Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

H.235

Annexe G

(01/2005)

SÉRIE H: SYSTÈMES AUDIOVISUELS ET MULTIMÉDIAS

Infrastructure des services audiovisuels – Aspects système

Sécurité et chiffrement pour les terminaux multimédias de la série H (terminaux H.323 et autres terminaux de type H.245)

Annexe G: Utilisation du protocole de gestion de clés MIKEY en association avec le protocole de transport en temps réel sécurisé (SRTP) dans les systèmes H.235

Recommandation UIT-T H.235 – Annexe G

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

Sécurité et chiffrement pour les terminaux multimédias de la série H (terminaux H.323 et autres terminaux de type H.245)

Annexe G

Utilisation du protocole de gestion de clés MIKEY en association avec le protocole de transport en temps réel sécurisé (SRTP) dans les systèmes H.235

Résumé

L'Annexe G/H.235 recommande des procédures de sécurité pour les systèmes H.323/H.235 qui utilisent le protocole de gestion de clés MIKEY IETF conjointement avec le protocole de sécurité SRTP IETF.

Cette annexe est écrite sous la forme d'un profil de sécurité H.235 qui est offert en option et qui peut compléter les autres fonctionnalités de sécurité de média H.235 (Annexe B, Annexe D.7).

L'Annexe G/H.235 permet de mettre en œuvre une sécurité de média SRTP pour laquelle la gestion de clés MIKEY fournit les clés et les paramètres de sécurité nécessaires aux points d'extrémité concernés de bout en bout. L'Annexe G peut être mise en œuvre dans un domaine H.323 parmi des systèmes H.323 conformes à l'Annexe G/H.235. Elle définit les extensions en termes de protocole de sécurité relatives aux messages RAS et à la signalisation d'appel H.225.0 ainsi qu'au protocole H.245 et définit aussi les procédures correspondantes. Elle spécifie en outre les capacités permettant de prendre en charge l'interfonctionnement avec les entités SIP IETF qui ont implémenté la gestion de clés MIKEY et le protocole SRTP.

Source

L'Annexe G de la Recommandation UIT-T H.235 a été approuvée le 8 janvier 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

Chiffrement de média, gestion de clés MIKEY, profil de sécurité, protocole de transport en temps réel sécurisé, sécurité multimédia, SRTP.

AVANT-PROPOS

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

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

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

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

NOTE

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

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

DROITS DE PROPRIÉTÉ INTELLECTUELLE

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

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

TABLE DES MATIÈRES

Recommandation UIT-T H.235

Sécurité et chiffrement pour les terminaux multimédias de la série H (terminaux H.323 et autres terminaux de type H.245)

Annexe G

Utilisation du protocole de gestion de clés MIKEY en association avec le protocole de transport en temps réel sécurisé (SRTP) dans les systèmes H.235

G.1 Domaine d'application

L'Annexe G/H.235 recommande des procédures de sécurité pour les systèmes H.323/H.235 qui utilisent le protocole de gestion de clés MIKEY conjointement avec le protocole de sécurité SRTP.

Le profil de sécurité ainsi défini est offert en option et peut compléter les autres fonctionnalités de sécurité de média H.235 (Annexe B, Annexe D.7).

G.2 Références

G.2.1 Références normatives

Les Recommandations UIT-T et autres références suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions de la présente Recommandation. Au moment de la publication, les éditions indiquées étaient en vigueur. Les Recommandations et autres références étant sujettes à révision, les utilisateurs de la présente Recommandation sont invités à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et autres références énumérées ci-dessous. Une liste des Recommandations UIT-T en vigueur est publiée périodiquement. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut de Recommandation.

[H.225.0] 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*.

[H.235] Recommandation UIT-T H.235, version 3 (2003), *Sécurité et chiffrement pour les terminaux multimédias de la série H (terminaux H.323 et autres terminaux de type H.245)*, plus Amd.1 (2004).

[H.245] Recommandation UIT-T H.245 (2005), *Protocole de commande pour communications multimédias*.

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

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

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

[RFC 3550] H. Schulzrinne, S. Casner *et al*: RTP: A Transport Protocol for Real-Time Applications, *RFC 3550, IETF*, 07/2003.

[RFC 3711] M. Baugher *et al*: The Secure Real Time Transport Protocol, *RFC 3711, IETF,* 03/2004.

[RFC 3830] J. Arkko, E. Carrara, F. Lindholm, M. Naslund, K. Norrman: MIKEY: Multimedia Internet KEYing, *RFC 3830, IETF*, 08/2004.

G.2.2 Références non normatives et bibliographie

[RFC 1305] D. Mills: Network Time Protocol (Version 3) Specification, Implementation and Analysis, *RFC 1305, IETF*, mars 1992.

[RFC 2327] M. Handley, V. Jacobson: SDP: Session Description Protocol, *RFC 2327, IETF*, avril 1998.

[RFC 2631] E. Rescorla: Diffie-Hellman Key Agreement Method, *RFC 2631, IETF,* juin 1999.

[RFC 3261] J. Rosenberg *et al*: SIP: Session Initiation Protocol, *RFC 3261, IETF,* juin 2002.

[RFC 3264] J. Rosenberg and H. Schulzrinne: An Offer/Answer Model with Session Description Protocol (SDP), *RFC 3264, IETF*, juin 2002.

[SDP-New] M. Handley, Van Jacobson, C. Perkins: SDP: Session Description Protocol, *draft-ietf-mmusic-sdp-new-24.txt, IETF*, 02/2005.

[KMGMT-ext] J. Arkko, E. Carrara *et al*: Key Management Extensions for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP), *Internet Draft draft-ietf-mmusic-kmgmt-ext-14.txt, Work in Progress, IETF*, 03/2005.

[MIKEY-DHHMAC] M. Euchner: HMAC-authenticated Diffie-Hellman for MIKEY, *Internet Draft draft-ietf-msec-MIKEY-DHHMAC-11.txt, Work in Progress, IETF*, 04/2005.

G.3 Termes et définitions

Pour les besoins de la présente Recommandation sont utilisées les définitions figurant au § 3 des Recommandations UIT-T H.323, H.225.0, H.235 et X.800 ainsi que celles qui figurent dans le présent paragraphe.

G.3.1 lot de sessions de chiffrement (CSB, *crypto session bundle*): ensemble d'une ou plusieurs sessions de chiffrement qui possèdent des clés TGK et des paramètres de sécurité communs. Un lot CSB peut également comprendre uniquement les paramètres de politique de sécurité MIKEY (voir [RFC 3830]).

G.3.2 domaine H.323: comprend une seule zone de portier ou un réseau H.323 parmi plusieurs zones de portier H.323.

G.4 Symboles et abréviations

La présente annexe utilise les abréviations suivantes:

{} zéro, une ou plusieurs occurrences

[] élément facultatif

a, b, e, d clé DH privée du point d'extrémité A, du point d'extrémité B, du portier E, du portier D

Cert certificat numérique (voir RFC 3830)

CP/C appel en cours de connexion (*callproceeding-to-connect*)

CSB lot de sessions de chiffrement (*crypto session bundle*) (voir RFC 3830)

CT_B, CT_A	ClearToken pour le point d'extrémité B, ClearToken pour le point d'extrémité A (voir l'Annexe I/H.235)
DH	Diffie-Hellman
DH_A	demi-clé DH du point d'extrémité A
DH_B	demi-clé DH du point d'extrémité B
DRC	appel à routage direct ou appel à cheminement direct (*direct-routed call*) (voir l'Annexe I/H.235)
$ENC_k(x)$	chiffrement de *X* à l'aide de la clé *k* (*encryption of X using key k*)
env_key	clé d'enveloppe (*envelope key*) (RFC 3830) entre les points d'extrémité B et A
EP	point d'extrémité (*endpoint*)
ESC	commande de fin de session H.245 (*endsessioncommand*)
g^a, g^b	demi-clé Diffie-Hellman du point d'extrémité A, du point d'extrémité B
g^e, g^d	demi-clé Diffie-Hellman du portier E, du portier D
GK	portier (*gatekeeper*)
HDR	charge utile d'en-tête MIKEY (*MIKEY header payload*) (voir RFC 3830)
ID_A, ID_B	identité du point d'extrémité A, identité du point d'extrémité B
IETF	Groupe de travail d'ingénierie Internet (*Internet Engineering Task Force*)
Imsg	message MIKEY de l'initiateur (*MIKEY message of the initiator*) (voir RFC 3830)
KEMAC	message de charge utile KEMAC MIKEY (*MIKEY KEMAC payload message*) (voir RFC 3830)
Ma	clé d'authentification MIKEY (*MIKEY authentication key*) (voir RFC 3830)
MAC(*k*, *x*)	code MAC avec clé *k* appliqué à *x*
Me	clé de chiffrement MIKEY (*MIKEY encryption key*) (voir RFC 3830)
MIKEY	gestion de clés Internet multimédia (*multimedia Internet keying*)
NTP	protocole relatif au temps dans le réseau (*network time protocol*)
PKE	message de charge utile PKE MIKEY (*MIKEY PKE payload message*) (voir RFC 3830)
PKI	infrastructure de clé publique (*public-key infrastructure*)
PRF	fonction pseudo-aléatoire (*pseudo-random function*) (MIKEY-PRF, voir sections 4.1.2 à 4.1.5 du Document RFC 3830)
Rand	pointeur aléatoire (*random nonce*) (voir RFC 3830)
rand()	valeur aléatoire (*random value*)
Rmsg	message MIKEY du répondeur (*MIKEY message of the responder*) (voir RFC 3830)
RSA	Rivest, Shamir et Adleman (algorithme à clé publique)
sa, *sb*	secret partagé entre le point d'extrémité A et un portier, secret partagé entre le point d'extrémité B et un portier
sl	secret partagé entre portiers
SDP	protocole de description de session (*session description protocol*)

SHA1 algorithme de hachage sécurisé 1 (*secure hash algorithm 1*) (ISO 10118-3)

SIP protocole d'ouverture de session (*session initiation protocol*)

SP politique de sécurité (*security policy*) (voir RFC 3830)

SRTCP protocole de commande de transport en temps réel sécurisé (*secure real-time transport control protocol*)

SRTP protocole de transport en temps réel sécurisé (*secure real-time transport protocol*) (voir [RFC 3711])

SSRC source de synchronisation (*synchronization source*) (RTP)

T horodate (*timestamp*) (voir RFC 3830)

TGK clé de génération de clé TEK (*TEK generating key*) (voir RFC 3830) entre les points d'extrémité A et B

V message de vérification (voir RFC 3830)

ZZ_{AB} secret H.323 partagé dynamique

G.5 Conventions

Les identificateurs d'objet sont cités sous la forme d'une référence symbolique dans le texte (par exemple "G1"). Les paragraphes G.8.4 et G.9.5 donnent les valeurs numériques des identificateurs d'objet symboliques. Pour plus d'informations, voir aussi le § 5/H.235.

Le Tableau G.1 définit les cinq protocoles de gestion de clés MIKEY qui sont cités tout au long de la présente annexe.

Tableau G.1/H.235 – Protocoles de gestion de clés MIKEY

Protocole MIKEY	Description	Valeur de l'identificateur d'objet	Identificateur de paramètre	Implémentation
MIKEY	N'importe quel protocole MIKEY	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 76}	76	Obligatoire
MIKEY-PS	Protocole de distribution de clés symétriques utilisant des clés symétriques prépartagées et des codes HMAC, voir [RFC 3830].	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 72}	72	Obligatoire
MIKEY-DHHMAC	Protocole de concordance de clés Diffie-Hellman utilisant des clés symétriques prépartagées et des codes HMAC; voir [MIKEY-DHHMAC].	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 73}	73	Facultative

Tableau G.1/H.235 – Protocoles de gestion de clés MIKEY

Protocole MIKEY	Description	Valeur de l'identificateur d'objet	Identificateur de paramètre	Implémentation
MIKEY-PK-SIGN	Protocole de distribution de clés publiques (fondé sur l'algorithme RSA) utilisant des signatures numériques; voir [RFC 3830].	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 74}	74	Obligatoire
MIKEY-DH-SIGN	Protocole de concordance de clés Diffie-Hellman utilisant des signatures numériques; voir [RFC 3830].	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 75}	75	Facultative

MIKEY (voir la 1re ligne du Tableau G.1) désigne la famille de protocoles MIKEY en général, sans indiquer de variante particulière MIKEY (MIKEY-PS, MIKEY-DHHMAC, MIKEY-PK-SIGN ou MIKEY-DH-SIGN). Son implémentation doit inclure le traitement des messages MIKEY, par exemple la charge utile d'en-tête commun MIKEY (section 6.1 du Document [RFC 3830]), mais ne nécessite pas obligatoirement d'implémenter un protocole de gestion de clés MIKEY particulier ou d'implémenter une charge utile informationnelle MIKEY particulière. L'identificateur d'objet et l'identificateur de paramètre correspondants doivent être utilisés dans les cas où un point d'extrémité H.323 ne sait pas quelle variante de protocole MIKEY est effectivement utilisée. Dans tous les autres cas, il est recommandé d'utiliser l'identificateur d'objet et l'identificateur de paramètre propres à la variante de protocole de gestion de clés MIKEY effectivement utilisée.

G.6 Introduction

Il s'avère intéressant d'utiliser les fonctionnalités de sécurité du protocole de transport en temps réel sécurisé (SRTP) IETF dans les systèmes H.235 [H.235]. Les anciennes versions de la Rec. UIT-T H.235 offrent déjà diverses fonctionnalités de sécurité de média (chiffrement par bloc des signaux vocaux par exemple) et une authentification RTP limitée (option antispam), mais la mise en œuvre du protocole SRTP répond à plusieurs objectifs importants:

- utiliser un chiffrement de flux afin d'améliorer la performance, la robustesse et la sécurité;
- assurer l'interopérabilité avec les autres terminaux SRTP, par exemple les terminaux médias fondés sur le protocole SIP;

  NOTE – La présente annexe ne spécifie pas de procédures de sécurité pour l'interfonctionnement avec le protocole SIP [RFC 3261]; ce sujet nécessite un complément d'étude.
- offrir une meilleure sécurité pour la protection RTCP;
- obtenir une meilleure intégrité couvrant la totalité du paquet RTP/RTCP;
- mettre en œuvre l'algorithme de chiffrement AES moderne;
- utiliser des clés de chiffrement/authentification de session obtenues à partir d'une fonction pseudo-aléatoire aux deux extrémités.

En outre, il s'est avéré nécessaire de définir une gestion de clés fondée sur l'algorithme RSA en plus des systèmes de concordance de clés Diffie-Hellman spécifiés dans la Rec. UIT-T H.235. De même, des techniques de gestion de clés non fondées sur l'infrastructure PKI sont jugées utiles dans le cas

où on considère que les infrastructures de clé publique ne sont pas adaptées. Par ailleurs, on estime utile de prendre en considération l'interception licite dans le contexte de la gestion de clés.

L'IETF s'est aussi attaché à définir un système de gestion de clés en temps réel MIKEY [RFC 3830]. Ce système de gestion de clés générique s'interface bien avec le protocole SRTP et est capable d'offrir des clés principales (clés TGK) et des clés de trafic de session de bout en bout ou éventuellement de bout à milieu/saut par saut. Le système MIKEY est un protocole de gestion de clés optimisé qui est exécuté en deux messages au maximum, ce qui le rend idéal pour l'établissement d'appel avec démarrage rapide H.323.

La présente annexe définit des procédures de sécurité applicables à la mise en œuvre des protocoles de gestion de clés MIKEY dans les systèmes H.323/H.235 afin de prendre en charge la sécurité de média SRTP. Il est à noter qu'il existe peut-être d'autres solutions de prise en charge du protocole SRTP dans les systèmes H.323/H.235 mais ces autres solutions ne sont pas traitées dans la présente annexe et nécessitent un complément d'étude.

Dans la présente annexe, les protocoles de gestion de clés MIKEY sont mis en œuvre de manière analogue sur le plan conceptuel à l'approche décrite dans le Document [KMGMT-ext], où le protocole SIP ([RFC 3261]) utilise le système MIKEY dans le protocole SDP ([RFC 2327], [SDP-New] et [RFC 3264]).

La présente annexe définit deux profils de sécurité avec des procédures de sécurité pour deux infrastructures de sécurité très différentes:

- infrastructure de sécurité fondée sur des clés symétriques prenant en charge plusieurs portiers (voir le § G.8);
- infrastructure de sécurité fondée sur des clés asymétriques (PKI) prenant en charge plusieurs portiers (voir le § G.9).

G.7 Aperçu général et scénarios

La Figure G.1 représente le scénario général sur lequel porte la présente annexe. Au moins deux points d'extrémité H.323 distincts A et B font partie de ce scénario. Ces points d'extrémité peuvent être des terminaux H.323 ou des passerelles médias H.323, ces dernières pouvant présenter une interface avec les autres réseaux fondés sur une transmission par paquets ou sur un autre mode de transmission. En outre, on suppose que l'environnement contient au moins un portier. Lorsqu'un seul portier est disponible, on suppose que tous les points d'extrémité H.323 sont compris dans la zone de ce portier. Lorsqu'il existe plusieurs portiers en chaîne, les points d'extrémité H.323 peuvent se trouver dans des zones de portier différentes. On suppose par ailleurs que les points d'extrémité H.323 communiquent directement de bout en bout au moyen du protocole de média RTP.

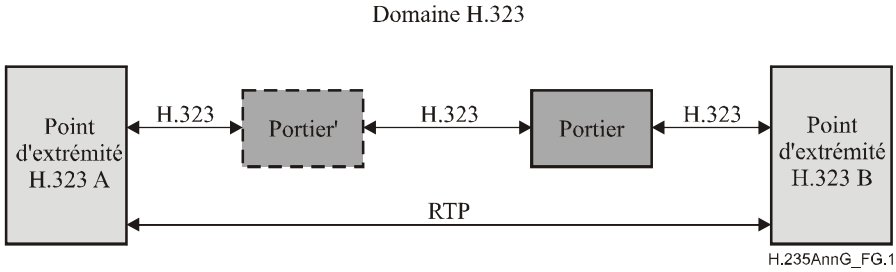

Figure G.1/H.235 – Scénario

La Figure G.2 représente le scénario de sécurité général avec les protocoles de gestion de clés MIKEY et le protocole de sécurité de média SRTP. Les protocoles de gestion de clés MIKEY sont exécutés entre les points d'extrémité H.323 A et B, ils sont encapsulés dans des conteneurs dans les messages de prise de contact de la signalisation H.245 (messages TerminalCapabilitySet, RequestMode, OpenLogicalChannel et **MiscellaneousCommand**) et sont transparents pour le ou les portiers intermédiaires.

Il est à noter qu'un point d'extrémité H.323 peut en fait être une passerelle, qui peut par exemple, contenir une fonction d'interfonctionnement servant d'interface avec des systèmes SIP. Dans ce cas, la passerelle ne termine pas nécessairement les protocoles MIKEY mais peut servir de relais pour ces protocoles et les prolonger afin d'assurer une véritable gestion de clés de bout en bout entre les terminaux multimédias concernés, assurant ainsi une sécurité de média de bout en bout avec le protocole SRTP. Cette approche permet d'assurer l'interfonctionnement sur le plan de la sécurité entre systèmes H.323/H.235 et systèmes SIP. La fonctionnalité ou la spécification exacte de l'interfonctionnement de ces passerelles n'est pas traitée dans la présente annexe et nécessite un complément d'étude.

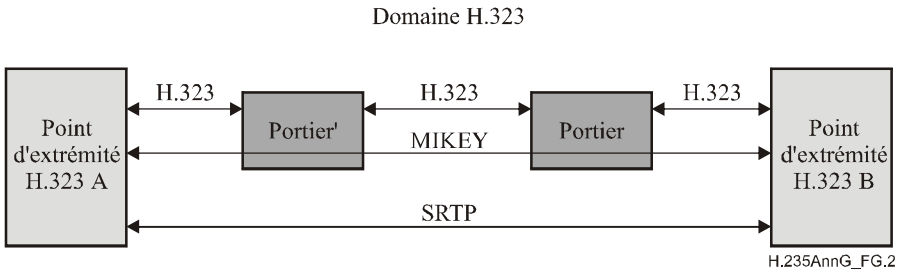

Figure G.2/H.235 – Scénario de sécurité avec MIKEY et SRTP

Tous les protocoles de gestion de clés décrits dans la présente annexe comprennent deux étapes:

- l'étape 1 se produit pendant la phase d'échange de messages RAS et de signalisation d'appel H.225.0. Pour les protocoles MIKEY à clés symétriques (MIKEY-PS et MIKEY-DHHMAC), cette étape sert à établir un secret partagé de bout en bout ZZ_{AB} entre les points d'extrémité A et B, il s'agit d'un secret prépartagé pour les protocoles MIKEY. Pour les protocoles MIKEY asymétriques (MIKEY-PK-SIGN et MIKEY-DH-SIGN), cette étape sert à établir un secret partagé dynamique entre le point d'extrémité et le saut suivant (généralement le portier qui le dessert); le secret partagé dynamique n'est pas lié aux protocoles MIKEY mais sert à sécuriser la signalisation d'appel H.225.0 entre le point d'extrémité et le saut suivant;
- l'étape 2 se produit pendant les phases de signalisation d'appel H.225.0 et de protocole H.245. Cette étape sert à négocier et à exécuter le protocole MIKEY (MIKEY-PS, MIKEY-DHHMAC, MIKEY-PK-SIGN ou MIKEY-DH-SIGN) entre les points d'extrémité A et B et à établir la clé TGK MIKEY. Pendant l'étape 2, les points d'extrémité MIKEY peuvent également exécuter un recalcul de clé ou une mise à jour de clé MIKEY pour renouveler ou mettre à jour la clé TGK. La terminaison d'un appel et l'élimination de la clé (TGK) peuvent également avoir lieu au cours de l'étape 2.

G.7.1 Exécution des protocoles MIKEY au "niveau session"

Les protocoles de gestion de clés MIKEY peuvent être exécutés au "niveau session", autrement dit la clé TGK MIKEY est appliquée à plusieurs flux médias. Il est recommandé d'exécuter les protocoles MIKEY au "niveau session" au cours de l'échange de messages de prise de contact TerminalCapability.

TerminalCapabilitySet doit utiliser **h235SecurityCapability, genericH235SecurityCapability** étant utilisé dans **encryptionAuthenticationAndIntegrity** comme suit:

- **capabilityIdentifier** doit contenir l'un des identificateurs d'objet MIKEY dans **standard**;
- **maxbitRate** et **collapsing** restent non utilisés;
- **nonCollapsing** avec l'ensemble suivant de **GenericParameters** lorsque les protocoles MIKEY sont exécutés au "niveau session" pour tous les canaux logiques:
  - **parameterIdentifier**: dans **standard** avec la valeur 0 pour indiquer que les protocoles MIKEY sont exécutés au "niveau session";
  - **parameterValue** avec le message codé binaire (I ou R) MIKEY dans **octetString**;
  - **supersedes** reste vide/non utilisé;
- **nonCollapsingRaw** reste non utilisé;
- **transport** (non utilisé ou paramètres de transport par défaut).

OpenLogicalChannel et **OpenLogicalChannelAck** ne doivent pas utiliser **encryptionSync** lorsque les protocoles MIKEY sont exécutés au "niveau session". De même, **RequestMode** ne doit pas utiliser **genericModeParameters** de **ModeElement** pour les protocoles MIKEY lorsque ceux-ci sont exécutés au "niveau session".

MiscellaneousCommand doit utiliser **encryptionUpdate**, **genericParameter** étant utilisé comme suit:

- **parameterIdentifier**: dans **standard** avec la valeur 0 pour indiquer le recalcul de clé TGK MIKEY et la mise à jour de lot CSB au "niveau session";
- **parameterValue** avec le message codé binaire (I ou R) MIKEY dans **octetString**;
- **supersedes** reste vide/non utilisé.

LogicalChannelNumber doit être ignoré pour les protocoles MIKEY au niveau session et peut prendre n'importe quelle valeur.

RequestMode doit utiliser **capabilityIdentifier** dans **genericModeParameters** de **ModeElement** comme suit:

- **capabilityIdentifier** doit prendre l'un des identificateurs d'objet MIKEY dans **standard**;
- **maxbitRate** et **collapsing** restent non utilisés;
- **nonCollapsing** avec l'ensemble suivant de **GenericParameters** suivants lorsque les protocoles MIKEY sont exécutés au "niveau session" pour un canal logique particulier:
  - **parameterIdentifier**: dans **standard** avec la valeur 0 pour indiquer que les protocoles MIKEY sont exécutés au "niveau session";
  - **parameterValue** avec le message codé binaire (I ou R) MIKEY dans **octetString**;
  - **supersedes** reste vide/non utilisé.
- **nonCollapsingRaw** reste non utilisé;
- **transport** (non utilisé ou paramètres de transport par défaut).

G.7.2 Exécution des protocoles MIKEY au "niveau média"

De même, les protocoles de gestion de clés MIKEY peuvent aussi être exécutés au "niveau média"; autrement dit, la clé TGK MIKEY est appliquée à un canal logique particulier sur un flux média. Il convient d'utiliser les messages de prise de contact TerminalCapability pour négocier le protocole MIKEY et d'utiliser les messages **OpenLogicalChannel/Ack** pour transporter le message MIKEY codé.

TerminalCapabilitySet doit utiliser **h235SecurityCapability, genericH235SecurityCapability** étant utilisé dans **encryptionAuthenticationAndIntegrity** comme suit:

- **capabilityIdentifier** doit contenir l'un des identificateurs d'objet MIKEY dans **standard**;
- **maxbitRate, nonCollapsing** et **collapsing** restent non utilisé;
- **nonCollapsingRaw** reste non utilisé;
- **transport** (non utilisé ou paramètres de transport par défaut).

OpenLogicalChannel ou **OpenLogicalChannelAck** doit utiliser le **genericParameter** dans **encryptionSync** comme suit:

- **parameterIdentifier**: dans **standard** avec la valeur de l'identificateur de paramètre (voir Tableau G.1) correspondant au protocole MIKEY négocié;
- **parameterValue** avec le message codé binaire (I ou R) MIKEY dans **octetString**;
- **supersedes** reste vide/non utilisé;
- **synchFlag** dans **encryptionSync** doit être mis au nombre de charges utiles dynamiques. **h235key** ne doit pas être utilisé par la présente Annexe et doit être une chaîne d'octets vide. **escrowentry** ne doit pas être utilisé.

MiscellaneousCommand doit utiliser **encryptionUpdate**, **genericParameter** dans **encryptionSync** étant utilisé comme suit:

- **parameterIdentifier**: dans **standard** avec la valeur de l'identificateur d'objet (voir Tableau G.1) correspondant au protocole MIKEY négocié;
- **parameterValue** avec le message codé binaire (I ou R) MIKEY dans **octetString**;
- **supersedes** reste vide/non utilisé.

RequestMode doit utiliser **capabilityIdentifier** dans **genericModeParameters** de **ModeElement** comme suit:

- **capabilityIdentifier** doit contenir l'un des identificateurs d'objet MIKEY dans **standard**;
- **maxbitRate** et **collapsing** restent non utilisés;
- **nonCollapsing** avec l'ensemble suivant de **GenericParameters** lorsque les protocoles MIKEY sont exécutés au "niveau média" pour un canal logique particulier:
  - **parameterIdentifier**: dans **standard** avec la valeur de l'identificateur de paramètre (voir Tableau G.1) correspondant au protocole MIKEY négocié;
  - **parameterValue** avec le message codé binaire (I ou R) MIKEY dans **octetString**;
  - **supersedes** reste vide/non utilisé;
- **nonCollapsingRaw** reste non utilisé;
- **transport** (non utilisé ou paramètres de transport par défaut).

G.7.3 Négociation des capacités MIKEY

Si les protocoles MIKEY sont acheminés à la fois dans les messages de prise de contact Terminal Capability Set/Request Mode et Open Logical Channel, les informations MIKEY contenues dans le message Open Logical Channel annulent et remplacent les informations de gestion de clés obtenues précédemment dans les messages Terminal Capability Set/Request Mode.

Comme les points d'extrémité n'implémentent pas nécessairement la totalité des protocoles de gestion de clés MIKEY, voire n'en implémentent aucun (autrement dit certains points d'extrémité peuvent ne pas prendre en charge du tout la présente annexe), le point d'extrémité appelant ne peut pas savoir quelles capacités MIKEY le point d'extrémité appelé prend en charge. Il est donc recommandé que la capacité de gestion de clés MIKEY soit négociée au moyen des messages de prise de contact Terminal Capability Set.

Pendant la négociation des capacités de terminal, le point d'extrémité appelant doit indiquer les protocoles de gestion de clés MIKEY qu'il prend en charge et qu'il peut accepter. Pour cela, il doit indiquer les capacités de sécurité MIKEY qu'il prend en charge. Dans **genericH235SecurityCapability**, il doit mettre **capabilityIdentifier** à la valeur de l'identificateur d'objet (voir Tableau G.1) correspondant au profil de sécurité et à la gestion de clés MIKEY préférés. Il est encouragé à indiquer aussi les autres protocoles MIKEY qu'il prend en charge, par ordre de préférence décroissant conformément à sa politique et à ses contraintes de sécurité.

Un point d'extrémité appelé qui ne prend pas en charge la présente annexe doit rejeter l'appel à l'aide de **ReleaseComplete** avec **ReleaseCompleteReason** mis à **securityDenied** ou peut continuer de manière non sécurisée si ses règles de politique de sécurité l'y autorisent. Si l'appelant constate que la capacité retournée n'indique pas de capacité MIKEY, il peut en déduire que l'appelé ne prend pas en charge la capacité MIKEY demandée.

Un point d'extrémité appelé qui prend en charge la présente annexe mais qui ne prend pas en charge une capacité de protocole MIKEY demandée doit indiquer les protocoles MIKEY qu'il prend en charge et qu'il peut accepter pendant la négociation Terminal Capability Set.

Un point d'extrémité appelé qui prend en charge la présente annexe et un protocole MIKEY demandé mais qui ne prend pas en charge une combinaison donnée d'algorithmes et de paramètres de sécurité MIKEY/SRTP (autrement dit la politique de sécurité MIKEY) doit répondre par un message d'erreur MIKEY (voir les sections 5.1.1, 5.1.2 et 6.1.2 du Document [RFC 3830]). Le point d'extrémité appelé doit inclure la politique de sécurité MIKEY qu'il prend en charge et qu'il peut accepter avec les algorithmes et paramètres de sécurité MIKEY/SRTP.

Dans la présente annexe, on utilise la tunnellisation des messages H.245 dans la signalisation d'appel H.225.0 afin de sécuriser les messages de signalisation d'appel H.225.0. On peut aussi ne pas utiliser la tunnellisation des messages H.245, mais dans ce cas, il faut utiliser au moins un transport sécurisé avec protection de l'intégrité (TLS, IPsec) afin de sécuriser les messages H.245. Cette variante n'est pas détaillée plus avant dans la présente annexe.

Dans la présente annexe, il est également préférable d'utiliser la connexion rapide, selon laquelle les messages H.245 tunnellisés sont encapsulés dans les messages Call Signalling Setup et CallProceeding-to-Connect H.225.0. Cela permet d'exécuter la prise de contact MIKEY en deux allers-retours au maximum.

Afin de se protéger contre les attaques de déclassement pendant la négociation de capacité, un point d'extrémité conforme à la présente spécification doit suivre la procédure décrite à la section 6.15 du Document [RFC 3830], selon laquelle l'appelant élabore la liste des identificateurs des protocoles de gestion de clés (KMID, *key management protocol identifier*) MIKEY offerts (voir la section 8.3 du Document [KMGMT-ext]) et inclut cette liste dans la charge utile d'extension générale MIKEY de chaque protocole MIKEY offert.

Pour un canal duplex intégral, le protocole SRTP est instancié deux fois, une fois dans chaque sens, tandis qu'une seule clé principale MIKEY dynamique (clé TGK) est négociée entre les points d'extrémité H.323. Les points d'extrémité instancient des clés de session SRTP dans chaque sens en appliquant des identificateurs de session de chiffrement MIKEY distincts à la fonction de détermination de clé MIKEY et SRTP.

G.8 Profil de sécurité utilisant des techniques de sécurité symétriques

Le présent paragraphe décrit un profil de sécurité de la présente annexe dans lequel seules des techniques de sécurité symétriques sont mises en œuvre.

La Figure G.3 représente un scénario dans lequel il existe des secrets partagés saut par saut (administrés ou configurés) entre les entités H.323 dans le domaine H.323 (*sa, sb* et *sl*), permettant ainsi de mettre en œuvre la sécurité de base de l'Annexe D/H.235 (authentification et/ou intégrité

des messages) des protocoles RAS et de signalisation d'appel H.225.0. Pour garantir l'authenticité (autrement dit l'intégrité) des messages de signalisation échangés entre les points d'extrémité B et A, la sécurité de base de l'Annexe D/H.235 doit obligatoirement être mise en œuvre saut par saut.

Le point d'extrémité B est supposé être relativement bien synchronisé temporellement avec les autres points d'extrémité H.323; autrement, le protocole MIKEY ne peut pas être exécuté de façon sécurisée.

NOTE 1 – La présente annexe ne décrit aucun moyen permettant de synchroniser (de façon sécurisée) les horloges entre les entités concernées. On suppose généralement que cette synchronisation temporelle peut être obtenue dans les réseaux d'entreprise.

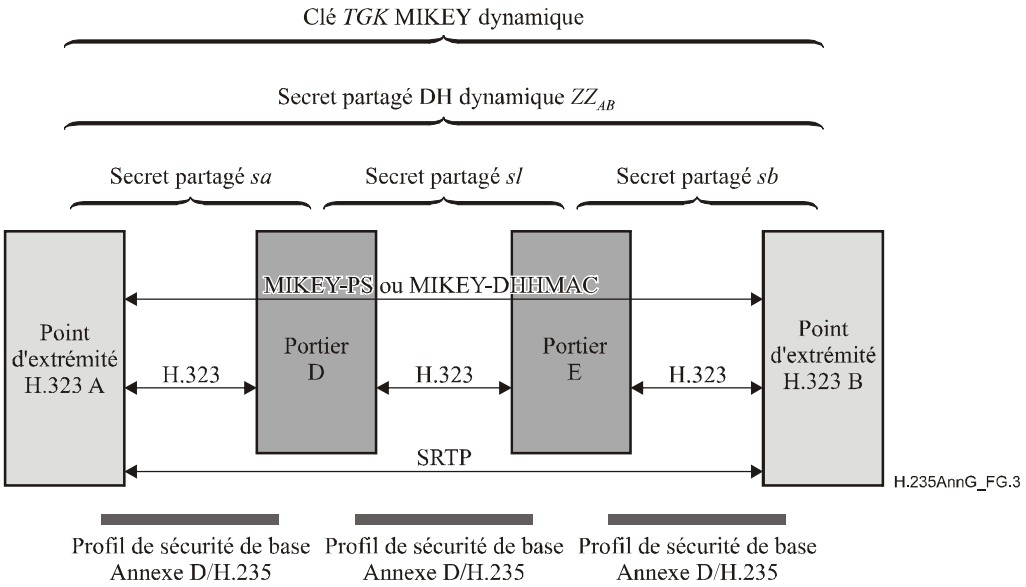

Figure G.3/H.235 – Scénario saut par saut uniquement avec des secrets partagés

Ce scénario repose sur le fait que le protocole de distribution de clés MIKEY-PS (symétrique avec secrets prépartagés) – ou, en cas de confidentialité totale vers l'avant, le protocole de concordance de clés MIKEY-DHHMAC (Diffie-Hellman avec HMAC) – est mis en œuvre dans le domaine H.323. [MIKEY-DHHMAC] est offert en tant qu'option (voir l'Appendice G.I).

Lorsque le point d'extrémité B (initiateur MIKEY) appelle le point d'extrémité A (répondeur MIKEY), un secret partagé dynamique ZZ_{AB} est établi entre les points d'extrémité A et B dans le cadre des procédures RAS et Setup H.225.0 pour un appel. Ce secret sert ensuite de secret prépartagé MIKEY, à partir duquel les points d'extrémité A et B déduisent les clés de chiffrement et d'authentification symétriques au moyen du protocole MIKEY (non reprenté sur la figure).

Le point d'extrémité appelant B génère la clé *TGK* MIKEY (il s'agit d'une clé principale) pour le point d'extrémité homologue A. Le point d'extrémité B élabore les messages de protocole MIKEY puis les encapsule en totalité dans un conteneur dans le message **TerminalCapabilitySet/OpenLogicalChannel** tunnellisé. Dans un environnement à routage par portier, le portier E ne fait que transmettre le conteneur MIKEY à l'autre point d'extrémité A sans aucun décodage des informations MIKEY proprement dites. Le point d'extrémité A termine le protocole MIKEY dans le domaine H.323.

Ainsi, les points d'extrémité B et A établissent une clé *TGK*.

Le protocole MIKEY-PS ou MIKEY-DHHMAC est exécuté entre les points d'extrémité B et A, ce qui leur permet d'obtenir la clé *TGK* et de déterminer les clés de session SRTP/SRTCP. Les protocoles SRTP et SRTCP appliquent ces clés de session de bout en bout.

NOTE 2 – Le protocole MIKEY offre tous les paramètres nécessaires au protocole SRTP (algorithmes, longueurs de clé, durée de vie de clé, etc.) dans le cadre des politiques MIKEY acheminées.

Les portiers ne participent pas activement au traitement MIKEY mais servent de relais d'enregistrement et retransmission des messages MIKEY encapsulés.

Dans le cas d'un appel établi par le point d'extrémité A, la procédure est analogue dans le sens inverse, le point d'extrémité A étant l'initiateur et le point d'extrémité B le destinataire.

NOTE 3 –

- Le scénario représenté sur la Figure G.3 prend également en charge le modèle de signalisation d'appel à routage direct avec un ou plusieurs portiers sans routage. Dans un tel environnement à routage direct, les messages de signalisation d'appel H.225.0 (Setup, etc.) sont envoyés de bout en bout dans le domaine H.323 sans être relayés par le portier. On trouvera à l'Appendice G.II des illustrations sur la façon d'utiliser l'Annexe I à cette fin.
- Le protocole MIKEY utilise des horodates dans le protocole de sécurité afin de garantir la protection contre la relecture du message de gestion de clés. Pour cela, les horloges des points d'extrémité doivent être relativement bien synchronisées temporellement (dans des limites acceptables). On considère que cette synchronisation temporelle peut être obtenue à l'aide d'horloges configurées manuellement ou d'un protocole de synchronisation de réseau (par exemple NTP [RFC 1305]). En tant que telle, la synchronisation temporelle dans le domaine H.323 devrait être possible au moins pour les réseaux d'entreprise; voir aussi les sections 5.4 et 9.3 du Document [RFC 3830].
- Il n'est pas recommandé de combiner le démarrage rapide et le média sans délai avec le protocole MIKEY-DHHMAC. Si démarrage rapide et média sans délai sont obligatoires, les points d'extrémité ne doivent pas utiliser MIKEY-DHHMAC mais appliquer MIKEY-PS.
- Un scénario avec un seul portier est un cas particulier du scénario représenté avec plusieurs portiers. Dans ce cas, il n'est pas nécessaire de procéder à la recherche du point d'extrémité/portier distant au moyen des messages LRQ/LCF.

Dans la suite, on donne plus de détails concernant les flux de messages associés au scénario de la Figure G.3, dans lequel on considère un ou plusieurs portiers avec routage dans le domaine H.323, les messages H.245 étant tunnellisés dans le protocole H.225.0 et un démarrage rapide étant appliqué.

NOTE 4 – Les diagrammes de flux englobent également le cas du routage direct (avec portiers sans routage), dans lequel les messages de signalisation d'appel H.225.0 sont échangés directement entre les points d'extrémité sans être retransmis par les portiers, voir l'Appendice G.II.

Dans la procédure décrite dans le présent paragraphe, un secret partagé de bout en bout ZZ_{AB} est établi entre les points d'extrémité H.323 A et B au cours de l'étape 1 au moyen d'une méthode de concordance de clés Diffie-Hellman. Cette méthode est appliquée au cours de la phase d'enregistrement et d'admission RAS H.225.0 ou, dans le cas de plusieurs portiers, au cours de l'échange de messages **LRQ/LCF** entre portiers. Le secret partagé Diffie-Hellman généré sert de clé d'authentification de bout en bout pendant toute la durée de l'appel. Le protocole MIKEY-PS (ou MIKEY-DHHMAC) est exécuté séparément au cours de l'étape 2 pendant l'établissement d'appel et permet d'établir des secrets MIKEY fondés sur l'appel pour le canal support.

L'Appendice G.II décrit une autre procédure, facultative, utilisant la procédure DRC de l'Annexe I/H.235 et telle que le portier génère et distribue un secret partagé aux points d'extrémité A et B.

Le diagramme de la Figure G.4 représente également le profil de sécurité de base de l'Annexe D/H.235, dans lequel chaque message est entièrement sécurisé (authentification et intégrité). Néanmoins, les flux de messages sont analogues lorsqu'on applique l'option d'authentification seule du profil de sécurité de base (non représenté). Dans ce cas, le code HMAC n'est pas calculé sur la totalité mais uniquement sur une partie (**ClearToken** dans **CryptoToken**) du message RAS/H.225.0.

Le flux de messages illustré correspond au cas où le point d'extrémité B (initiateur MIKEY) appelle le point d'extrémité A (répondeur MIKEY) à l'aide du démarrage rapide (voir la Figure G.4). Les points d'extrémité H.323 A et B commencent par s'enregistrer auprès du portier au moyen du message **RRQ** et soumettent leur demi-clé DH (g^a et g^b). Le **ClearToken** (dans le **CryptoHashedToken**) doit être utilisé pour acheminer la demi-clé Diffie-Hellman pendant l'échange de messages **RRQ** et **ACF**. A cette fin, le champ **challenge** ne doit pas être utilisé.

La demi-clé Diffie-Hellman doit être acheminée dans **dhkey** dans le **ClearToken.** Le ClearToken doit utiliser l'identificateur d'objet "TG" (voir le § G.8.5) et non pas l'identificateur d'objet "T" du ClearToken de base de l'Annexe D, indiquant que ce profil de sécurité est utilisé conjointement avec l'Annexe D/H.235. Le portier doit conserver chaque demi-clé pendant toute la durée d'enregistrement du point d'extrémité. Lorsque les points d'extrémité exécutent des maintiens d'enregistrement ou utilisent un nouvel enregistrement simplifié (re-RRQ), ils ne doivent pas inclure de demi-clé DH. Le message **RCF** doit utiliser l'identificateur d'objet "TG" dans le ClearToken pour indiquer que le portier prend en charge ce profil de sécurité.

Le point d'extrémité B essaie d'appeler le point d'extrémité A et, pour cela, il demande l'admission au portier D (**ARQ**). Le message **ARQ** doit utiliser l'identificateur d'objet "TG" dans le ClearToken. Cet identificateur d'objet "TG" doit être utilisé dans tous les autres messages RAS dans le ClearToken.

Le scénario englobe plusieurs portiers en chaîne mais peut tout aussi bien ne prendre en charge qu'un seul portier. La recherche du point d'extrémité distant doit se faire conformément au § 8.1.6/H.323 "Signalisation facultative par l'extrémité appelée" au moyen des messages **LRQ/LCF**. Il s'agit de la manière dont le point d'extrémité d'origine localise la zone du portier distant et obtient la demi-clé Diffie-Hellman du point d'extrémité appelé cible. Si le portier E a besoin de localiser la zone du portier distant, il envoie un message **LRQ**. Dans le cas de la multidiffusion, le **generalID** dans le CryptoToken du message **LRQ** ne doit pas être utilisé. Si le portier D ne prend pas en charge ce profil, il retourne le message **LRJ**. Dans le cas contraire, il retourne le message **LCF** incluant la demi-clé Diffie-Hellman du point d'extrémité A. Le portier E répond ensuite par un message **ACF** contenant la demi-clé Diffie-Hellman du point d'extrémité A ou, s'il ne parvient pas à localiser le point d'extrémité distant A, il retourne le message **ARJ**.

Les communications entre deux portiers doivent être sécurisées conformément à l'Annexe D/H.235. Pour cela, on suppose qu'un secret partagé commun *sl* est disponible. Comme le message **LRQ** entre portiers est généralement un message de multidiffusion, le secret partagé *sl* ne peut généralement pas être un secret partagé entre deux mais on suppose qu'il s'agit en fait d'un secret partagé par un groupe au sein du nuage potentiel de portiers. Cette hypothèse limite l'évolutivité dans le cas général et ne permet pas de procéder à une authentification de la source. Toutefois, on considère que dans les réseaux d'entreprise comportant un petit nombre de portiers bien connus, ces contraintes et ces limitations de sécurité restent acceptables. La sécurisation des communications de multidiffusion entre portiers au moyen de signatures numériques permettrait de surmonter ces limitations, mais un complément d'étude est nécessaire.

Le point d'extrémité B obtient la demi-clé Diffie-Hellman du point d'extrémité A (**ACF**). Le message **ACF** doit contenir la clé Diffie-Hellman du point d'extrémité appelé dans **dhkey** dans le **ClearToken** de base de l'Annexe D, celui-ci utilisant l'identificateur d'objet "TG" et non l'identificateur d'objet "T". Tous les autres champs du **ClearToken** doivent être laissés en l'état par ce profil de sécurité.

NOTE 5 – Les points d'extrémité fonctionnent avec une demi-clé DH qui est statique pendant toute la durée d'enregistrement et pour tous les appels. Il ne doit pas s'agir d'une faiblesse sur le plan de la sécurité étant donné que chaque point d'extrémité applique des demi-clés vraiment aléatoires.

Toutefois, les points d'extrémité doivent fournir une nouvelle valeur aléatoire de 512 bits (autrement dit 64 octets) dans **challenge** en même temps que leur demi-clé DH, voir la section 2.3

du Document [RFC 2631]. Ces valeurs de **challenge**, qui sont fondées sur l'appel, permettent de garantir que les clés DH sont générées de façon aléatoire et en temps utile, comme requis.

Le point d'extrémité d'origine B peut alors calculer g^{ab} puis le secret partagé dynamique ZZ_{AB} au moyen d'un **challenge** aléatoire, le résultat étant obtenu à partir de MIKEY-PRF(g^{ab} , 0x12F905FE || **challenge**) (voir les sections 4.1.2 à 4.1.5 du Document [RFC 3830]). La fonction MIKEY-PRF permet ensuite de déterminer les clés de chiffrement (*Me*) et d'authentification (*Ma*) (voir les sections 4.1.2 à 4.1.5 du Document [RFC 3830]).

Au cours de l'étape 2, le point d'extrémité d'origine B doit générer une nouvelle clé *TGK* MIKEY puis élaborer l'I_message MIKEY Imsg conformément au protocole MIKEY-PS au moyen de *Me* et *Ma*; par ailleurs, les clés de session SRTP peuvent être obtenues à partir de la clé TGK comme décrit à la section 4.3 du Document [RFC 3711] (non représenté sur les figures).

L'I_message MIKEY doit être codé binaire.

Le point d'extrémité d'origine B doit toujours inclure sa demi-clé DH dans **dhkey** dans un **ClearToken**, ce qui permet de prendre également en charge le modèle à routage direct avec portiers. Le **ClearToken** doit être inclus dans le message Setup et doit être envoyé au point d'extrémité homologue A. Un portier avec routage doit transmettre le ClearToken acheminé (sans modification des messages MIKEY) au saut suivant.

Le point d'extrémité de destination A calcule alors g^{ab} et le secret partagé dynamique ZZ_{AB} à partir de MIKEY-PRF(g^{ab} , 0x12F905FE || **challenge**) (voir les sections 4.1.2 à 4.1.5 du Document [RFC 3830]). La fonction MIKEY-PRF permet ensuite de déterminer les clés de chiffrement (*Me*) et d'authentification (*Ma*) (voir les sections 4.1.2 à 4.1.5 du Document [RFC 3830]). Les clés TGK acheminées peuvent alors être récupérées.

A partir de la clé *TGK*, le point d'extrémité de destination A peut ensuite déterminer les clés de session SRTP comme décrit à la section 4.3 du Document [RFC 3711] (non représenté sur les figures).

Le point d'extrémité A peut élaborer un R_message Rmsg analogue mais il ne doit le faire qu'à la demande du point d'extrémité B ou si nécessaire (DH). Ce R_message est acheminé dans le message CallProceeding-to-Connect (CP/C).

Le message CallProceeding-to-Connect (CP/C) est envoyé au point d'extrémité B.

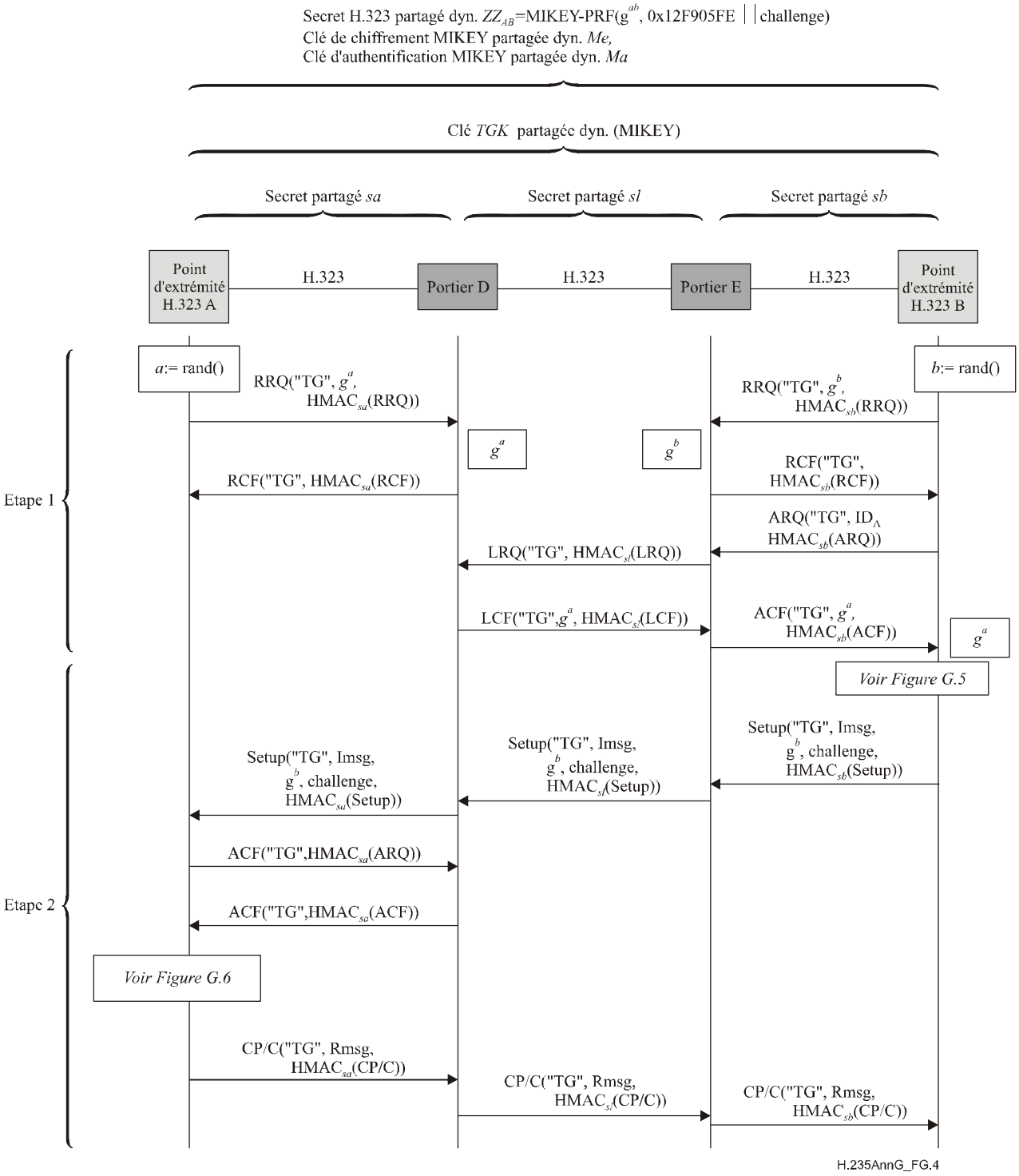

Figure G.4/H.235 – Exemple dans lequel le point d'extrémité B appelle le point d'extrémité A (routage par portier) avec MIKEY-PS

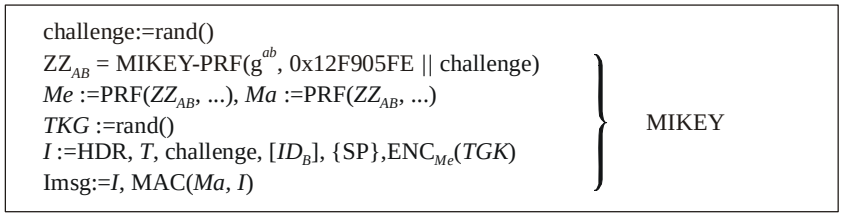

Figure G.5/H.235 – Traitement MIKEY-PS par le point d'extrémité B

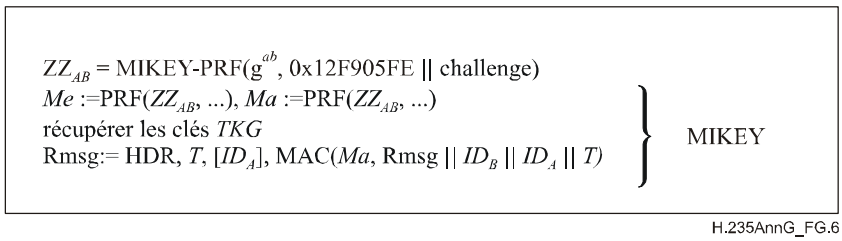

Figure G.6/H.235 – Traitement MIKEY-PS par le point d'extrémité A

G.8.1 Terminaison d'un appel H.323

Comme les points d'extrémité considérés conservent l'état pour les protocoles MIKEY et SRTP, une procédure de terminaison à part entière est indispensable. La Figure G.7 donne un exemple de flux de messages correspondant au cas où le point d'extrémité B (initiateur MIKEY) termine un appel. Fondamentalement, le flux est conforme au § 8.5/H.323 " Phase E – Fin de la communication".

NOTE – La figure illustre également les procédures de retrait facultatives correspondant au cas où les points d'extrémité se désenregistrent complètement. Les points d'extrémité doivent alors éliminer également la clé DH privée (*a* ou *b*) et la demi-clé DH publique (g^a ou g^b).

Comme la procédure de terminaison d'un appel est indépendante de ce profil de sécurité, il est possible d'utiliser n'importe quel identificateur d'objet applicable du profil de sécurité sous-jacent (Annexe D, F, etc.); la Figure G.7 n'indique donc pas d'identificateur d'objet.

Si le point d'extrémité s'enregistre à nouveau auprès du portier, il faut générer de nouvelles demi-clés DH. Toutefois, un désenregistrement complet n'est pas nécessaire dans tous les cas de terminaison d'appel. Si le point d'extrémité décide de rester enregistré auprès du portier, il est possible de continuer à utiliser les demi-clés DH statiques.

Dans le cas où les points d'extrémité restent enregistrés et où le retrait n'est pas appliqué, les points d'extrémité doivent éliminer uniquement les informations liées à l'appel (demi-clé DH de leur homologue, **challenge**, clés MIKEY *Me*, *Ma*, *TGK* et informations de session SRTP connexes).

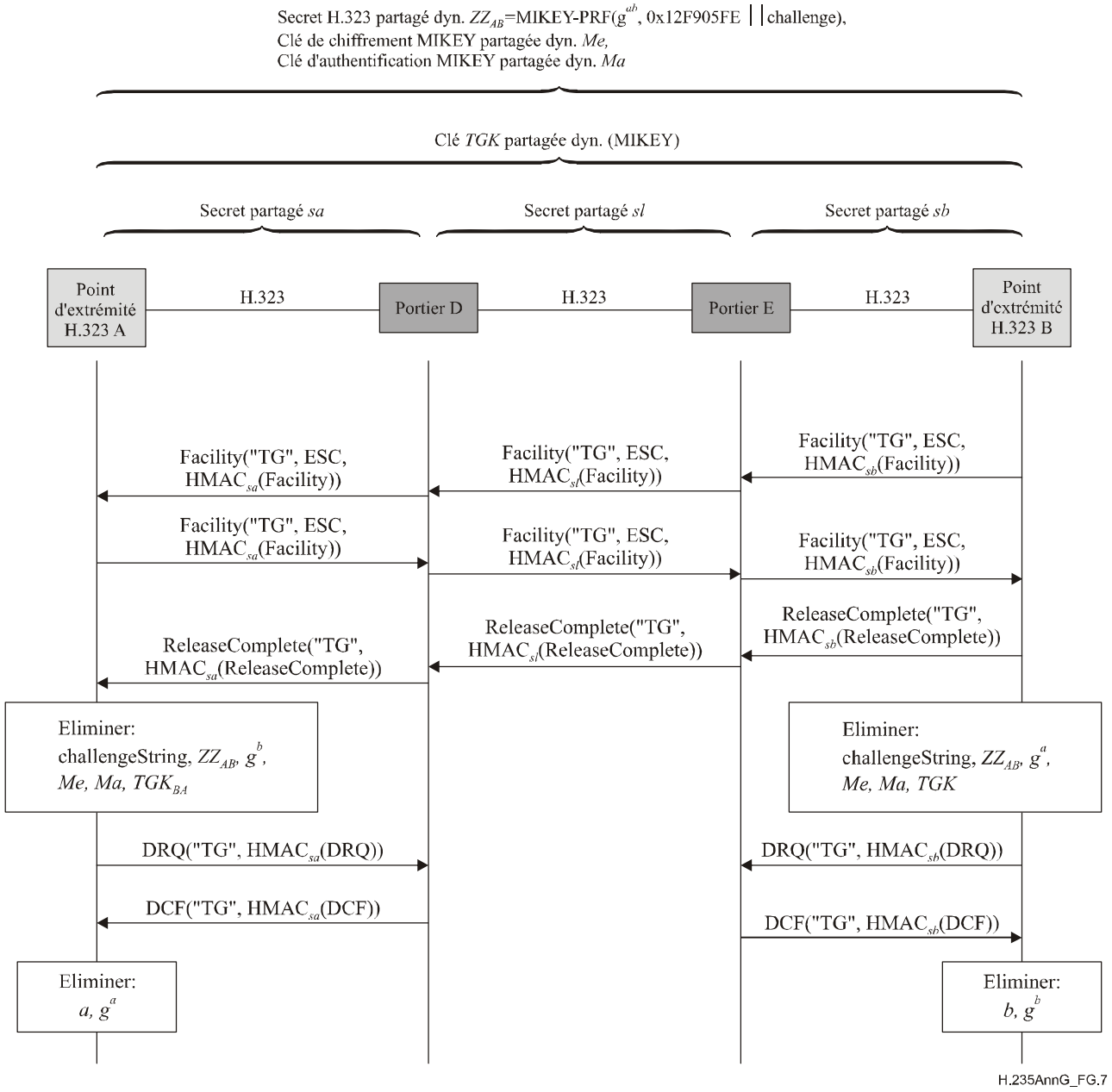

Figure G.7/H.235 – Exemple dans lequel le point d'extrémité B termine un appel

G.8.2 Recalcul de clé TGK et mise à jour de lot CSB

Le protocole MIKEY prend intrinsèquement en charge le recalcul de clé TGK et/ou la mise à jour des informations de lot CSB. Le profil de la présente annexe doit utiliser à cette fin la procédure MIKEY-PS de la section 4.5 du Document [RFC 3830] ou, en cas de confidentialité totale vers l'avant, la procédure de la section 3.1 du Document [MIKEY-DHHMAC], permettant de mettre à jour la clé TGK avant expiration ou de mettre à jour d'autres informations sans modifier la clé TGK.

Le mécanisme de recalcul de clé TGK et de mise à jour de lot CSB est utile pour protéger un ensemble de canaux logiques relevant de la même politique de sécurité. Pour cela, il est recommandé d'exécuter le protocole (complet) MIKEY-PS comme décrit au § G.8 uniquement pour le premier canal logique. Pour les canaux logiques suivants pour lesquels on doit appliquer la même politique de sécurité MIKEY ou la même clé TGK, il convient d'utiliser le mécanisme de mise à jour de lot CSB sans le mécanisme de recalcul de clé TGK du présent paragraphe en faisant référence à l'identificateur de lot CSB initial et en omettant les données de clé TGK mises à jour.

Cela permet d'établir des canaux logiques ou des sessions de chiffrement MIKEY de façon plus efficace que ne le permet l'exécution du protocole MIKEY complet pour chaque canal logique.

Les messages de recalcul de clé TGK MIKEY ou de mise à jour de lot CSB doivent être encapsulés et acheminés dans un **MiscellaneousCommand** dans un message Facility. Le **tokenOID** du **ClearToken** doit être mis à "TG".

Si le protocole MIKEY est exécuté au "niveau média", le point d'extrémité B doit déterminer le canal logique pour lequel il convient d'appliquer le recalcul de clé TGK et/ou la mise à jour de lot CSB. Le point d'extrémité A en tant que répondeur utilise aussi le **MiscellaneousCommand** dans Facility pour acheminer l'éventuel R_message MIKEY.

Pour le recalcul de clé TGK (voir la Figure G.8), le point d'extrémité B en tant qu'initiateur MIKEY doit générer une nouvelle clé TGK.

Le point d'extrémité A en tant que répondeur peut confirmer le message de recalcul de clé TGK obtenu si nécessaire à la demande du point d'extrémité B. Le point d'extrémité A élabore un R_message analogue, qu'il envoie dans le message Facility au point d'extrémité B.

Pour la mise à jour de lot CSB, la procédure est analogue à la procédure ci-dessus sauf que le message MIKEY ne doit pas contenir de clé TGK.

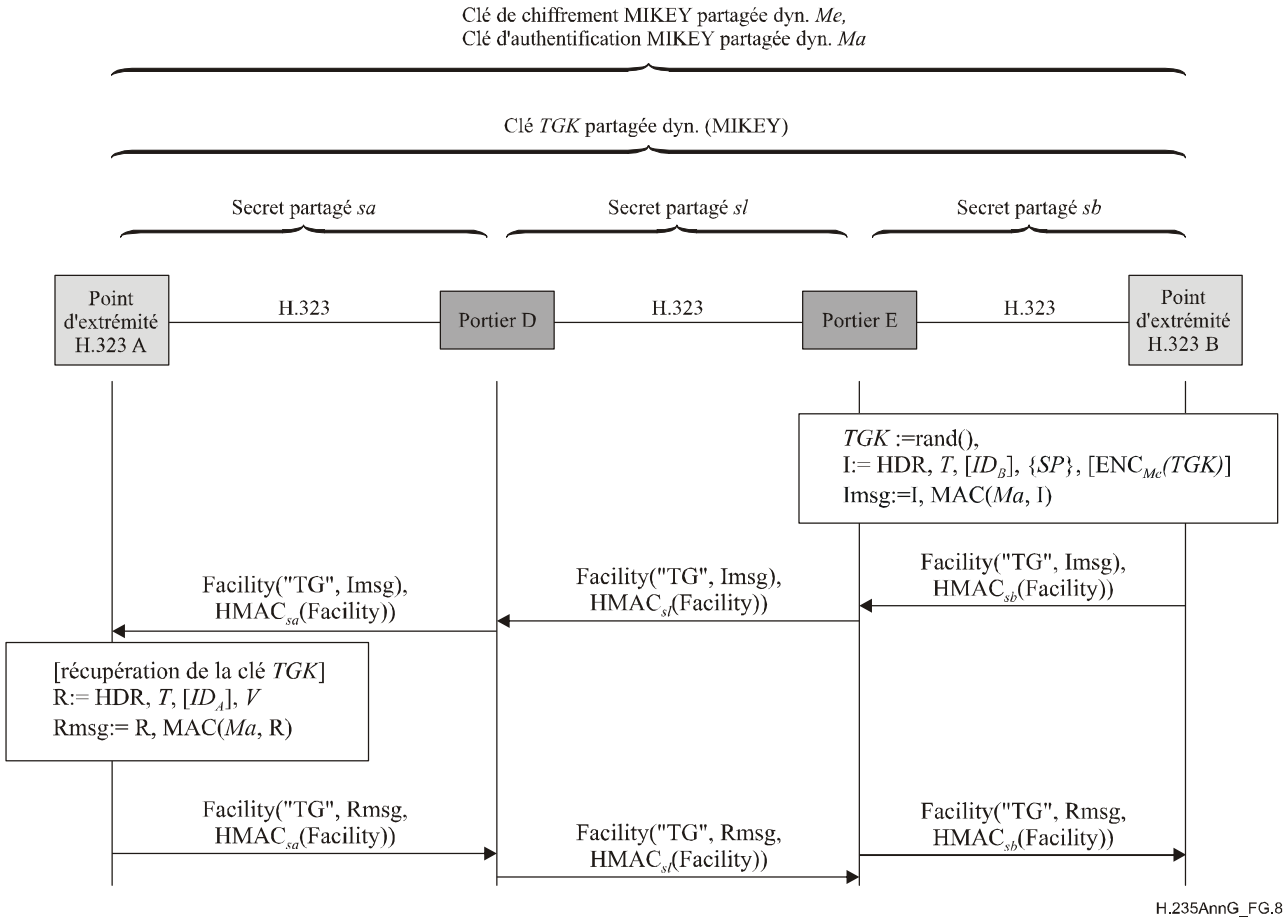

Figure G.8/H.235 – Exemple dans lequel le point d'extrémité B met à jour une clé

NOTE – Le message Facility de confirmation du point d'extrémité A au point d'extrémité B est facultatif et il n'est nécessaire que lorsque le point d'extrémité B a également demandé un message de vérification R_message MIKEY au moyen du fanion V dans HDR MIKEY.

La présente annexe ne définit pas de procédure pour le cas où le recalcul de clé TGK et/ou la mise à jour de lot CSB sont invoqués par le répondeur; un complément d'étude est nécessaire.

G.8.3 Prise en charge de la tunnellisation H.245

Si d'autres canaux logiques doivent être ajoutés pendant une session, il faut mettre en œuvre le mode de tunnellisation H.245, dans lequel les messages H.245 tunnellisés sont acheminés dans un message Facility.

G.8.4 Algorithmes SRTP

Ce profil de sécurité doit utiliser l'algorithme HMAC-SHA1-32 tronqué avec une longueur d'étiquette d'authentification *n_tag* égale à 32 bits comme algorithme d'authentification par défaut pour le protocole RTP. D'autres longueurs d'étiquette d'authentification comme celles qui sont définies dans le Document [RFC 3711] doivent également être prises en charge et doivent être négociées par le biais du paramètre de politique de sécurité MIKEY en fonction des besoins.

G.8.5 Liste des identificateurs d'objet

"TG"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 70}	Indique un ClearToken de base pour l'Annexe D/H.235 dans le contexte de la présente annexe. Cet identificateur d'objet indique également que le secret partagé ZZ_{AB} est calculé au moyen de la fonction MIKEY-PRF.

G.9 Profil de sécurité utilisant des techniques de sécurité asymétriques

Le présent paragraphe décrit un profil de sécurité de la présente annexe dans lequel des techniques de sécurité asymétriques sont mises en œuvre. Un tel scénario offre une plus grande évolutivité.

L'existence d'entités intermédiaires (les portiers) capables d'intercepter la clé TGK MIKEY et/ou les clés de session SRTP n'est pas nécessairement toujours acceptable. La Figure G.9 suivante représente un scénario dans lequel est mise en œuvre une infrastructure de clé publique (PKI, *public-key infrastructure*) pour l'établissement de clés de média SRTP entièrement de bout en bout.

Hypothèses: on suppose que les deux points d'extrémité A et B possèdent une clé privée (*SK*) ainsi qu'une clé publique certifiée (*cert*). Néanmoins, le point d'extrémité A et le portier E ainsi que le point d'extrémité B et le portier D peuvent partager des secrets partagés (administrés/configurés) dans le cas où les messages RAS et de signalisation d'appel H.225.0 sont sécurisés au moyen de l'Annexe D/H.235. On suppose aussi que les points d'extrémité A et B sont relativement bien synchronisés temporellement; dans le cas contraire, le protocole MIKEY ne peut pas être exécuté de façon sécurisée.

L'authentification et l'intégrité des messages peuvent être obtenues soit avec des secrets partagés saut par saut préconfigurés (*sa*, *sb* et *sl*) et avec le profil de sécurité de base H.235 soit, de façon plus générale, avec une infrastructure PKI pour établir des secrets partagés dynamiques et avec le profil de sécurité de l'Annexe F/H.235.

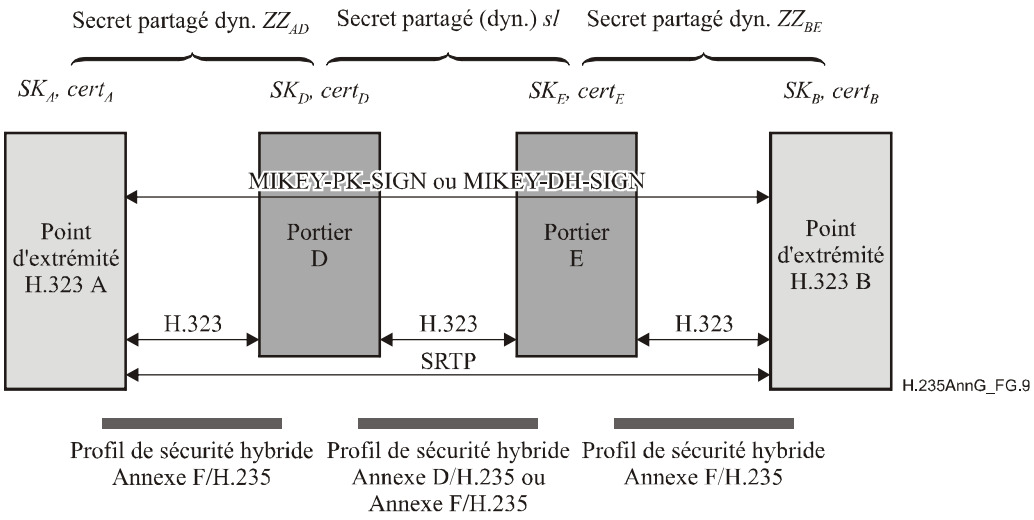

Figure G.9/H.235 – Scénario de bout en bout avec infrastructure PKI (plusieurs portiers)

Les points d'extrémité A et B exécutent le protocole MIKEY-PK-SIGN ou MIKEY-DH-SIGN de bout en bout, ce qui leur permet d'établir la clé TGK MIKEY à partir de laquelle les systèmes d'extrémité déterminent les clés de session SRTP.

NOTE 1 – Le protocole MIKEY-PK-SIGN répond aux exigences d'une gestion de clés fondée sur l'algorithme RSA.

NOTE 2 – L'utilisation de techniques PKI est très certainement mieux adaptée à l'environnement H.323 général dans lequel il existe plusieurs portiers en chaîne que les architectures limitées et moins évolutives qui utilisent des techniques de sécurité symétriques.

NOTE 3 – Il n'est pas recommandé de combiner le démarrage rapide et le média sans délai avec le protocole MIKEY-DH-SIGN. Si démarrage rapide et média sans délai sont obligatoires, les points d'extrémité ne doivent pas utiliser MIKEY-DH-SIGN mais appliquer MIKEY-PK-SIGN.

Dans la suite, on donne plus de détails concernant les flux de messages associés au scénario de la Figure G.9, dans lequel plusieurs portiers se trouvent dans le domaine H.323.

Sur les figures qui suivent, on considère en outre un portier avec routage (modèle à routage par portier), qui tunnellise les messages H.245 dans H.225.0 (démarrage rapide).

NOTE 4 – Les diagrammes de flux englobent aussi le cas du routage direct (avec portiers sans routage), dans lequel les messages de signalisation d'appel H.225.0 sont échangés directement entre les points d'extrémité sans être retransmis par aucun portier.

Sur les diagrammes, apparaît également le profil de sécurité hybride de l'Annexe F/H.235 permettant de sécuriser entièrement les messages RAS initiaux (authentification et intégrité) au moyen de signatures numériques et de certificats facultatifs. Il s'agit d'établir des secrets partagés dynamiques ZZ_{BE} et ZZ_{AD} entre les points d'extrémité et le portier du saut suivant, rendant ainsi superflus les secrets partagés statiques. Néanmoins, les flux de messages sont analogues lorsqu'on applique l'option d'authentification seule du profil de sécurité avec signatures (non représenté).

Le flux de messages illustré correspond au cas où le point d'extrémité B (initiateur MIKEY) appelle le point d'extrémité A (répondeur MIKEY) (voir la Figure G.10).

Au cours de l'étape 1, les points d'extrémité H.323 commencent par s'enregistrer auprès du portier du saut suivant et soumettent leur demi-clé DH (g^a et g^b).

Le point d'extrémité B essaie d'appeler le point d'extrémité A et, pour cela, demande l'admission au portier E. Le point d'extrémité B peut demander le certificat de son homologue $cert_c$ en incluant un élément de profil de sécurité dans le **ClearToken** s'il ne dispose pas encore des informations de certificat. Cet élément de profil de sécurité doit utiliser les champs suivants:

- **elementID** mis à 7 pour indiquer un élément de demande de certificat, ce qui est représenté par certFlag sur la Figure G.10;
- **paramS** reste non utilisé;
- **element** contient un Element dont **flag** est mis à TRUE.

Le message ARQ et les messages RAS et de signalisation d'appel H.225.0 qui suivent sont sécurisés par le secret partagé dynamique ZZ_{BE} au moyen du profil de sécurité de base de l'Annexe D/H.235. Si le point d'extrémité B a demandé une recherche des certificats, le portier E extrait $cert_c$ d'un répertoire de certificats, local ou non, et fournit le ou les résultats dans le message ACF dans **certificate** du **ClearToken** et inclut un élément de profil de sécurité. Cet élément doit utiliser les champs qui suivent:

- **elementID** mis à 8 pour indiquer un élément de réponse de certificat, ce qui est représenté par certFlag sur la Figure G.10;
- **paramS** reste non utilisé;
- **element** contient un Element dont **flag** est mis à TRUE.

Si le portier obtient plusieurs certificats pour un point d'extrémité/UA homologue, le message ACF inclut en fait plusieurs **ClearToken** – chacun contenant un seul certificat dans **certificate**. Le point d'extrémité choisit alors celui qui convient. Toutefois, il se peut que la recherche des certificats prenne trop de temps, ce qui peut par exemple être le cas lorsque des répertoires externes sont contactés. Si le portier n'est pas capable de fournir le ou les certificats à temps ou s'il n'est pas capable du tout de les fournir, le message ACF est retourné avec un **certificate** vide dans le **ClearToken**, qui contient un élément de profil de sécurité avec:

- **elementID** mis à 8 pour indiquer un élément de réponse de certificat;
- **paramS** reste non utilisé;
- **element** contient un Element dont **flag** est mis à FALSE.

Il appartient ensuite au point d'extrémité de procéder à un abandon et de tenter de localiser le certificat approprié par des moyens non spécifiés dans la présente annexe. Si le portier parvient à obtenir le certificat en dehors du délai de réponse imparti, il doit indiquer cette situation en laissant **certificate** vide et en incluant un élément de profil de sécurité dans le **ClearToken** avec:

- **elementID** mis à 8 pour indiquer un élément de réponse de certificat;
- **paramS** reste non utilisé;
- **element** contient un Element dont **flag** est mis à TRUE.

Dans ce cas, le portier doit retourner ce **ClearToken** dans un message ACF.

Au cours de l'étape 2, le point d'extrémité d'origine B (initiateur MIKEY) peut alors générer la nouvelle clé TGK MIKEY et calculer l'I_message MIKEY Imsg associé en appliquant le protocole de gestion de clés MIKEY-PK-SIGN (voir les Figures G.11 et G.12) ou, en cas de confidentialité totale vers l'avant, le protocole de gestion de clés MIKEY-DH-SIGN (Diffie-Hellman avec signatures numériques). MIKEY-DH-SIGN est offert en option.

Les clés de session SRTP peuvent être obtenues à partir de la clé TGK comme décrit à la section 4.3 du Document [RFC 3711] (non représenté sur les figures).

NOTE 5 – Les Figures G.11 et G.12 illustrent partiellement le protocole MIKEY, certaines parties n'étant pas représentées.

L'I_message MIKEY est codé binaire puis est encapsulé dans l'**OpenLogicalChannel** H.245.

Le **ClearToken** est inclus dans le message Setup et est envoyé au point d'extrémité A. Un portier avec routage retransmet l'I_message MIKEY acheminé (sans modification du message MIKEY) au saut suivant.

S'il existe plusieurs portiers avec routage, les messages de signalisation d'appel entre les portiers peuvent être sécurisés grâce à l'application d'un secret partagé administré et à l'utilisation de l'Annexe D ou de l'Annexe F/H.235 et de clés privées/publiques.

Le point d'extrémité A peut alors se servir de la clé *TGK* pour déterminer les clés de session SRTP comme décrit à la section 4.3 du Document [RFC 3711] (non représenté sur les figures).

Le point d'extrémité A en tant que répondeur MIKEY peut alors élaborer le R_message MIKEY Rmsg à l'aide de la clé *Ma* MIKEY et l'inclure dans le message CallProceeding-to-Connect (CP/C).

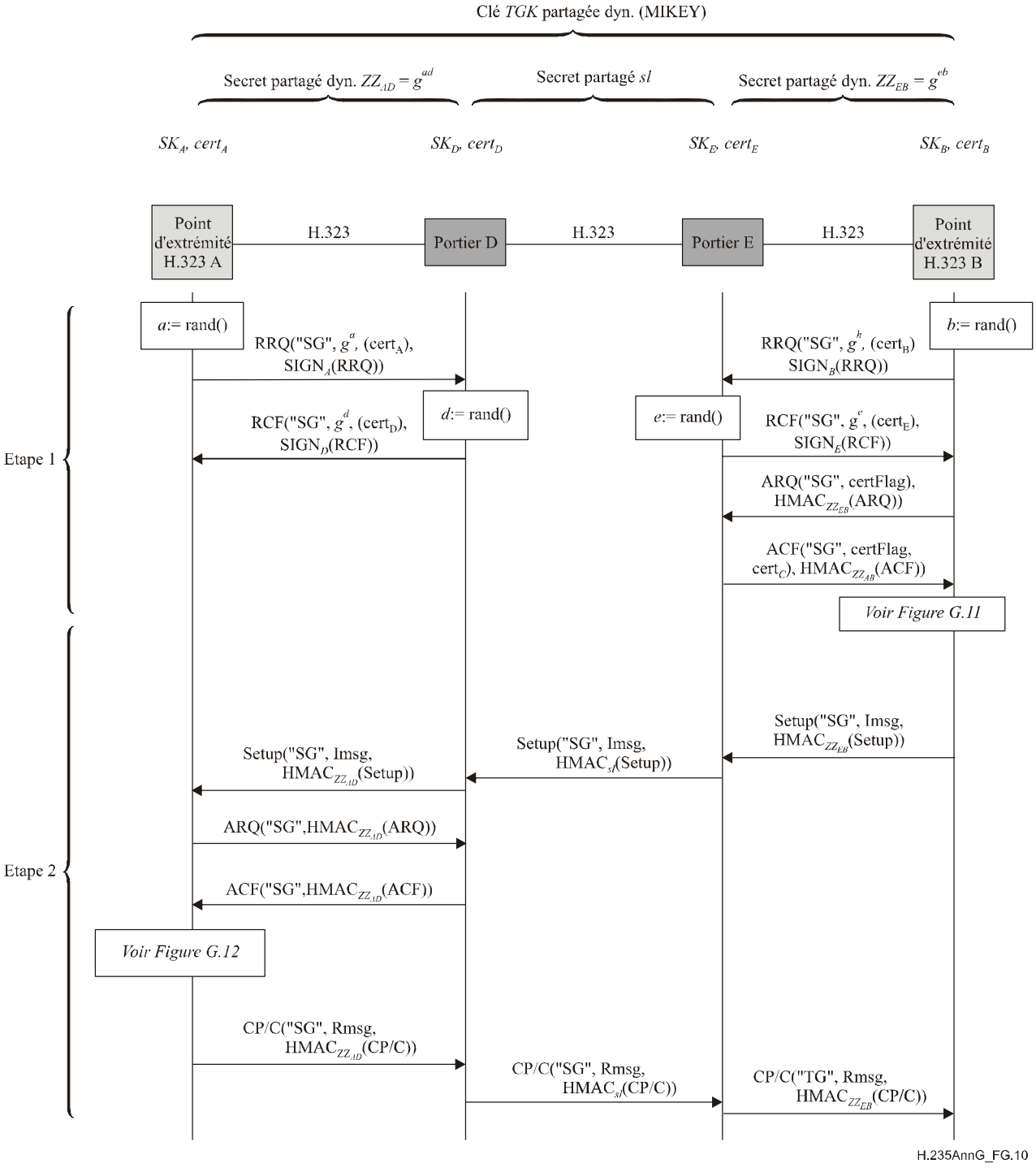

Figure G.10/H.235 – Exemple dans lequel le point d'extrémité B appelle le point d'extrémité A (routage par plusieurs portiers) avec MIKEY-PK-SIGN

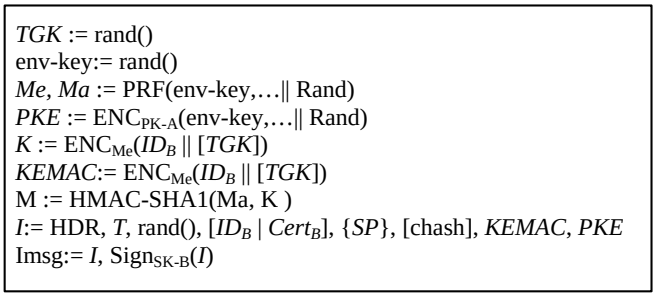

Figure G.11/H.235 – Traitement MIKEY-PK-SIGN par le point d'extrémité B

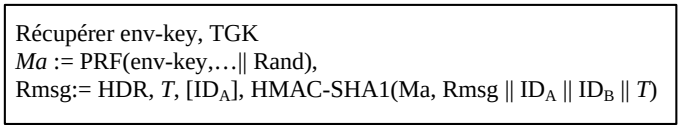

Figure G.12/H.235 – Traitement MIKEY-PK-SIGN par le point d'extrémité A

Un scénario avec un seul portier est un cas particulier du scénario représenté avec plusieurs portiers. Dans ce cas, il n'est pas nécessaire de procéder à la recherche du portier/point d'extrémité distant au moyen des messages LRQ/LCF.

G.9.1 Terminaison d'un appel H.323

Comme les points d'extrémité considérés conservent l'état pour les protocoles MIKEY et SRTP, une procédure de terminaison à part entière est indispensable. La Figure G.13 donne un exemple de flux de messages correspondant au cas où le point d'extrémité B (initiateur MIKEY) termine un appel. Fondamentalement, le flux est conforme au § 8.5/H.323 " Phase E – Fin de la communication".

NOTE – La figure illustre également les procédures de retrait facultatives correspondant au cas où les points d'extrémité se désenregistrent complètement. Les points d'extrémité doivent alors éliminer également la clé DH privée (*a* ou *b*) et la demi-clé DH publique (g^a ou g^b).

Comme la procédure de terminaison d'un appel est indépendante de ce profil de sécurité, il est possible d'utiliser n'importe quel identificateur d'objet applicable du profil de sécurité sous-jacent; la Figure G.13 n'indique donc pas d'identificateur d'objet.

Si le point d'extrémité s'enregistre à nouveau auprès du portier, il faut générer de nouvelles demi-clés DH. Toutefois, un désenregistrement complet n'est pas nécessaire dans tous les cas de terminaison d'appel. Si le point d'extrémité décide de rester enregistré auprès du portier, il est possible de continuer à utiliser les demi-clés DH statiques.

Dans le cas où les points d'extrémité restent enregistrés et où le retrait n'est pas appliqué, les points d'extrémité doivent éliminer uniquement les informations liées à l'appel (demi-clé DH de leur homologue, **challenge**, clés MIKEY *Me*, *Ma*, *TGK* et informations de session SRTP connexes).

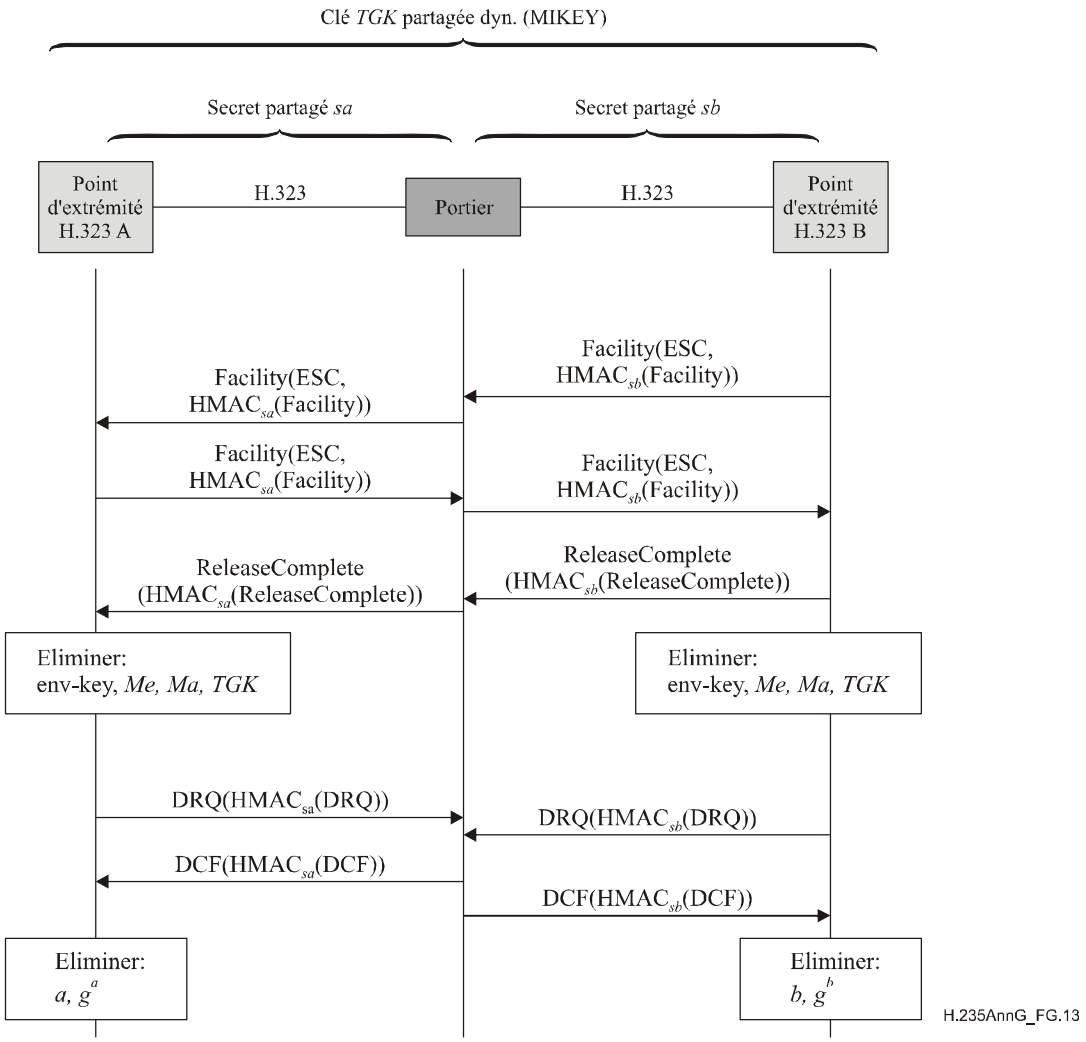

Figure G.13/H.235 – Exemple dans lequel le point d'extrémité B termine un appel

G.9.2 Recalcul de clé TGK et mise à jour de lot CSB

Le protocole MIKEY prend intrinsèquement en charge le recalcul de clé TGK et/ou la mise à jour des informations de lot CSB. A cette fin, il faut utiliser la procédure MIKEY-PKSIGN de la section 4.5 du Document [RFC 3830], permettant de mettre à jour la clé TGK avant expiration ou de mettre à jour d'autres informations (lot CSB) sans modifier la clé TGK.

Le mécanisme de recalcul de clé TGK et de mise à jour de lot CSB est utile pour protéger un ensemble de canaux logiques relevant de la même politique de sécurité. Pour cela, il est recommandé d'exécuter le protocole (complet) MIKEY-PKSIGN comme décrit au § G.8 uniquement pour le premier canal logique. Pour les canaux logiques suivants pour lesquels on doit appliquer la même politique de sécurité MIKEY ou la même clé TGK, il convient d'utiliser le mécanisme de mise à jour de lot CSB sans le mécanisme de recalcul de clé TGK du présent paragraphe en faisant référence à l'identificateur de lot CSB initial et en omettant les données de clé TGK mises à jour. Cela permet d'établir des canaux logiques ou des sessions de chiffrement MIKEY de façon plus efficace que ne le permet l'exécution du protocole MIKEY complet pour chaque canal logique.

Les messages de recalcul de clé TGK ou de mise à jour de lot CSB MIKEY doivent être inclus dans un **MiscellaneousCommand** d'un message Facility. Le **tokenOID** du **ClearToken** doit être mis à "SG".

Si le protocole MIKEY est exécuté au "niveau média", le point d'extrémité B doit déterminer le canal logique pour lequel il convient d'appliquer le recalcul de clé TGK et/ou la mise à jour de lot CSB. Le point d'extrémité A en tant que répondeur utilise aussi le **MiscellaneousCommand** dans Facility pour acheminer l'éventuel R_message MIKEY.

Pour le recalcul de clé TGK (voir la Figure G.14), le point d'extrémité B en tant qu'initiateur MIKEY doit générer une nouvelle clé TGK. **mikey** doit contenir l'I_message MIKEY correspondant.

Le répondeur (point d'extrémité A) peut confirmer le message de recalcul de clé TGK obtenu si nécessaire à la demande du point d'extrémité B. Le point d'extrémité A élabore un R_message Rmsg analogue. Ce R_message est acheminé dans le message Facility. Rmsg est le message de réponse MIKEY correspondant et doit être acheminé dans **octetString** du **GenericParameter**. Le point d'extrémité A envoie le message Facility au point d'extrémité B.

Pour une mise à jour de lot CSB lancée par l'initiateur, la procédure est analogue à la procédure ci-dessus sauf que le message MIKEY ne doit pas contenir de clé TGK (voir la Figure G.14).

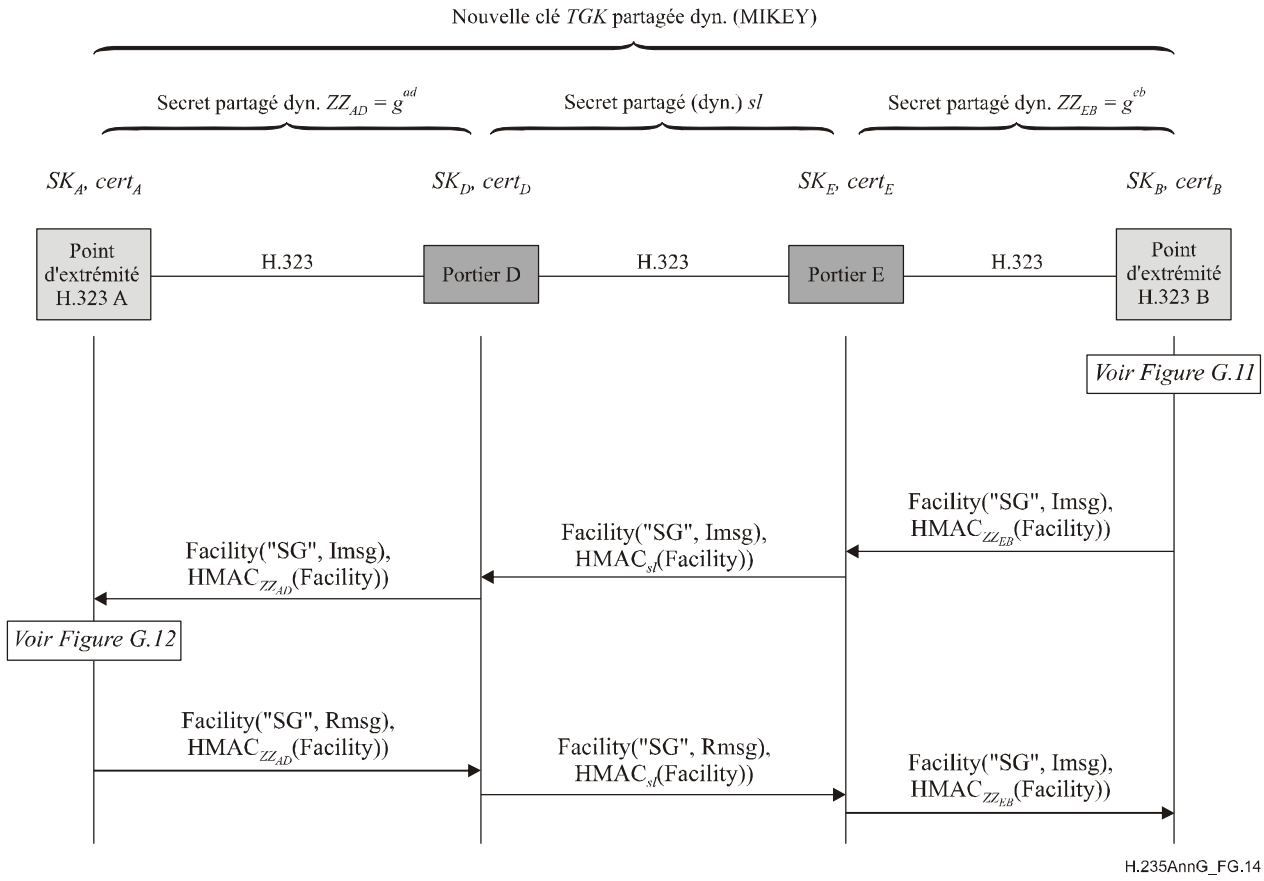

Figure G.14/H.235 – Exemple dans lequel le point d'extrémité B (initiateur) lance un recalcul de clé TGK et une mise à jour de lot CSB

NOTE – Le message Facility de confirmation du point d'extrémité A au point d'extrémité B est facultatif et il n'est nécessaire que lorsque le point d'extrémité B a également demandé un message de vérification R_message MIKEY au moyen du fanion V dans HDR MIKEY.

La présente annexe ne définit pas de procédure pour le cas où le recalcul de clé TGK et/ou la mise à jour de lot CSB sont invoqués par le répondeur; un complément d'étude est nécessaire.

G.9.3 Prise en charge de la tunnellisation H.245

Si d'autres canaux logiques doivent être ajoutés pendant une session, il faut mettre en œuvre le mode de tunnellisation H.245, dans lequel les messages H.245 tunnellisés sont acheminés dans un message Facility.

G.9.4 Algorithmes SRTP

Ce profil de sécurité doit utiliser la méthode HMAC-SHA1-32 tronquée avec une longueur d'étiquette d'authentification *n_tag* égale à 32 bits comme algorithme d'authentification par défaut pour le protocole RTP. D'autres longueurs d'étiquette d'authentification comme celles qui sont définies dans le Document [RFC 3711] doivent également être prises en charge et doivent être négociées par le biais du paramètre de politique de sécurité MIKEY en fonction des besoins.

G.9.5 Liste des identificateurs d'objet

"SG"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 71}	Indique un ClearToken de base pour l'Annexe F/H.235 dans le contexte de la présente annexe.

Appendice G.I

Option MIKEY-DHHMAC

Le présent appendice donné à titre d'information décrit comment mettre en œuvre l'option de gestion de clés MIKEY-DHHMAC dans ce profil de sécurité.

Pour cette option de gestion de clés, on considère uniquement une infrastructure de sécurité dans laquelle des clés partagées sont disponibles. L'option MIKEY-DHHMAC [MIKEY-DHHMAC] offre, comme propriété de sécurité, la confidentialité totale vers l'avant (PFS, *perfect-forward secrecy*) car elle possède le mécanisme Diffie-Hellman comme capacité intrinsèque. Par conséquent, cette option de gestion de clés est applicable lorsque la confidentialité totale vers l'avant est requise et qu'on ne dispose pas d'infrastructure PKI ou de certificats numériques.

Dans ce scénario, on suppose que des portiers se trouvent dans le domaine H.323.

La procédure décrite dans le présent paragraphe est la suivante: un secret partagé de bout en bout est établi entre les points d'extrémité H.323 A et B à l'aide d'une méthode de concordance de clés Diffie-Hellman. Cette méthode est appliquée pendant la phase d'enregistrement et d'admission RAS H.225.0 ou, dans le cas de plusieurs portiers, pendant l'échange de messages LRQ/LCF entre portiers. Le secret partagé Diffie-Hellman généré sert de clé d'authentification de bout en bout pendant toute la durée de l'appel. Le protocole MIKEY-DHHMAC, exécuté séparément pendant l'établissement d'appel, permet d'établir des secrets MIKEY fondés sur l'appel pour le canal support.

La Figure G.I-1 illustre un exemple dans lequel le point d'extrémité B appelle le point d'extrémité A par le biais d'un ou plusieurs portiers avec routage. Le flux est analogue à celui de la Figure G.4, sauf que le protocole MIKEY-DHHMAC est mis en œuvre. Dans le scénario, on considère un ou plusieurs portiers avec routage (modèle avec routage par portiers), les messages H.245 étant tunnellisés dans H.225.0 (démarrage rapide). La signalisation d'appel peut passer par un portier mais ce n'est pas obligatoire; un portier avec routage n'est donc pas nécessaire dans ce scénario.

NOTE 1 – Le diagramme de flux englobe également le cas du routage direct (avec portiers sans routage), dans lequel les messages de signalisation d'appel H.225.0 sont échangés directement entre les points d'extrémité sans être retransmis par les portiers.

Le diagramme de la Figure G.I-1 représente également le profil de sécurité de base de l'Annexe D/H.235, dans lequel chaque message est entièrement sécurisé (authentification et intégrité). Néanmoins, les flux de messages sont analogues lorsqu'on applique l'option d'authentification seule du profil de sécurité de base (non représenté). Dans ce cas, le code HMAC n'est pas calculé sur la totalité mais uniquement sur une partie (**ClearToken** dans **CryptoToken**) du message RAS/H.225.0.

Le flux de messages illustré correspond au cas où le point d'extrémité B (initiateur MIKEY) appelle le point d'extrémité A (répondeur MIKEY) à l'aide du démarrage rapide (voir la Figure G.I-1). Au cours de l'étape 1, les points d'extrémité H.323 A et B commencent par s'enregistrer auprès du portier au moyen du message **RRQ** et soumettent leur demi-clé DH (g^a et g^b). Le **ClearToken** (dans le **CryptoHashedToken**) doit être utilisé pour acheminer la demi-clé Diffie-Hellman pendant l'échange de messages **RRQ** et **ACF**. A cette fin, le champ **challenge** ne doit pas être utilisé.

La demi-clé Diffie-Hellman doit être acheminée dans **dhkey** dans le **ClearToken**. Le **ClearToken** doit utiliser l'identificateur d'objet "TG" (voir le § G.8.5) et non pas l'identificateur d'objet "T" du **ClearToken** de l'Annexe D, indiquant que ce profil de sécurité est utilisé conjointement avec l'Annexe D/H.235. Le portier doit conserver chaque demi-clé pendant toute la durée d'enregistrement du point d'extrémité. Lorsque les points d'extrémité exécutent des maintiens d'enregistrement ou utilisent un nouvel enregistrement simplifié (re-RRQ), ils ne doivent pas inclure de demi-clé DH. Le message **RCF** doit utiliser l'identificateur d'objet "TG" dans le **ClearToken** pour indiquer que le portier prend en charge ce profil de sécurité.

Le point d'extrémité B essaie d'appeler le point d'extrémité A et, pour cela, il demande l'admission au portier D (**ARQ**). Le message **ARQ** doit utiliser l'identificateur d'objet "TG" dans le **ClearToken**. Cet identificateur d'objet "TG" doit être utilisé dans tous les autres messages RAS dans le **ClearToken**.

Le scénario englobe plusieurs portiers en chaîne. La recherche du point d'extrémité distant doit se faire conformément au § 8.1.6/H.323 "Signalisation facultative par l'extrémité appelée" au moyen des messages **LRQ/LCF**. Il s'agit de la manière dont le point d'extrémité d'origine localise la zone du portier distant et obtient la demi-clé Diffie-Hellman du point d'extrémité appelé cible. Si le portier E a besoin de localiser la zone du portier distant, il envoie un message **LRQ**. Dans le cas de la multidiffusion, le generalID dans le **CryptoToken** du message **LRQ** ne doit pas être utilisé. Si le portier D ne prend pas en charge ce profil, il retourne le message **LRJ**. Dans le cas contraire, il retourne le message **LCF** incluant la demi-clé Diffie-Hellman du point d'extrémité A ou, s'il répond ensuite par un message **ACF** contenant la demi-clé Diffie-Hellman du point d'extrémité A ou, s'il ne parvient pas à localiser le point d'extrémité distant A, il retourne le message **ARJ**.

Les communications entre deux portiers doivent être sécurisées conformément à l'Annexe D/H.235. Pour cela, on suppose qu'un secret partagé commun *sl* est disponible. Comme le message **LRQ** entre portiers est généralement un message de multidiffusion, le secret partagé *sl* ne peut généralement pas être un secret partagé entre deux mais on suppose qu'il s'agit en fait d'un secret partagé par un groupe au sein du nuage potentiel de portiers. Cette hypothèse limite l'évolutivité dans le cas général et ne permet pas de procéder à une authentification de la source. Toutefois, on considère que dans les réseaux d'entreprise comportant un petit nombre de portiers bien connus, ces contraintes et ces limitations de sécurité restent acceptables. La sécurisation des communications de multidiffusion entre portiers au moyen de signatures numériques permettrait de surmonter ces limitations, mais un complément d'étude est nécessaire.

Le point d'extrémité B obtient la demi-clé Diffie-Hellman du point d'extrémité A (**ACF**). Le message **ACF** doit contenir la clé Diffie-Hellman du point d'extrémité appelé dans **dhkey** dans le **ClearToken** de base de l'Annexe D, celui-ci utilisant l'identificateur d'objet "TG" et non l'identificateur d'objet "T". Tous les autres champs du **ClearToken** doivent être laissés en l'état par ce profil de sécurité.

NOTE 2 – Les points d'extrémité fonctionnent avec une demi-clé DH qui est statique pendant toute la durée d'enregistrement et pour tous les appels. Il ne doit pas s'agir d'une faiblesse sur le plan de la sécurité étant donné que chaque point d'extrémité applique des demi-clés vraiment aléatoires.

Toutefois, les points d'extrémité doivent fournir une nouvelle valeur aléatoire de 512 bits (autrement dit 64 octets) dans **challenge** en même temps que leur demi-clé DH, voir la section 2.3 du Document [RFC 2631]. Ces valeurs de **challenge**, qui sont fondées sur l'appel, permettent de garantir que les clés DH sont générées de façon aléatoire et en temps utile, comme requis.

Le point d'extrémité d'origine B peut alors calculer g^{ab} puis le secret partagé dynamique ZZ_{AB} au moyen d'un **challenge** aléatoire, le résultat étant obtenu à partir de MIKEY-PRF(g^{ab} , 0x12F905FE || **challenge**) (voir les sections 4.1.2 à 4.1.5 du Document [RFC 3830]). La fonction MIKEY-PRF permet ensuite de déterminer la clé d'authentification (*Ma*) (voir les sections 4.1.2 à 4.1.5 du Document [RFC 3830]).

Au cours de l'étape 2, le point d'extrémité d'origine B doit générer de nouvelles valeurs aléatoires MIKEY *y* avec la demi-clé g^y correspondante puis élaborer l'I_message MIKEY Imsg conformément au protocole MIKEY-DHHMAC au moyen de *Ma*.

L'I_message MIKEY doit être codé binaire.

Le point d'extrémité d'origine B doit toujours inclure sa demi-clé DH dans **dhkey** dans un **ClearToken**, ce qui permet de prendre également en charge le modèle à routage direct avec portiers. Le **ClearToken** doit être inclus dans le message Setup et doit être envoyé au point d'extrémité homologue A. Un portier avec routage doit transmettre le **ClearToken** acheminé (sans modification des messages MIKEY) au saut suivant.

Le point d'extrémité de destination A calcule alors g^{ab} et le secret partagé dynamique ZZ_{AB} à partir de MIKEY-PRF(g^{ab} , 0x12F905FE || **challenge**) (voir les sections 4.1.2 à 4.1.5 du Document [RFC 3830]). La fonction MIKEY-PRF permet ensuite de déterminer la clé d'authentification (*Ma*) (voir les sections 4.1.2 à 4.1.5 du Document [RFC 3830]). Le point d'extrémité A génère une valeur aléatoire MIKEY *w* et calcule g^w. Il calcule ensuite la clé *TGK* au moyen des demi-clés DH reçues.

A partir de la clé *TGK*, le point d'extrémité de destination A peut ensuite déterminer les clés de session SRTP comme décrit à la section 4.3 du Document [RFC 3711] (non représenté sur les figures).

Le point d'extrémité A peut élaborer un R_message Rmsg analogue. Ce R_message est acheminé dans le message CallProceeding-to-Connect (CP/C). Rmsg est le message de réponse MIKEY correspondant qui est envoyé dans un message CallProceeding-to-Connect (CP/C) au point d'extrémité B.

Le message CallProceeding-to-Connect (CP/C) est envoyé au point d'extrémité B.

Le point d'extrémité B récupère la demi-clé DH et calcule la clé *TGK*. Il détermine ensuite les clés de session SRTP à partir de la clé TGK comme décrit à la section 4.3 du Document [RFC 3711] (non représenté sur la figure).

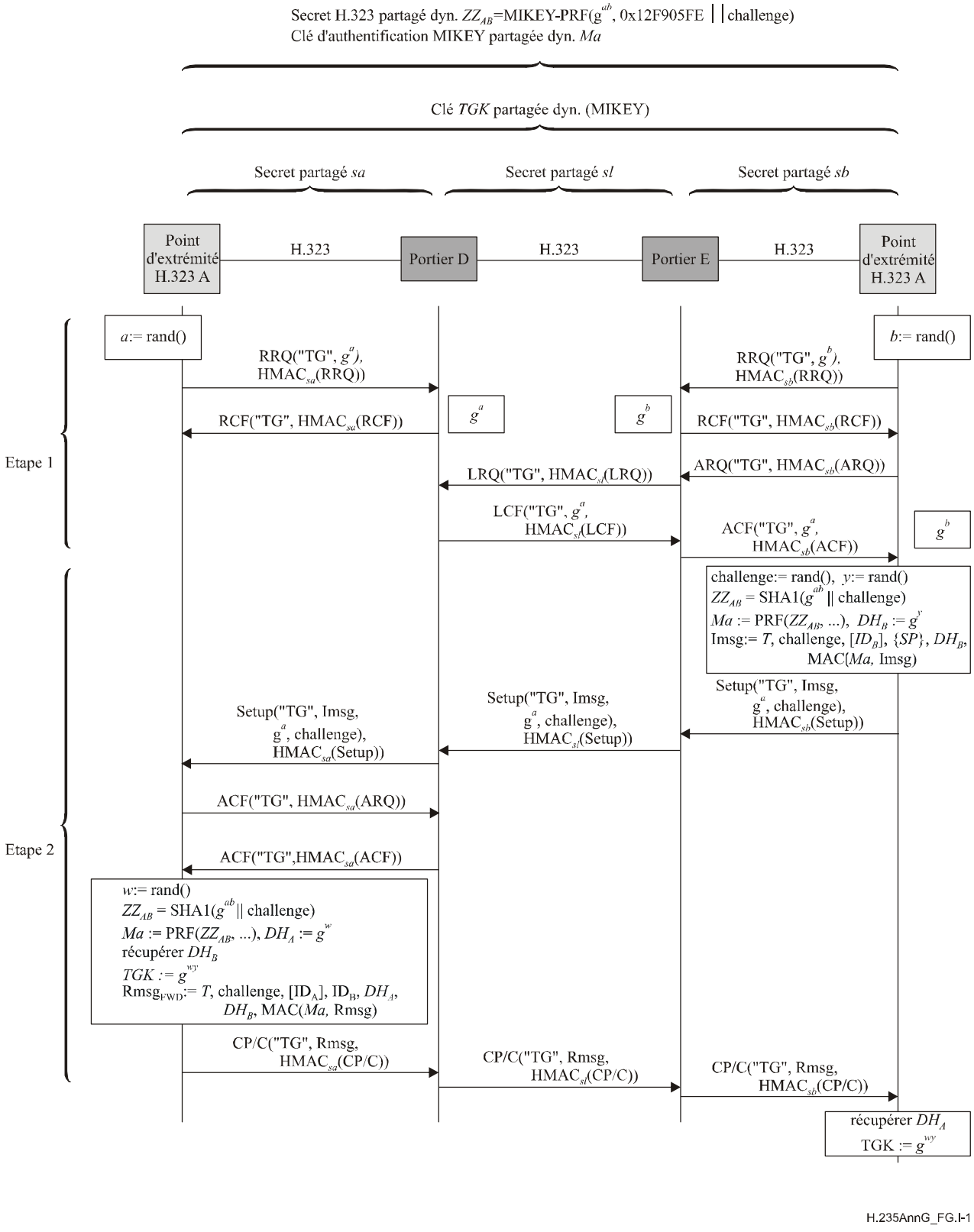

Figure G.I-1/H.235 – Exemple dans lequel le point d'extrémité B appelle le point d'extrémité A (routage par portiers) avec MIKEY-DHHMAC

G.I.1 Terminaison d'un appel H.323

Comme les points d'extrémité considérés conservent l'état pour les protocoles MIKEY et SRTP, une procédure de terminaison à part entière est indispensable. La Figure G.I-2 donne un exemple de flux de messages correspond au cas où le point d'extrémité B (initiateur MIKEY) termine un appel. Fondamentalement, le flux est conforme au § 8.5/H.323 " Phase E – Fin de la communication".

NOTE – La figure illustre également les procédures de retrait facultatives correspondant au cas où les points d'extrémité se désenregistrent complètement. Les points d'extrémité doivent alors éliminer également la clé DH privée (*a* ou *b*) et la demi-clé DH publique (g^a ou g^b).

Comme la procédure de terminaison d'un appel est indépendante de ce profil de sécurité, il est possible d'utiliser n'importe quel identificateur d'objet applicable du profil de sécurité sous-jacent (Annexe D, F, etc.); la Figure G.I-2 n'indique donc pas d'identificateur d'objet.

Si le point d'extrémité s'enregistre à nouveau auprès du portier, il faut générer de nouvelles demi-clés DH. Toutefois, un désenregistrement complet n'est pas nécessaire dans tous les cas de terminaison d'appel. Si le point d'extrémité décide de rester enregistré auprès du portier, il est possible de continuer à utiliser les demi-clés DH statiques.

Dans le cas où les points d'extrémité restent enregistrés et où le retrait n'est pas appliqué, les points d'extrémité doivent éliminer uniquement les informations liées à l'appel (demi-clé DH de leur homologue, **challenge**, clés MIKEY *Me*, *Ma*, *TGK* et informations de session SRTP connexes).

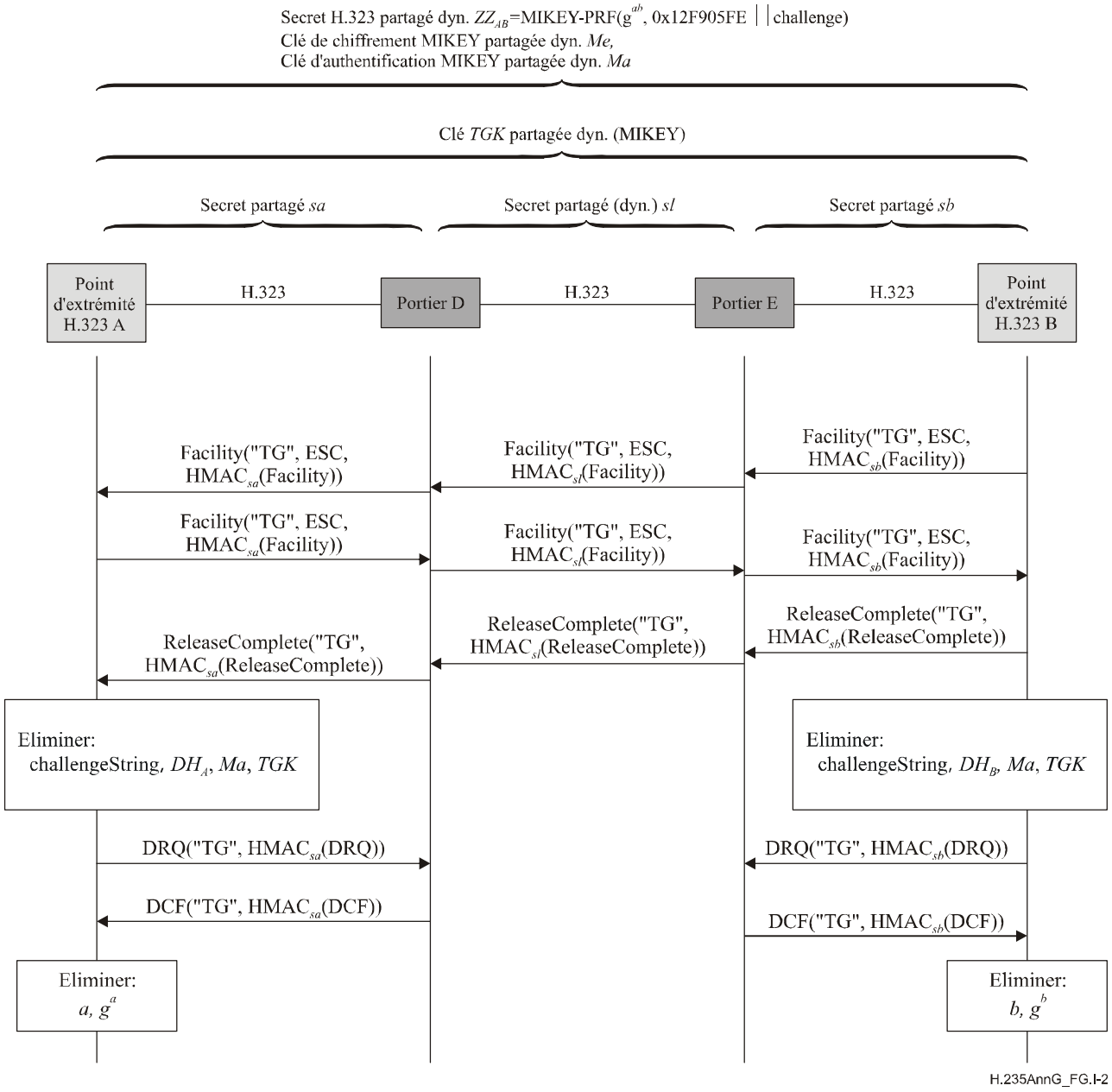

Figure G.I-2/H.235 – Exemple dans lequel le point d'extrémité B termine un appel

G.I.2 Recalcul de clé TGK et mise à jour de lot CSB

Le protocole MIKEY prend intrinsèquement en charge le recalcul de clé TGK et/ou la mise à jour des informations de lot CSB. Le profil de la présente annexe doit utiliser à cette fin la procédure MIKEY-DHHMAC de la section 3.1 du Document [MIKEY-DHHMAC], permettant de mettre à jour la clé TGK avant expiration ou de mettre à jour d'autres informations sans modifier la clé TGK.

Le mécanisme de recalcul de clé TGK et de mise à jour de lot CSB est utile pour protéger un ensemble de canaux logiques relevant de la même politique de sécurité. Pour cela, il est recommandé d'exécuter le protocole (complet) MIKEY-DHHMAC comme décrit ci-dessus uniquement pour le premier canal logique. Pour les canaux logiques suivants pour lesquels on doit appliquer la même politique de sécurité MIKEY ou la même clé TGK, il convient d'utiliser le mécanisme de mise à jour de lot CSB sans le mécanisme de recalcul de clé TGK du présent paragraphe en faisant référence à l'identificateur de lot CSB initial et en omettant les données de clé TGK mises à jour. Cela permet d'établir des canaux logiques ou des sessions de chiffrement

MIKEY de façon plus efficace que ne le permet l'exécution du protocole MIKEY complet pour chaque canal logique.

Les messages de recalcul de clé TGK ou de mise à jour de lot CSB MIKEY doivent être encapsulés et acheminés dans un **MiscellaneousCommand** dans un message Facility. Le **tokenOID** du **ClearToken** doit être mis à "TG".

Si le protocole MIKEY est exécuté au "niveau média", le point d'extrémité B doit déterminer le canal logique pour lequel il convient d'appliquer le recalcul de clé TGK et/ou la mise à jour de lot CSB. Le point d'extrémité A en tant que répondeur utilise aussi le **MiscellaneousCommand** dans Facility pour acheminer l'éventuel R_message MIKEY.

Pour le recalcul de clé TGK (voir la Figure G.I-3), le point d'extrémité B en tant qu'initiateur MIKEY doit générer une nouvelle clé TGK. **parameterValue** doit contenir l'I_message MIKEY codé binaire correspondant.

Le point d'extrémité A en tant que répondeur peut confirmer le message de recalcul de clé TGK obtenu si nécessaire à la demande du point d'extrémité B. Le point d'extrémité A élabore un R_message analogue, qu'il achemine dans le message Facility au point d'extrémité B.

Pour la mise à jour de lot CSB, la procédure est analogue à la procédure ci-dessus sauf que le message MIKEY ne doit pas contenir de clé TGK.

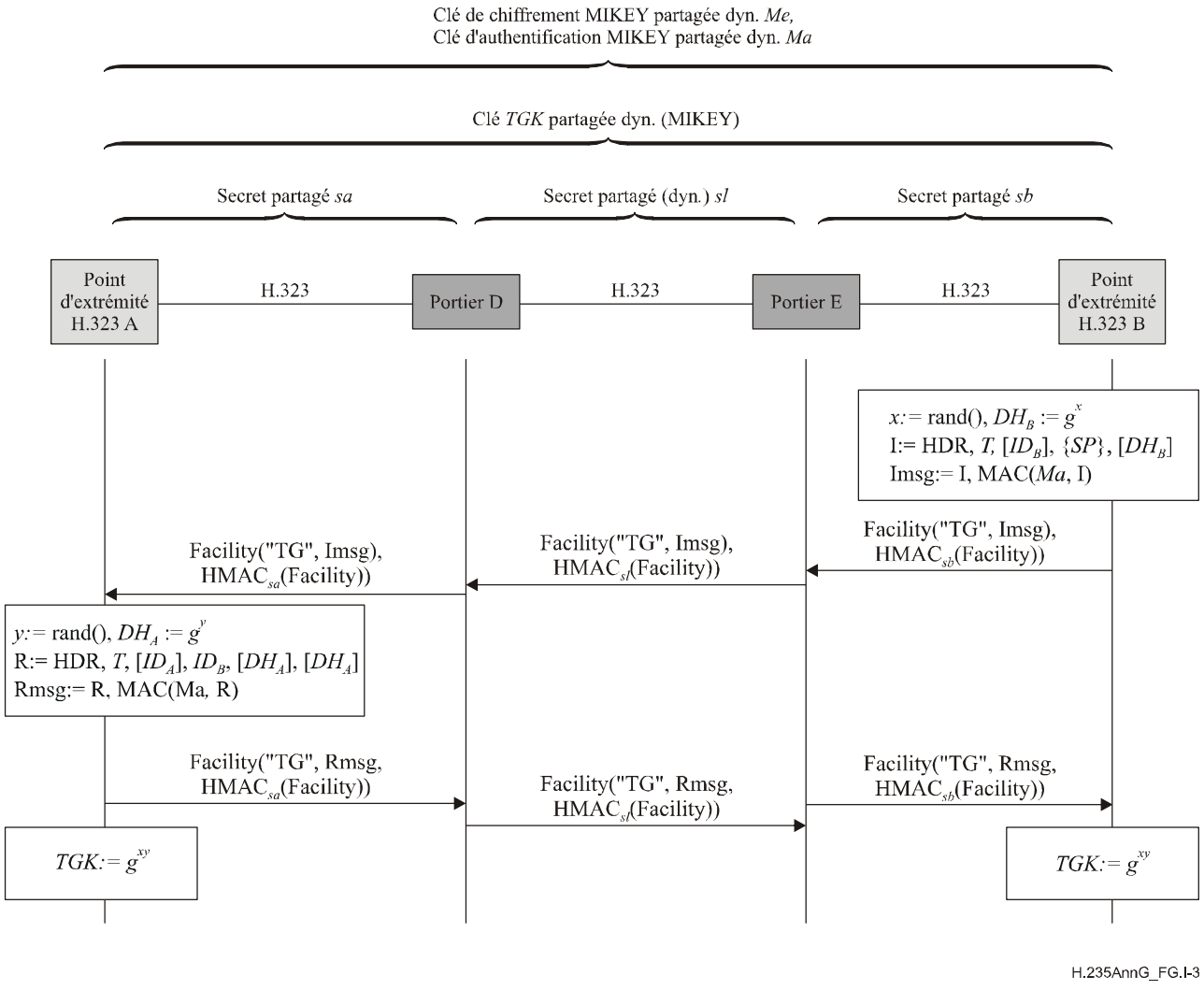

Figure G.I-3/H.235 – Exemple dans lequel le point d'extrémité B met à jour une clé

La présente annexe ne définit pas de procédure pour le cas où le recalcul de clé TGK et/ou la mise à jour de lot CSB sont invoqués par le répondeur; un complément d'étude est nécessaire.

Appendice G.II

Utilisation de l'Annexe I/H.235 pour l'établissement d'un secret prépartagé

Le présent appendice donné à titre d'information définit comment mettre en œuvre la procédure DRC de l'Annexe I/H.235 pour l'établissement d'un secret prépartagé ZZ_{AB} entre les points d'extrémité B et A, dans l'hypothèse où il n'existe pas a priori de tel secret de bout en bout. La méthode décrite dans le présent appendice s'applique au scénario avec un seul portier ou avec plusieurs portiers. La procédure du présent appendice ne fait pas intervenir de calcul DH pendant l'enregistrement et l'admission RAS mais met en œuvre un chiffrement symétrique.

La Figure G.II-1 montre l'exemple d'un diagramme de flux dans le cas où le point d'extrémité B appelle le point d'extrémité A.

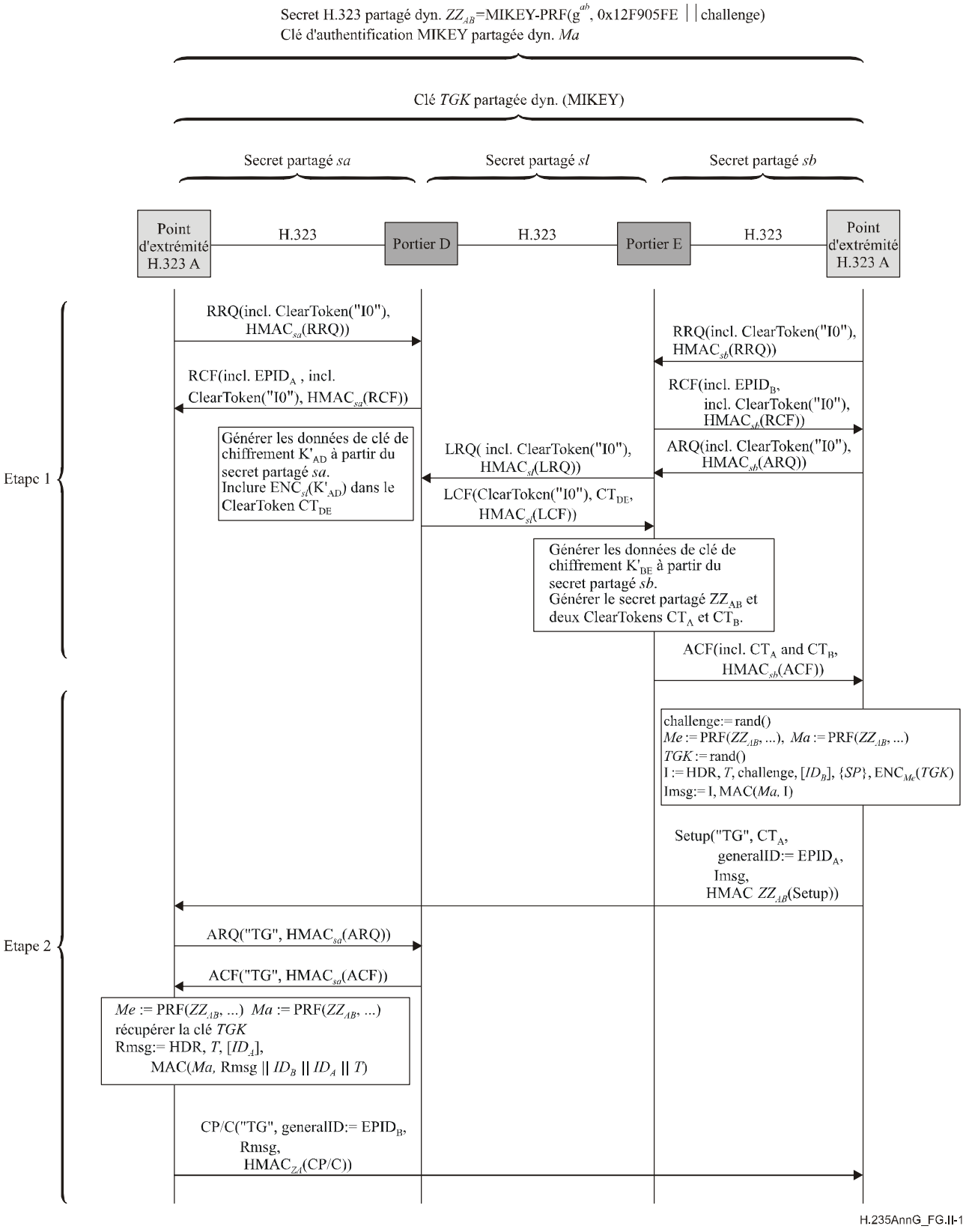

Figure G.II-1/H.235 – Exemple dans lequel le point d'extrémité B appelle le point d'extrémité A (routage sans portier) avec MIKEY-PS et la procédure DRC de l'Annexe I/H.235

G.II.1 Terminaison d'un appel H.323

La procédure de terminaison d'un appel H.323 se déroule comme décrit au § G.8.1.

G.II.2 Recalcul de clé TGK et mise à jour de lot CSB

La procédure de recalcul de clé TGK et/ou de mise à jour de lot CSB se déroule comme décrit au § G.8.2.

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