UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

H.235
Annexe F
(03/2002)

SÉRIE H: SYSTÈMES AUDIOVISUELS ET MULTIMÉDIAS

Infrastructure des services audiovisuels – Aspects système

Sécurité et cryptage des terminaux multimédias de la série H (terminaux H.323 et autres terminaux de type H.245)

Annexe F: profil de sécurité hybride

Recommandation UIT-T H.235 – Annexe F

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.399
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

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

Recommandation UIT-T H.235

Sécurité et cryptage des terminaux multimédias de la série H (terminaux H.323 et autres terminaux de type H.245)

Annexe F

Profil de sécurité hybride

Résumé

La présente annexe vise à décrire un profil de sécurité hybride efficace et modulable, fondé sur l'infrastructure de clés publiques (PKI) pour la Version 2 de la Rec. UIT-T H.235. Ce profil hybride tire parti des profils de sécurité des Annexes D et E de la Rec. UIT-T H.235 par l'utilisation du profil de sécurité élémentaire de la première et des signatures numériques de la seconde.

Source

L'Annexe F de la Recommandation H.235 de l'UIT-T, élaborée par la Commission d'études 16 (2001-2004) de l'UIT-T, a été approuvée le 29 mars 2002 selon la procédure définie dans la Résolution 1 de l'AMNT.

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.

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

Sécurité et cryptage des terminaux multimédias de la série H (terminaux H.323 et autres terminaux de type H.245)

Annexe F

Profil de sécurité hybride

F.1 Aperçu général

La présente annexe décrit un profil de sécurité hybride à base d'infrastructure de clés publiques (PKI, *public key infrastructure*), efficace et modulable, utilisant les signatures numériques de l'Annexe E/H.235 et le profil de sécurité élémentaire de l'Annexe D/H.235. La présente annexe 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 pour l'assurer en cas de nécessité.

Dans le présent contexte, "hybride" signifie que les procédures de sécurité des profils de signature de l'Annexe E/H.235 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 élémentaire de l'Annexe D/H.235 qui seront employées.

Ce profil de sécurité hybride est applicable à la téléphonie IP "mondiale" modulable; il n'est pas exposé aux limitations du profil de sécurité élémentaire simple de l'Annexe D/H.235, lorsqu'il est appliqué de manière stricte. De plus, il n'est pas exposé à certains inconvénients du profil de l'Annexe E/H.235 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 de signature ne dépend pas de l'administration (statique) de secrets mutuellement partagés dans les bonds de différents domaines. Les utilisateurs peuvent donc très facilement choisir leur fournisseur de téléphonie IP. Le profil de sécurité accepte 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 sinon aux techniques symétriques, plus simples et plus efficaces. Il assure la mise en tunnel des messages H.245 pour l'intégrité de ceux-ci. Il offre également des dispositions pour la non-répudiation des messages.

Ce profil de sécurité hybride utilise le modèle acheminé par portier; il est fondé sur les techniques de mise en tunnel H.245. La prise en charge de modèles non acheminés par portier nécessite un complément d'étude.

Les caractéristiques proposées par ces profils sont, pour les messages RAS, H.225.0 et H.245:

- l'authentification de l'utilisateur jusqu'à une entité voulue, indépendamment du nombre de bonds[1] au niveau applicatif qu'effectue le message;
- l'intégrité de toutes les parties déterminantes (champs) des messages arrivant à une entité, indépendamment du nombre de bonds au niveau applicatif qu'effectue le message.

[1] Par "bond", on entend dans le cas présent un élément de réseau H.235 de confiance (tel que portier, passerelle, pont MCU, serveur mandataire ou pare-feu). Donc, la sécurité bond par bond de niveau applicatif, lorsqu'elle est utilisée avec des techniques symétriques, ne donne pas une sécurité vraie de bout en bout entre les terminaux.

L'intégrité du message proprement dite, obtenue au moyen d'un nombre aléatoire fort est proposée en option;

- l'authentification du message bond par bond au niveau applicatif, l'intégrité et la non-répudiation (dans une certaine mesure) assurent ces services de sécurité pour l'ensemble du message;
- par l'infrastructure de clés publiques, les utilisateurs peuvent choisir le fournisseur du service. La gestion des clés pour la distribution des clés de gestion est judicieusement intégrée dans le profil de sécurité hybride.

Les services de sécurité ci-dessus assurent correctement la résistance à diverses agressions telles que les suivantes:

- *agressions par entremetteur*: l'authentification et l'intégrité du message bond par bond au niveau applicatif protègent contre de telles agressions lorsque l'entremetteur se trouve entre un bond au niveau applicatif et un routeur hostile, par exemple;
- *agressions par répétition*: l'emploi d'horodateurs et de numéros de séquence protège contre de telles agressions;
- *parodie*: l'authentification de l'utilisateur protège contre de telles agressions;
- *détournement de la connexion*: l'utilisation de l'authentification/intégrité pour chaque message de signalisation empêche de telles agressions.

F.2 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.

– Recommandation UIT-T H.225.0, Version 4 (2000), *Protocoles de signalisation d'appel et mise en paquets des trains multimédias dans les systèmes de communication multimédia en mode paquet*.

– Recommandation UIT-T H.323, Version 4 (2000), *Systèmes de communication multimédia en mode paquet*.

– 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.245, Version 8 (2001), *Protocole de commande pour communications multimédias*.

– IETF RFC 2459 (1999), *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*.

F.3 Abréviations

La présente Recommandation utilise les abréviations suivantes:

GCF confirmation de portier (*gatekeeper confirm*)

GK portier (*gatekeeper*)

GRQ demande de portier (*gatekeeper request*)

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

LRQ demande d'emplacement (*location request*)

OID identificateur d'objet (*object identifier*)

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

RCF confirmation d'enregistrement (*registration confirm*)

RRQ demande d'enregistrement (*registration request*)

RSA algorithme de cryptage de Rivest, Shamir et Adleman (*Rivest, Shamir and Adleman encryption algorithm*)

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

URQ demande d'annulation d'enregistrement (*unregistration request*)

F.4 Conventions de spécification

La description du profil de sécurité hybride utilise les termes et définitions des Annexes D et E de la Rec. UIT-T H.235.

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

Le présent profil de sécurité est applicable dans les environnements pouvant comporter de nombreux terminaux, dans lesquels l'attribution d'un mot de passe ou d'une clé symétrique n'est pas possible, par exemple les scénarios à grande échelle, voire mondiaux. Le présent profil de sécurité part plutôt de l'hypothèse de la disponibilité d'une infrastructure de clés publiques avec des certificats attribués et des clés privées ou publiques, des répertoires, etc. Par ailleurs, le présent profil de sécurité utilise, dans la mesure du possible, les techniques cryptographiques symétriques.

Le présent profil introduit les termes de "premier message" et "dernier message". 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 circulant entre deux entités H.323 qui établit un contexte de sécurité. Il met à la disposition de ces deux entités les données relatives aux clés symétriques et marque par exemple le début d'un appel. Dans le cas des messages RAS H.225.0, le premier message est le message RRQ avec le message de réponse correspondant. Dans le cas de la signalisation d'appel H.225.0 utilisant le démarrage rapide, le premier message correspond à SETUP et CONNECT.

Le "dernier message" met fin au contexte de sécurité qui a été établi. Les données relatives aux clés qui auront été établies seront 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.

Le profil de sécurité part de l'hypothèse d'un modèle d'appel acheminé par portier dans lequel est appliquée la méthode de signalisation d'appel à connexion rapide. Les messages de commande d'appel H.245 sont mis en tunnel sécurisé 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 des signatures permet de mettre en tunnel sécurisé les unités PDU de commande d'appel H.245 dans les messages de service supplémentaire H.225.0. Les mécanismes de mise à jour et de synchronisation des clés H.245 doivent être mis en tunnel pour signaler le message FACILITY de mise à jour des clés. Ces mécanismes s'avèrent utiles dans les appels de très longue durée, par exemple.

La zone en gris clair du Tableau F.1 représente les mécanismes de sécurité qui sont utilisés par le profil de sécurité hybride.

NOTE – Les certificats RSA avec hachage MD5 ne font pas partie du présent profil de sécurité.

Le profil de sécurité de cryptage vocal de l'Annexe D/H.235 (voir § D.7) pourrait être facultativement 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 F.1/H.235 – 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)	Signature numérique RSA (SHA1)	Signature numérique RSA (SHA1)	
	HMAC-SHA1-96	HMAC-SHA1-96	HMAC-SHA1-96	
Non-répudiation	(Possible sur premier message seulement)	(Possible sur premier message seulement)		
Intégrité	Signature numérique RSA (SHA1)	Signature numérique RSA (SHA1)	Signature numérique RSA (SHA1)	
	HMAC-SHA1-96	HMAC-SHA1-96	HMAC-SHA1-96	
Confidentialité				
Commande d'accès				
Gestion de clé	Attribution de certificats	Attribution de certificats		
	Echange de clés Diffie-Hellman authentifiées	Echange de clés Diffie-Hellman 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 serveurs mandataires H.235).

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

NOTE 3 – Fonction mise en tunnel H.245 ou intégrée H.245 dans une connexion rapide H.225.0.

Pour l'authentification, il convient que l'utilisateur se serve d'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 le service d'annuaire, pour les paramètres CA spécifiques, pour l'annulation des certificats, pour la mise à jour ou pour le rétablissement de paires de clés. Elle ne définit pas non plus d'autres procédures opérationnelles ou de gestion relatives à 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 annexe.

Les entités de communication concernées ont la capacité de déterminer implicitement l'utilisation du profil de sécurité élémentaire de l'Annexe D/H.235, du profil de signature de l'Annexe E/H.235 ou du présent profil de sécurité hybride dans l'évaluation des identificateurs d'objet de sécurité signalés dans les messages (**tokenOID** et **algorithmOID**; voir également § E.8).

F.5 Prescriptions H.323

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

- la connexion rapide;
- la mise en tunnel H.245;
- le modèle à routage par portier.

F.6 Authentification et intégrité

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

- **authentification et intégrité**: service de sécurité combiné prenant en charge l'intégrité de message en plus de l'authentification de l'utilisateur. L'utilisateur s'authentifie par la signature numérique correcte d'un élément de données, au moyen de la clé privée ou par l'application correcte d'un secret partagé correspondant. Cela protège en outre le message 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 qu'en mode bond par bond.

NOTE – L'utilisation des signatures numériques permet de prendre en charge un service de sécurité de non-répudiation; cela dépend aussi des réglages des bits d'utilisation de la clé de signature dans le certificat (voir également RFC 2459).

Les procédures ci-après sont destinées à être utilisées dans le présent profil.

La procédure IV est fondée sur des signatures numériques utilisant une paire de clés privées/publiques et des 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 modulable 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.

Les portiers qui détectent une authentification qui n'a pas abouti et/ou une validation de l'intégrité qui n'a pas abouti non plus dans un message RAS/signalisation d'appel reçu d'un terminal ou d'un portier homologue répondent par un message de rejet correspondant indiquant l'absence de sécurité par la mise du motif de rejet à **securityDenial,** ou par un code d'erreur de sécurité conforme au § B.2/H.235. Dans sa réponse, l'expéditeur peut donner une liste de certificats acceptables dans des jetons individuels afin de faciliter le choix du destinataire.

Une signalisation H.235 implicite permet d'indiquer l'utilisation de la procédure IV et le mécanisme de sécurité appliqué sur la base de la valeur des identificateurs d'objet (voir également § F.12) et les champs de message qui ont été remplis. Les identificateurs d'objet sont désignés symboliquement au moyen de lettres (par exemple "A") dans le présent texte.

Ce profil n'utilise pas les champs ICV H.235; au lieu de cela, les valeurs de contrôle d'intégrité cryptographique sont placées dans le champ **signature** du jeton **token** du **cryptoSignedToken**, lorsqu'il se réfère à l'Annexe E, ou bien les valeurs de contrôle d'intégrité sont placées dans les champs de hachage de **CryptoToken** s'il se réfère à l'Annexe D.

F.7 Procédure IV

Si on utilise la procédure IV pour la sécurité en mode bond par bond, il est nécessaire de se conformer aux procédures ci-après. La présente procédure réunit la procédure I de l'Annexe D (voir § D.6.3.2) et la procédure II de l'Annexe E (voir § E.5).

Pour le premier message, comportant la réponse correspondante, envoyé dans chaque sens, on utilise la procédure de l'Annexe E (authentification et intégrité en mode bond par bond, voir § E.5) avec les valeurs suivantes:

- identificateur OID "A1" au lieu de "A" et identificateur OID "S1" au lieu de "S". L'emploi de ces identificateurs OID permet d'identifier le profil de sécurité hybride;
- identificateur **algorithmOID** de **tokenOID** sera mis à "W" pour indiquer l'utilisation de la signature RSA-SHA1;
- le champ **signature** contiendra une signature RSA codée en ASN.1 (voir § E.10/H.235);
- le champ **certificate** contiendra le certificat d'utilisateur de l'expéditeur s'il n'est pas autrement accessible par le destinataire.

Dans un scénario à un seul domaine administratif, le premier message/réponse est défini comme étant le message/réponse RSA 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.

L'expéditeur et le destinataire échangent et calculent une chaîne de bits secrète de Diffie-Hellman authentifiée. Le Tableau D.4/H.235 donne un exemple de paramètres de groupe de Diffie-Hellman et recommande de choisir si possible, pour des raisons de sécurité, une clé primaire de 1 024 bits. Le secret Diffie-Hellman sera calculé pour chaque tronçon indépendamment de l'utilisation du profil de cryptage, vocal ou non.

A partir de la chaîne des bits 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 l'Annexe D.

Dans un scénario à portiers dans des domaines administratifs distincts, l'expéditeur et le destinataire utiliseront 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 § D.7.1). Cela est uniquement nécessaire en cas d'utilisation du cryptage 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 l'Annexe D. Le jeton **tokenOID** de ce **ClearToken** sera mis à "Q", indiquant 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 § D.7.1).

NOTE – Dans le cas des environnements à routage indirect, les entités et terminaux d'expéditeur/destinataire correspondent. Dans les environnements à routage par portier, la clé de liaison est partagée en mode 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 renverra 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, on utilisera la procédure I de l'Annexe D (voir § D.6.3.2). 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 asymétrique n'est pas requise, les moyens de l'Annexe D/H.235 étant suffisants.

La présente annexe peut être utilisée avec des systèmes H.235 Version 1 si l'on tient compte de l'utilisation restreinte des identificateurs ID et generalID des expéditeurs, comme indiqué dans le paragraphe E.17/H.235.

F.8 Association de sécurité pour appels simultanés

Une optimisation a été prévue pour les cas dans lesquels une paire d'entités fixe 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 une paire fixe d'entités 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 connexion de signalisation d'appel unique, il ne faut établir qu'une seule liaison commune (voir Figure F.1).

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

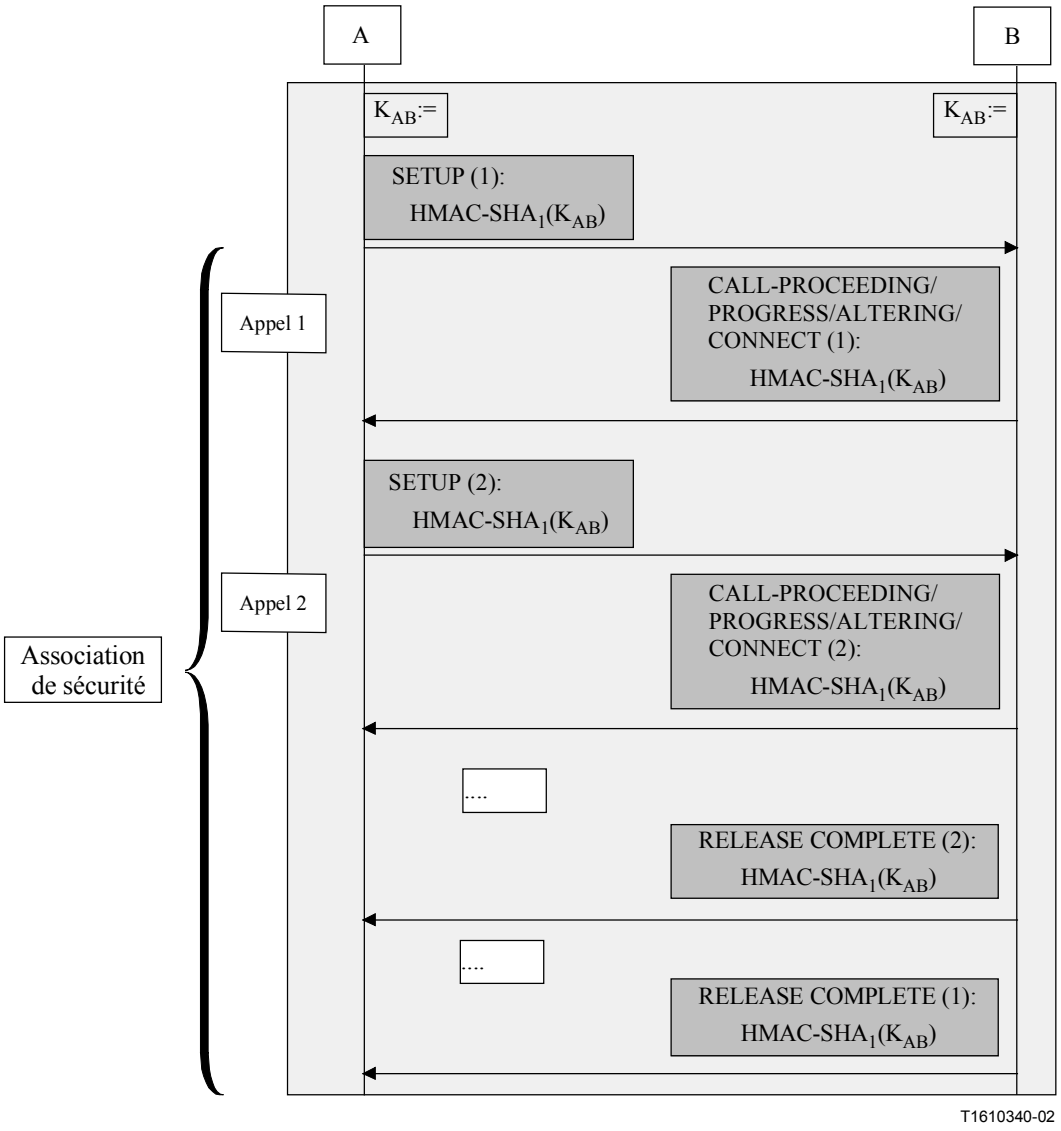


Figure F.1/H.235 – Association de sécurité pour appels simultanés

F.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 par une autre. Une telle mise à jour de la clé devrait être lancée par celui des deux correspondants 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'expéditeur demande la mise à jour de la clé au moyen du message FACILITY. Celui-ci achemine alors un nouveau jeton de Diffie-Hellman, un certificat numérique facultatif et la signature numérique de l'expéditeur. 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. Jusqu'à la fin de la procédure de mise à jour de la clé, l'expéditeur et le destinataire utilisent la nouvelle clé de liaison calculée.

- le champ **tokenOID** de **ClearToken** dans le message FACILITY sera mis à "Q", indiquant l'utilisation de la clé 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 § D.7.1).

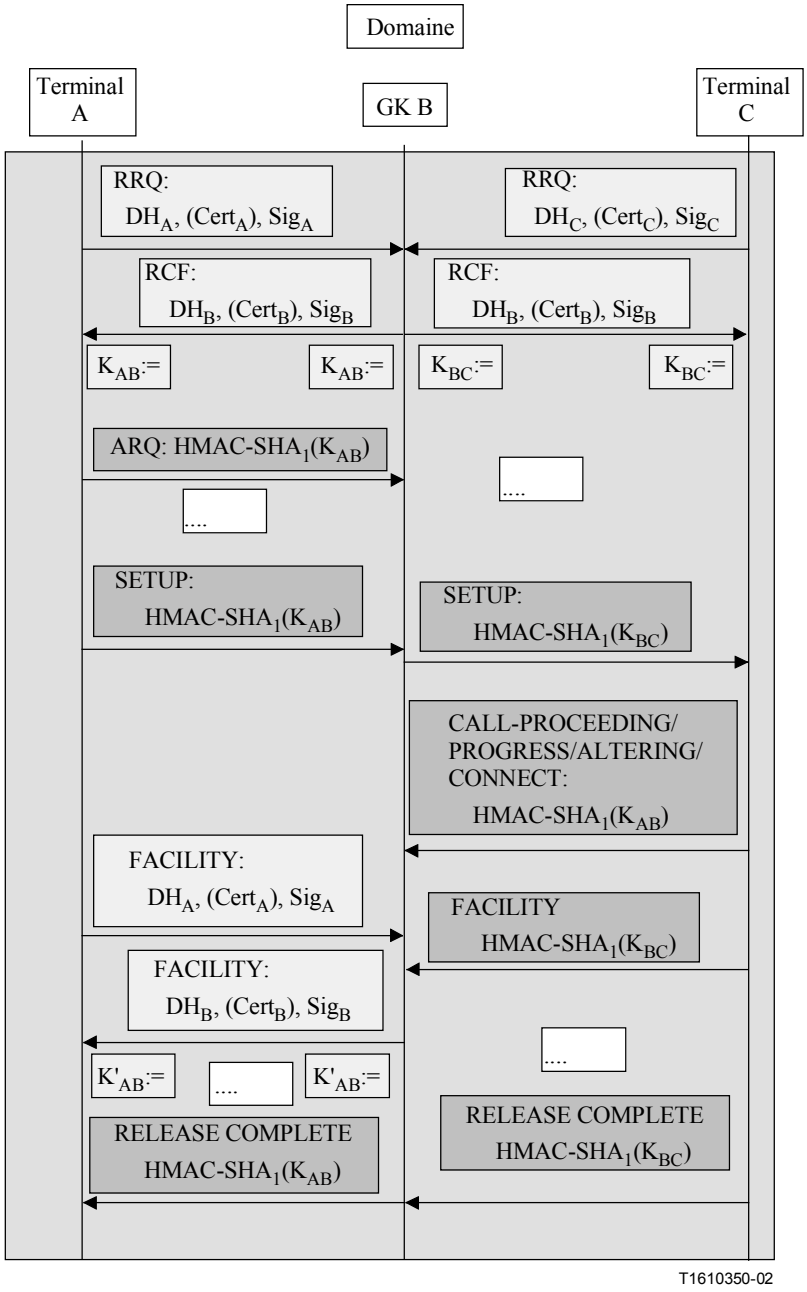
Le message FACILITY pour la mise à jour de la clé sera protégé conformément à la procédure II de l'Annexe E/H.235. Tout autre message FACILITY sans jeton de Diffie-Hellman ne sera pas utilisé pour la mise à jour de la clé et sera protégé conformément à la procédure I de l'Annexe D/H.235.

F.10 Exemples avec organigrammes

Les diagrammes des Figures F.2 et F.3 présentent l'utilisation du profil de l'Annexe F 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 de signature de l'Annexe E/H.235 et les messages ombrés de gris foncé au profil de base de l'Annexe D/H.235. Les figures mettent l'accent sur les parties touchant à la sécurité (les plus importantes) de chaque message (CryptoTokens H.235, jetons) et omettent les détails.

Le diagramme de la Figure F.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.

NOTE 1 – Les Figures F.2 et F.3 ci-après traitent de 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, on suppose le mode de démarrage non rapide conformément au § 7.3.1/H.323. La Figure F.2 montre également la procédure de mise à jour de la clé par le Terminal A et le Portier B au moyen du message FACILITY.



Cert	Certificat d'utilisateur	K, K'	Clé de liaison symétrique
DH_A	Jeton g^a mod p Diffie-Hellman	Sig	Signature numérique
DH_B	Jeton g^b mod p Diffie-Hellman		
EP	Point d'extrémité (Terminal)		
GK	Portier		

Figure F.2/H.235 – Flux de messages dans un domaine administratif unique

La Figure F.3 présente un exemple de flux de messages dans un scénario à plusieurs domaines administratifs différents. Alors que le profil de sécurité hybride est appliqué dans chaque domaine entre le terminal et le portier comme indiqué à la Figure F.2, le profil de sécurité hybride peut également être appliqué entre deux domaines pendant la phase d'établissement de l'appel.

NOTE 2 – La Figure F.3 omet toute communication entre éléments frontières (BE, *border elements*) et toute communication entre portier et éléments frontières. La Figure F.3 montre également la procédure de mise à jour de la clé par les deux domaines au moyen du message FACILITY.

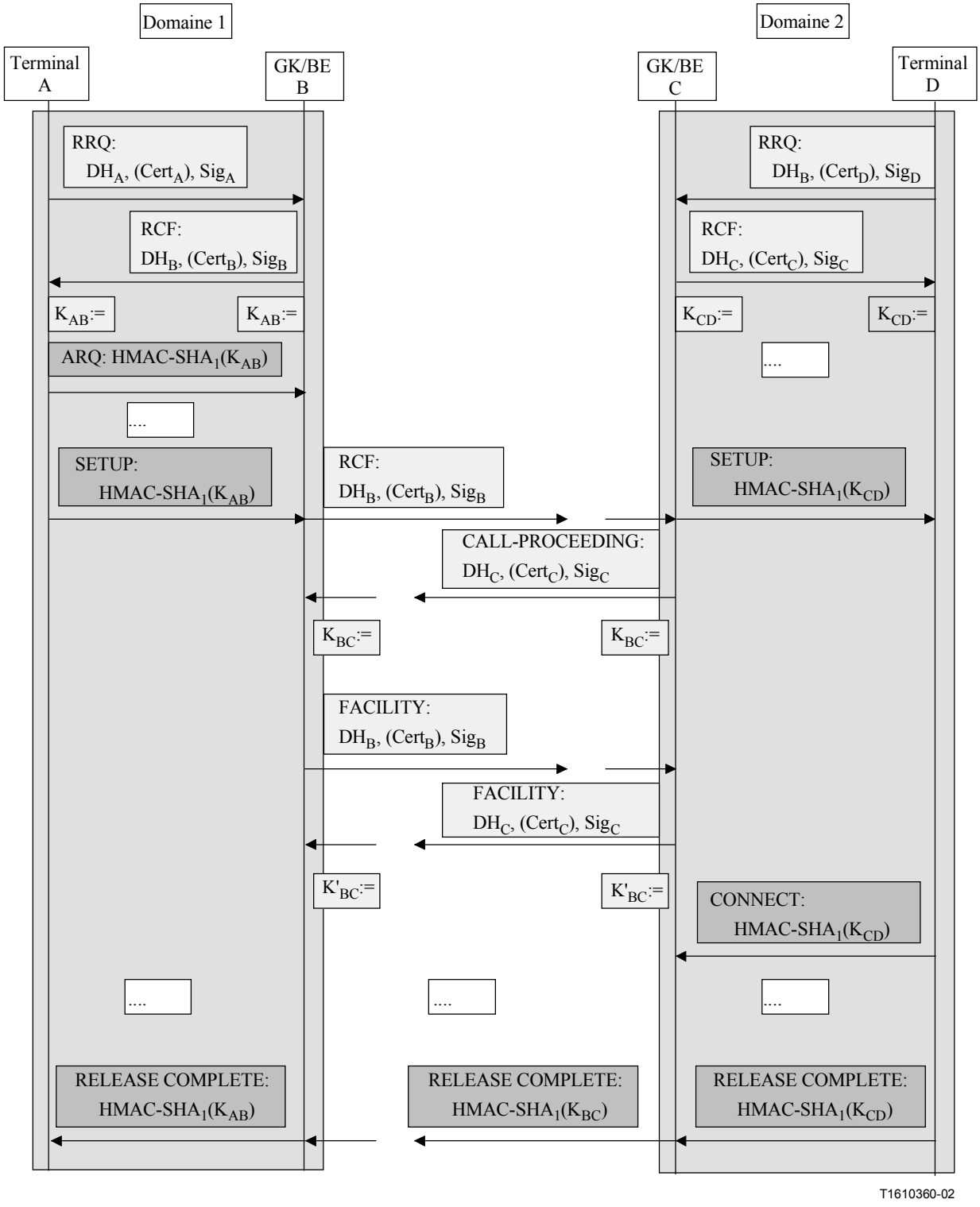


Figure F.3/H.235 – Flux de messages dans un domaine à plusieurs administrations

F.11 Messages multidiffusion

Les messages H.225.0 multidiffusion tels que **GRQ** et **LRQ** engloberont 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 englobent un champ **CryptoToken** ayant un identificateur **generalID** défini.

F.12 Liste des messages de signalisation de sécurité

La procédure IV utilise la procédure I de l'Annexe D ou la procédure II de l'Annexe E, selon le scénario et le message proprement dit, comme indiqué ci-dessous.

F.12.1 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, les procédures II sont appliquées avec les champs de sécurité **CryptoToken** définis. NOTE 2 – Les messages de découverte de portier et les messages à plusieurs destinataires ne sont pas envoyés.			

F.12.2 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[a)], Facility-UUIE[b)], 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[c)]	CryptoToken	Procédure II	Procédure II
a) A supposer que chaque message soit le premier dans chaque sens. b) N'importe lequel de ces messages survient comme premier message dans chaque sens. c) Utilisé pour la mise à jour de la clé.			

F.12.3 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[a)], Alerting-UUIE[b)], CallProceeding-UUIE, Facility-UUIE[c)], Progress-UUIE, Information-UUIE, ReleaseComplete-UUIE	CryptoToken, ClearToken	Procédure II	Procédure II
Alerting-UUIE[d)], CallProceeding-UUIE, Facility-UUIE[e)], Progress-UUIE, Information-UUIE, ReleaseComplete-UUIE, Status-UUIE, StatusInquiry-UUIE, SetupAcknowledge-UUIE, Notify-UUIE	CryptoToken, ClearToken	Procédure I	Procédure I

a) A supposer que chaque message soit le premier dans chaque sens.

b) N'importe lequel de ces messages survient comme premier message dans chaque sens.

c) Utilisé pour la mise à jour de la clé.

d) Aucun de ces messages ne survient comme premier message dans chaque sens.

e) Pas utilisé pour la mise à jour de la clé.

F.13 Liste d'identificateurs d'objet

Le Tableau F.2 énumère tous les identificateurs OID mentionnés.

Tableau F.2/H.235 – Identificateurs d'objet utilisés par l'Annexe F

Référence 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 l'Annexe E pour CryptoToken-tokenOID indiquant que la signature RSA ou le hachage englobe tous les champs du message RAS/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 l'Annexe E pour 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 comme identification d'algorithme indiquant l'utilisation d'une signature numérique à base RSA SHA1.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série B	Moyens d'expression: définitions, symboles, classification
Série C	Statistiques générales des télécommunications
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	RGT et maintenance des réseaux: systèmes de transmission, circuits téléphoniques, télégraphie, télécopie et circuits loués internationaux
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 et communication entre systèmes ouverts
Série Y	Infrastructure mondiale de l'information et protocole Internet
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Genève, 2002