UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T H.530

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

Corrigendum 1
(07/2003)

SERIE H: SISTEMAS AUDIOVISUALES Y MULTIMEDIOS

Procedimientos de movilidad y de colaboración – Seguridad para los sistemas y servicios móviles multimedios

---

Procedimientos de seguridad simétricos para movilidad de sistemas H.323 según la Recomendación H.510

Corrigendum 1

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

RECOMENDACIONES UIT-T DE LA SERIE H

SISTEMAS AUDIOVISUALES Y MULTIMEDIOS

CARACTERÍSTICAS DE LOS SISTEMAS VIDEOTELEFÓNICOS	H.100–H.199
INFRAESTRUCTURA DE LOS SERVICIOS AUDIOVISUALES	
Generalidades	H.200–H.219
Multiplexación y sincronización en transmisión	H.220–H.229
Aspectos de los sistemas	H.230–H.239
Procedimientos de comunicación	H.240–H.259
Codificación de imágenes vídeo en movimiento	H.260–H.279
Aspectos relacionados con los sistemas	H.280–H.299
SISTEMAS Y EQUIPOS TERMINALES PARA LOS SERVICIOS AUDIOVISUALES	H.300–H.399
SERVICIOS SUPLEMENTARIOS PARA MULTIMEDIOS	H.450–H.499
PROCEDIMIENTOS DE MOVILIDAD Y DE COLABORACIÓN	
Visión de conjunto de la movilidad y de la colaboración, definiciones, protocolos y procedimientos	H.500–H.509
Movilidad para los sistemas y servicios multimedios de la serie H	H.510–H.519
Aplicaciones y servicios de colaboración en móviles multimedios	H.520–H.529
Seguridad para los sistemas y servicios móviles multimedios	**H.530–H.539**
Seguridad para las aplicaciones y los servicios de colaboración en móviles multimedios	H.540–H.549
Procedimientos de interfuncionamiento de la movilidad	H.550–H.559
Procedimientos de interfuncionamiento de colaboración en móviles multimedios	H.560–H.569
SERVICIOS DE BANDA ANCHA Y DE TRÍADA MULTIMEDIOS	
Servicios multimedios de banda ancha sobre VDSL	H.610–H.619

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T H.530

Procedimientos de seguridad simétricos para movilidad de sistemas H.323 según la Recomendación H.510

Corrigendum 1

Resumen

El presente corrigendum subsana un fallo de seguridad identificado en la Rec. UIT-T H.530 (2002/03): no hay forma de que el V-GK compruebe si el mensaje AuthenticationConfirmation recibido es nuevo. Por tanto, este fallo permite la reproducción fraudulenta y la impostura. Este problema se ha corregido introduciendo parámetros de seguridad adicionales (parámetro W) en el mensaje de respuesta de gestión de claves.

Orígenes

El corrigendum 1 a la Recomendación UIT-T H.530 (2002) fue aprobado por la Comisión de Estudio 16 (2001-2004) del UIT-T por el procedimiento de la Recomendación UIT-T A.8 el 14 de julio de 2003.

PREFACIO

La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB.

ÍNDICE

Recomendación UIT-T H.530

Procedimientos de seguridad simétricos para movilidad de sistemas H.323 según la Recomendación H.510

Corrigendum 1

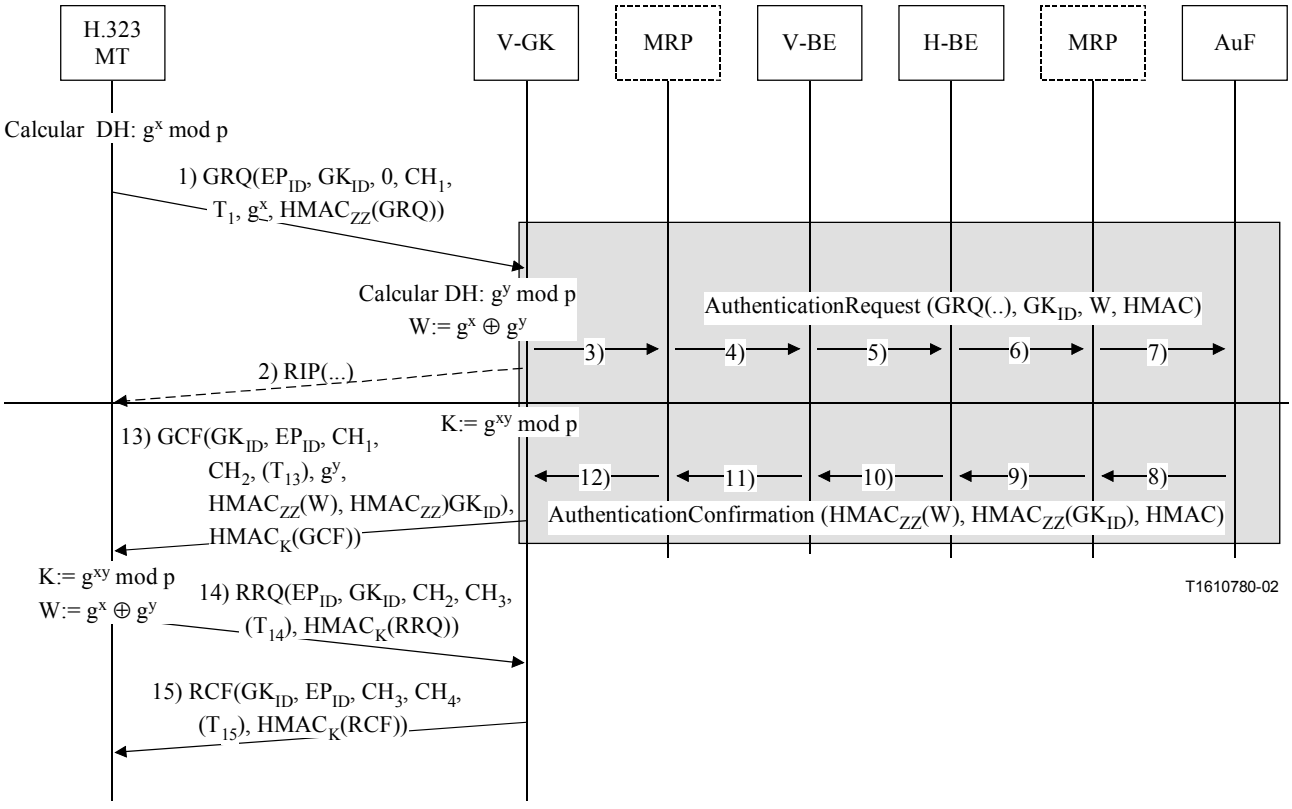
1) Cláusula 6, Referencias

Añádase una nueva referencia [8] como sigue y renumérense las referencias [8] y [9] como [9] y [10], respectivamente:

[8] Recomendación UIT-T H.235 versión 3 (2003), *Seguridad y criptado para terminales multimedios de la serie H (basados en las Recomendaciones H.323 y H.245).*

2) Cláusula 8.2

a) Reemplácese la figura 2:



Por:

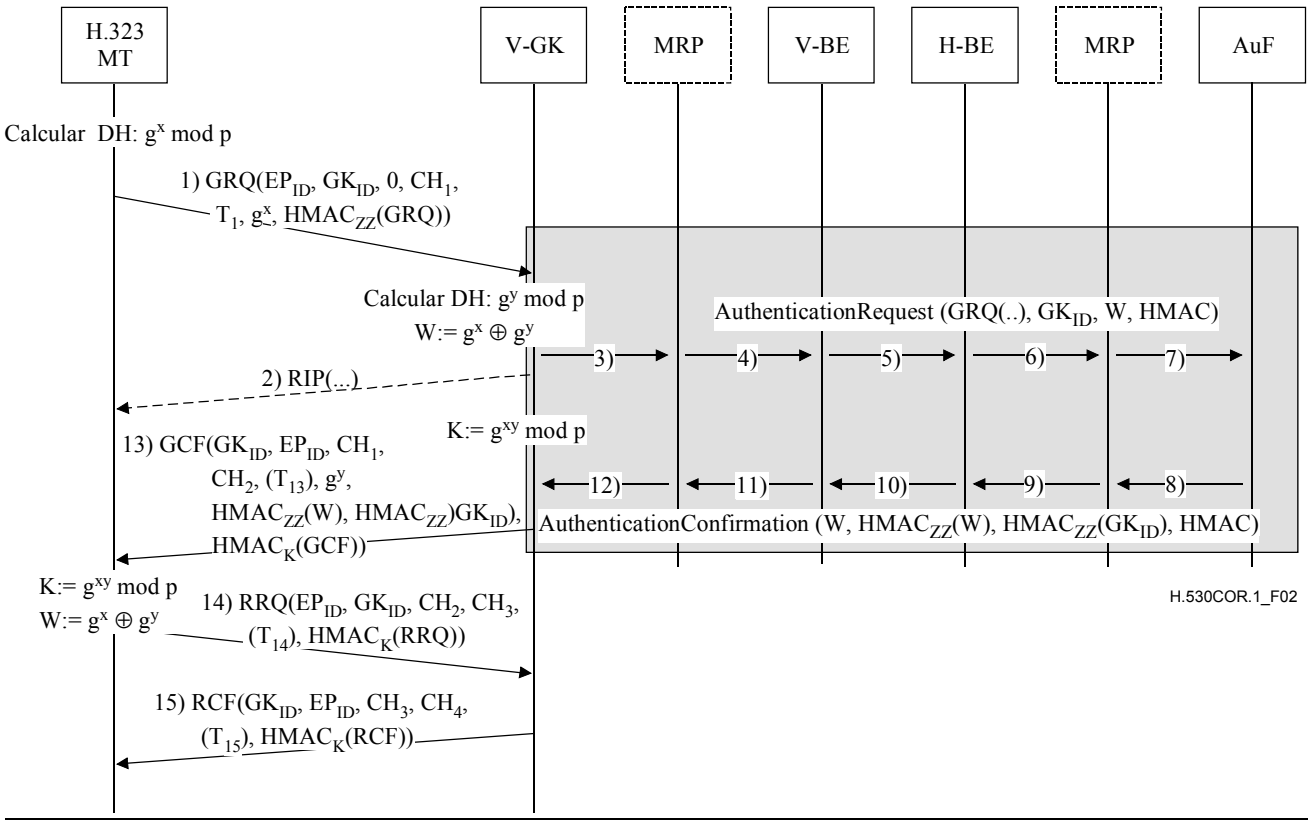
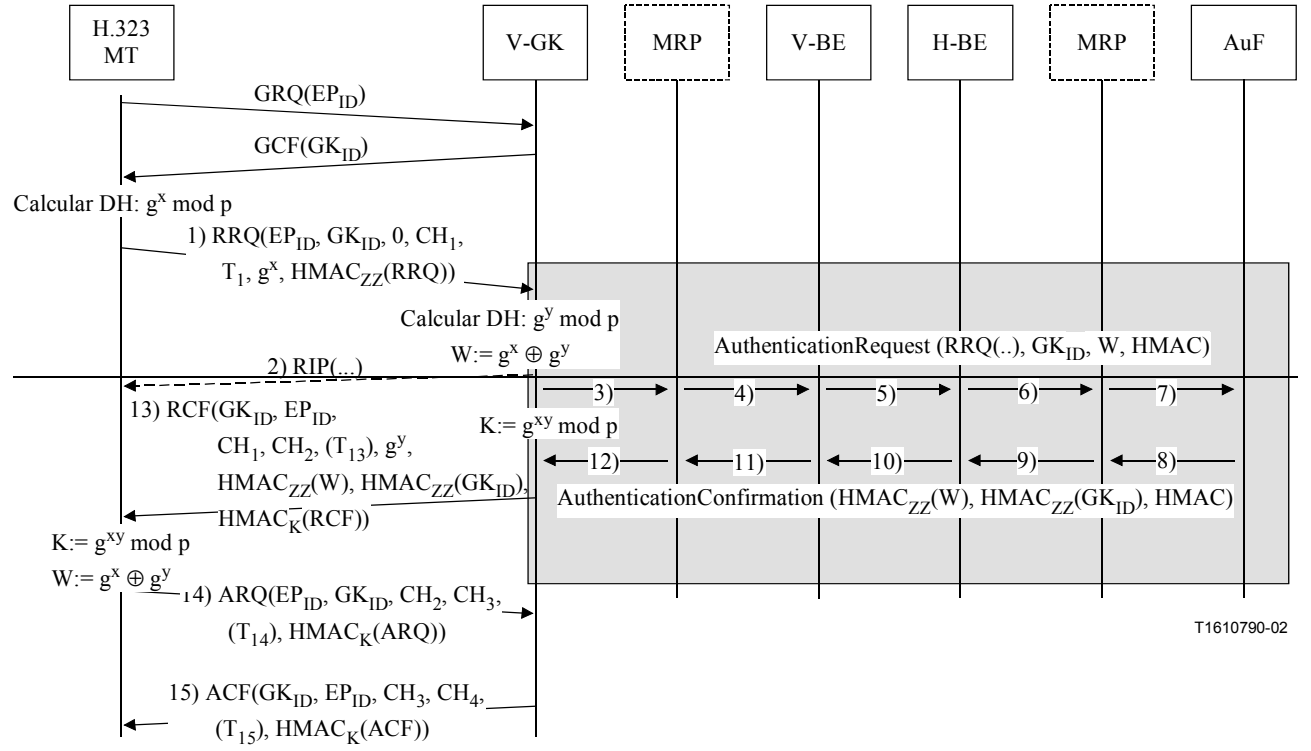


Figura 2/H.530 – Autenticación y gestión de clave en la fase de descubrimiento de GK

b) Cámbiese la figura 3:



Por:

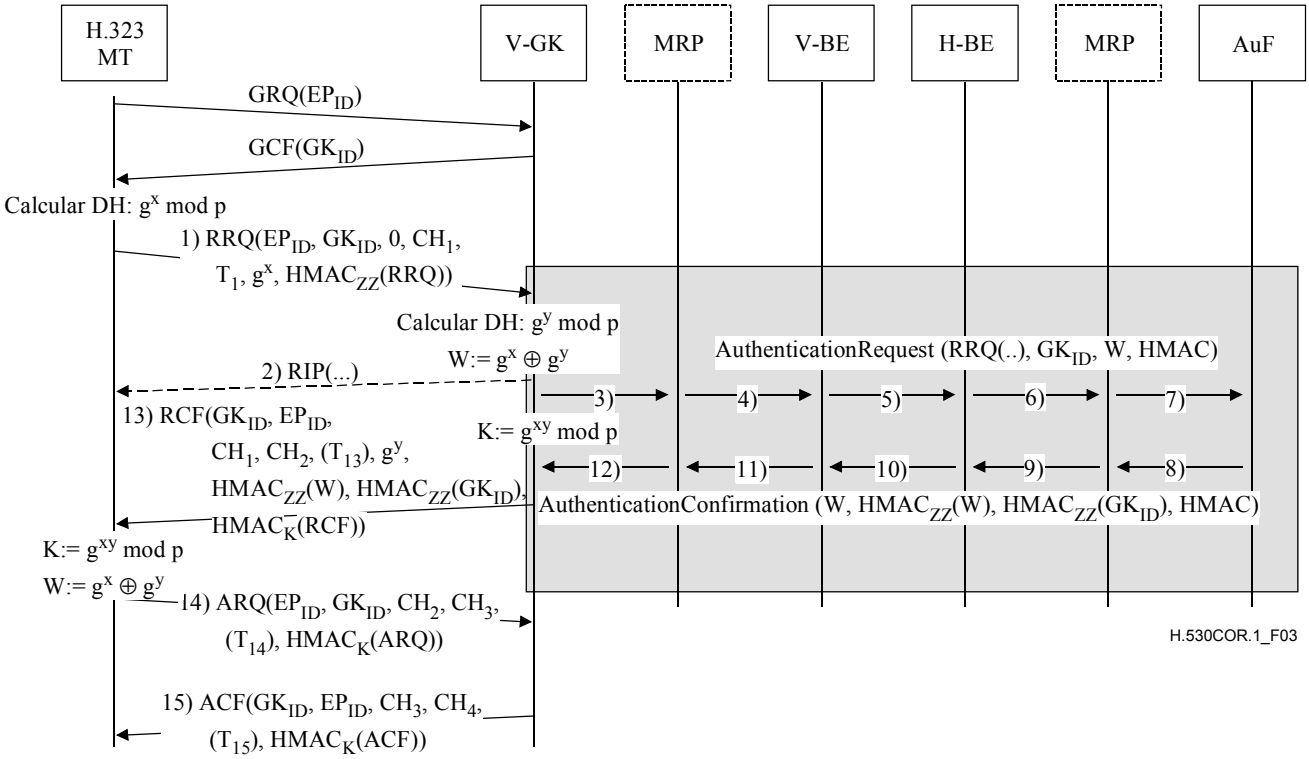


Figura 3/H.530 – Autenticación y gestión de clave en la fase de registro

3) Cláusula 8.2.1

Añádase lo siguiente como se indica:

...

8.2.1 MT a V-GK

...

Hasta que el **RCF** haya sido depositado como mensaje 13), el V-GK tiene tiempo de calcular el enlace dinámico *K* utilizando la semiclave Diffie-Hellman del MT y su propio secreto *y*. En el caso de la protección de integridad de mensaje HMAC-SHA1-96 de los mensajes RAS H.225.0 [1], los 96 bits más a la izquierda se tomarán del secreto compartido Diffie-Hellman resultante representado con el orden de octetos en la red.

El V-GK recibe un mensaje **AuthenticationConfirmation**/**AuthenticationRejection** junto con el resultado de la autenticación y de la comprobación de autorización por la AuF y credenciales transportadas; véase el mensaje 12). El V-GK verificará si el **ClearToken** de movilidad transportado posee el mismo valor *W* que se envió en el mensaje 3). Cualquier diferencia indica una reproducción fraudulenta. En este caso, el V-GK considerará que la AuF no ha autenticado el MT y responderá con un **GRJ/RRJ** que indica el motivo (**reason**), puesto a denegación de seguridad u otro código de error de seguridad apropiado, de conformidad con B.2.2/H.235 [8].

El V-GK puede supervisar la recepción de mensajes **AuthenticationConfirmation**/**AuthenticationRejection** utilizando un temporizador. La duración del temporizador debe elegirse de modo que sea suficientemente larga, para que tenga en cuenta el tránsito por la red y el procesamiento en la AuF. Si el temporizador expira sin que haya llegado la correspondiente respuesta de la AuF, el V-GK enviará un **RCF** no protegido.

El V-GK generará un nuevo desafío CH_2 y construirá **RCF**. El **RCF** conllevará el anterior desafío CH_1 dentro de la **contraseña**, un nuevo desafío CH_2 dentro de **challenge** dentro del **ClearToken** dentro del **CryptoToken** de **RCF**. Este **ClearToken** también conllevará la semiclave Diffie-Hellman calculada del V-GK en el campo **halfkey** del campo **dhkey** dentro del **ClearToken** de ese mensaje. El número primo aplicado se incluirá en **modsize** mientras que el generador DH se incluirá en **generator** de ese **ClearToken**.

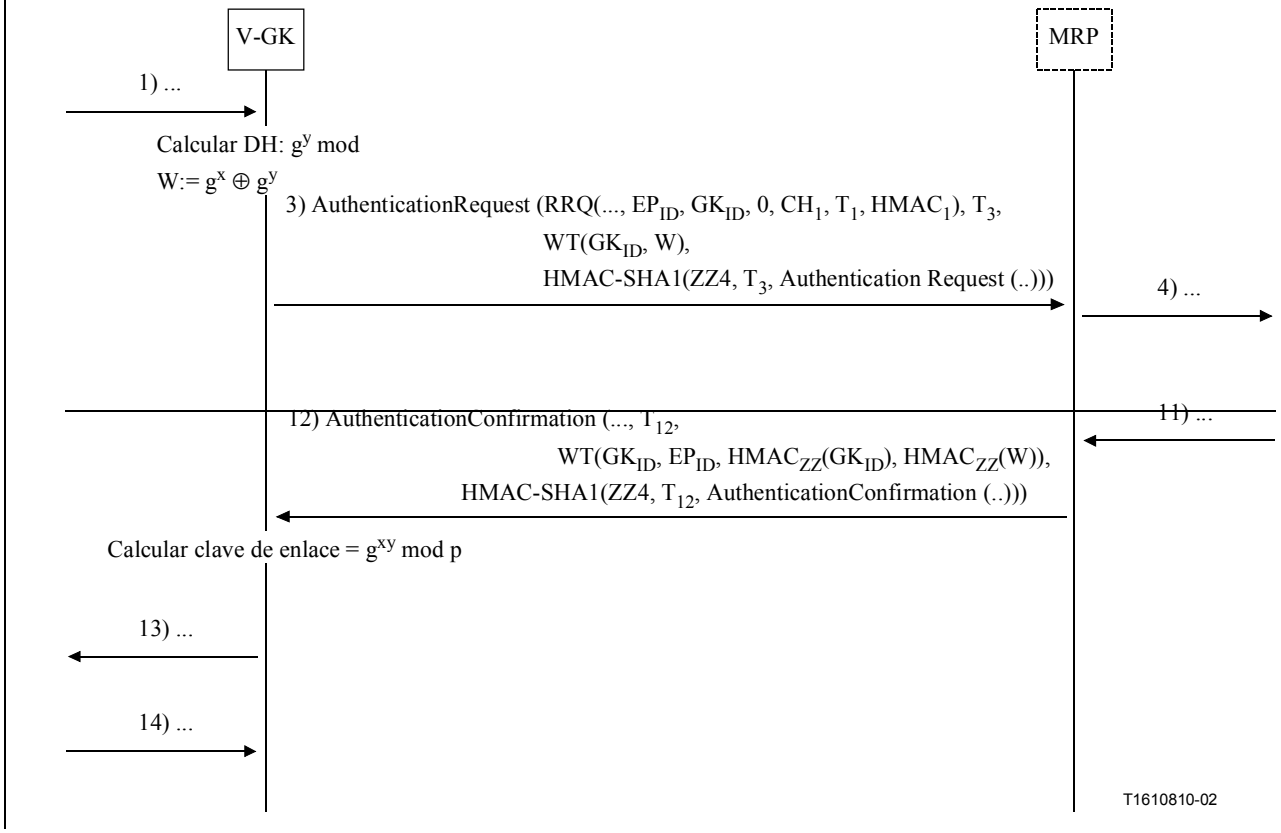
Además, el V-GK reenviará las credenciales desde la AuF al MT. Las credenciales comprenden el **ClearToken** de movilidad que se muestra como **WT()**. Este **ClearToken** de movilidad conlleva por una parte el valor compuesto autenticado *W* en el campo **halfkey** del campo **dhkey** y por otra parte el ID de V-GK autenticado; el valor *W* no deberá formar parte del **WT()** reenviado. El **tokenOID** se fijará a "G2" y no se utilizará ningún otro parámetro en ese **ClearToken** de movilidad.

El V-GK calcula el HMAC sobre la totalidad del mensaje **RCF** utilizando la clave de enlace *K*. Por tanto, el HMAC sirve de respuesta al anterior desafío de acuerdo con el procedimiento I del anexo D/H.235 [4]; véase el mensaje 13).

...

4) Cláusula 8.2.2

Reemplácese la figura 5:



Por:

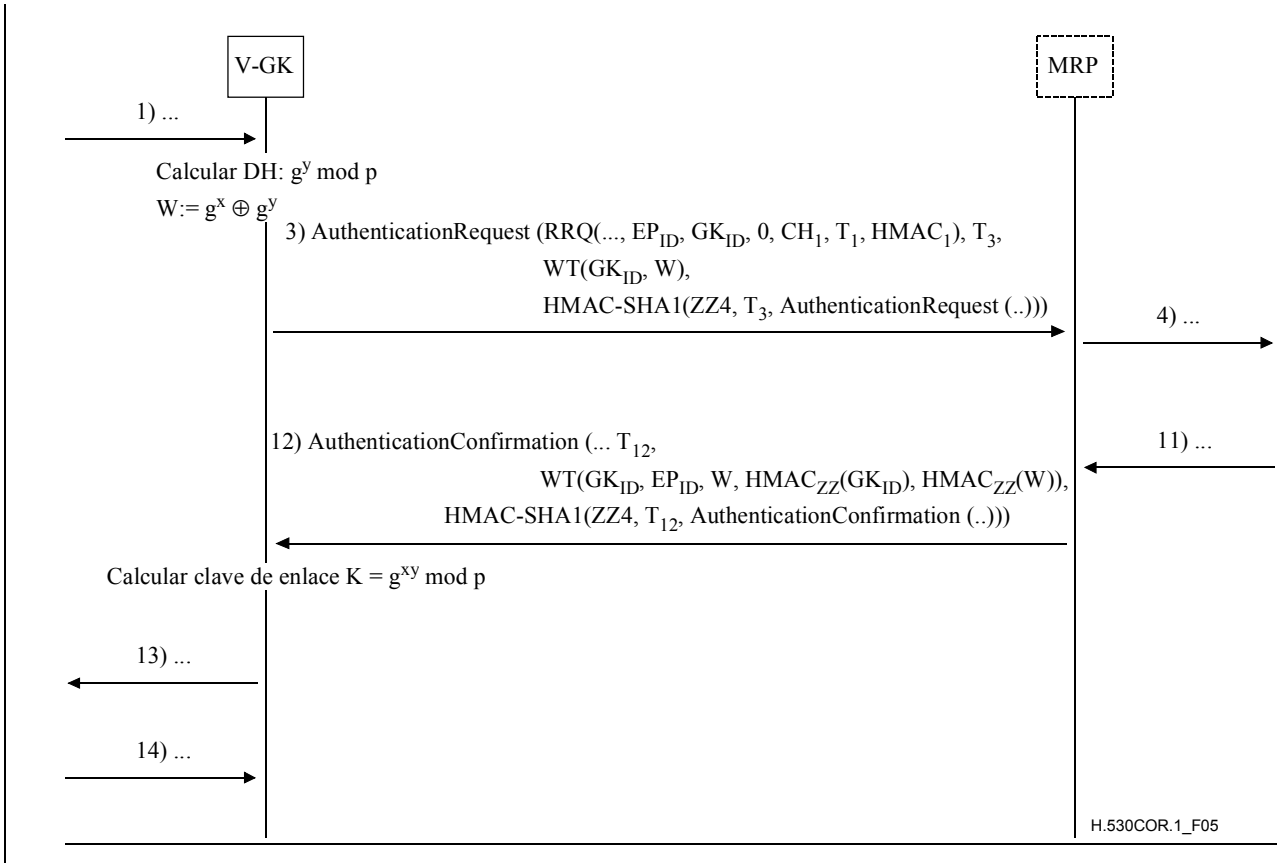
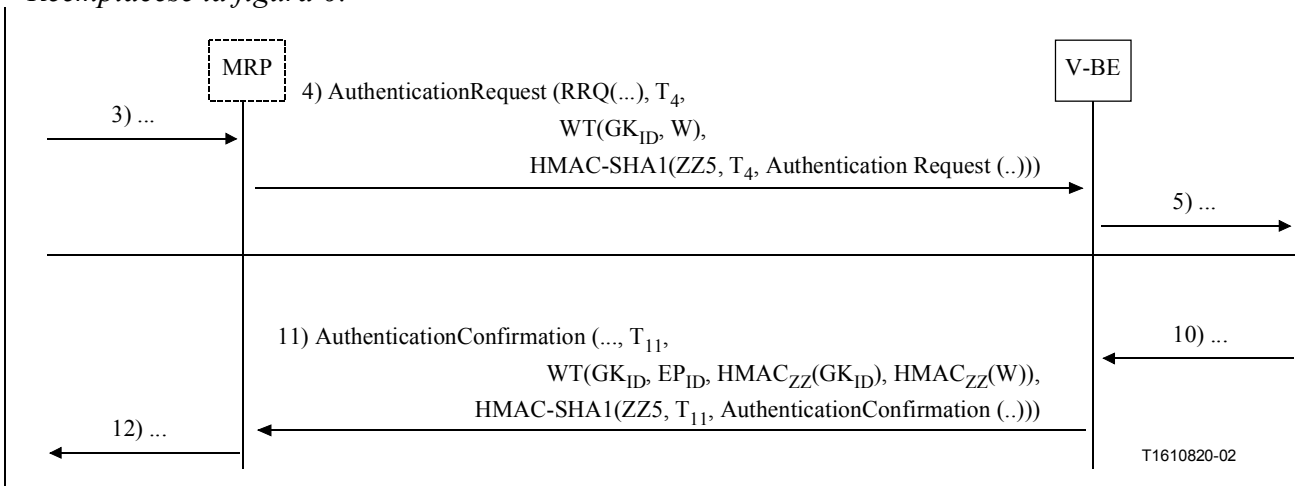


Figura 5/H.530 – Transmisión de información de autenticación entre V-GK y MRP

5) Cláusula 8.2.3

Reemplácese la figura 6:



Por:

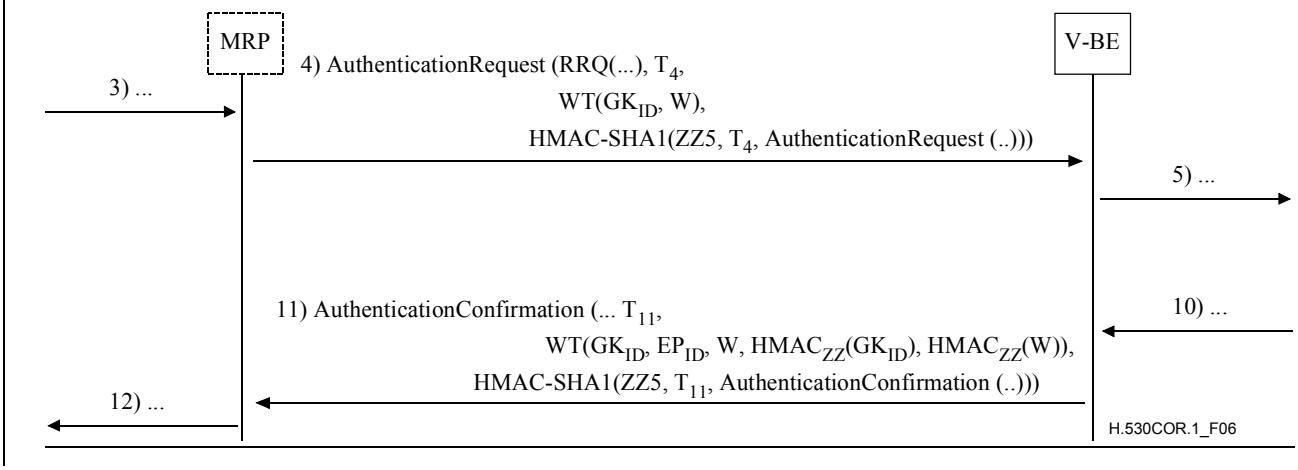
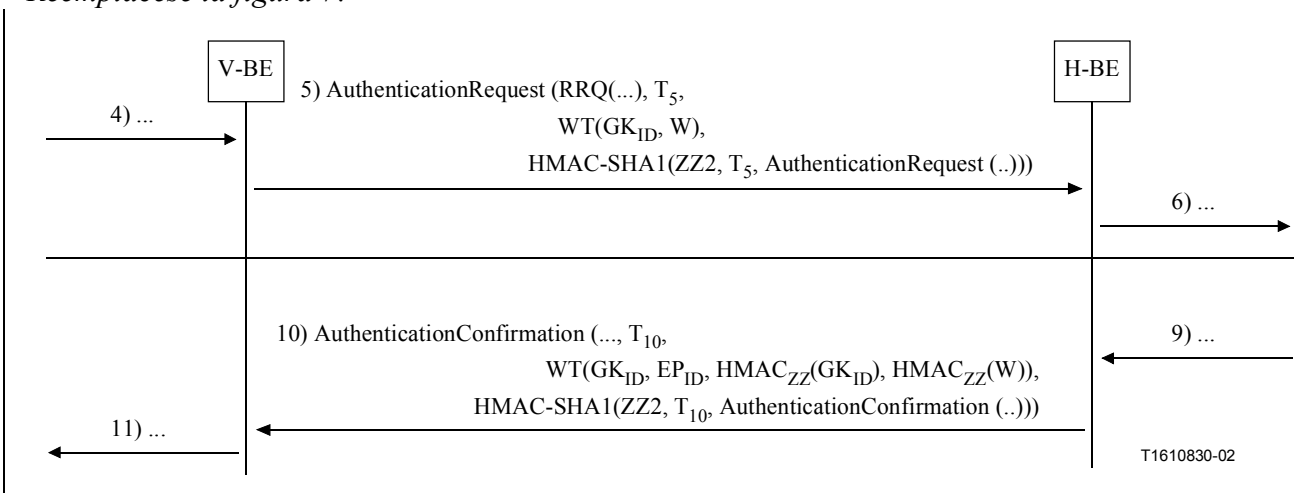


Figura 6/H.530 – Transmisión de información de autenticación entre MRP y V-BE

6) Cláusula 8.2.4

Reemplácese la figura 7:



Por:

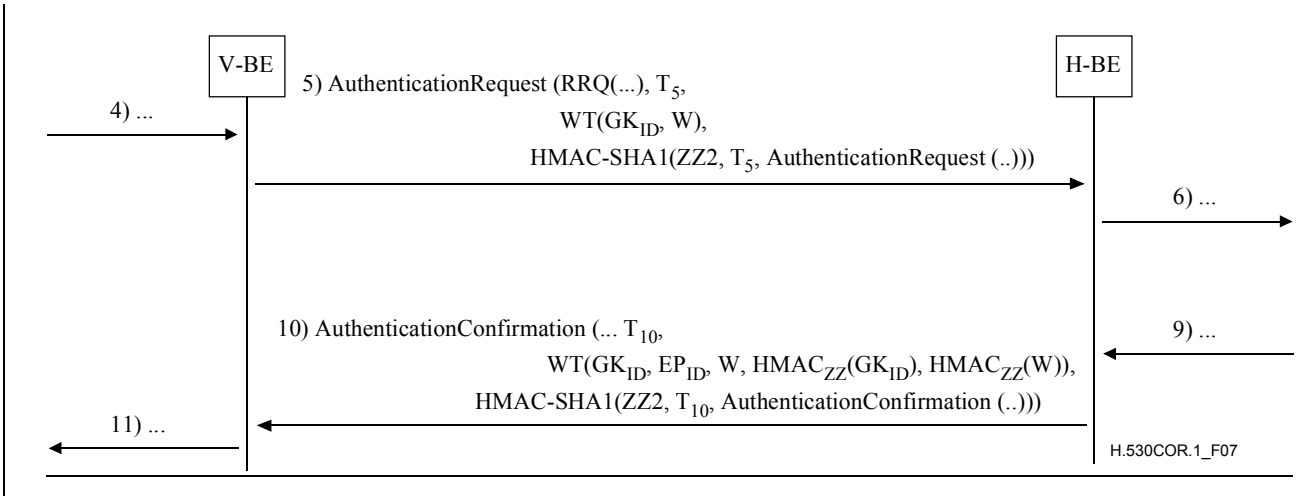
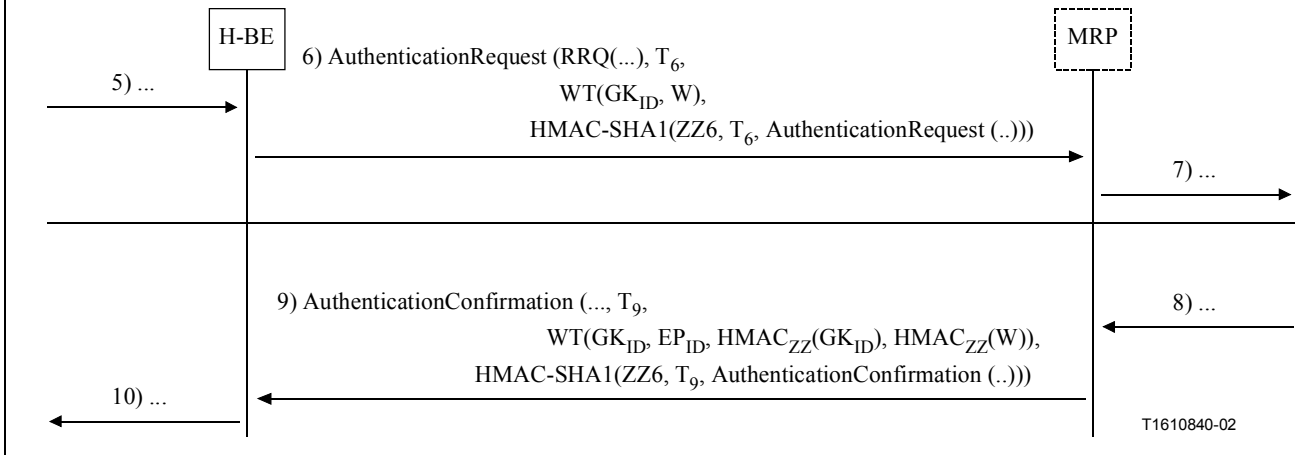


Figura 7/H.530 – Transmisión de información de autenticación entre dos BE

7) Cláusula 8.2.5

Reemplácese la figura 8:



Por:

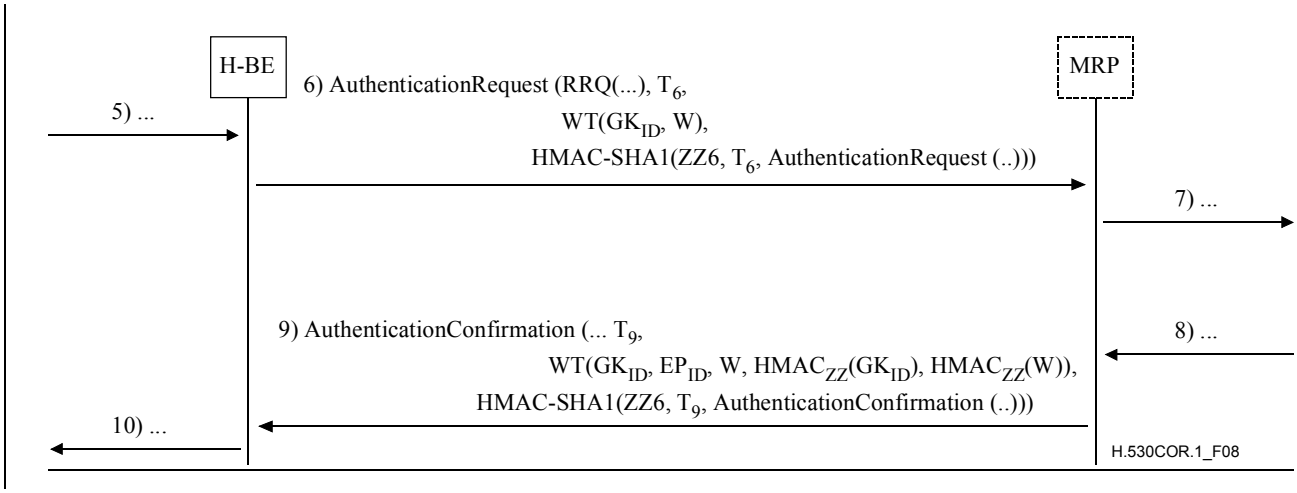
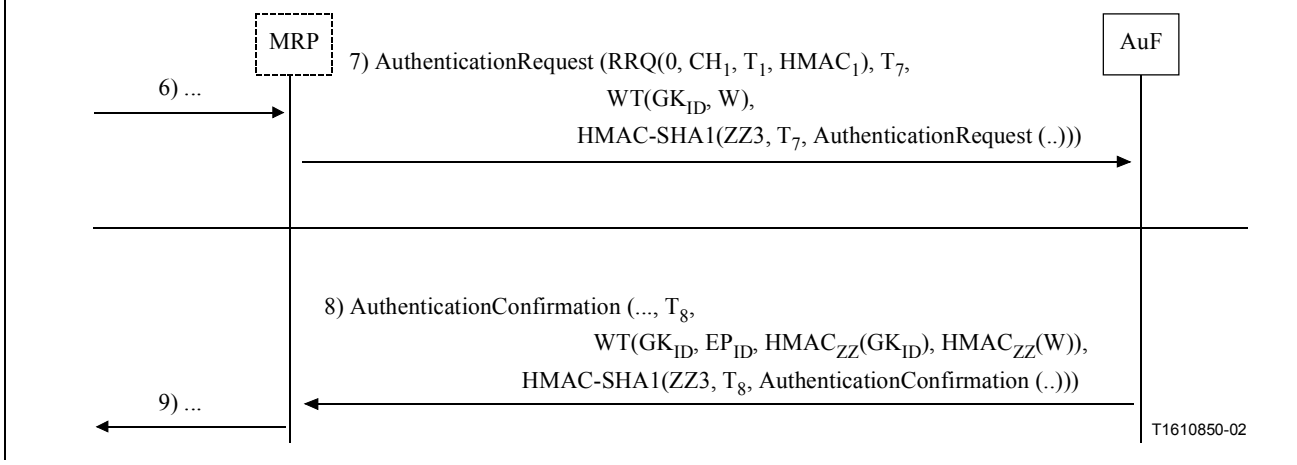


Figura 8/H.530 – Transmisión de información de autenticación entre H-BE y MRP

8) Cláusula 8.2.6

Reemplácese la figura 9:



Por:

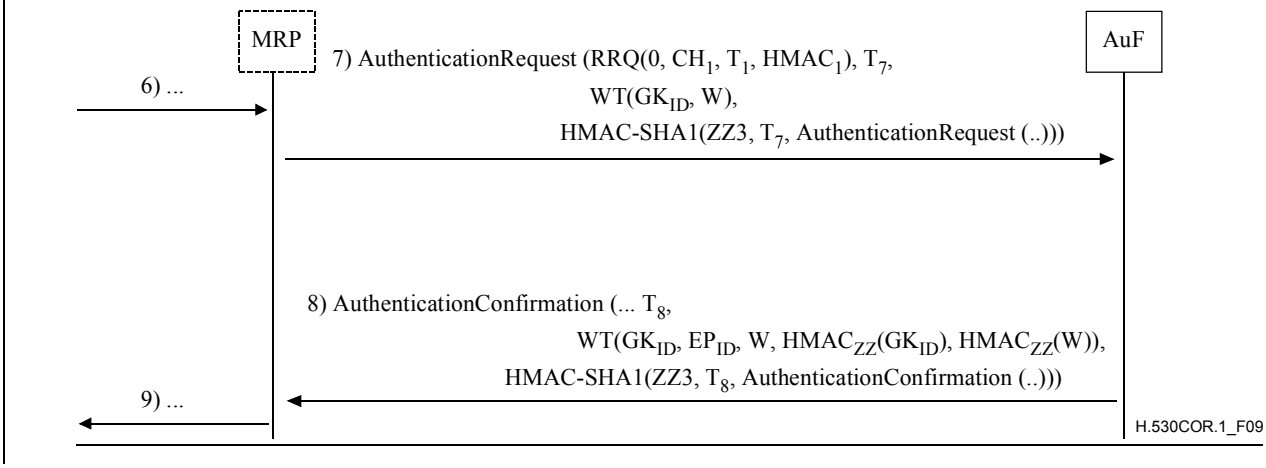


Figura 9/H.530 – Transmisión de información de autenticación entre MRP y AuF

9) Cláusula 8.2.6

Cámbiese el texto como sigue:

…

8.2.6 MRP a AuF

…

Cuando la AuF no está apta para aplicar el secreto compartido *ZZ* se omitirá el cálculo de los valores autenticados para las credenciales como se describe más adelante, y el resultado de dicho cálculo se incluirá en el mensaje **AuthenticationRejection**. En tal caso no hay **ClearToken** de movilidad en el mensaje **AuthenticationRejection**.

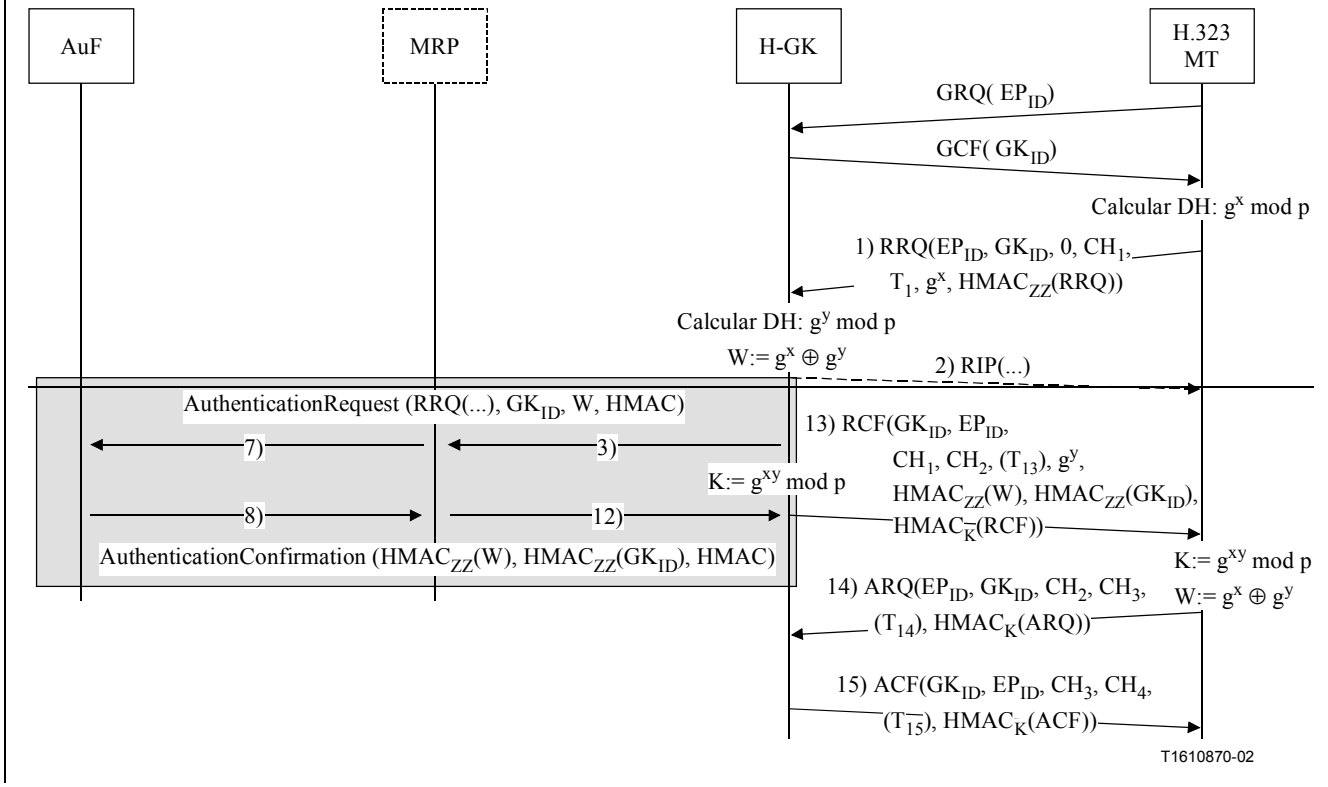
En los demás casos, la AuF calculará también las credenciales del valor compuesto autenticado *W* utilizando la función de troceado de clave HMAC-SHA1-96 y *ZZ* como la clave compartida. El valor compuesto autenticado *W* se incluirá en un **ClearToken** de movilidad separado, almacenándose el resultado en el campo **halfkey** del campo **dhkey** en ese **ClearToken** de movilidad. Además, la AuF calculará un GK_{ID} autenticado, como otra credencial, utilizando la función de troceado de clave HMAC-SHA1-96 y *ZZ* como la clave compartida. El resultado se incluirá dentro de **generator** en ese **ClearToken**. La AuF también incluirá *W* en el campo **modsize** de **dhkey**, lo que permite que el V-GK reconozca el mensaje **AuthenticationConfirmation**/**AuthenticationRejection** como nuevo. El **generalID** conllevará el GK_{ID}, mientras que el **sendersID** conllevará el EP_{ID} en ese **ClearToken**. Esto permitirá al V-GK asociar un mensaje **AuthenticationConfirmation**/**AuthenticationRejection** con el correspondiente mensaje **AuthenticationRequest**. El **tokenOID** de ese **ClearToken** se fijará a "G2" y no se utilizará ningún otro parámetro en ese **ClearToken** de movilidad. El **ClearToken** de movilidad se muestra como **WT()**.

Se utilizará una nueva indicación de tiempo T_8 y el mensaje de respuesta será securizado de acuerdo con el procedimiento I del anexo D/H.235 [4] utilizando el secreto compartido *ZZ3*; véase el mensaje 8).

…

10) Cláusula 8.5

Reemplácese la figura 11:



Por:

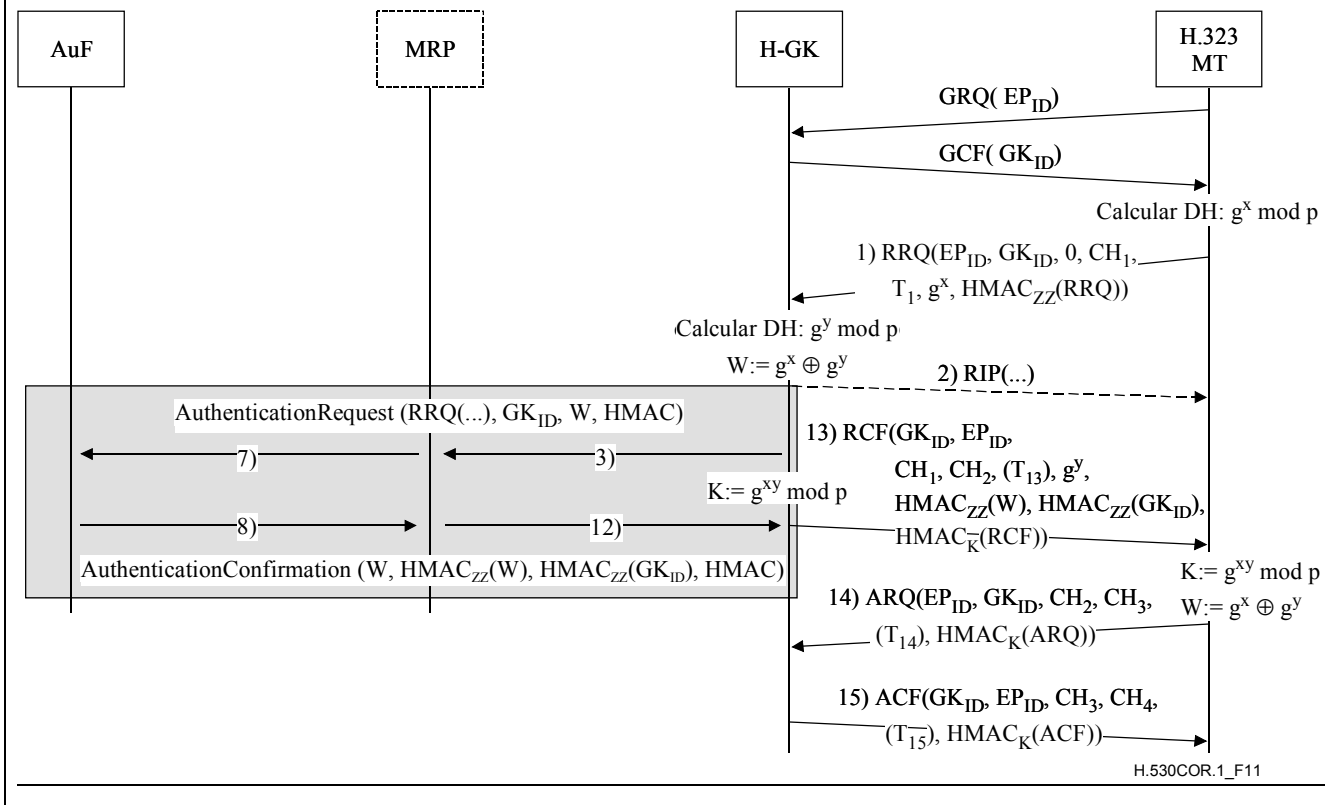


Figura 11/H.530 – Autenticación de MT en el dominio de base en la fase de registro

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie B	Medios de expresión: definiciones, símbolos, clasificación
Serie C	Estadísticas generales de telecomunicaciones
Serie D	Principios generales de tarificación
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	**Sistemas audiovisuales y multimedios**
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedios
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	RGT y mantenimiento de redes: sistemas de transmisión, circuitos telefónicos, telegrafía, facsímil y circuitos arrendados internacionales
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de transmisión telefónica, instalaciones telefónicas y redes locales
Serie Q	Conmutación y señalización
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	Redes de datos y comunicación entre sistemas abiertos
Serie Y	Infraestructura mundial de la información y aspectos del protocolo Internet
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Ginebra, 2003