UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T H.530

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

(03/2002)

SÉRIE H: SYSTÈMES AUDIOVISUELS ET MULTIMÉDIAS

Procédures de mobilité et de collaboration – Sécurité pour les systèmes et services multimédias mobiles

Procédures de sécurité symétrique pour la mobilité des systèmes H.323 selon la Recommandation H.510

Recommandation UIT-T H.530

RECOMMANDATIONS UIT-T DE LA SÉRIE H

SYSTÈMES AUDIOVISUELS ET MULTIMÉDIAS

CARACTÉRISTIQUES DES SYSTÈMES VISIOPHONIQUES	H.100–H.199
INFRASTRUCTURE DES SERVICES AUDIOVISUELS	
Généralités	H.200–H.219
Multiplexage et synchronisation en transmission	H.220–H.229
Aspects système	H.230–H.239
Procédures de communication	H.240–H.259
Codage des images vidéo animées	H.260–H.279
Aspects liés aux systèmes	H.280–H.299
SYSTÈMES ET ÉQUIPEMENTS TERMINAUX POUR LES SERVICES AUDIOVISUELS	H.300–H.399
SERVICES COMPLÉMENTAIRES EN MULTIMÉDIA	H.450–H.499
PROCÉDURES DE MOBILITÉ ET DE COLLABORATION	
Aperçu général de la mobilité et de la collaboration, définitions, protocoles et procédures	H.500–H.509
Mobilité pour les systèmes et services multimédias de la série H	H.510–H.519
Applications et services de collaboration multimédia mobile	H.520–H.529
Sécurité pour les systèmes et services multimédias mobiles	**H.530–H.539**
Sécurité pour les applications et services de collaboration multimédia mobile	H.540–H.549
Procédures d'interfonctionnement de la mobilité	H.550–H.559
Procédures d'interfonctionnement de collaboration multimédia mobile	H.560–H.569

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

Recommandation UIT-T H.530

Procédures de sécurité symétrique pour la mobilité des systèmes H.323 selon la Recommandation H.510

Résumé

La présente Recommandation décrit des procédures de sécurité pour un environnement multimédia H.323 avec mobilité. Elle décrit en détail les procédures de sécurité pour la Rec. UIT-T H.510.

Source

La Recommandation H.530 de l'UIT-T, élaborée par la Commission d'études 16 (2001-2004) de l'UIT-T, a été approuvée le 29 mars 2002 selon la procédure définie dans la Résolution 1 de l'AMNT.

Mots clés

Annexe D/H.235, authentification, cryptage, gestion de clés, intégrité, mobilité, profil de sécurité, sécurité multimédia.

AVANT-PROPOS

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

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

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

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

NOTE

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

DROITS DE PROPRIÉTÉ INTELLECTUELLE

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

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

TABLE DES MATIÈRES

Recommandation UIT-T H.530

Procédures de sécurité symétrique pour la mobilité des systèmes H.323 selon la Recommandation H.510

1 Domaine d'application

La présente Recommandation porte sur des procédures de sécurité dans les environnements H.323 avec mobilité, notamment pour la Rec. UIT-T H.510, pour laquelle lesdites procédures sont décrites en détail.

2 Introduction

Jusque-là, les capacités de signalisation de la Rec. UIT-T H.235 dans ses versions 1 et 2 [4] sont conçues pour prendre en charge la sécurité dans des environnements H.323 [5] essentiellement sans mobilité. Dans ces environnements et dans les systèmes multimédias, une mobilité limitée est possible dans des zones de portier; la Rec. UIT-T H.323 [5] en général et la Rec. UIT-T H.235 [4] en particulier ne permettent qu'une prise en charge très réduite de la sécurité des utilisateurs et des terminaux mobiles lorsqu'ils passent d'un domaine à un autre et que de nombreuses entités interviennent dans un environnement réparti avec mobilité, par exemple.

Les scénarios H.323 avec mobilité décrits dans la Rec. UIT-T H.510 [6] relatifs à la mobilité des terminaux étant souples et dynamiques, ils constituent une situation nouvelle, notamment du point de vue de la sécurité. Lorsqu'ils passent d'un domaine à un autre, les terminaux mobiles et les utilisateurs H.323 doivent être authentifiés par le domaine étranger visité. De même, les utilisateurs mobiles souhaitent avoir la preuve de la véritable identité du domaine visité. En outre, il peut aussi être utile d'obtenir la preuve de l'identité des terminaux en plus de l'authentification des utilisateurs. Par conséquent, une authentification mutuelle de l'utilisateur et du domaine visité est absolument nécessaire, l'authentification de l'identité du terminal étant facultative.

D'une manière générale, seul l'utilisateur mobile n'est connu que du domaine de rattachement dans lequel il est abonné et un mot de passe lui est attribué; ainsi, le domaine visité ne connaît pas cet utilisateur au départ. En tant que tel, le domaine visité ne partage aucune relation de sécurité établie avec l'utilisateur mobile et le terminal mobile. Concernant l'authentification et l'autorisation de l'utilisateur mobile et du terminal mobile, le domaine visité pourrait déléguer certaines tâches liées à la sécurité, telles que les contrôles d'autorisation ou la gestion des clés, au domaine de rattachement via des entités de réseau et de service intermédiaires. Pour cela, il faut sécuriser les communications et la gestion des clés entre le domaine visité et le domaine de rattachement.

En principe, les environnements H.323 avec mobilité sont plus ouverts que les réseaux H.323 fermés, mais il faut bien évidemment sécuriser aussi de façon appropriée les tâches liées à la gestion des clés. Par ailleurs, il faut aussi protéger contre toute altération malveillante les communications intra et interdomaines de mobilité.

En résumé, la présente Recommandation décrit un concept générique de sécurité applicable à la mobilité entre domaines pour les applications et services multimédias. Les détails techniques qu'elle contient concernent une mise en œuvre pour les Recs. UIT-T H.323 et H.510 en particulier, mais il est envisageable de les étendre à d'autres environnements.

3 Conventions de la spécification

Dans la présente Recommandation, on utilise les conventions suivantes:

– l'emploi du futur et de "doit/doivent" indiquent une prescription impérative;

– l'emploi de "devrait/devraient" indique une mesure suggérée mais facultative;

– l'emploi de "peut/peuvent" indique une mesure possible mais non recommandée.

Sauf indication explicite d'une autre Recommandation, les références aux paragraphes, sous-paragraphes, annexes et appendices renvoient à des éléments de la présente Recommandation. Par exemple, la référence "1.4" renvoie au § 1.4 de la présente Recommandation; la référence "6.4/H.245" renvoie au § 6.4 de la Rec. UIT-T H.245.

Il est question, dans la présente Recommandation, de plusieurs entités fonctionnelles pour la mobilité telles que les éléments frontière. On trouvera une description générale de ces éléments fonctionnels et de leur interaction dans la Rec. UIT-T H.510 [6]. La présente Recommandation décrit uniquement la sécurité liée à la mobilité de l'utilisateur/du terminal, elle ne fait donc que mentionner brièvement l'interaction avec les autres entités fonctionnelles pour la mobilité telles que les proxys de routage pour la mobilité (entités VLF, HLF par exemple); ces entités fonctionnelles ne sont pas considérées comme faisant partie intégrante de la présente Recommandation. Plus particulièrement, l'architecture de sécurité ne dépend pas de la présence ou de l'absence de ces éléments fonctionnels et elle ne nécessite pas non plus une séparation des fonctions concernées. Pour plus de simplicité, on suppose en revanche, dans la présente Recommandation, que ces fonctions sont situées au même endroit dans des éléments de réseau composites, mais, dans un souci d'exhaustivité, ces entités de réseau sont représentées sous forme d'entités fonctionnelles décomposées. Bien entendu, il serait aisé d'étendre les concepts de sécurité si l'on veut tenir compte de ces éléments lorsqu'ils sont présents ou si l'on veut les décomposer et les séparer sur le plan fonctionnel.

Toutes les entités de réseau facultatives apparaissent dans des cases en pointillés sur les diagrammes. S'agissant du domaine de rattachement, une entité d'authentification (AuF) fonctionnant comme un service de sécurité principal peut être séparée ou peut être située au même endroit que l'élément frontière du domaine de rattachement ou que d'autres entités H.323 appropriées [5], par exemple le portier du domaine de rattachement (H-GK). L'instanciation à opérer en pratique fait l'objet d'une implémentation locale.

Dans la présente Recommandation, la **fonction d'authentification** (**AuF**) désigne l'entité fonctionnelle de sécurité qui appartient au domaine de rattachement et qui maintient une relation de sécurité avec les utilisateurs mobiles abonnés et les terminaux mobiles abonnés en cas de nécessité. Parmi les tâches non décrites dans la présente Recommandation, la fonction AuF doit au moins:

- évaluer les messages **AuthenticationRequest** entrants provenant d'un domaine visité, vérifier l'authenticité et l'intégrité de ces messages et, en particulier, authentifier l'utilisateur mobile et facultativement le terminal mobile (MT, *mobile terminal*), si cela est prévu et souhaité;
- si l'utilisateur/le terminal mobile a pu être authentifié, décider d'accorder ou non l'autorisation. Le processus exact suivi par la fonction AuF pour prendre cette décision est hors du domaine d'application de la présente Recommandation, mais il pourrait être utile que cette fonction utilise une certaine base de données politiques ou certaines règles d'accès;
- puis apporter son assistance au domaine visité dans sa tâche liée à la gestion des clés; en particulier, la fonction AuF doit authentifier une demi-clé Diffie-Hellman et l'identificateur GK_{ID} qu'elle reçoit du domaine visité en utilisant le secret partagé avec l'utilisateur correspondant;
- enfin, communiquer au domaine visité la décision prise concernant l'autorisation du point de vue de la sécurité et lui transmettre la demi-clé Diffie-Hellman et l'identificateur GK_{ID} authentifiés.

La fonction AuF peut être assimilée à un module de sécurité – éventuellement séparé physiquement des autres entités fonctionnelles – avec des fonctionnalités de sécurité spécifiques (stockage des clés protégées, prise en charge d'un algorithme et d'un mécanisme cryptographiques, accès sécurisé pour l'administration et la maintenance, fiabilité, etc.). Toutefois, on ne suppose pas, dans la présente Recommandation, que l'une quelconque de ces fonctionnalités soit présente dans la fonction AuF. En revanche, la fonction AuF peut tout aussi bien être située au même endroit que d'autres entités fonctionnelles H.323 [5] dans le domaine de rattachement, par exemple dans l'élément frontière, dans le portier, dans un proxy de routage pour la mobilité (MRP, *mobility routing proxy*) ou dans toute autre entité appropriée. Le concept de la fonction AuF ne préjuge pas de la meilleure façon d'implémenter cette fonction, à savoir sous forme matérielle, sous forme logicielle ou sous la forme d'une combinaison des deux.

Dans la présente Recommandation, on introduit un **proxy de routage pour la mobilité (MRP)**, entité fonctionnelle facultative qui joue le rôle d'une entité fonctionnelle intermédiaire, terminant l'association de sécurité d'une liaison bond par bond. Le proxy MRP doit retransmettre les jetons de sécurité en calculant à nouveau les codes d'authentification des messages bond par bond figurant dans le jeton **CryptoToken**. Il peut inclure la fonctionnalité d'une entité fonctionnelle de gestion de la mobilité (par exemple d'une entité HLF ou VLF ou de toute autre entité de service principale pour la mobilité). Le proxy MRP peut se trouver dans le domaine visité ou dans le domaine de rattachement ou dans tout autre domaine traversé.

Lorsqu'un proxy MRP illustré n'intervient pas dans la communication réelle, les liaisons bond par bond qui entrent dans le proxy MRP et celles qui en sortent doivent être considérées comme appartenant à la même association de sécurité et le jeton **CryptoToken** n'a pas à être recalculé.

La présente Recommandation utilise le terme **password (mot de passe)** pour désigner une chaîne de mot de passe saisie par un utilisateur. Il s'agit, dans la présente Recommandation, de la clé de sécurité attribuée que l'utilisateur mobile partage avec son domaine de rattachement. Ce mot de passe de l'utilisateur et le secret partagé de l'utilisateur qui en découle doivent être utilisés aux fins d'authentification de l'utilisateur.

A la différence du mot de passe, un **shared secret (secret partagé)** est la clé de sécurité qui fait partie des paramètres de sécurité pour les algorithmes cryptographiques; il peut être déduit d'un mot de passe (voir la procédure 10.3.5 de la Rec. UIT-T H.235 [4]) ou il peut être attribué par la configuration ou par d'autres moyens.

De même, le domaine de rattachement peut avoir attribué au terminal mobile un secret partagé distinct pour la sécurité aux fins d'authentification du terminal.

L'attribution et la distribution des mots de passe et des secrets partagés entre les entités fonctionnelles sont hors du domaine d'application de la présente Recommandation.

Le terme **service relationship (relation de service)** est employé dans la présente Recommandation pour désigner une association de sécurité établie entre deux entités fonctionnelles, par exemple entre un élément frontière du domaine visité (V-BE, *visited border element*) et un élément frontière du domaine de rattachement (H-BE, *home border element*). Parmi les paramètres d'une telle relation de service, il faut au moins qu'une clé partagée *ZZn* soit présente, permettant de sécuriser le trafic entre les entités fonctionnelles (par exemple IPSEC ou Annexe D/H.235 [4]).

Le message **AuthenticationRejection** utilisé dans la présente Recommandation indique un échec du contrôle de sécurité par la fonction AuF. Il doit contenir les mêmes jetons **ClearToken** et **CryptoToken** que le message **AuthenticationConfirmation** associé.

Les identificateurs d'objet sont désignés par un symbole dans le texte (par exemple "G1"). Le paragraphe 8.6 donne la liste des valeurs numériques effectives de ces identificateurs d'objet.

4 Termes et définitions

Dans la présente Recommandation, on utilise les définitions données au paragraphe 3 des Recs. UIT-T H.323 [5] H.225.0 [1] et de son Annexe G [2], H.235 [4], H.501 [3], H.510 [6] et X.800 [7] ainsi que les définitions suivantes.

4.1 fonction d'authentification (AuF, *authentication function*): entité fonctionnelle de sécurité qui appartient au domaine de rattachement et qui maintient une relation de sécurité avec les utilisateurs mobiles abonnés et les terminaux mobiles abonnés.

4.2 pouvoir: dans la présente Recommandation, un pouvoir [par exemple $HMAC_{ZZ}(GK_{ID})$ ou $HMAC_{ZZ}(W)$] désigne des données que la fonction AuF a cryptées au moyen du secret *ZZ* qu'elle partage avec l'utilisateur mobile. Le pouvoir est transféré pour prouver que l'autorisation a été accordée et qu'elle a été vérifiée en temps voulu.

4.3 élément frontière du domaine de rattachement (H-BE, *home border element*): élément frontière (BE) situé dans le domaine de rattachement.

4.4 proxy de routage pour la mobilité (MRP, *mobility routing proxy*): entité fonctionnelle facultative qui joue le rôle d'une entité fonctionnelle intermédiaire, terminant l'association de sécurité d'une liaison bond par bond.

4.5 mot de passe: chaîne de mot de passe saisie par l'utilisateur.

4.6 relation de service: association de sécurité établie entre deux entités fonctionnelles pour laquelle au moins une clé partagée est présente.

4.7 secret partagé: clé de sécurité pour les algorithmes cryptographiques; le secret partagé peut être déduit d'un mot de passe.

4.8 élément frontière du domaine visité (V-BE, *visited border element*): élément frontière (BE) situé dans le domaine visité.

5 Abréviations et symboles

La présente Recommandation utilise les abréviations et symboles suivants:

AuF	fonction d'authentification (*authentication function*), voir la Rec. UIT-T H.510 [6]
BE	élément frontière (*border element*), voir l'Annexe G/H.225.0 [2]
CH_n	défi numéro *n* (*challenge number n*)
DH	Diffie-Hellman
EP_{ID}	identificateur de point d'extrémité MT (*MT endpoint identifier*), voir la Rec. UIT-T H.225.0 [1]
GK	portier (*gatekeeper*), voir la Rec. UIT-T H.510 [6]
GK_{ID}	identificateur de portier du domaine visité (*visited gatekeeper identifier*), voir la Rec. UIT-T H.225.0 [1]
GRJ	rejet de portier (*gatekeeper reject*)
GRQ	demande de portier (*gatekeeper request*)
H-BE	élément frontière du domaine de rattachement (*home BE*)
H-GK	portier du domaine de rattachement (*home GK*)
HLF	fonction de localisation du domaine de rattachement (*home location function*)

HMAC-SHA1-96	code d'authentification de message haché avec l'algorithme 1 de hachage sécurisé (*hashed message authentication code with secure hash algorithm 1*)
$HMAC_Z$	code/réponse d'authentification de message haché par clé avec secret partagé *Z*; si *Z* n'est pas montré, on applique le secret lié au bond suivant
IPSEC	sécurité du protocole Internet (*Internet protocol security*)
K	clé de session/liaison dynamique (*dynamic session/link key*)
MRP	proxy de routage pour la mobilité (*mobility routing proxy*)
MT	terminal mobile (*mobile terminal*), voir la Rec. UIT-T H.510 [6]
NTP	protocole relatif au temps dans le réseau (*network time protocol*)
OID	identificateur d'objet (*object identifier*)
PKI	infrastructure à clés publiques (*public-key infrastructure*)
PW	mot de passe de l'utilisateur mobile (*mobile user password*)
R_1	nombre aléatoire (*random number*)
RIP	demande en cours (*request in progress*)
RRJ	rejet d'enregistrement (*registration reject*)
RRQ	demande d'enregistrement (*registration request*)
SNTP	protocole simple relatif au temps dans le réseau (*simple network time protocol*)
T_n	horodate numéro *n* (*timestamp number n)*
V-BE	élément frontière du domaine visité (*visited BE*)
V-GK	portier du domaine visité (*visited GK*)
VLF	fonction de localisation du domaine visité (*visitor location function*)
W	valeur composite avec combinaison arithmétique de demi-clés Diffie-Hellman
WT	jeton ClearToken pour la mobilité
XT	jeton CryptoToken pour l'authentification du terminal mobile
ZZ	secret partagé/mot de passe de l'utilisateur mobile, partagé avec la fonction AuF correspondante
ZZMT	secret partagé du terminal mobile (MT), partagé avec la fonction AuF correspondante
ZZ_n	secret partagé numéro *n*
$\oplus$	opérateur OU exclusif sur les bits

6 Références

6.1 Références normatives

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

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

[2] Recommandation UIT-T H.225.0, Annexe G (Projet), *Communication entre domaines administratifs*.

[3] Recommandation UIT-T H.501 (2002), *Protocole de gestion de la mobilité et communications interdomainiales dans les systèmes multimédias*.

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

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

[6] Recommandation UIT-T H.510 (2002), *Mobilité pour systèmes multimédias H.323*.

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

6.2 Références non normatives et bibliographie

[8] IETF RFC 1305 (1992), Network Time Protocol (Version 3) Specification, Implementation and Analysis [*Spécification, mise en œuvre et analyse du protocole relatif au temps dans le réseau (version 3)*]; Internet Engineering Task Force.

[9] IETF RFC 2030 (1996), Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI (*Protocole simple relatif au temps dans le réseau (SNTP) version 4 pour IPv4, IPv6 et OSI*); Internet Engineering Task Force.

7 Prescriptions de sécurité et contraintes pour la mobilité

La gestion de la mobilité multimédia et son application aux environnements H.323 avec mobilité sont soumises aux prescriptions de sécurité et contraintes suivantes:

- Dans le cadre de la présente Recommandation, il faut prendre en charge et améliorer l'interfonctionnement, sur le plan de la sécurité, des systèmes sécurisés H.323 lorsqu'ils sont déployés dans un environnement avec mobilité avec des composantes réparties et des domaines gérés séparément.
- L'utilisateur mobile doit être authentifié lorsqu'il passe d'un domaine à un autre. Cette authentification est essentielle pour pouvoir accorder l'accès et la permission de service à l'utilisateur. Elle doit être accomplie via la fonction AuF du domaine de rattachement au moment de l'entrée dans un domaine visité étranger. Pour toute interaction ultérieure avec le domaine visité, l'authentification de l'utilisateur mobile doit être accomplie via le domaine visité sans nécessairement interroger la fonction AuF du domaine de rattachement à chaque fois.
- Le terminal mobile devrait être authentifié lorsqu'il passe d'un domaine à un autre. Cette authentification peut servir à détecter et suivre les terminaux mobiles sur liste noire/sur liste blanche. Elle devrait être accomplie conjointement avec l'authentification de l'utilisateur mobile, et non pas faire l'objet d'une autre procédure distincte.
- Il convient de prévoir un scénario dans lequel les terminaux mobiles sont pris en charge dans une fonction AuF différente (éventuellement dans un domaine différent) de celle associée aux utilisateurs mobiles. Dans un tel scénario, le domaine visité doit envoyer au domaine de rattachement de l'utilisateur une seule demande d'authentification et non des demandes d'authentification distinctes. La fonction AuF du domaine de rattachement de l'utilisateur

peut ensuite déléguer les demandes d'authentification du terminal mobile, mais cette communication est hors du domaine d'application de la présente Recommandation.

- Sur la base de la relation de confiance qui existe entre le domaine visité et le domaine de rattachement, le domaine visité doit s'authentifier auprès de l'utilisateur mobile, par exemple de telle sorte que le terminal mobile puisse authentifier le portier du domaine visité. De même, le domaine visité devrait s'authentifier auprès de la fonction AuF du domaine de rattachement.

  NOTE – Etant donné que le domaine visité et le domaine de rattachement ne partagent généralement pas de relation de sécurité établie, on ne peut pas s'attendre à une forte authentification entre ces deux domaines au sens strict. Toutefois, une certaine confiance peut être garantie grâce aux liaisons sécurisées bond par bond qui existent entre le domaine visité et le domaine de rattachement.

- Les protocoles de gestion de la mobilité intra et interdomaines doivent être protégés contre les usurpations d'identité, contre les pertes d'intégrité et, si possible, contre les pertes de confidentialité.
- Les attaques de type refus de service devraient, autant que possible, être minimisées.
- La transmission intra/interdomaines des informations du profil d'utilisateur et de celles du profil de service d'utilisateur ainsi que des clés de sécurité doit être sécurisée. Pour la transmission intradomaine, la gestion des clés doit être sécurisée dans un environnement avec mobilité. Il faut notamment que ces informations sensibles ne soient transmises à aucune entité et à aucun domaine intermédiaire sauf si c'est nécessaire. Cela signifie que le mot de passe de l'utilisateur du terminal mobile et le secret partagé du terminal mobile ne doivent être transmis à aucune entité fonctionnelle autre que le terminal mobile et la fonction AuF. Cela signifie aussi que la clé de session dynamique négociée afin de sécuriser la communication entre le terminal mobile et le domaine visité ne doit pas être transmise aux autres entités de réseau intermédiaires.
- La clé de session dynamique doit être authentique et être liée, sur le plan cryptographique, à l'authentification accomplie. La clé de session doit donc être nouvelle.
- L'architecture de sécurité globale doit tenir compte des relations de confiance entre domaines. Cela nécessite, d'une part, de tenir compte de la relation de sécurité entre entités et domaines et, d'autre part, de détecter les entités cherchant à tricher [par exemple, une entité usurpant l'identité d'un portier de domaine visité (V-GK, *visited gatekeeper*)] et de réduire au minimum la probabilité de tricherie.
- Les techniques de sécurité à appliquer doivent tenir compte des techniques de sécurité existantes (par exemple celles de la Rec. UIT-T H.235 [4]) et ne doivent les renforcer qu'en cas de besoin.
- L'architecture de sécurité déployée doit être simple et ne doit pas reposer sur d'autres mesures de sécurité telles que des cartes à puce ou sur des protocoles de gestion complexes.

8 Sécurité bond par bond avec techniques de cryptage symétrique

De même que des techniques de sécurité symétrique sont mises en œuvre conformément à l'Annexe D/H.235 [4] dans des environnements H.323 quasi statiques sans mobilité, la présente Recommandation décrit l'architecture de sécurité avec des procédures de sécurité dans un environnement H.323 avec mobilité, dans lequel les mêmes techniques de sécurité sont mises en œuvre. Fondamentalement, la présente Recommandation décrit une architecture de sécurité qui repose sur une infrastructure de sécurité utilisant uniquement des secrets partagés symétriquement. Les secrets partagés sont définis bond par bond ou pour chaque paire d'entités communicantes.

Il s'agit d'un modèle de sécurité simple pour lequel il n'est pas nécessaire, par exemple, d'utiliser une infrastructure de sécurité à clés publiques spécifique. L'architecture de sécurité bond par bond est conçue de manière à pouvoir mettre largement en œuvre les techniques de sécurité symétrique bien définies de l'Annexe D/H.235 [4]. Les techniques de cryptage symétrique sont connues pour être relativement performantes et sont donc applicables d'une manière générale dans les environnements avec mobilité.

La Figure 1 illustre l'architecture de sécurité pour un environnement H.323 avec mobilité conforme à la Rec. UIT-T H.510 [6], reposant sur la Rec. UIT-T H.501 [3]. Elle montre la relation architecturale principale entre les entités fonctionnelles ainsi que la relation de sécurité entre les entités (clés). Elle illustre en outre le cas où le terminal mobile est lié au portier du domaine de rattachement.

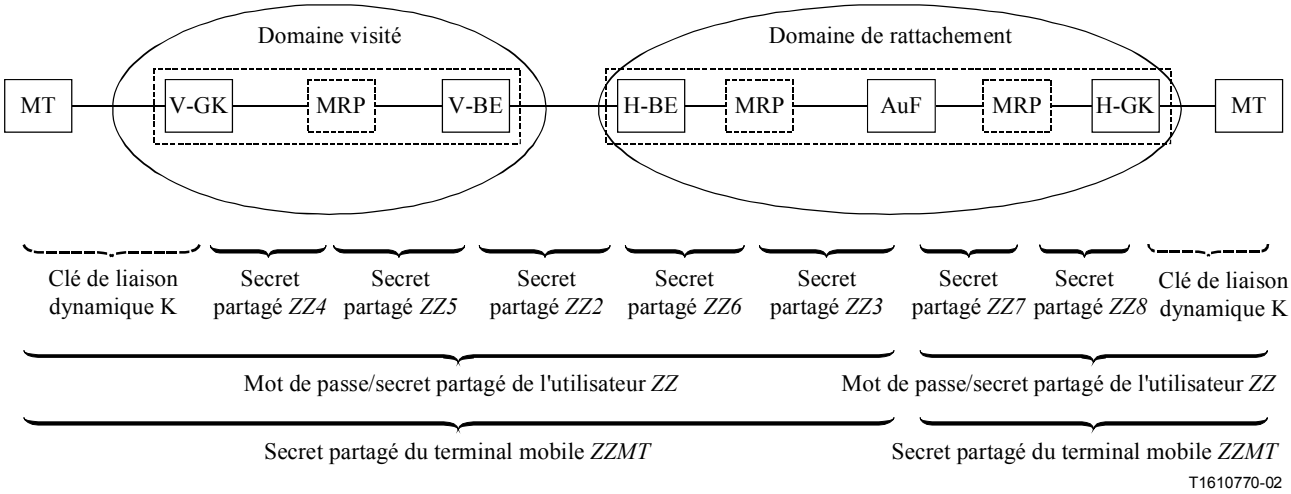

Figure 1/H.530 – Architecture de sécurité pour un environnement H.323 avec mobilité

On suppose que le terminal mobile et la fonction AuF du domaine de rattachement partagent un mot de passe administré *ZZ* qui est attribué pendant le processus d'abonnement de l'utilisateur. Par ailleurs, le portier du domaine visité (V-GK) et l'élément fonctionnel correspondant au bond suivant (par exemple un proxy MRP) partagent un secret partagé *ZZ4* et le proxy MRP partage un secret partagé *ZZ5* avec l'élément frontière du domaine visité (V-BE). A titre d'exemple, en l'absence de proxy MRP dans un environnement donné, un secret partagé doit alors exister entre le portier V-GK et l'élément V-BE et il faut protéger en conséquence, sur le plan de la sécurité, les messages retransmis.

On suppose que l'élément frontière du domaine de rattachement (H-BE) et un proxy MRP partagent un secret partagé *ZZ6* et que le proxy MRP partage un secret partagé *ZZ3* avec la fonction AuF. Entre les domaines, on suppose qu'il existe un secret partagé *ZZ2* entre l'entité V-BE et l'entité H-BE ou bien il convient de mettre en œuvre des moyens de sécurité génériques tels que IPSEC ou une autre protection de sécurité du réseau. Les secrets partagés *ZZ2* à *ZZ6* peuvent être utilisés pour la protection de sécurité dans le cadre du protocole de gestion de la mobilité H.501 [3] ou peuvent servir de secret partagé pour la sécurité IPSEC sous-jacente. Le mot de passe de l'utilisateur et les secrets partagés *ZZ2* à *ZZ6* et *ZZMT* sont administrés statiquement, mais la clé de liaison *K* est attribuée dynamiquement dans le cadre de la procédure de signalisation et d'authentification. La clé de liaison dynamique *K* est partagée entre le terminal mobile et le portier V-GK.

Comme décrit au § 8.5, la fonction AuF et le proxy MRP partagent un secret partagé *ZZ7* et le proxy MRP et le portier H-GK partagent un secret partagé *ZZ8*.

NOTE 1 – Cette architecture de sécurité repose sur des nœuds intermédiaires de confiance. Autrement dit, les nœuds intermédiaires tels que les entités V-BE et H-BE et éventuellement aussi les proxys MRP, la fonction AuF et les portiers (GK) peuvent lire et intercepter des informations de signalisation en transit qui ne leur sont pas véritablement destinées. Cela ne devrait pas poser de problème tant que l'on suppose que la confiance est totale dans un même domaine et que, par ailleurs, il existe une relation étroite de confiance mutuelle entre le domaine visité et le domaine de rattachement et qu'aucun autre domaine intermédiaire n'est impliqué dans la communication H.323 [5] entre ces deux domaines.

NOTE 2 – D'une manière générale, l'utilisation de secrets partagés limite la possibilité d'extension; ainsi, seul un petit nombre de domaines et d'éléments frontière peuvent utiliser ce principe dans des environnements commandés. A titre d'exemple, on prévoit que l'architecture de sécurité décrite dans la présente Recommandation peut couvrir jusqu'à environ 500 domaines de réseau, cette faisabilité étant prouvée dans les réseaux GSM. On suppose que l'architecture de sécurité dont il est question ici ne pourra pas couvrir un nombre de domaines de réseau très supérieur à 500. La prise en charge d'un environnement avec mobilité sécurisé à grande échelle nécessite donc un complément d'étude.

8.1 Hypothèses

Lorsque le protocole de sécurité H.530 mis en œuvre dans la présente Recommandation est utilisé conjointement avec la Rec. UIT-T H.501 [3], on suppose que le temps est synchronisé sur chaque tronçon dans le cas où les techniques de l'Annexe D/H.235 [4] sont appliquées au niveau de la couche Application (c'est-à-dire V-GK – MRP, MRP – V-BE, V-BE – H-BE, H-BE – MRP et MRP – AuF). Dans le cas où des techniques de sécurité de réseau ou de transport sont appliquées sur ces liaisons, la synchronisation du temps entre les entités énumérées n'est pas nécessaire. Dans le cadre de l'architecture de sécurité, on suppose en outre que les horloges entre les terminaux mobiles et la fonction AuF du domaine de rattachement sont synchronisées. Pour cela, on peut par exemple utiliser les protocoles de synchronisation du temps et des horloges NTP (IETF RFC 1305 [8]) ou SNTP (IETF RFC 2030 [9]).

NOTE – On suppose qu'il n'y a pas de synchronisation du temps entre le terminal mobile et le portier du domaine visité. Pour une authentification mutuelle du terminal mobile et du portier du domaine visité, des techniques de sécurité de type défi-réponse sont mises en œuvre. Aucune synchronisation du temps n'est requise pour la protection de sécurité IPSEC de la Rec. UIT-T H.501 [3].

Il faut appliquer le protocole RAS H.225.0 [1] pour la communication de signalisation entre le terminal mobile et le portier du domaine visité et le protocole de gestion de la mobilité H.501 [3] entre les autres entités fonctionnelles illustrées. Le protocole H.501 [3] doit utiliser les fonctionnalités de signalisation H.235 [4] en vue d'une protection de sécurité des messages et d'une gestion sécurisée de la mobilité et peut en outre utiliser la sécurité IPSEC en vue d'un renforcement de la sécurité.

8.2 Procédures en vue d'une mise à jour sécurisée de la position

Le terminal mobile et le portier du domaine visité (V-GK) n'ont généralement jamais été en contact auparavant et ne peuvent donc pas utiliser d'informations d'abonnement communes. Ainsi, lorsque le portier V-GK reçoit un premier message en provenance du terminal mobile, il n'est pas capable d'authentifier immédiatement le terminal mobile, et inversement. C'est pourquoi le portier V-GK délègue la tâche d'authentification et d'autorisation de l'utilisateur du terminal mobile à la fonction AuF située dans le domaine dans lequel l'utilisateur du terminal mobile est abonné. La fonction AuF doit procéder à l'authentification de l'utilisateur/du terminal mobile et prendre une décision quant à l'autorisation. La fonction AuF envoie une réponse contenant le résultat de la vérification de sécurité et transmet des informations de sécurité (par exemple des pouvoirs) au portier V-GK ainsi qu'au terminal mobile pour la session.

Comme la demande d'authentification et d'autorisation n'est généralement faite à la fonction AuF qu'au moment où le terminal mobile et l'utilisateur entrent dans le domaine visité, il n'est a priori pas nécessaire d'exécuter cette procédure ultérieurement pendant le même appel ou pendant la même session, sauf si cela est explicitement requis par la politique de sécurité du portier V-GK. Ainsi, le

portier V-GK est capable de fonctionner de manière autonome par rapport à la fonction AuF une fois qu'il a reçu les pouvoirs d'autorisation. Le portier V-GK se comporte alors comme un serveur de sécurité local dans le domaine visité.

La présente Recommandation prend en charge deux procédures en vue d'une mise à jour sécurisée de la position.

Les deux procédures se déroulent pendant l'authentification initiale: pour les deux procédures, l'authentification est identique, utilisant les messages **AuthenticationRequest** et **AuthenticationConfirmation** au-delà du portier V-GK. La seule différence entre les deux tient à ce qu'on utilise soit le message **GRQ** soit le message **RRQ**.

- Authentification pendant la phase de découverte du portier V-GK: cette procédure s'applique lorsque le terminal mobile a déjà un identificateur de point d'extrémité et connaît a priori l'identificateur du portier V-GK. Dans ce cas, il est possible de sécuriser le message **GRQ** conformément à l'Annexe D; voir Figure 2.
- Authentification pendant l'enregistrement du terminal mobile et de l'utilisateur: cette procédure s'applique lorsque le terminal mobile ne connaît pas l'identificateur du portier V-GK et qu'aucun identificateur de point d'extrémité ne lui est encore attribué. Dans ce cas, le terminal mobile et le portier commencent par exécuter la procédure de découverte (non sécurisée) qui leur permet d'échanger leurs identificateurs. Puis ils s'authentifient au moyen du message **RRQ** initial; voir Figure 3.

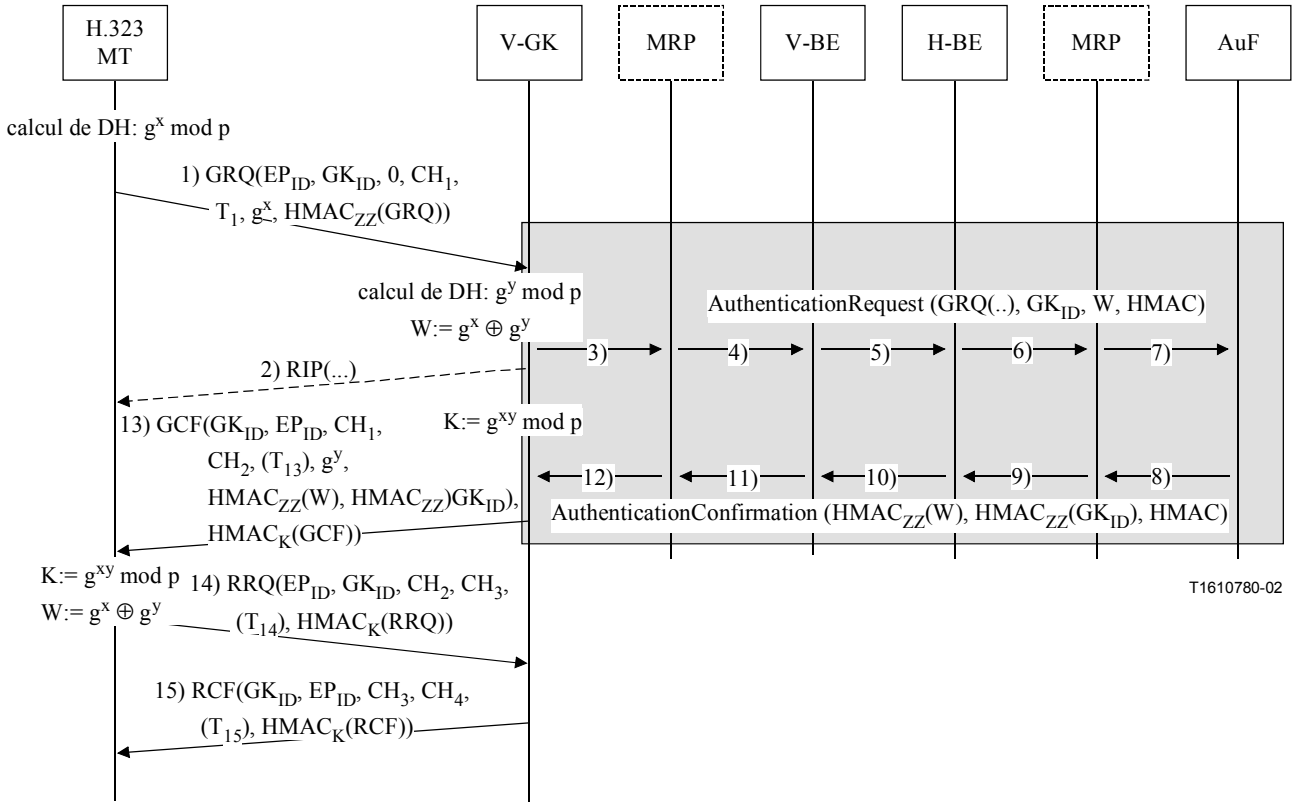

Figure 2/H.530 – Authentification et gestion des clés pendant la phase de découverte du portier

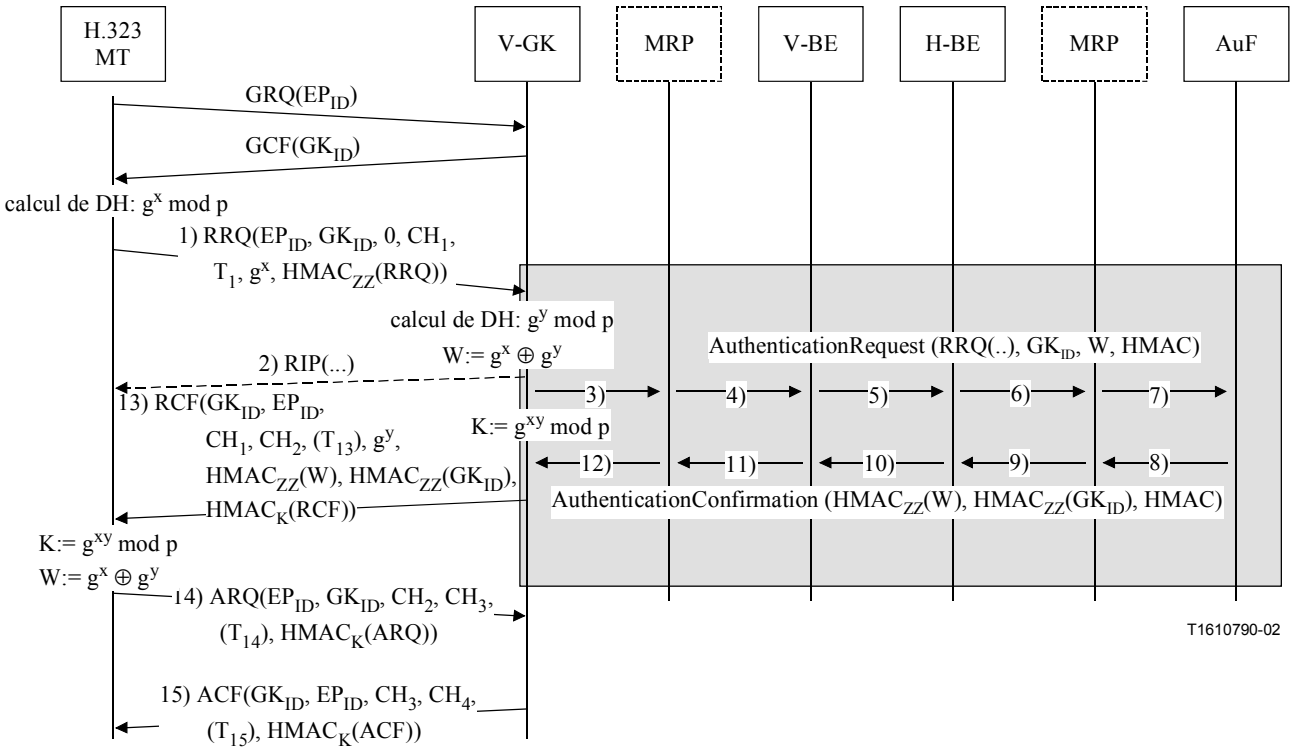

Figure 3/H.530 – Authentification et gestion des clés pendant la phase d'enregistrement

La mise à jour sécurisée de la position intervient:

- lorsqu'un utilisateur et un terminal mobile contactent un domaine visité pour la première fois sans qu'aucune information préalable ne soit disponible dans le domaine visité;
- lorsque certaines informations temporaires au sujet du terminal mobile et de l'utilisateur sont déjà disponibles dans le domaine visité.

Dans le premier cas, la procédure d'authentification doit être exécutée entièrement pour que le domaine visité puisse rassembler suffisamment d'informations à partir du domaine de rattachement afin de desservir le terminal mobile. Cette procédure comprend la communication des résultats de l'authentification, de la vérification de l'autorisation et des pouvoirs par le domaine de rattachement. Des informations de profil de service peuvent par ailleurs être acheminées au portier V-GK. Il est à noter que cette procédure fait généralement intervenir une communication réseau et une interaction avec éventuellement plusieurs entités et que son exécution peut donc prendre un certain temps.

Dans le second cas, il n'est pas nécessaire que le portier V-GK contacte le domaine de rattachement, même si ce n'est pas interdit. Le portier V-GK réutilise les informations stockées localement sans contacter le domaine de rattachement. Ce cas correspond par exemple au cas de la perte et du rétablissement d'une connexion ou au cas d'une modification locale du point d'attache dans le réseau. Chaque fois que le terminal mobile possède une clé de liaison valable, il doit d'abord tenter de l'utiliser avant de se rabattre sur la mise en œuvre d'une mise à jour initiale de la position.

L'utilisateur commence par s'authentifier explicitement en utilisant le mot de passe qu'il a obtenu au moment de l'abonnement. En ce qui concerne l'authentification du terminal mobile, celui-ci peut facultativement s'authentifier auprès de la fonction AuF; voir la procédure décrite au § 8.3.

Sur le fond, la procédure en vue d'une mise à jour sécurisée de la position se déroule comme suit: le message RAS initial que le portier V-GK reçoit est encapsulé dans un message **AuthenticationRequest** et il est transmis à la fonction AuF du domaine de rattachement par l'intermédiaire d'une ou de plusieurs entités fonctionnelles. Cette opération découle du fait que le portier V-GK n'est pas capable d'authentifier le terminal mobile et l'utilisateur. La fonction AuF vérifie les informations transmises, authentifie le terminal mobile/l'utilisateur puis prend une

décision quant à l'autorisation du terminal mobile/de l'utilisateur sur la base de certains critères. Autre solution: la fonction AuF peut se souvenir du terminal mobile/de l'utilisateur et doit alors fournir au portier V-GK et au terminal mobile le résultat de l'authentification et de la vérification d'autorisation ainsi que des pouvoirs en utilisant les messages **AuthenticationConfirmation/AuthenticationRejection**.

Le domaine visité s'authentifie auprès du terminal mobile/de l'utilisateur lorsqu'il fournit la clé de liaison dynamique, en réponse au défi lancé par le terminal mobile. Le terminal mobile/l'utilisateur s'authentifie grâce à un quelconque message RAS subséquent auprès du portier V-GK en utilisant les techniques de défi et de réponse. De même, le terminal mobile est capable d'authentifier le portier V-GK.

En raison du principe de sécurité bond par bond, tout nœud intermédiaire ou proxy doit vérifier la sécurité H.235 [4] appliquée sur chaque tronçon et recalculer le jeton **CryptoToken** avec le résumé du message, si des moyens de sécurité de réseau ou de transport ne sont pas disponibles. Dans le cas contraire, le résumé du message dans le jeton **CryptoToken** n'a pas à être recalculé.

Comme l'authentification et la communication réseau entre le portier V-GK et la fonction AuF peuvent prendre un certain temps, il peut être nécessaire que le portier V-GK envoie un message **RIP** au terminal mobile indiquant que la demande est en cours.

Les diagrammes des Figures 4 à 10 donnent le flux de messages et mettent l'accent sur la sécurité H.235 [4]. Le flux de messages illustré est donné pour le scénario dans lequel l'authentification se déroule pendant la phase d'enregistrement. La description des procédures est analogue lorsque la mise à jour sécurisée de la position intervient pendant la découverte du portier V-GK; dans ce cas, le message **RRQ** encapsulé doit être remplacé par le message **GRQ**. Les éléments de signalisation pour l'authentification facultative du terminal mobile sont définis au § 8.3 et, pour plus de simplicité, ils ne sont pas représentés sur la plupart des figures. Pour des raisons d'espace et de clarté, le flux de messages est subdivisé en plusieurs phases successives, faisant chacune l'objet d'une figure distincte. La lecture des messages numérotés en séquence conduit à un flux logique de messages de bout en bout.

8.2.1 Terminal mobile (MT) – Portier du domaine visité (V-GK)

La Figure 4 illustre la phase d'enregistrement initial entre le terminal mobile et le portier V-GK. Chaque message RAS achemine un nouveau défi et la valeur du défi précédent. A l'exception du premier message, la valeur de vérification d'intégrité de message HMAC sert de réponse calculée au défi précédent; cette valeur HMAC doit être calculée conformément à l'Annexe D/H.235 [4] en utilisant la clé de liaison dynamique *K* comme secret partagé. Pour calculer la valeur HMAC, il faut suivre la procédure I du D.6.3.2/H.235 [4], sans utiliser le champ **timeStamp**. Si le terminal mobile ou le portier V-GK inclut quand même des horodates (telles que T_{13}, T_{14} et T_{15}), il convient de ne pas vérifier ces horodates car on ne peut pas supposer que le temps est synchronisé entre le terminal mobile et le portier V-GK.

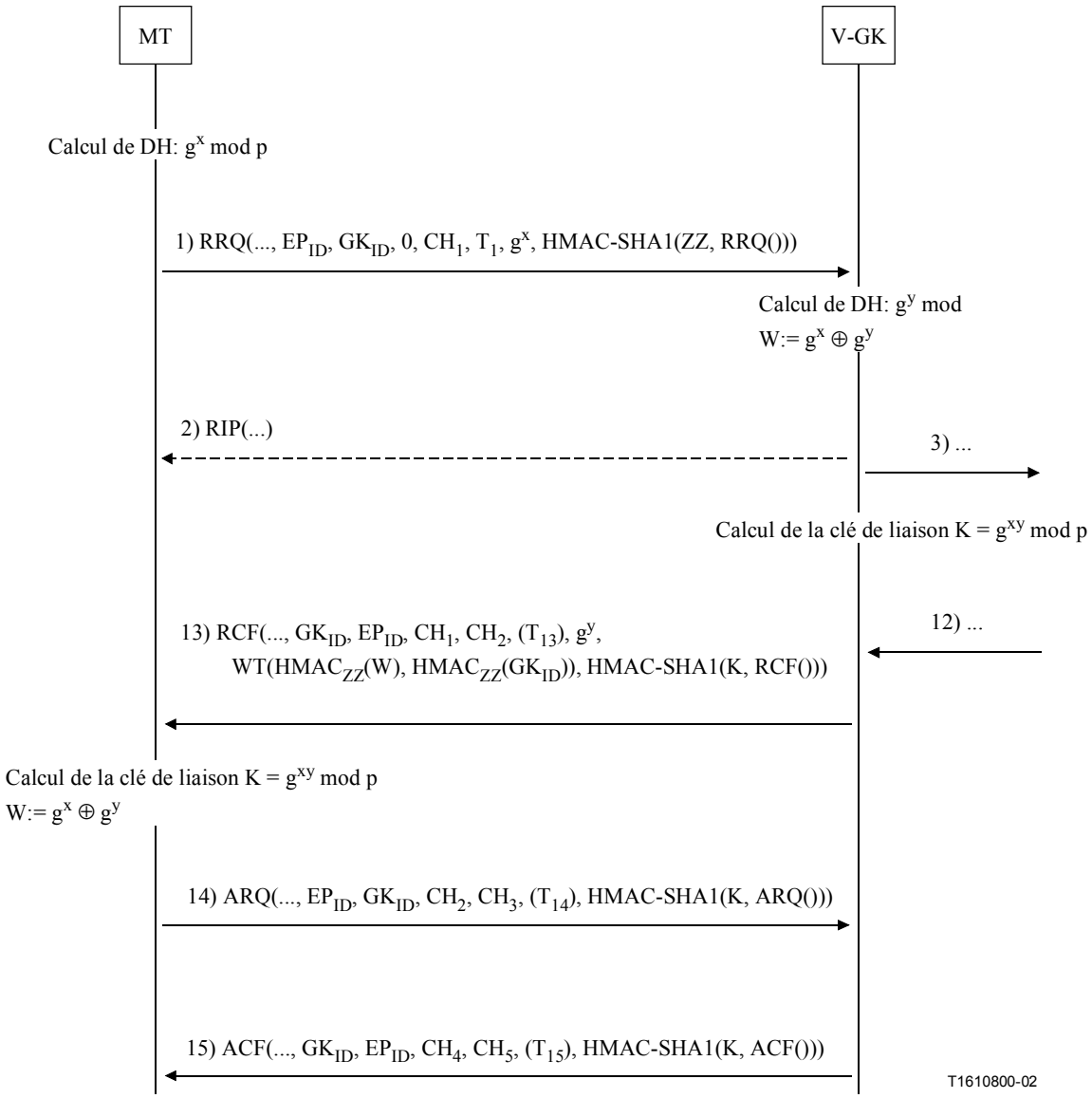

Figure 4/H.530 – Phase d'enregistrement initial et messages RAS subséquents entre le terminal mobile et le portier V-GK

En ce qui concerne l'enregistrement initial, le terminal mobile doit générer un nouveau défi CH_1 et l'inclure dans le champ **challenge** du jeton **ClearToken** du message **RRQ**, voir le message 1). Le champ **password** du jeton **ClearToken** doit acheminer la valeur du défi précédent. En ce qui concerne les messages **RRQ**/**GRQ** initiaux, il faut attribuer la valeur zéro au défi précédent.

Ensuite, le terminal mobile doit générer une nouvelle demi-clé Diffie-Hellman $g^x \ mod \ p$ avec la valeur aléatoire *x* gardée secrète et inclure cette demi-clé dans le champ **halfkey** du champ **dhkey** du jeton **ClearToken** du message. Le nombre premier appliqué doit être inclus dans le champ **modsize** tandis que le générateur Diffie-Hellman doit être inclus dans le champ **generator** de ce jeton **ClearToken**. En ce qui concerne les paramètres de système Diffie-Hellman (DH), il faut prendre les paramètres disponibles figurant dans le Tableau D.4/H.235 [4], où le générateur vaut *2* et le nombre premier mod-P à *1024* bits désigné par "Z" est recommandé.

Le portier V-GK reçoit le message **RRQ** de défi et l'encapsule dans le champ **applicationMessage** d'un message **AuthenticationRequest**, voir le message 3), qu'il envoie au bond suivant (par exemple au proxy MRP).

Le portier V-GK doit générer une demi-clé Diffie-Hellman non altérée $g^y \ mod \ p$ avec la valeur aléatoire *y* gardée secrète. En ce qui concerne les paramètres de système Diffie-Hellman, il faut prendre les paramètres disponibles figurant dans le Tableau D.4/H.235 [4], où le générateur vaut *2* et le nombre premier mod-P à *1024* bits désigné par "Z" est recommandé.

Prenant la demi-clé Diffie-Hellman reçue $g^x \ mod \ p$ et sa propre demi-clé Diffie-Hellman $g^y \ mod \ p$, le portier V-GK doit calculer une valeur composite *W* en appliquant l'opérateur OU exclusif sur les bits à ces deux valeurs.

Cette valeur composite *W* doit être incluse dans le champ **halfkey** du champ **dhkey** d'un jeton **ClearToken** distinct pour la mobilité du message **AuthenticationRequest**. Le champ **generalID** de ce jeton **ClearToken** doit acheminer l'identificateur GK_{ID}. Le champ **tokenOID** de ce jeton **ClearToken** pour la mobilité doit être mis à "G2". Les autres paramètres de ce jeton **ClearToken** pour la mobilité ne doivent pas être utilisés. La fonction AuF authentifiera les informations de ce jeton **ClearToken** et calculera les pouvoirs correspondants. Le jeton **ClearToken** pour la mobilité est représenté sous forme de **WT()**.

Le message **AuthenticationRequest** doit acheminer la protection d'intégrité conformément à l'Annexe D/H.235 [4], sauf si la liaison entre le portier V-GK et le bond suivant (par exemple, un proxy MRP) est sécurisée par IPSEC.

NOTE 1 – Etant donné que le jeton **ClearToken** pour la mobilité fait partie intégrante du message **AuthenticationRequest**, la protection d'intégrité du message complet couvre déjà l'intégrité de tous les jetons **Clear** et/ou **CryptoToken** acheminés. Ainsi, aucune protection distincte du jeton **ClearToken** pour la mobilité n'est nécessaire.

Le portier V-GK peut soumettre un message **RIP** non sécurisé au terminal mobile pour indiquer que le traitement du message est en cours; voir le message 2). Etant donné que le terminal mobile et le portier V-GK ne partagent pas encore de secret commun, le portier V-GK n'est pas capable d'authentifier et de protéger l'intégrité de ce message **RIP** immédiat.

NOTE 2 – Le terminal mobile ne devrait pas faire confiance aux messages **RIP** non protégés car il se peut qu'ils ne soient pas authentiques, que ce soient des doubles ou qu'ils proviennent d'attaques de type refus de service. Le terminal mobile devrait être prêt à traiter les messages **RIP** en double et à faire face à une éventuelle inondation de messages. Le traitement à appliquer aux messages **RIP** non protégés est déterminé par la politique de sécurité du terminal mobile.

Tant que le message **RCF** n'est pas soumis en tant que message 13), le portier V-GK a le temps de calculer la clé de liaison dynamique *K* au moyen de la demi-clé Diffie-Hellman du terminal mobile et de son propre secret *y*. En ce qui concerne la protection d'intégrité HMAC-SHA1-96 des messages RAS H.225.0 [1], il faut considérer que les 96 bits les plus à gauche du secret partagé Diffie-Hellman résultant sont représentés dans l'ordre des octets de réseau.

Le portier V-GK reçoit un message **AuthenticationConfirmation/AuthenticationRejection** contenant le résultat de l'authentification et de la vérification d'autorisation par la fonction AuF ainsi que les pouvoirs transmis; voir le message 12).

Le portier V-GK peut superviser la réception des messages **AuthenticationConfirmation/AuthenticationRejection** au moyen d'une temporisation. La durée de la temporisation devrait être choisie suffisamment longue compte tenu du transit dans le réseau et du traitement par la fonction AuF. Si la temporisation expire et que la réponse correspondante en provenance de la fonction AuF n'est pas arrivée, le portier V-GK doit envoyer un message **RCF** non protégé.

Le portier V-GK doit générer un nouveau défi CH_2 et construire le message **RCF**. Ce dernier doit acheminer le défi précédent CH_1 dans le champ **password**, un nouveau défi CH_2 dans le champ **challenge** du jeton **ClearToken** à l'intérieur du jeton **CryptoToken** du message **RCF**. Ce jeton **ClearToken** doit également acheminer la demi-clé Diffie-Hellman calculée du portier V-GK dans le

champ **halfkey** du champ **dhkey** dans le jeton **ClearToken** de ce message. Le nombre premier appliqué doit être inclus dans le champ **modsize** tandis que le générateur DH doit être inclus dans le champ **generator** de ce jeton **ClearToken**.

Le portier V-GK doit ensuite retransmettre les pouvoirs de la fonction AuF au terminal mobile. Les pouvoirs comprennent le jeton **ClearToken** pour la mobilité représenté sous forme de **WT()**. Ce jeton **ClearToken** pour la mobilité achemine d'une part, la valeur composite authentifiée *W* dans le champ **halfkey** du champ **dhkey** et, d'autre part, l'identificateur du portier V-GK authentifié. Le champ **tokenOID** doit être mis à "G2" et les autres paramètres de ce jeton **ClearToken** pour la mobilité ne doivent pas être utilisés.

Le portier V-GK calcule la valeur HMAC sur la totalité du message **RCF** au moyen de la clé de liaison *K*. Ainsi, la valeur HMAC sert de réponse au défi précédent conformément à la procédure I de l'Annexe D/H.235 [4]; voir le message 13).

Une fois que la fonction AuF a vérifié l'autorisation, le portier V-GK peut décider, selon ses propres critères, d'autoriser ou non le terminal mobile. Ainsi, le portier V-GK peut rejeter un message **GRQ**/**RRQ** même si la fonction AuF a confirmé l'authentification et l'autorisation. En pareil cas, le portier V-GK doit répondre avec un message **GRJ**/**RRJ** avec un champ **reason** conforme au B.2.2/H.235 [4].

Le terminal mobile reçoit le message **RCF** protégé avec des défis, la demi-clé Diffie-Hellman et des pouvoirs tels que la valeur composite authentifiée *W* et l'identificateur GK_{ID} authentifié [voir le message 13)]. Il extrait ces paramètres du jeton **ClearToken** pour la mobilité. Il doit calculer la clé de liaison dynamique *K* de manière analogue au calcul effectué par le portier V-GK, décrit ci-dessus. Il doit vérifier la valeur HMAC en tant que réponse pour la totalité du message **RCF** en utilisant la clé de liaison *K*. Il doit calculer la valeur composite *W* en appliquant l'opérateur OU exclusif sur les bits à la demi-clé $g^y \ mod \ p$ reçue et à sa propre demi-clé $g^x \ mod \ p$. Il doit vérifier que la valeur composite authentifiée *W* du champ **halfkey** figurant dans le jeton **ClearToken** pour la mobilité est correcte en appliquant le secret partagé *ZZ*. Il doit vérifier que l'identificateur GK_{ID} authentifié figurant dans le champ **generator** du jeton **ClearToken** pour la mobilité est correct en appliquant le secret partagé *ZZ*. Si l'authenticité de l'une ou l'autre valeur ne peut être prouvée, on ne peut pas supposer non plus que la clé de liaison *K* ou le portier V-GK sont authentiques. Cela peut indiquer la présence d'entités de réseau frauduleuses ou un échec d'authentification d'une manière générale. Dans ce cas, le terminal mobile doit ignorer le message **RCF** et recommencer avec un nouveau message **RRQ**.

Lorsque le portier V-GK reçoit un message **AuthenticationRejection** avec une valeur présente dans le champ **reason**, il doit envoyer un message **RRJ** au terminal mobile; voir le message 13). La valeur "security" dans le champ **reason** indique une erreur liée à la sécurité, étant donné que la fonction AuF n'a probablement pas pu identifier le terminal mobile/l'utilisateur. Le portier V-GK doit alors retransmettre cette erreur dans le champ **reason** du message **RRJ**.

Etant donné que le terminal mobile et le portier V-GK ne partagent d'horloges synchronisées, il faut ignorer les éventuelles horodates facultatives acheminées dans un message RAS.

NOTE 3 – Etant donné que le portier V-GK ne peut pas authentifier un message **GRQ**/**RRQ** non protégé initial, de tels messages peuvent être transmis plusieurs fois ou peuvent provenir d'attaques de type refus de service. Les portiers V-GK qui reçoivent un nombre anormalement élevé de messages RAS protégés ou non protégés peuvent supposer qu'ils résultent d'une attaque de type refus de service et peuvent refuser immédiatement de continuer à traiter ces messages.

8.2.2 Portier du domaine visité (V-GK) – Proxy de routage pour la mobilité (MRP)

La communication entre le portier V-GK et l'élément fonctionnel correspondant au bond suivant (par exemple un proxy MRP) sert à:

- transférer à la fonction AuF l'authentification et l'autorisation du terminal mobile et de l'utilisateur;
- transférer de la fonction AuF au terminal mobile la confirmation d'autorisation.

La Figure 5 illustre le flux de messages de protocole. Le message 2) **AuthenticationRequest** contient la totalité du message RAS RRQ/GRQ reçu du terminal mobile. Par ailleurs, le message **AuthenticationRequest** comporte un jeton **ClearToken** pour la mobilité acheminant la valeur composite *W* et l'identificateur GK_{ID}. Le jeton **ClearToken** pour la mobilité est représenté sous forme de **WT()**. Si l'authentification du terminal mobile est réalisée, le portier V-GK inclut un jeton **CryptoToken** distinct à cette fin; voir le § 8.3.

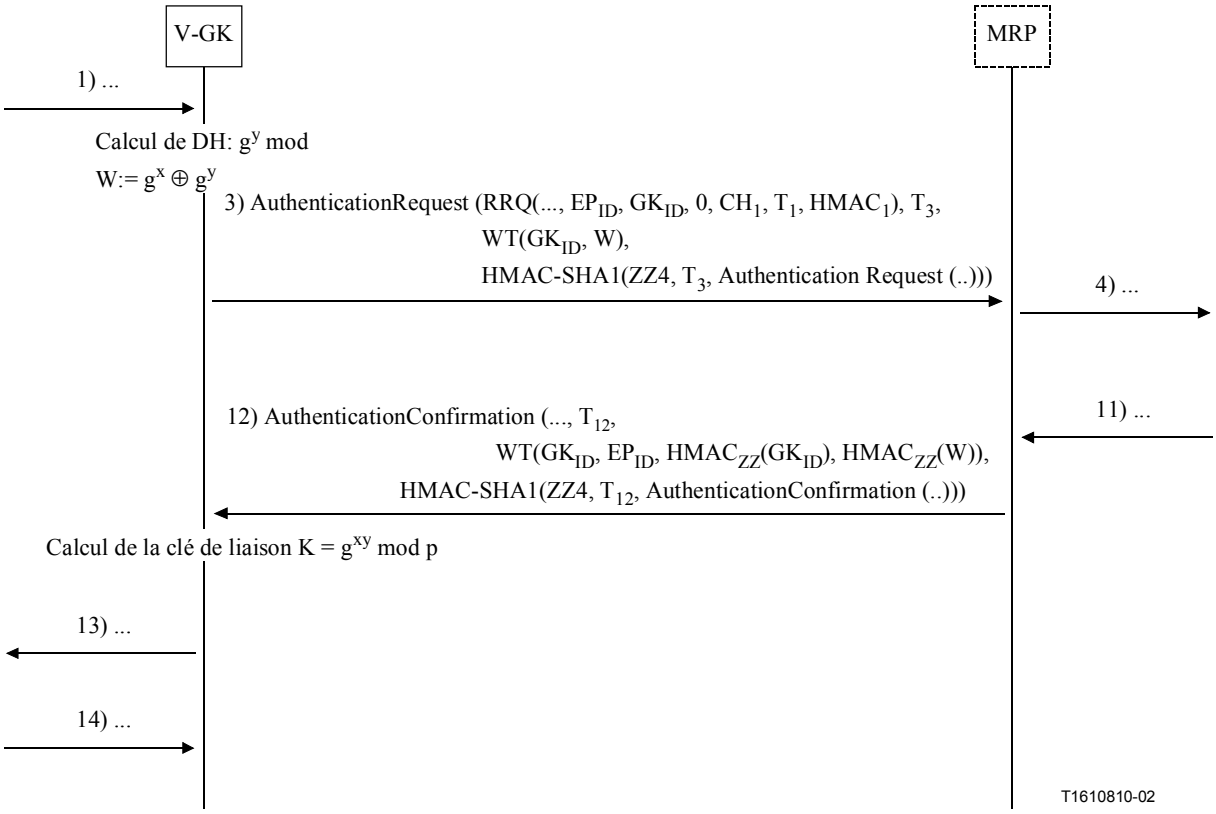

Figure 5/H.530 – Transmission d'informations d'authentification entre le portier V-GK et le proxy MRP

Si la liaison entre le portier V-GK et le proxy MRP n'est pas protégée par une sécurité réseau (par exemple IPSEC), le message **AuthenticationRequest** doit être sécurisé conformément à l'Annexe D/H.235 [4] avec une nouvelle horodate T_3 et une valeur HMAC calculée avec la clé *ZZ4*. Dans le cas contraire, le message **AuthenticationRequest** n'a pas besoin d'être protégé sur le plan de la sécurité conformément à l'Annexe D/H.235 [4].

Le message 12) **AuthenticationConfirmation** ou **AuthenticationRejection** dans le message achemine les valeurs authentifiées par la fonction AuF sous forme de pouvoirs dans un jeton **ClearToken** pour la mobilité distinct représenté sous forme de **WT()**. Si la liaison entre le portier V-GK et le proxy MRP n'est pas protégée par une sécurité de réseau (par exemple IPSEC), le message **AuthenticationConfirmation** doit être sécurisé conformément à l'Annexe D/H.235 [4] avec une nouvelle horodate T_{12} et une valeur HMAC au moyen de la clé *ZZ4*. Dans le cas contraire,

le message **AuthenticationConfirmation/AuthenticationRejection** n'a pas besoin d'être protégé sur le plan de la sécurité conformément à l'Annexe D/H.235 [4].

Les identificateurs GK_{ID} et EP_{ID} acheminés dans ce jeton **ClearToken** pour la mobilité permettent au portier V-GK d'associer le message **AuthenticationConfirmation**/**AuthenticationRejection** reçu au message **AuthenticationRequest** correspondant.

Si le portier V-GK n'a pas de relation de service avec le proxy MRP (par exemple clé *ZZ4* manquante), il ne doit pas envoyer de message **AuthenticationRequest**; il doit en revanche répondre avec un message **AuthenticationRejection** dont le champ **reason** est mis à **noServiceRelationship**.

8.2.3 Proxy de routage pour la mobilité (MRP) – Elément frontière du domaine visité (V-BE)

Un proxy MRP (s'il est présent, si le nombre de bonds acheminé n'est pas dépassé et si une relation de service existe avec l'élément V-BE) doit retransmettre le message **AuthenticationRequest** reçu à l'élément V-BE; voir, sur la Figure 6 le message 4). Le message retransmis doit être sécurisé conformément à l'Annexe D/H.235 [4] avec une nouvelle horodate T_4 et une valeur HMAC calculée au moyen de la clé *ZZ5*. Dans les autres cas, le message **AuthenticationRequest** n'a pas besoin d'être protégé sur le plan de la sécurité conformément à l'Annexe D/H.235 [4].

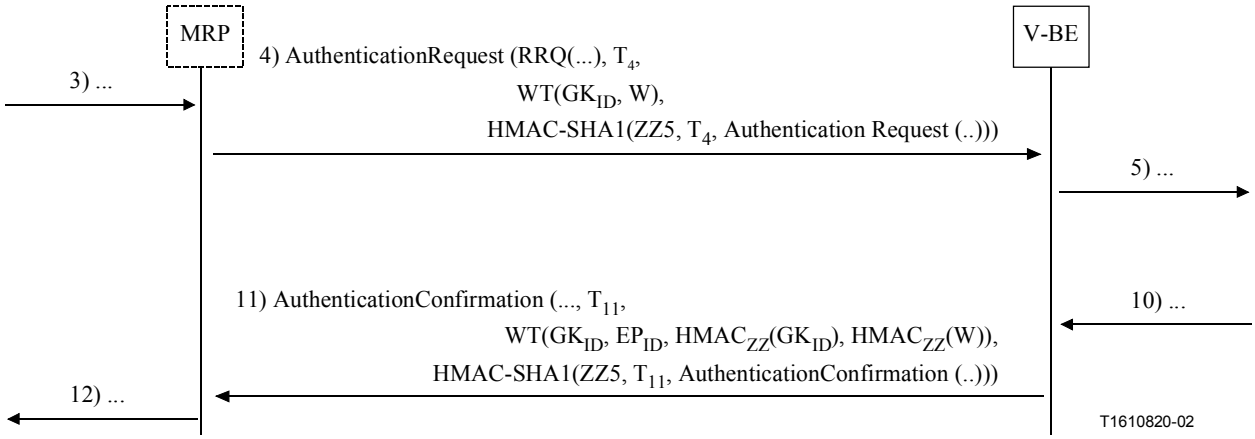

Figure 6/H.530 – Transmission d'informations d'authentification entre le proxy MRP et l'élément V-BE

L'élément V-BE doit retransmettre un message **AuthenticationConfirmation** ou **AuthenticationRejection** au proxy MRP.

Le message 11) **AuthenticationConfirmation** ou **AuthenticationRejection** achemine les valeurs authentifiées sous forme de pouvoirs émanant de la fonction AuF. Si la liaison entre l'élément V-BE et le proxy MRP n'est pas protégée par une sécurité de réseau (par exemple IPSEC), le message **AuthenticationConfirmation/AuthenticationRejection** doit être sécurisé conformément à l'Annexe D/H.235 [4] avec une nouvelle horodate T_{11} et une valeur HMAC au moyen de la clé *ZZ5*. Dans le cas contraire, le message **AuthenticationConfirmation/AuthenticationRejection** n'a pas besoin d'être protégé sur le plan de la sécurité conformément à l'Annexe D/H.235 [4].

Si le nombre de bonds est dépassé, le proxy MRP ne doit pas envoyer de message **AuthenticationRequest**; il doit en revanche répondre avec un message **AuthenticationRejection** dont le champ **reason** est mis à **hopCountExceeded**; voir le message 12).

Si le proxy MRP n'a pas de relation de service avec l'élément V-BE (par exemple clé *ZZ5* manquante), le portier V-GK ne doit pas envoyer de message **AuthenticationRequest**; en revanche, il doit répondre avec un message **AuthenticationRejection** dont le champ **reason** est mis à **noServiceRelationship**; voir le message 12).

8.2.4 Elément frontière du domaine visité (V-BE) – Elément frontière du domaine de rattachement (H-BE)

La Figure 7 illustre le flux de messages entre deux éléments frontière de deux domaines adjacents au moment de l'enregistrement initial. La sécurité peut être assurée grâce à l'utilisation de IPSEC conformément à la Rec. UIT-T H.501 [3] ou grâce à l'utilisation du secret *ZZ2* qui est partagé entre les éléments V-BE et H-BE. Dans le second cas, le message H.501 [3] doit être sécurisé conformément à l'Annexe D/H.235 [4].

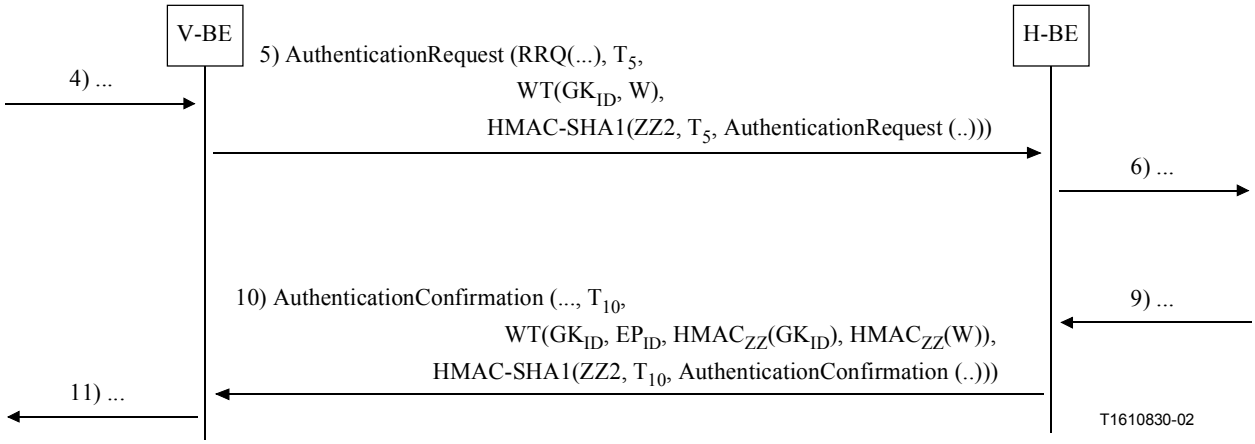

Figure 7/H.530 – Transmission d'informations d'authentification entre éléments frontière

Si le nombre de bonds acheminé n'est pas dépassé et si une relation de service existe avec l'élément H-BE, le message **AuthenticationRequest** H.501 [3] achemine la totalité du message **RRQ** y compris les jetons Clear-Token et CryptoToken associés; voir le message 5). Cela permet à la fonction AuF de valider le message **RRQ** et d'authentifier l'utilisateur/le terminal mobile. Pour sécuriser un message H.501 [3], on protège la totalité du message sur le plan de l'intégrité de manière analogue à la protection décrite dans l'Annexe D/H.235, où la valeur du champ "hash" calculée est stockée dans le jeton **CryptoToken** du **MessageCommonInfo**. Les éléments frontière doivent insérer de nouvelles horodates (T_5, T_{10}) pour chaque message H.501 [3].

Le message **AuthenticationConfirmation/AuthenticationRejection** achemine les valeurs authentifiées sous forme de pouvoirs émanant de la fonction AuF dans un jeton **ClearToken** pour la mobilité représenté sous forme de **WT()**.

Si l'utilisateur du terminal mobile n'est pas autorisé à utiliser le service H.323 mobile, la fonction AuF devrait envoyer un message **AuthenticationRejection** dont le champ **reason** est mis à "security". Pour tout autre échec lié à la sécurité, la fonction AuF doit mettre dans le champ **reason** une erreur appropriée conformément au B.2.2/H.235 [4].

Si le nombre de bonds est dépassé, l'élément V-BE ne doit pas envoyer de message **AuthenticationRequest**; en revanche, il doit répondre avec un message **AuthenticationRejection** dont le champ **reason** est mis à **hopCountExceeded**; voir le message 11).

Si l'élément V-BE n'a pas de relation de service avec l'élément H-BE (par exemple clé *ZZ2* manquante), il ne doit pas envoyer de message **AuthenticationRequest**; en revanche il doit répondre avec un message **AuthenticationRejection** dont le champ **reason** est mis à **noServiceRelationship**; voir le message 11).

8.2.5 Elément frontière du domaine de rattachement (H-BE) vers proxy de routage pour la mobilité (MRP)

Si un proxy MRP est présent, le flux de messages est tel qu'indiqué sur la Figure 8.

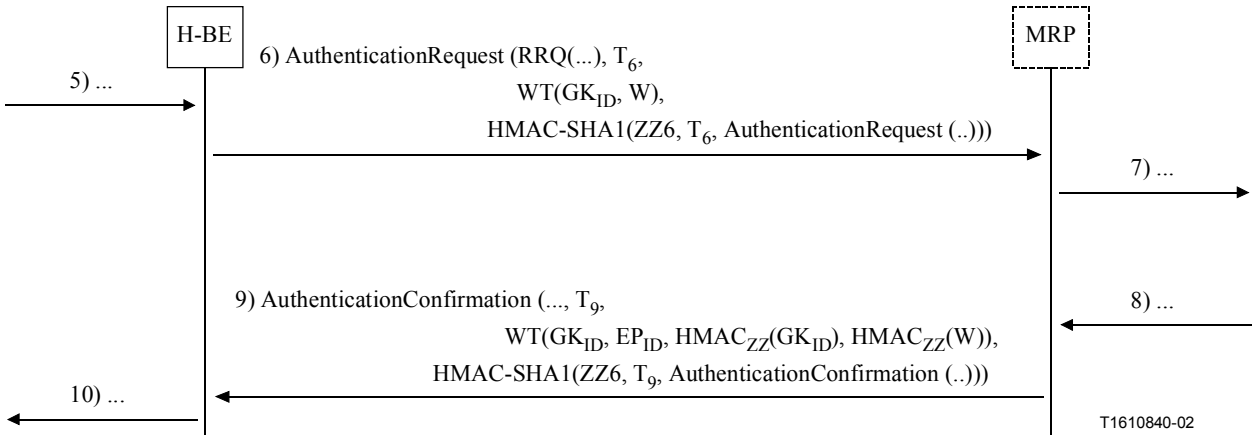

Figure 8/H.530 – Transmission d'informations d'authentification entre l'élément H-BE et le proxy MRP

8.2.6 Proxy de routage pour la mobilité (MRP) vers fonction d'authentification (AuF)

La Figure 9 montre le flux de messages entre le proxy MRP (s'il est présent, si le nombre de bonds n'est pas dépassé et si une relation de service existe) et la fonction AuF. Si aucun proxy MRP n'est présent, il faut alors prendre l'entité de réseau précédente. De manière analogue aux figures d'avant, le secret partagé *ZZ3* permet de sécuriser les messages transmis.

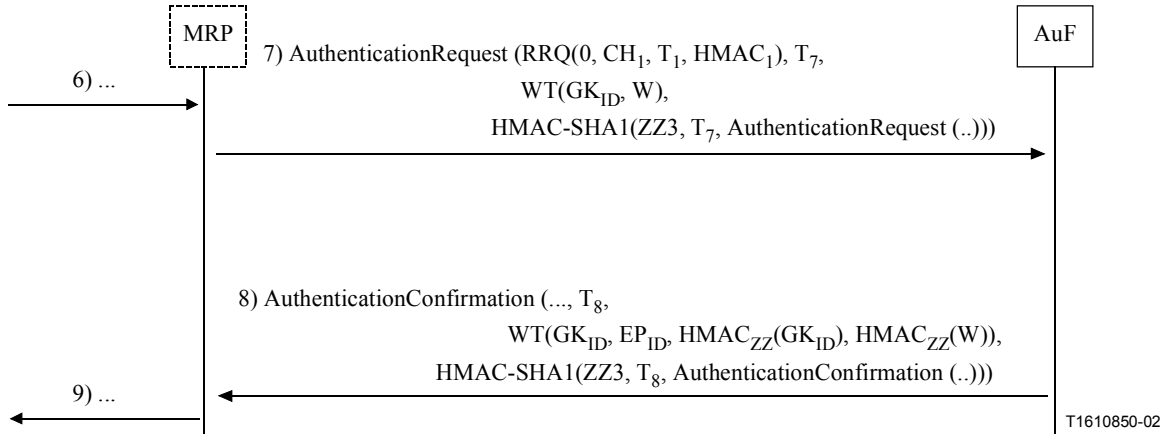

Figure 9/H.530 – Transmission d'informations d'authentification entre le proxy MRP et la fonction AuF

Dès réception du message **AuthenticationRequest**, la fonction AuF peut successivement faire confiance aux autres entités fonctionnelles de la chaîne concernant la préservation de l'intégrité du message **RRQ** acheminé; voir le message 7). La fonction AuF doit vérifier le message **AuthenticationRequest** puis vérifier le message **RRQ** encapsulé tel que décrit dans la procédure I de l'Annexe D/H.235 [4]. L'horodate T_1 acheminée indique que le message **RRQ** est nouveau et elle doit être vérifiée.

Si le terminal mobile/l'utilisateur est connu de la fonction AuF et autorisé, la fonction AuF doit répondre avec un message **AuthenticationConfirmation**; voir le message 8). Ensuite, si l'authentification du terminal mobile est souhaitée, la fonction AuF doit vérifier le jeton **CryptoToken** acheminé correspondant. Dans les autres cas, c'est-à-dire si le terminal mobile/l'utilisateur ne peut pas être authentifié ou s'il est inconnu de la fonction AuF, un message **AuthenticationRejection** protégé doit être soumis, le champ **reason** devant contenir une erreur appropriée comme défini au B.2.2/H.235 [4].

Si la fonction AuF n'est pas capable d'appliquer le secret partagé *ZZ*, le calcul des valeurs authentifiées pour les pouvoirs comme décrit ci-dessous doit être omis et aucun résultat ne doit être inclus dans le message **AuthenticationRejection**. Dans ce cas, aucun jeton **ClearToken** pour la mobilité ne figure dans le message **AuthenticationRejection**.

Dans le cas contraire, la fonction AuF doit aussi calculer les pouvoirs associés à la valeur composite authentifiée *W* au moyen de la fonction de hachage avec clé HMAC-SHA1-96 et de la clé partagée *ZZ*. La valeur composite authentifiée *W* doit être incluse dans un jeton distinct **ClearToken** pour la mobilité, le résultat étant stocké dans le champ **halfkey** du champ **dhkey** de ce jeton **ClearToken** pour la mobilité. La fonction AuF doit ensuite calculer un identificateur GK_{ID} authentifié sous la forme d'un autre pouvoir au moyen de la fonction de hachage avec clé HMAC-SHA1-96 et de la clé partagée *ZZ*. Le résultat doit être inclus dans le champ **generator** de ce jeton **ClearToken**. Le champ **generalID** doit acheminer l'identificateur GK_{ID}, tandis que le champ **sendersID** doit acheminer l'identificateur EP_{ID} dans ce jeton **ClearToken**. Cela doit permettre au portier V-GK d'associer un message **AuthenticationConfirmation**/**AuthenticationRejection** au message **AuthenticationRequest** correspondant. Le champ **tokenOID** de ce jeton **ClearToken** doit être mis à "G2" et les autres paramètres de ce jeton **ClearToken** pour la mobilité ne doivent pas être utilisés. Le jeton **ClearToken** pour la mobilité est représenté sous forme de **WT()**.

Une nouvelle horodate T_8 doit être utilisée et le message de réponse doit être sécurisé conformément à la procédure I de l'Annexe D/H.235 [4] au moyen du secret partagé *ZZ3*; voir le message 8).

Si le nombre de bonds est dépassé, le proxy MRP ne doit pas envoyer de message **AuthenticationRequest**; en revanche, il doit répondre avec un message **AuthenticationRejection** dont le champ **reason** est mis à **hopCountExceeded**; voir le message 9).

Si le proxy MRP n'a pas de relation de service avec la fonction AuF (par exemple clé *ZZ3* manquante), il ne doit pas envoyer de message **AuthenticationRequest**; en revanche, il doit répondre avec un message **AuthenticationRejection** dont le champ **reason** est mis à **noServiceRelationship**; voir le message 9).

NOTE – La fonction AuF n'est pas capable de procéder strictement à une authentification complète du portier V-GK. En effet, celui-ci n'est pas en mesure de prouver sur le plan cryptographique son identité. Toutefois, la fonction AuF certifie par le pouvoir l'identité du portier V-GK qui est soumise. Ainsi, le terminal mobile/l'utilisateur est assuré que le portier V-GK avec lequel il communique est toujours le même que celui qui a été certifié pendant la procédure d'authentification.

8.3 Authentification du terminal

L'authentification du terminal mobile (MT, *mobile terminal*) est une autre fonctionnalité facultative, qui est prise en charge en plus de l'authentification de l'utilisateur mobile. Elle doit être utilisée lorsque l'authentification de l'utilisateur mobile seule est jugée insuffisante et lorsque le terminal mobile a un secret partagé correspondant *ZZMT*. On suppose que le terminal mobile possède un secret partagé attribué *ZZMT*, qu'il partage avec la fonction AuF. L'attribution et la distribution de ce secret partagé sont hors du domaine d'application de la présente Recommandation.

En réalité, deux scénarios d'authentification du terminal mobile sont pris en charge:

- la fonction AuF à laquelle l'utilisateur mobile est abonné est identique à la fonction AuF prenant en charge les terminaux mobiles abonnés. Dans ce cas, la fonction AuF est capable de procéder à l'authentification et de prendre une décision quant à l'autorisation de l'utilisateur et du terminal mobile;
- la fonction AuF à laquelle l'utilisateur mobile est abonné est différente de la fonction AuF à laquelle le terminal mobile est abonné. Dans ce cas, le message **AuthenticationRequest** doit d'abord être envoyé à la fonction AuF de l'utilisateur. Il appartient à cette dernière de localiser et de contacter la fonction AuF responsable du terminal mobile, laquelle peut être

située dans un domaine différent. Les communications en question et la protection de sécurité nécessaire au-delà de la fonction AuF ou entre les fonctions AuF sont hors du domaine d'application de la présente Recommandation.

L'authentification du terminal mobile, accomplie conjointement avec l'authentification d'utilisateur, utilise un jeton **CryptoToken** XT() distinct. Ce jeton **CryptoToken** est acheminé dans les champs de sécurité des messages d'authentification d'utilisateur **GRQ** ou **RRQ**, suivant si l'authentification d'utilisateur et de terminal a lieu pendant la phase de découverte du portier V-GK ou pendant la phase d'enregistrement; voir le § 8.2.

Le terminal mobile s'authentifie auprès de la fonction AuF en prouvant qu'il connaît ou qu'il possède le secret partagé *ZZMT*. Cela permet à la fonction AuF de vérifier que le jeton **CryptoToken** fourni est correct et d'en accuser réception dans le cadre de la réponse d'autorisation (**AuthenticationConfirmation/AuthenticationRejection**) faite au domaine visité. Ensuite, le domaine visité peut prendre une décision quant à l'autorisation du terminal mobile.

L'algorithme HMAC-SHA1-96 avec clé est utilisé en tant que fonction d'authentification cryptographique. La procédure mise en œuvre suit, dans les grandes lignes, la procédure I de l'Annexe D/H.235 [4], sauf que la vérification d'intégrité concerne uniquement le jeton **CryptoToken** propre au terminal mobile, et non la totalité du message comme décrit dans la procédure I de l'Annexe D/H.235 [4].

Le jeton **CryptoH323Token** spécifique destiné à l'authentification du terminal mobile doit contenir les champs suivants:

- **NestedCryptoToken** contenant un jeton **CryptoToken**, qui à son tour contient le jeton **cryptoHashedToken** contenant les champs suivants:
  - TokenOID mis à:
    - "G1" indiquant que la vérification de l'authenticité/de l'intégrité porte uniquement sur le contenu de ce jeton **CryptoToken**.
- **HashedVals** contenant le champ **ClearToken** utilisé avec les champs suivants:
  - **TokenOID** mis à:
    - "T" indiquant que ce jeton **ClearToken** est utilisé pour la vérification d'authenticité/d'intégrité (voir le D.11/D/H.235 [4]);
    - **timestamp** contenant l'horodate;
    - **random** contenant un numéro de séquence à croissance stricte. Ce numéro permet de rendre uniques deux messages ayant la même horodate (compte tenu de la résolution d'horloge);
    - **generalID** contenant l'identificateur du destinataire (uniquement dans le cas de messages monodiffusés). Dans ce scénario, il s'agit de l'identificateur du domaine de rattachement;
    - **sendersID** contenant l'identificateur de l'expéditeur. Dans ce scénario, il s'agit de l'identificateur de point d'extrémité du terminal mobile.
- **Token** contenant **HASHED** avec les champs:
  - **algorithmOID** mis à "U" indiquant HMAC-SHA1-96; (voir le D.11/H.235 [4]);
  - **params** mis à NULL;
  - **hash** contenant la valeur d'authentification calculée au moyen de HMAC-SHA1-96. Cette valeur doit être calculée sur la totalité du jeton **CryptoH323Token**.

La fonction AuF réceptrice doit vérifier le jeton **CryptoToken** trouvé, qui achemine l'authentification du terminal mobile. En cas d'échec de la vérification, la fonction AuF doit considérer que le terminal mobile n'est pas autorisé. Dans ce cas, elle doit répondre avec un message

AuthenticationRejection dont le champ **reason** est mis à **security**. Pour tout autre échec lié à la sécurité, la fonction AuF doit mettre dans le champ **reason** une erreur conforme au B.2.2/H.235 [4].

La Figure 10 montre le flux de messages pour l'authentification du terminal mobile pendant la phase d'enregistrement du terminal mobile. Le jeton **CryptoToken** spécifique destiné à l'authentification du terminal mobile est représenté sous forme de XT().

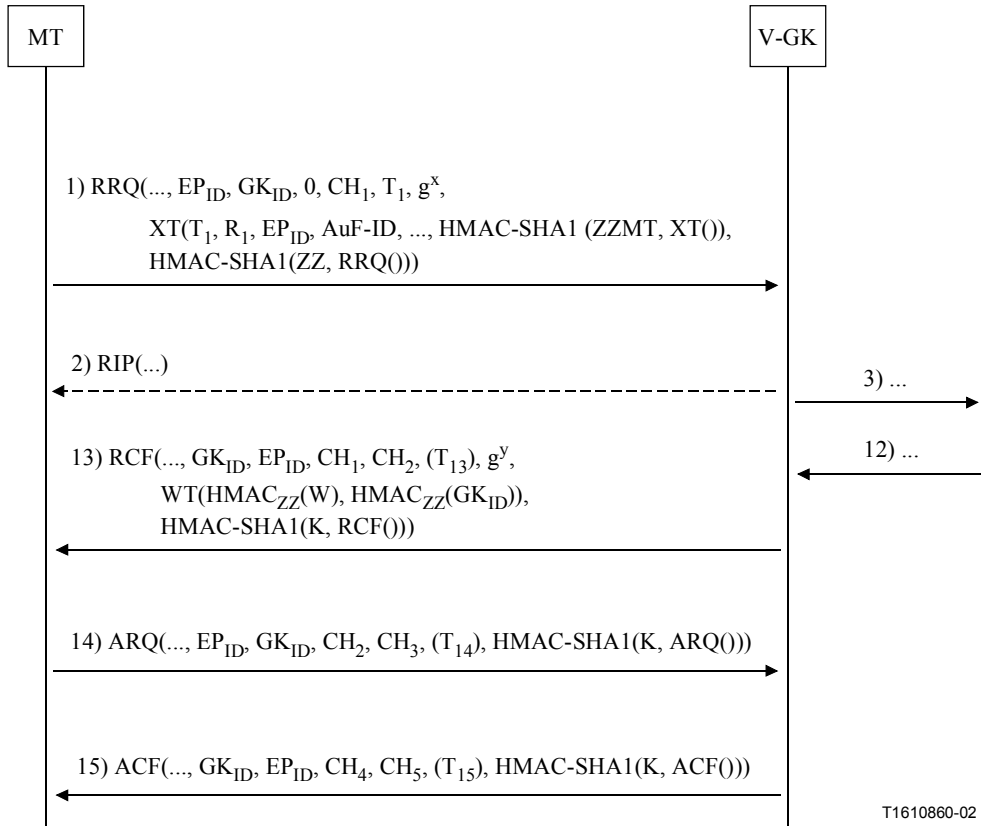

Figure 10/H.530 – Authentification du terminal mobile

La procédure d'authentification du terminal mobile est exécutée explicitement uniquement dans le cadre des messages **GRQ** ou **RRQ**. En ce qui concerne les messages RAS ultérieurs échangés entre le terminal mobile et le portier V-GK, l'authentification du terminal mobile est faite implicitement par le biais de l'authentification d'utilisateur et du contrôle d'intégrité de message en cours. Aucun autre procédé n'est nécessaire pour l'authentification du terminal mobile.

8.4 Annulation d'enregistrement

Dès qu'il reçoit un message **UCF**, un terminal mobile ou un portier V-GK doit libérer la clé de liaison *K*.

8.5 Application du protocole de sécurité symétrique dans le domaine de rattachement

Le protocole de sécurité pour la mobilité décrit dans la présente Recommandation serait généralement mis en œuvre pour les terminaux mobiles lorsque ceux-ci dépendent de domaines visités étrangers, mais le présent paragraphe décrit la façon dont ce protocole peut également être mis en œuvre pour les terminaux mobiles lorsque ceux-ci dépendent de leur domaine de rattachement. Ainsi, ce protocole peut être mis en œuvre indépendamment du domaine dont le terminal mobile dépend réellement. La mise en œuvre de ce protocole couvre également le cas des environnements sans mobilité, qui prennent néanmoins en charge les procédures H.530.

La Figure 11 illustre le scénario dans lequel un terminal mobile est relié au portier du domaine de rattachement (H-GK) et l'authentification et l'autorisation ont lieu pendant la phase d'enregistrement.

On peut également envisager un scénario analogue non illustré, dans lequel l'authentification et l'autorisation ont lieu pendant la phase de découverte du portier.

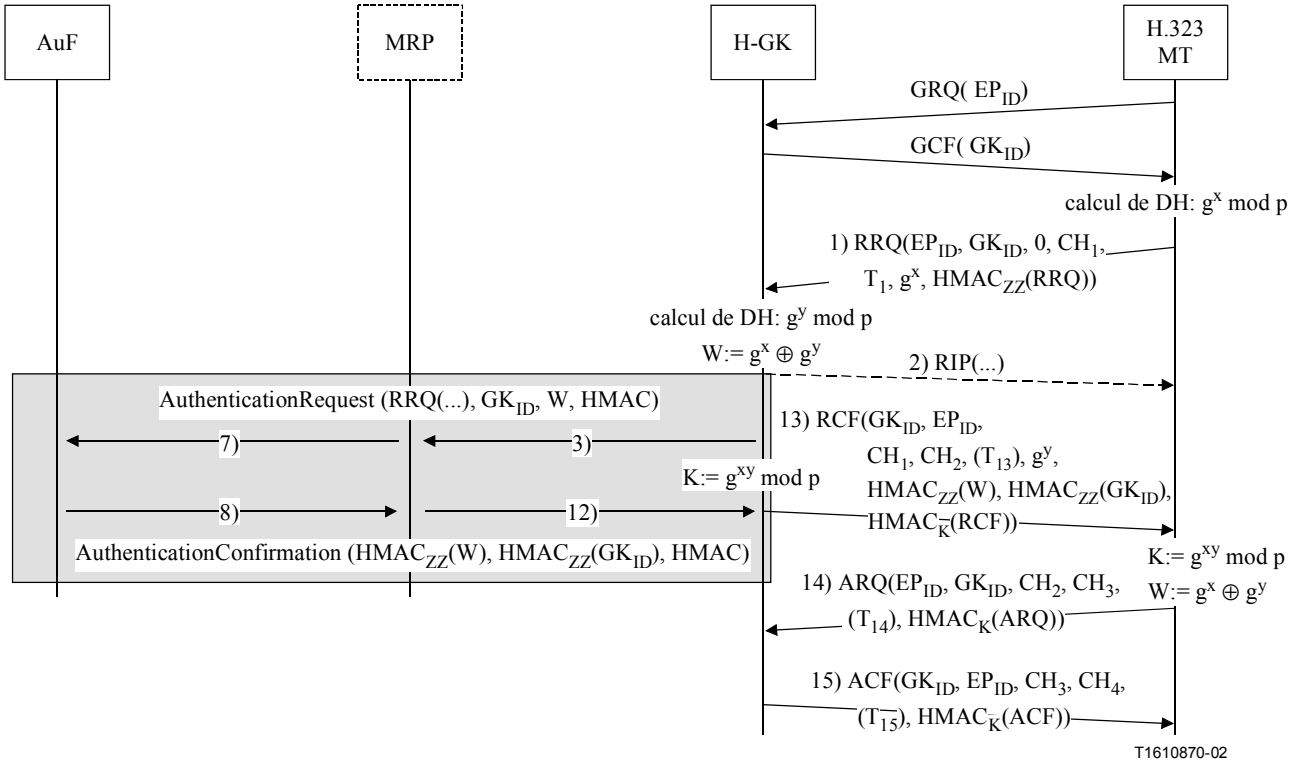

Figure 11/H.530 – Authentification du terminal mobile dans le domaine de rattachement pendant la phase d'enregistrement

Dans l'un ou l'autre cas, le portier H-GK doit se comporter exactement comme un portier V-GK, comme illustré sur la Figure 11, et suivre les procédures de sécurité décrites ci-dessus. Le secret partagé *ZZ4* doit être remplacé par *ZZ8*, et le secret partagé *ZZ3* par *ZZ7*.

Le proxy MRP montré est une entité facultative. Lorsqu'il est absent, une relation de sécurité directe est établie entre la fonction AuF et le portier H-GK. Cas particulier: la fonction AuF et le portier H-GK peuvent même être situés au même endroit, auquel cas la communication entre les deux entités est alors une question locale.

8.6 Liste des identificateurs d'objet

Le Tableau 1 contient la liste de tous les identificateurs d'objet utilisés dans la présente Recommandation.

Tableau 1/H.530 – Identificateurs d'objet utilisés dans la H.530

Symbole de l'identificateur d'objet	Valeur(s) de l'identificateur d'objet	Description
"G1"	{itu-t (0) Recommendation (0) h (8) 235 version (0) 2 10}	Indique un jeton **CryptoToken** pour la mobilité en vue de l'authentification du terminal mobile.
"G2"	{itu-t (0) Recommendation (0) h (8) 235 version (0) 2 11}	Indique un jeton **ClearToken** pour la mobilité contenant un identificateur GK_{ID} et une valeur composite *W* figurant dans un message **AuthenticationRequest** ou les valeurs correspondantes authentifiées par la fonction AuF figurant dans des messages **AuthenticationConfirmation/AuthenticationRejection** ou GCF/GRJ, RCF/RCF

9 Sécurité de bout en bout

L'architecture de sécurité de bout en bout dans un environnement H.323 avec mobilité, reposant sur des concepts d'infrastructure à clés publiques (PKI, *public-key infrastructure*), nécessite un complément d'étude.

SÉRIES DES RECOMMANDATIONS UIT-T

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

Imprimé en Suisse
Genève, 2002