B et le portier C. L'appel est à routage par portier. Au début, le terminal A et l'entité GKSP B négocient une clé de liaison dynamique K_{AB} conformément à la Recommandation H.235.3 pendant l'enregistrement RAS. Pour cela, le terminal A produit le message **RRQ** qui achemine la demi-clé Diffie-Hellman DH_A de A et qui contient le certificat de A (facultatif) et la signature numérique de A sur tout ou partie du message **RRQ**.

L'entité GKSP B reçoit le message **RRQ** et vérifie la signature numérique (validation et vérification du certificat numérique X.509 acheminé (s'il est inclus) par rapport au certificat racine de A, vérification du trajet, contrôles de liste CRL, etc.).

L'entité GKSP retransmet le message **RRQ** au portier C après y avoir ajouté un jeton de processeur (PT) contenant les éléments de profil de sécurité suivants:

– 0 indiquant H.235.3 (5);

– 2 contenant le champ subjectAltName du certificat de A;

– 3 contenant le numéro de série du certificat de A;

– 5 contenant l'identificateur de point d'extrémité de A,

et avoir appliqué le profil de sécurité de base H.235.1 avec la clé partagée K_{BC}; le contrôle d'intégrité HMAC-SHA1 est réalisé sur la totalité du message **RRQ** ou uniquement sur certaines de ses parties.

Si la validation du certificat ou celle de la signature numérique échoue, l'entité GKSP B ne peut pas authentifier et autoriser le terminal A; elle journalise une erreur et retransmet le message RRQ incorrect au portier C.

Le portier C reçoit le message **RRQ**, vérifie l'intégrité en appliquant la clé K_{BC} et traite le jeton de processeur PT avec les éléments de profil qui y sont inclus. Si le portier C est capable de valider avec succès le message **RRQ**, il autorise le terminal A. Puis il répond à l'entité GKSP B par un message **RCF**.

L'entité GKSP B reçoit le message **RCF**, reconnaît que le portier C a autorisé avec succès le terminal A et retransmet le message **RCF** au terminal A après avoir calculé et inclus sa demi-clé Diffie-Hellman DH_B, avoir inclus son certificat (facultatif) et avoir signé le message **RRQ** (en totalité ou en partie) avec sa clé privée. Le terminal A valide l'authenticité du message **RCF** reçu.

Si l'entité GKSP B a pu authentifier et autoriser avec succès le terminal A, l'entité GKSP B et le terminal A calculent le secret partagé dynamique K_{AB}. Ce secret représente la relation de confiance établie entre le terminal A et l'entité GKSP B. Dans le cas contraire et si le portier C n'a pas autorisé le terminal A, l'entité GKSP B retransmet le message **RCF** au terminal A après avoir calculé et inclus sa demi-clé Diffie-Hellman DH_B, avoir inclus son certificat (facultatif) et avoir signé le message **RRQ** (en totalité ou en partie) avec sa clé privée. Comme le terminal A n'est pas autorisé, l'entité GKSP B ne conserve pas plus longtemps la clé K_{AB}. L'entité GKSP B peut enregistrer le message **RCF** d'échec dans un fichier de journalisation.

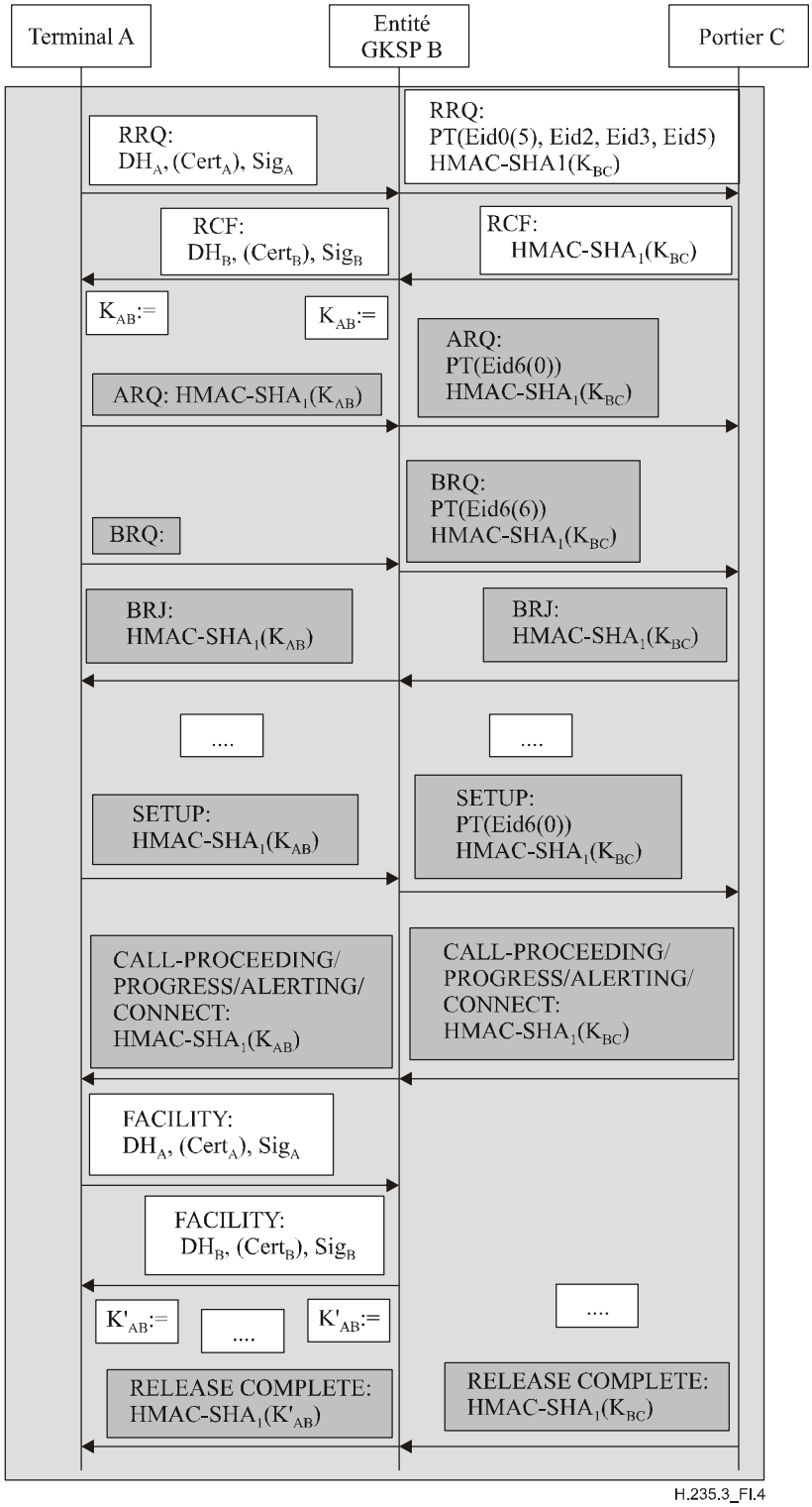
Le terminal A et l'entité GKSP B utilisent ce secret partagé dynamique K_{AB} pour protéger les messages RAS et de signalisation d'appel H.225.0 au moyen du profil de sécurité de base H.235.1. L'entité GKSP B et le portier C utilisent le profil de sécurité de base H.235.1 pour la protection de tous les messages RAS et de signalisation d'appel H.225.0.

Si le terminal A reçoit un message **RCF**, il ne poursuit pas l'établissement d'appel.

La Figure I.4 montre également un cas d'erreur dans lequel le terminal A (ou quelqu'un d'autre) envoie un message **BRQ** non protégé à l'entité GKSP; ce message peut aussi provenir d'une attaque dans laquelle l'attaquant a supprimé ou altéré d'une manière ou d'une autre la protection de sécurité H.235.1. L'entité GKSP détecte l'échec de vérification de l'intégrité et retransmet au portier le message **BRQ** avec un jeton de processeur, l'élément de profil de sécurité indiquant

securityMessageIntegrityFailed (6). Le portier reconnaît la violation de sécurité et rejette la demande de largeur de bande par une réponse **BRJ**.

Un certain temps après que l'appel a été établi, le terminal A décide de rafraîchir la clé K_{AB} en exécutant une procédure de mise à jour de la clé K_{AB} avec l'entité GKSP B; K'_{AB} représente la nouvelle clé mise à jour. A la fin de l'appel, le portier C termine l'appel.



Cert	certificat d'utilisateur	GK	portier
DH_A	jeton Diffie-Hellman g^a mod p	GKSP	processeur de sécurité portier
DH_B	jeton Diffie-Hellman g^b mod p	HMAC-SHA1	valeur de contrôle d'intégrité calculée
Eid*n*	ID d'élément de profil de sécurité de valeur *n*	K, K'	clé de liaison symétrique
		PT	jeton de processeur
EP	point d'extrémité (Terminal)	Sig	signature numérique

Figure I.4/H.235.3 – Déroulement d'un appel avec processeur de sécurité de portier et protection de message H.235.1 (entité GKSP vers portier)

Sur la Figure I.5, l'entité GKSP et le portier mettent en œuvre le profil de sécurité hybride H.235.3 pour la protection des messages RAS et de signalisation d'appel H.225.0. K_{BC} représente le secret partagé dynamique que l'entité GKSP et le portier négocient puis partagent en vue de son utilisation dans le profil de sécurité de base H.235.1 pour la protection des messages RAS et de signalisation d'appel H.225.0. La Figure I.5 représente aussi un terminal D H.323 de type H.235.1 qui partage un secret partagé statique K_{DB} avec son entité GKSP B.

La Figure I.5 illustre le déroulement de la totalité d'un appel provenant du terminal I.5 et passant par l'entité GKSP B et le portier C. L'appel est à routage par portier. Sur la Figure I.5, on suppose que le terminal A est en fait le premier point d'extrémité qui s'enregistre auprès du portier par le biais de l'entité GKSP.

Le terminal A et l'entité GKSP B utilisent le secret partagé dynamique K_{AB} pour protéger les messages RAS et de signalisation d'appel H.225.0 au moyen du profil de sécurité de base H.235.1. L'entité GKSP B et le portier C utilisent le profil de sécurité de base H.235.1 pour protéger les messages RAS et de signalisation d'appel H.225.0 au moyen du secret partagé dynamique K_{BC}.

Au début, le terminal A et l'entité GKSP B négocient une clé de liaison dynamique K_{AB} conformément à la Rec. UIT-T H.235.3. Pendant le premier échange de messages **RRQ**/**RCF** de prise de contact entre le terminal A et l'entité GKSP pendant lequel les deux entités établissent un secret partagé dynamique K_{AB}, l'entité GKSP et le portier mettent aussi en œuvre la Recommandation H.235.3 pour établir un secret partagé dynamique K_{BC}.

L'entité GKSP retransmet le message **RRQ** reçu du terminal A après avoir ajouté un jeton de processeur contenant les trois éléments de profil de sécurité suivants:

– 0 indiquant H.235.3 (5);

– 3 contenant le numéro de série du certificat de A;

– 6 indiquant l'absence d'erreur (0),

et avoir appliqué le profil de sécurité hybride H.235.3. Comme l'entité GKSP B et le portier C ne partagent pas encore de secret, ils exécutent le protocole H.235.3 et établissent un secret partagé dynamique K_{BC}.

Un peu plus tard, le terminal D s'enregistre auprès de l'entité GKSP B au moyen du message **RRQ** sécurisé H.235.1. L'entité GKSP B retransmet ce message **RRQ** au portier C après y avoir inclus un jeton de processeur contenant les trois éléments de profil de sécurité suivants:

– 0 indiquant H.235.1 (3);

– 5 contenant l'identificateur de point d'extrémité de D;

– 6 indiquant l'absence d'erreur (0),

et avoir appliqué le profil de sécurité hybride H.235.3. Comme le secret partagé dynamique H.235.3 K_{BC} a déjà été établi avant, l'entité GKSP sécurise le message **RRQ** retransmis au moyen du profil H.235.1 en appliquant la clé K_{BC}. Le portier C autorise le terminal D et répond par un message **RCF** que l'entité GKSP retransmet au terminal D.

Un certain temps après que l'appel provenant du terminal A et passant par le portier C a été établi, l'entité B décide de rafraîchir la clé K_{BC} en exécutant une procédure de mise à jour de la clé K_{BC} avec le portier C; K'_{BC} représente la nouvelle clé mise à jour.

La Figure I.5 montre également un cas d'erreur dans lequel l'entité GKSP reçoit un message RELEASE-COMPLETE en provenance du portier. L'entité GKSP B détecte l'échec de vérification de l'intégrité; ce message n'utilise pas la clé courante. Il est possible que le message provienne d'une réexécution ou d'une manipulation par un attaquant ou que le portier utilise une ancienne clé obsolète. L'entité GKSP B journalise l'événement de sécurité et élimine le message sans le retransmettre au terminal A.

A la fin de l'appel, le portier C termine l'appel.

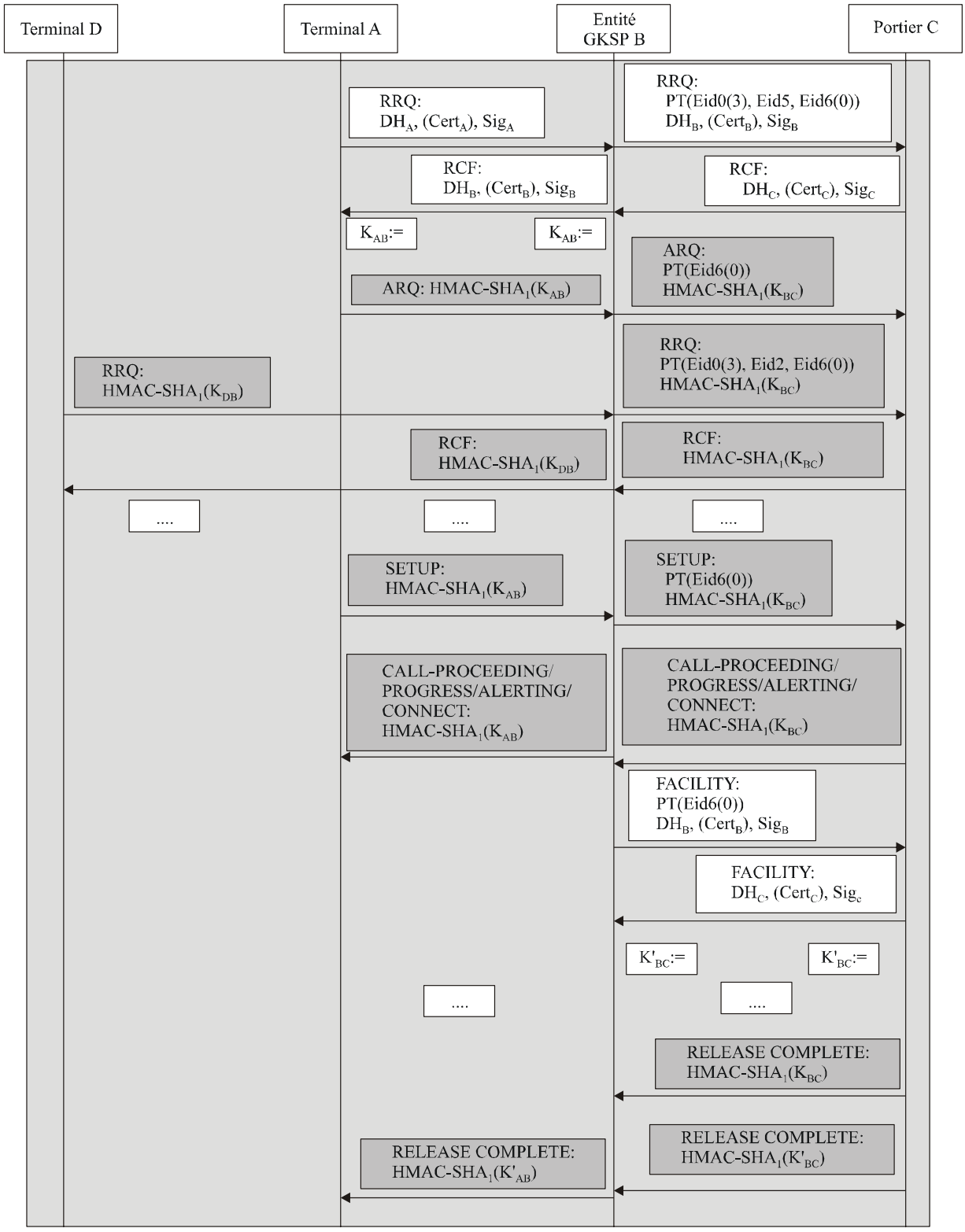


Figure I.5/H.235.3 – Déroulement d'un appel avec processeur de sécurité de portier et protection de message H.235.3 (entité GKSP vers portier)

I.5 Liste des identificateurs d'objet

Le Tableau I.2 donne l'identificateur d'objet mentionné qui est à utiliser conjointement avec le Tableau I.1.

Tableau I.2/H.235.3 – Identificateurs d'objet utilisés par l'Appendice I

Désignation de l'identificateur d'objet	Valeur(s) de l'identificateur d'objet	Description
"PT"	{itu-t (0) recommendation (0) h (8) 235 version (0) 4 15}	Utilisé pour indiquer le jeton ClearToken de processeur de portier pour les communications d'une entité GKSP vers un portier.

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