UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

H.530

Corrigendum 1
(07/2003)

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

Corrigendum 1

Recommandation UIT-T H.530 (2002) – Corrigendum 1

RECOMMANDATIONS UIT-T DE LA SÉRIE H

SYSTÈMES AUDIOVISUELS ET MULTIMÉDIAS

CARACTÉRISTIQUES DES SYSTÈMES VISIOPHONIQUES	H.100–H.199
INFRASTRUCTURE DES SERVICES AUDIOVISUELS	
Généralités	H.200–H.219
Multiplexage et synchronisation en transmission	H.220–H.229
Aspects système	H.230–H.239
Procédures de communication	H.240–H.259
Codage des images vidéo animées	H.260–H.279
Aspects liés aux systèmes	H.280–H.299
SYSTÈMES ET ÉQUIPEMENTS TERMINAUX POUR LES SERVICES AUDIOVISUELS	H.300–H.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
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.530

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

Corrigendum 1

Résumé

Le présent corrigendum remédie à un défaut identifié dans la Rec. UIT-T H.530 (2002/03) au niveau de la sécurité et qui mettait le portier du domaine visité (V-GK) dans l'impossibilité de vérifier si le message AuthenticationConfirmation reçu était nouveau, ce qui favorisait les agressions par répétition ou par usurpation d'identité. On a remédié à ce défaut en introduisant des paramètres de sécurité supplémentaires (c'est-à-dire le paramètre W) dans le message de réponse de gestion de clé.

Source

Le Corrigendum 1 de la Recommandation H.530 (2002) de l'UIT-T a été approuvé par la Commission d'études 16 (2001-2004) de l'UIT-T le 14 juillet 2003 selon la procédure définie dans la Recommandation UIT-T A.8.

AVANT-PROPOS

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

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

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

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

NOTE

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

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

DROITS DE PROPRIÉTÉ INTELLECTUELLE

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

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

TABLE DES MATIÈRES

Recommandation UIT-T H.530

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

Corrigendum 1

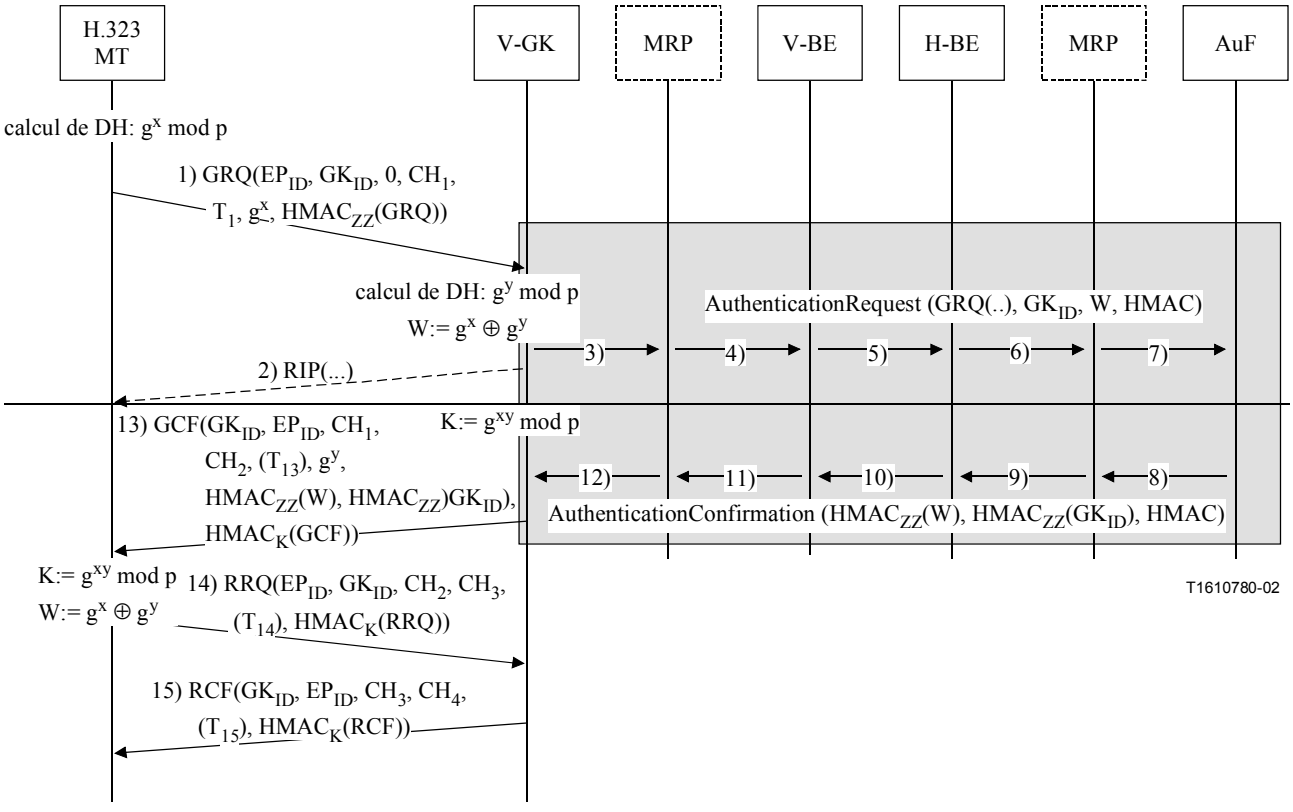
1) Paragraphe 6, Références

Ajouter une nouvelle référence [8], comme suit et mettre à jour toutes les références de [8] et [9] à [9] et [10], respectivement:

[8] Recommandation UIT-T H.235 version 3 (2003), *Sécurité et cryptage des terminaux multimédias de la série H (terminaux H.323 et autres terminaux de type H.245).*

2) Paragraphe 8.2

a) Remplacer la Figure 2:



Par la suivante:

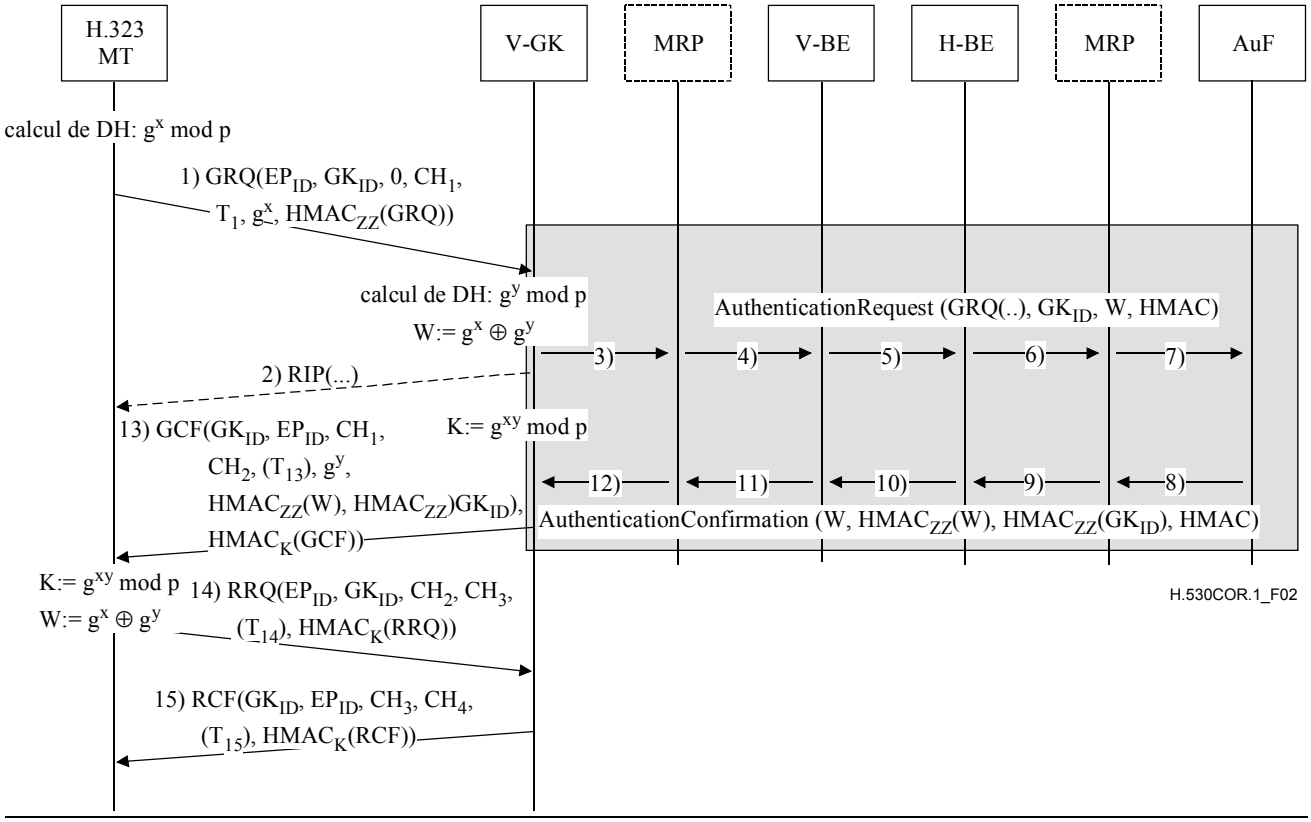
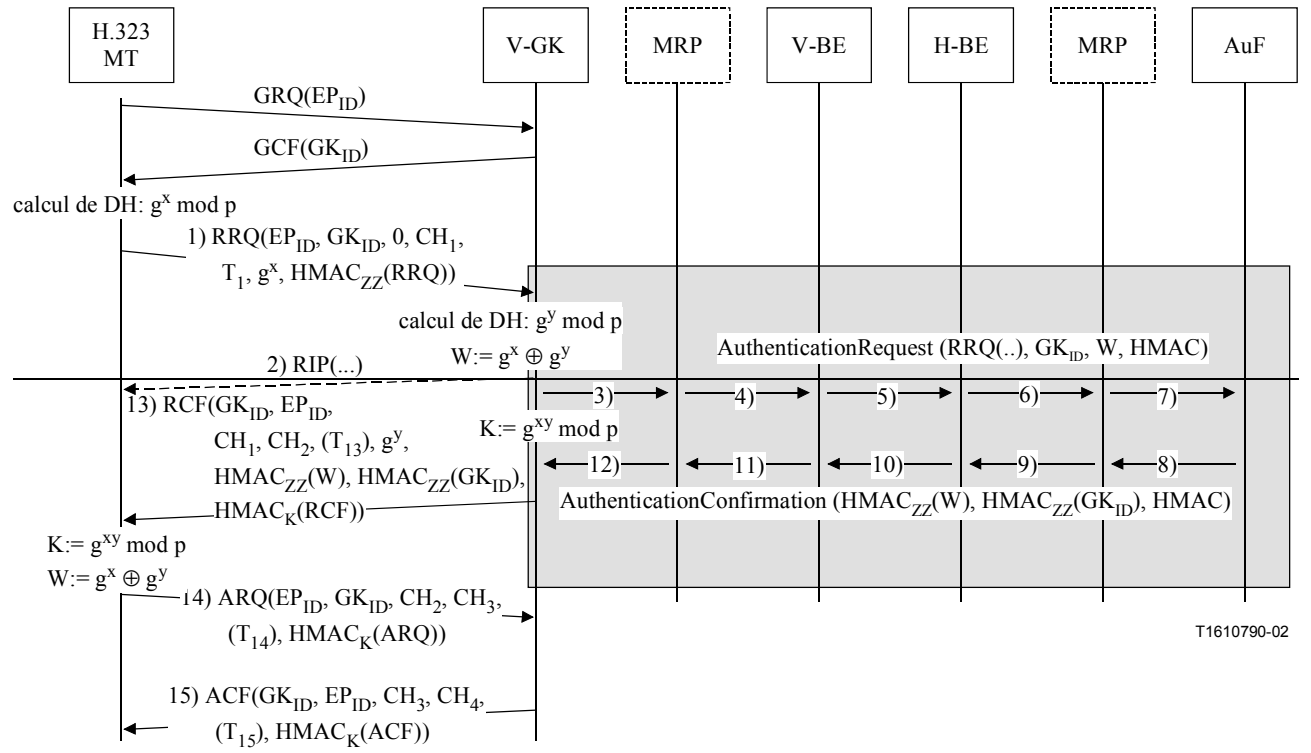


Figure 2/H.530 – Authentification et gestion des clés pendant la phase de découverte du portier

b) Remplacer la Figure 3:



Par la suivante:

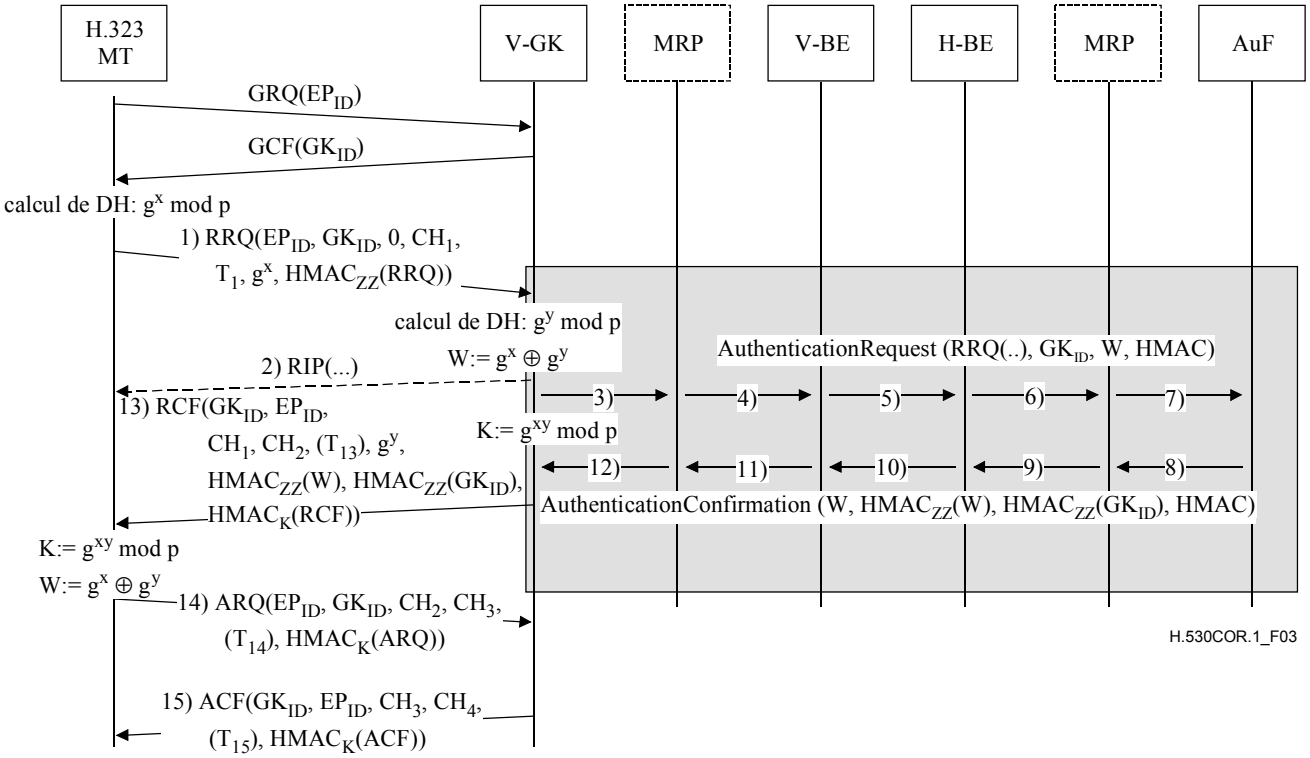


Figure 3/H.530 – Authentification et gestion des clés pendant la phase d'enregistrement

3) Paragraphe 8.2.1

Ajouter ce qui suit:

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

...

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 doit vérifier que le jeton **ClearToken** pour la mobilité acheminé contient la même valeur *W* que celle qui a été envoyée dans le message 3). Une absence de concordance entre ces deux valeurs signale une agression par répétition; dans ce cas, le portier V-GK doit considérer que l'authentification du terminal mobile par la fonction AuF a échoué et répondre par un message **GRJ/RRJ** avec le champ **reason** mis à la valeur securityDenial ou tout autre code d'erreur de sécurité approprié, conformément au B.2.2/H.235 [8].

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**.

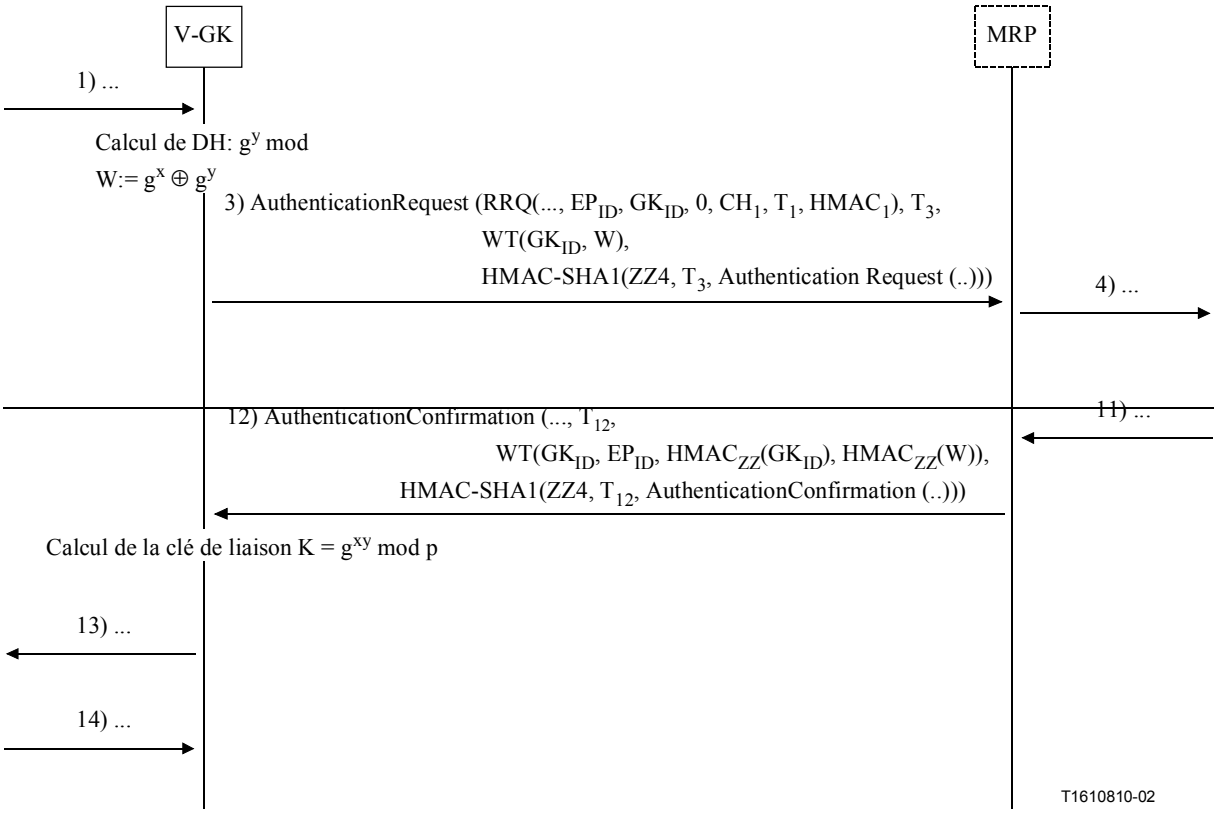
Le portier V-GK doit ensuite retransmettre les pouvoirs de la fonction AuF au terminal mobile. Les pouvoirs comprennent le jeton **ClearToken** pour la mobilité représenté sous forme de **WT()**. Ce jeton **ClearToken** pour la mobilité achemine d'une part, la valeur composite authentifiée *W* dans le champ **halfkey** du champ **dhkey** et, d'autre part, l'identificateur du portier V-GK authentifié; la valeur *W* ne devrait pas faire partie du jeton **WT()** retransmis. 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).

...

4) Paragraphe 8.2.2

Remplacer la Figure 5:



Par la suivante:

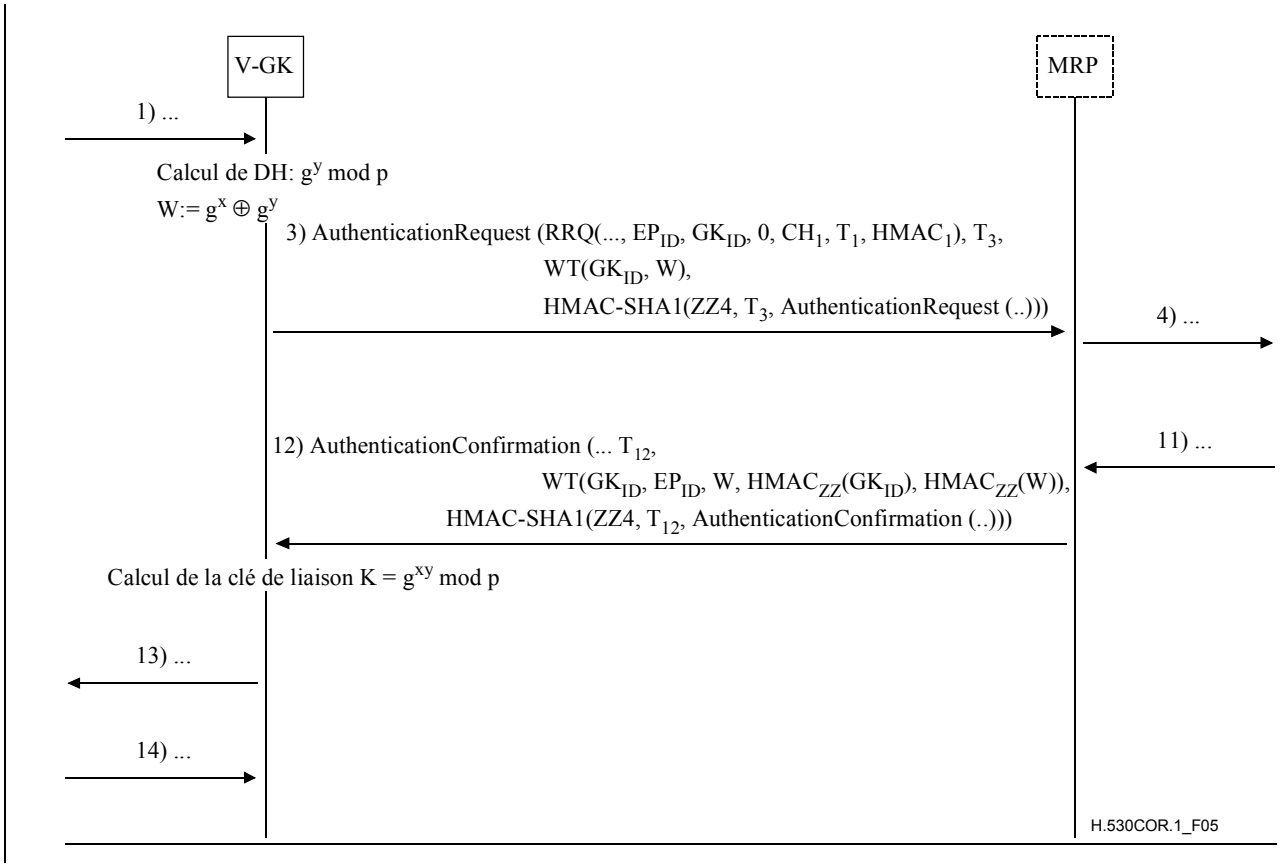
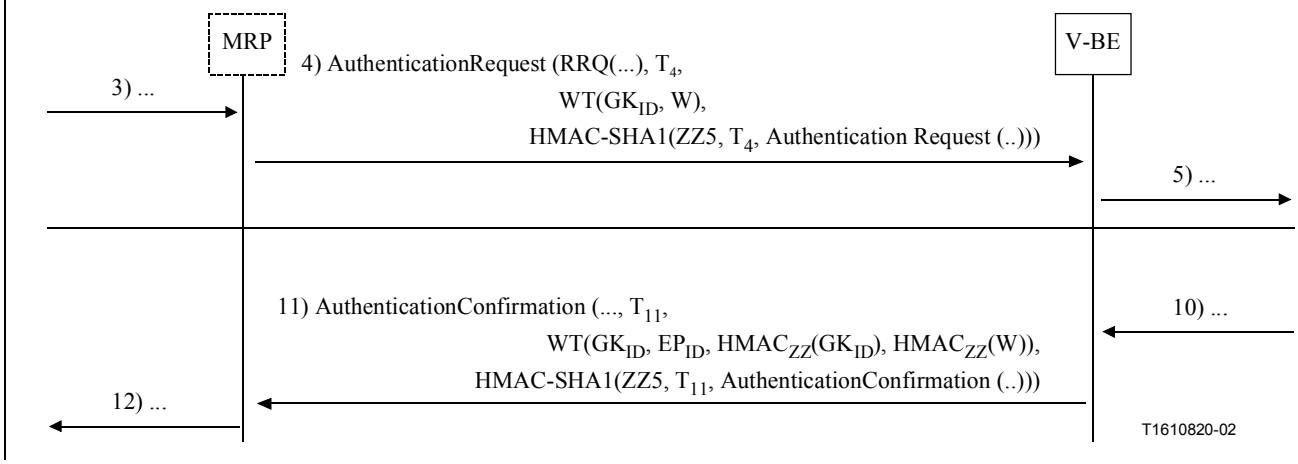


Figure 5/H.530 – Transmission d'informations d'authentification entre le portier V-GK et le proxy MRP

5) Paragraphe 8.2.3

Remplacer la Figure 6:



Par la suivante:

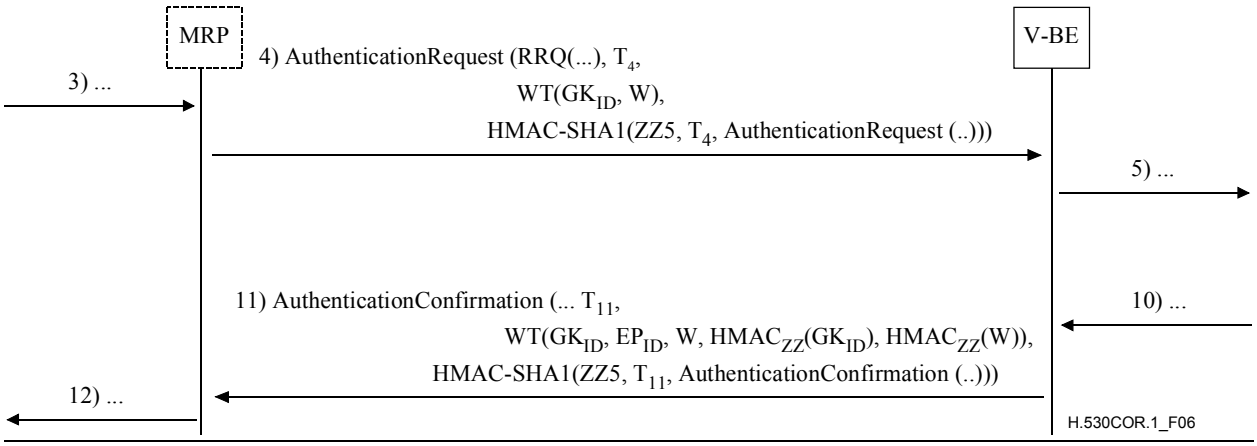
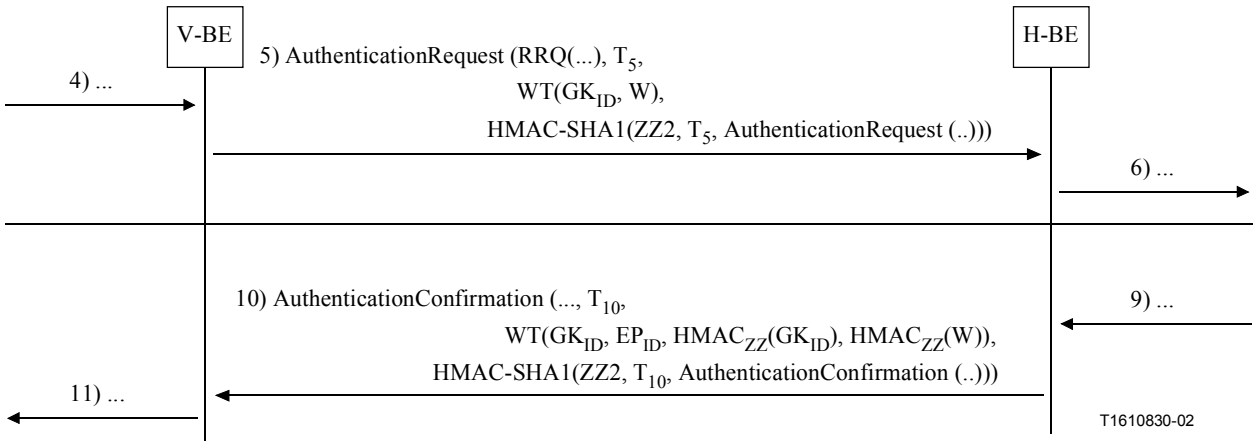


Figure 6/H.530 – Transmission d'informations d'authentification entre le proxy MRP et l'élément V-BE

6) Paragraphe 8.2.4

Remplacer la Figure 7:



Par la suivante:

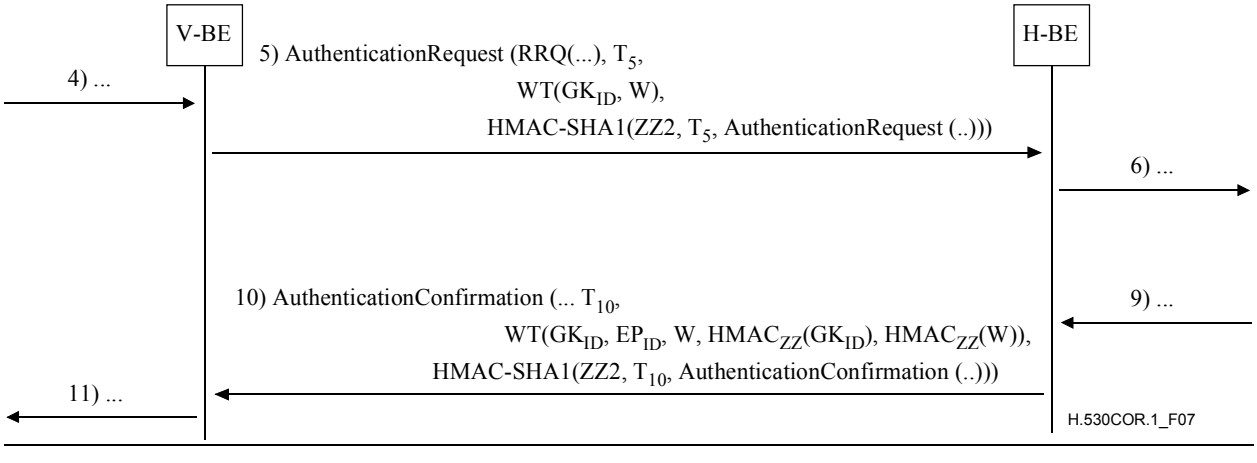
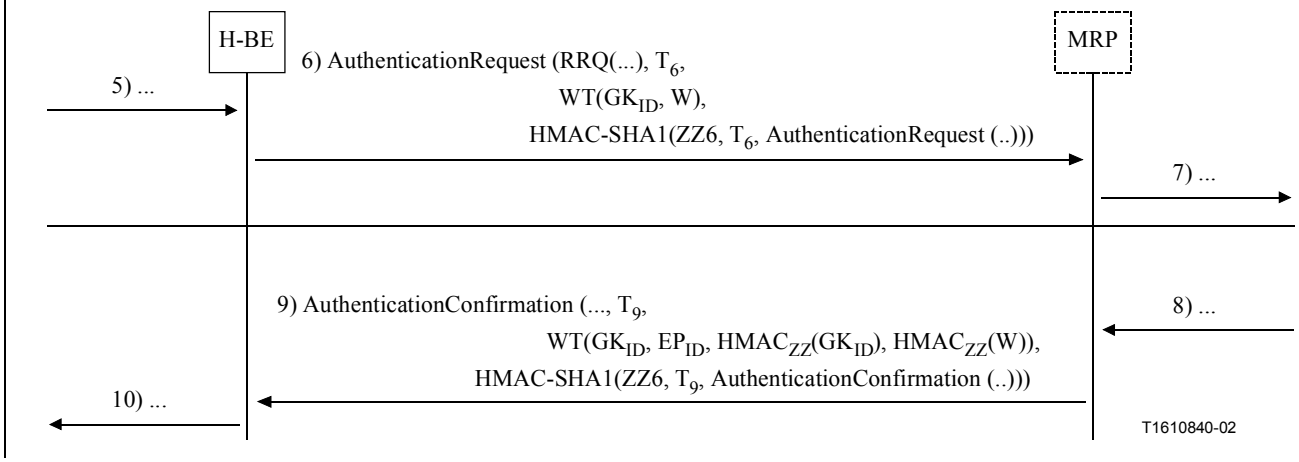


Figure 7/H.530 – Transmission d'informations d'authentification entre éléments frontière

7) Paragraphe 8.2.5

Remplacer la Figure 8:



Par la suivante:

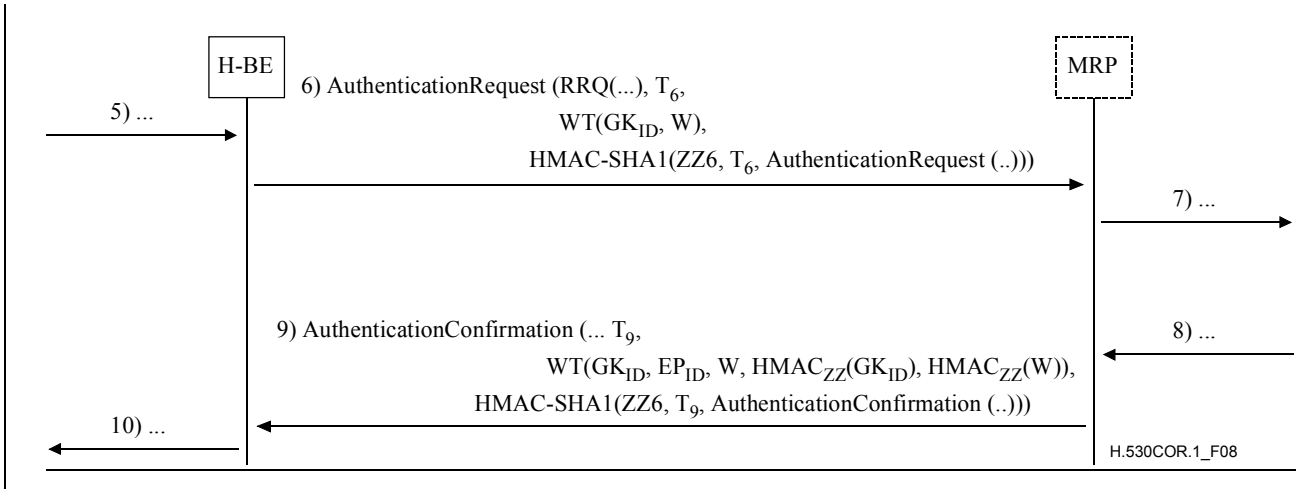
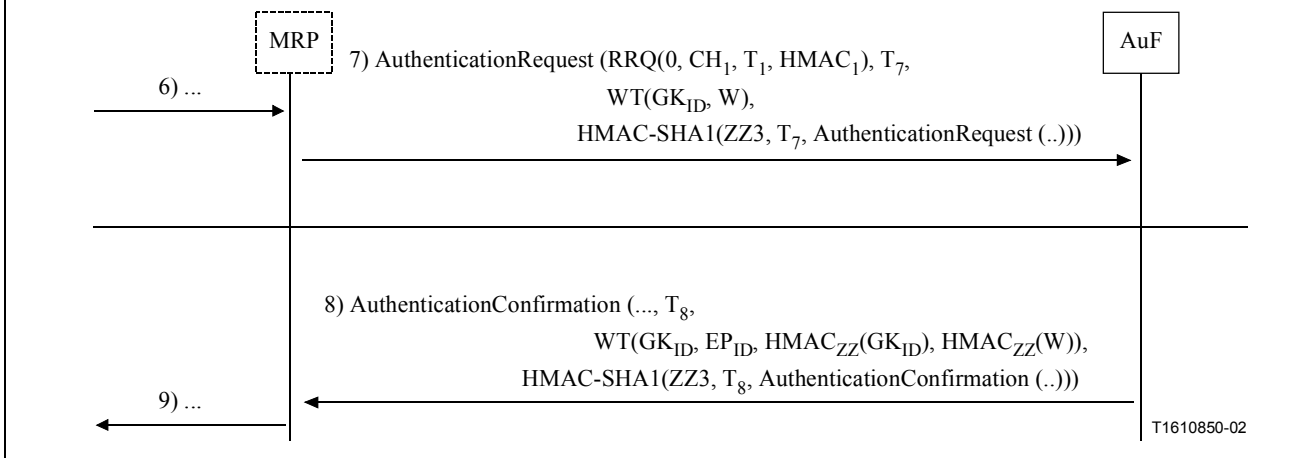


Figure 8/H.530 – Transmission d'informations d'authentification entre l'élément H-BE et le proxy MRP

8) Paragraphe 8.2.6

Remplacer la Figure 9:



Par la suivante:

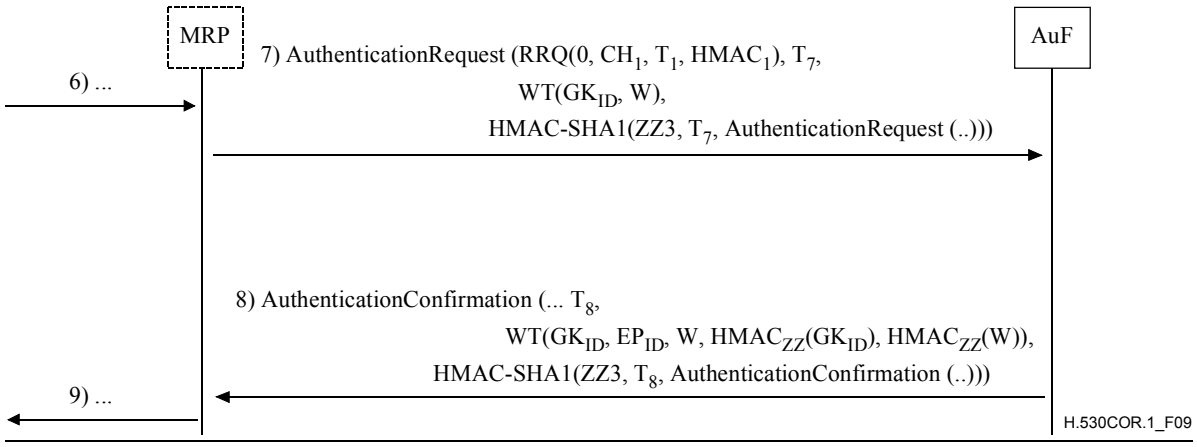


Figure 9/H.530 – Transmission d'informations d'authentification entre le proxy MRP et la fonction AuF

9) Paragraphe 8.2.6

Modifier le texte comme suit:

...

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

...

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**.

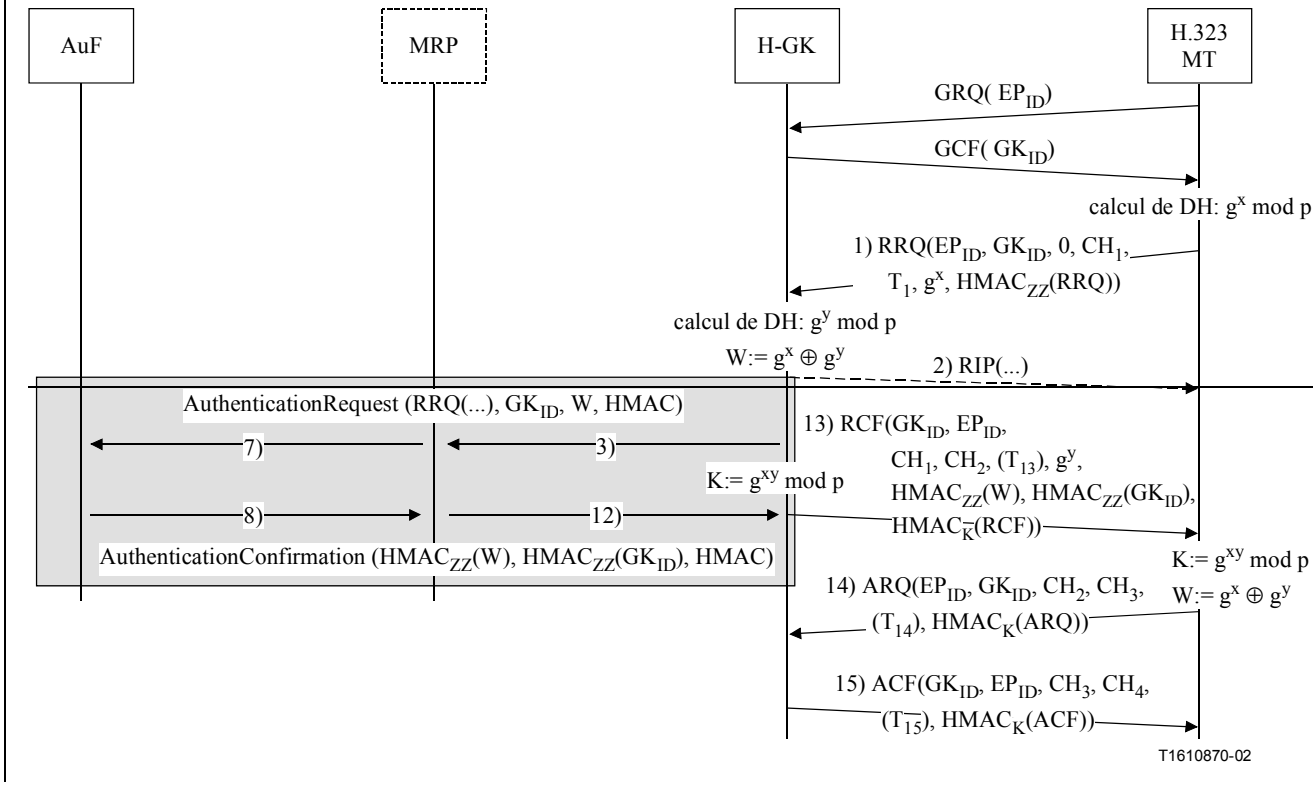
Dans le cas contraire, la fonction AuF doit aussi calculer les pouvoirs associés à la valeur composite authentifiée *W* au moyen de la fonction de hachage avec clé HMAC-SHA1-96 et de la clé partagée *ZZ*. La valeur composite authentifiée *W* doit être incluse dans un jeton distinct **ClearToken** pour 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**. La Fonction AuF doit également inclure la valeur *W* dans le champ **modsize** du champ **dhkey**; cela permet au portier V-GK de savoir que le message **AuthenticationConfirmation/AuthenticationRejection** est nouveau. 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).

...

10) Paragraphe 8.5

Remplacer la Figure 11:



Par la suivante:

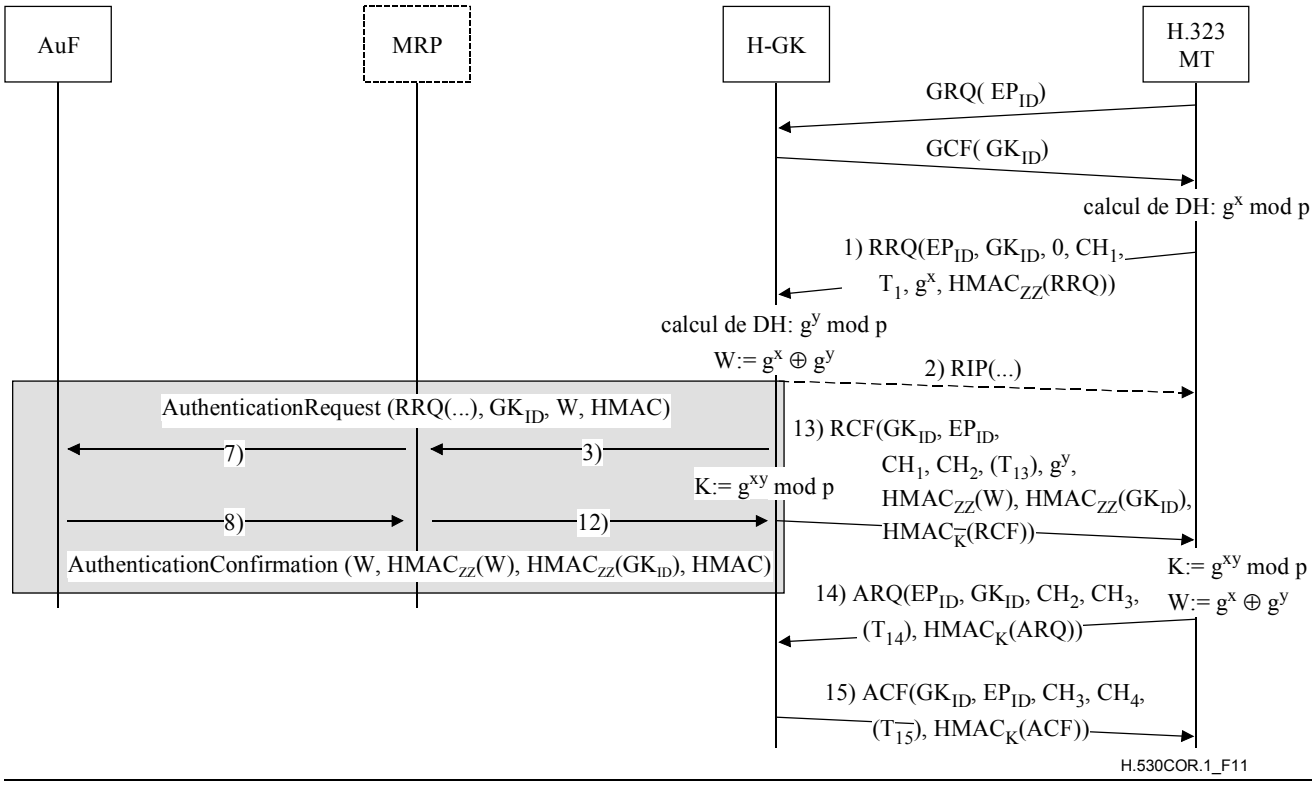


Figure 11/H.530 – Authentification du terminal mobile dans le domaine de rattachement pendant la phase d'enregistrement

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, protocole Internet et réseaux de nouvelle génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Genève, 2003