UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T H.530

(03/2002)

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

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

Recomendación UIT-T H.530

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

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

Resumen

Esta Recomendación tiene por finalidad describir procedimientos de seguridad para un entorno de movilidad multimedios H.323. Proporciona detalles sobre los procedimientos de seguridad para la Rec. UIT-T H.510.

Orígenes

La Recomendación UIT-T H.530, preparada por la Comisión de Estudio 16 (2001-2004) del UIT-T, fue aprobada por el procedimiento de la Resolución 1 de la AMNT el 29 de marzo de 2002.

Palabras clave

Anexo D/H.235, autenticación, criptación, gestión de clave, integridad, movilidad, perfil de seguridad, seguridad multimedios.

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.

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

1 Alcance

Esta Recomendación tiene por finalidad hacer recomendaciones sobre procedimientos de seguridad en entornos de movilidad H.323. Proporciona detalles sobre los procedimientos de seguridad para la Rec. UIT-T H.510.

2 Introducción

Hasta el presente, las capacidades de señalización de la Rec. UIT-T H.235, versiones 1 y 2 [4] están previstas para el tratamiento de la seguridad en entornos H.323 [5], que suelen ser estáticos. Esos entornos y sistemas multimedios pueden lograr cierta movilidad limitada dentro de zonas de controladores de acceso; la Rec. UIT-T H.323 [5] en general y la Rec. UIT-T H.235 [4] en particular sólo proporcionan un soporte muy reducido para una itinerancia securizada de usuarios y terminales móviles a través de dominios diferentes en los que, por ejemplo, numerosas entidades participan en un entorno de movilidad, distribuido.

Los escenarios de movilidad H.323 descritos en la Rec. UIT-T H.510 [6] relativos a la movilidad del terminal plantean una nueva situación que refleja el carácter flexible y dinámico de esos escenarios, también desde el punto de vista de la seguridad. Los usuarios y terminales móviles H.323 en itinerancia tienen que ser autenticados por un dominio visitado, extranjero. Asimismo, interesa al usuario móvil tener la prueba de la verdadera identidad del dominio visitado. También puede ser conveniente tener la prueba de la identidad de los terminales que complementan la autenticación del usuario. Por tanto, se requiere la mutua autenticación del usuario y del dominio visitado y, facultativamente, también la autenticación de la identidad del terminal.

Como generalmente el usuario móvil sólo se conoce en el dominio de base en el que está inscrito y se la ha asignado una contraseña, el dominio visitado inicialmente no conoce al usuario móvil. En consecuencia, el dominio visitado no comparte ninguna relación de seguridad establecida con el usuario y el terminal móviles. Para que el dominio visitado pueda obtener debidamente la autenticación y las condiciones de seguridad relativas al usuario móvil y al terminal móvil, el dominio visitado transmitirá ciertas tareas de seguridad como las comprobaciones de autorización o la gestión de clave al dominio de base a través de entidades de red y de servicio intermedias. Esto exige también la securización de la comunicación y de la gestión de clave entre el dominio visitado y el dominio de base.

Si bien, en principio, los entornos H.323 de movilidad son más abiertos que las redes H.323 cerradas, también es necesario, desde luego, securizar debidamente las tareas de gestión de clave. También es cierto que la comunicación dentro y a través de los dominios de movilidad merece protección contra las manipulaciones maliciosas.

En resumen, esta Recomendación describe un concepto de seguridad genérico con miras a la movilidad entre los dominios para aplicaciones y servicios multimedios. Los detalles técnicos describen el despliegue en entornos H.323 y H.510 en particular, pero se consideran potencialmente abiertos a otros entornos.

3 Convenios de especificación

En esta Recomendación se observan los siguientes convenios:

– La obligatoriedad de una acción o aspecto se indica por un verbo en futuro simple con carácter obligatorio, o por la expresión "tener que".

– El carácter de sugerido pero no obligatorio, de una acción o aspecto, se indica por el verbo modal "deber".

– El carácter facultativo de una acción o aspecto se indica por el verbo modal "poder" en el sentido de estar permitido o autorizado, por oposición a algo que esté recomendado.

Las referencias a cláusulas, subcláusulas, anexos y apéndices aluden a elementos pertenecientes a esta Recomendación, a menos que se indique explícitamente que pertenecen a otra Recomendación. Por ejemplo "1.4" hace referencia a la cláusula 1.4 de esta Recomendación; "6.4/H.245" hace referencia a la cláusula 6.4 de la Recomendación H.245.

Esta Recomendación muestra varias entidades funcionales de movilidad, tales como elementos de frontera. Para una descripción general de esos elementos funcionales y su interacción, véase la Rec. UIT-T H.510 [6]. Puesto que la presente Recomendación sólo describe la seguridad del usuario/terminal en un entorno de movilidad, la interacción con otras entidades funcionales relacionadas con la movilidad tales como los apoderados para encaminamiento de movilidad, por ejemplo las funciones VLF, HLF, sólo se menciona brevemente; se considera que esas entidades funcionales están fuera del ámbito de esta Recomendación. Específicamente, la arquitectura de seguridad no depende de la presencia o ausencia de tales elementos funcionales y no requiere la separación de ninguna de esas funciones. Por razones de simplicidad, la presente Recomendación presupone que estas funciones están coubicadas en elementos de red compuestos, pero para facilitar la exposición esas entidades de red se representan como entidades funcionales individuales. Desde luego, los conceptos de seguridad podrían ampliarse directamente de manera que abarcaran esos elementos cuando estuvieran presentes, sea descomponiéndolos funcionalmente, sea separándolos.

Todas esas entidades de red facultativas se representan por casillas de trazo discontinuo en los diagramas. En cuanto al dominio de base, una entidad de autenticación (AuF) que funciona como un servicio de seguridad en el fondo puede estar separada o coubicada con el elemento de frontera de base o con otras entidades H.323 adecuadas [5], por ejemplo, con el controlador de acceso de base (H-GK). La determinación de cuál de estas soluciones habrá de aplicarse es una cuestión de implementación local.

A los efectos de esta Recomendación, la **función autenticación** (**AuF**) es la entidad funcional de seguridad en el dominio de base que mantiene una relación de seguridad con los usuarios móviles abonados y los terminales móviles abonados, si es necesario. Entre otras tareas que no se describen en esta Recomendación, la AuF realizará al menos las siguientes:

- La AuF evaluará los mensajes **AuthenticationRequest** entrantes procedentes de un dominio visitado, comprobará la autenticidad e integridad de esos mensajes y, sobre todo, autenticará al usuario móvil y también, facultativamente, al terminal móvil (MT, *mobile terminal*), si se proporciona y si así se desea.
- Tras una autenticación exitosa del usuario/terminal móvil, la AuF tomará la decisión de otorgar o no la autorización. La forma precisa en que la AuF toma esta decisión está fuera del ámbito de esta Recomendación, pero pudiera ser conveniente prever alguna base de datos de políticas o ciertas reglas.
- Además, la AuF soportará y ayudará al dominio visitado en la tarea de gestión de clave; concretamente, la AuF autenticará la semiclave Diffie-Hellman y el GK_{ID} recibidos del dominio visitado utilizando el correspondiente secreto compartido con el usuario.

- Por último, la AuF enviará al dominio visitado una respuesta relativa a la decisión que se haya tomado sobre la autorización de seguridad, en la que se incluirá el valor autenticado la semiclave Diffie-Hellman y el GK_{ID}.

La AuF podría imaginarse como un módulo de seguridad – que puede estar separado físicamente de otras entidades funcionales – con funcionalidad de seguridad específica como el almacenamiento protegido de claves, soporte de algoritmos y mecanismos criptográficos, acceso securizado para administración y mantenimiento, fiabilidad, etc. Sin embargo, esta Recomendación no presupone la presencia de ninguna de esas prestaciones en la AuF. Más bien, la AuF puede estar coubicada con otras entidades funcionales H.323 [5] en el dominio de base por ejemplo en el elemento de frontera, en el controlador de acceso, en un apoderado de encaminamiento de movilidad (MRP, *mobility routing proxy*) o en cualquier otra entidad adecuada. El concepto de la AuF deja abierta la cuestión de determinar cuál sería la mejor forma de implementarla: como soporte físico, como soporte lógico, o como una combinación de ambos.

Esta Recomendación introduce un **apoderado de encaminamiento (en un entorno) de movilidad** (**MRP**) como una entidad funcional facultativa. El MRP actúa como una entidad funcional intermedia, que termina la asociación de seguridad de un enlace salto por salto. El MRP reenviará los testigos de seguridad calculando nuevamente los códigos de autenticación de mensaje salto por salto en el **CryptoToken**. El MRP puede abarcar la funcionalidad de una entidad funcional de gestión de la movilidad (por ejemplo, de una HLF o de una VLF o de cualquier otra entidad de servicio de fondo en un entorno de movilidad). El MRP puede aparecer en el dominio visitado, o en el dominio de base, o en cualquier otro dominio que deba ser atravesado.

Si un MRP aquí mostrado no está presente en la comunicación real, se considerará que los enlaces salto por salto que entran y salen del MRP pertenecen a la misma asociación de seguridad y se omitirá el nuevo cálculo del **CryptoToken**.

En esta Recomendación se utiliza el termino **contraseña** para designar una cadena de caracteres introducida por el usuario, como contraseña. La contraseña en esta Recomendación habrá de entenderse como la clave de seguridad asignada, que el usuario móvil comparte con su dominio de base. Esta contraseña del usuario y el secreto compartido del usuario, derivado, se aplicarán a efectos de autenticación del usuario

En cambio, un **secreto compartido** es la clave de seguridad que forma parte de los parámetros de seguridad para los algoritmos criptográficos; puede derivarse de una contraseña (véase el procedimiento descrito en 10.3.5 de H.235 [4]) o puede ser asignado para cada configuración o por otros medios.

Asimismo, el dominio de base puede haber asignado al terminal móvil un secreto compartido distinto para fines de autenticación del terminal.

La asignación y distribución de contraseñas y secretos compartidos entre las entidades funcionales está fuera del ámbito de esta Recomendación.

La presente Recomendación utiliza el término **relación de servicio** para hacer referencia a una asociación de seguridad establecida entre dos entidades funcionales, como por ejemplo entre un elemento de frontera visitado (V-BE) y el elemento de frontera de base (H-BE). Entre otros parámetros de tal relación de servicio, es esencial que al menos esté presente una clave compartida *ZZn*, por la cual el tráfico entre ambas entidades funcionales queda securizado (por ejemplo, IPSEC o anexo D/H.235 [4]).

El mensaje **AuthenticationRejection** utilizado en esta Recomendación indica que una comprobación de seguridad efectuada por la AuF ha fracasado. El mensaje **AuthenticationRejection** mantendrá el mismo **Clear** y el mismo **CryptoToken** que el correspondiente mensaje **AuthenticationConfirmation**.

A los identificadores de objeto se alude mediante una referencia simbólica en el texto (por ejemplo, "G1"). En la cláusula 8.6 se indican los valores numéricos reales de los identificadores de objeto simbólicos.

4 Términos y definiciones

A los efectos de esta Recomendación, las definiciones de la cláusula 3 de las Recomendaciones UIT-T H.323 [5], H.225.0 [1], H.225.0 anexo G [2], H.235 [4], H.501 [3], H.510 [6] y X.800 [7] son aplicables junto con las formuladas en esta cláusula.

4.1 función de autenticación (AuF, *authentication function*): Entidad funcional de seguridad en el dominio de base que mantiene una relación de seguridad con los usuarios móviles abonados y con los terminales móviles abonados.

4.2 credencial: En esta Recomendación, por una credencial [por ejemplo, $HMAC_{ZZ}(GK_{ID})$ o $HMAC_{ZZ}(W)$] ha de entenderse un dato al cual la AuF ha aplicado criptográficamente su secreto compartido *ZZ*, que comparte con el usuario móvil. La credencial se transfiere para probar la autorización y tempestividad en la comprobación de autorización.

4.3 elemento de frontera de base (H-BE, *home border element*): Elemento de frontera (BE) situado dentro del dominio de base.

4.4 apoderado de encaminamiento (en un entorno) de movilidad (MRP): Entidad funcional facultativa que actúa como una entidad funcional intermedia, terminando la asociación de seguridad de un enlace salto por salto.

4.5 contraseña: Cadena de caracteres introducida por el usuario como contraseña.

4.6 relación de servicio: Asociación de seguridad establecida entre dos entidades funcionales en el supuesto de que está presente al menos una clave compartida.

4.7 secreto compartido: Clave de seguridad para los algoritmos cripotográficos; se puede derivar de una contraseña.

4.8 elemento de frontera visitado (V-BE, *visited border element*): Elemento de frontera (BE) situado dentro del dominio visitado.

5 Símbolos y abreviaturas

En esta Recomendación se utilizan las siguientes siglas.

AuF	Función de autenticación (*authentication function*), (véase la Rec. UIT-T H.510 [6]
BE	Elemento de frontera (*border element*), (véase la Rec. UIT-T H.225.0 anexo G [2])
CH_n	Desafío número *n* (*challenge number n*)
DH	Diffie-Hellman
EP_{ID}	Identificador de punto extremo de MT (*MT endpoint identifier*), (véase la Rec. UIT-T H.225.0 [1]
GK	Controlador de acceso (*gatekeeper*), (véase la Rec. UIT-T H.510 [6]
GK_{ID}	Identificador de controlador de acceso visitado (*visited gatekeeper identifier*), (véase la Rec. UIT-T H.225.0 [1])
GRJ	Rechazo de controlador de acceso (*gatekeeper reject*)
GRQ	Petición de controlador de acceso (*gatekeeper request*)

H-BE	BE de base (*home BE*)
H-GK	GK de base (*home GK*)
HLF	Función ubicación de base (*home location function*)
HMAC-SHA1-96	Código de autenticación de mensaje troceado con algoritmo hash securizado 1 (*hashed message authentication code with secure hash algorithm 1*)
$HMAC_Z$	Código de autenticación de mensaje troceado para clave/respuesta con secreto compartido *Z* (*key hashed message authentication code/response with shared secret Z*)*;* si no se indica *Z* se aplica el secreto del salto siguiente
IPSEC	Seguridad del protocolo Internet (*Internet protocol security*)
K	Clave de sesión/enlace dinámico (*dynamic session/link key*)
MRP	Apoderado de encaminamiento (en un entorno) de movilidad (*mobility routing proxy*)
MT	Terminal móvil (*mobile terminal*), (véase la Rec. UIT-T H.510 [6])
NTP	Protocolo de señales horarias de red (*network time protocol*)
OID	Identificador de objeto (*object identifier*)
PKI	Infraestructura de claves públicas (*public-key infrastructure*)
PW	Contraseña de usuario móvil (*mobile user password*)
R_1	Número aleatorio (*random number*)
RIP	Petición en curso (*request in progress*)
RRJ	Rechazo de registro (*registration reject*)
RRQ	Petición de registro (*registration request*)
SNTP	Protocolo de señales horarias de red simple (*simple network time protocol*)
T_n	Indicación de tiempo número *n* (*timestamp number n*)
V-BE	BE visitado (*visited BE*)
V-GK	GK visitado (*visited GK*)
VLF	Función ubicación del visitante (*visitor location function*)
W	Valor compuesto con combinación aritmética de semiclaves Diffie-Hellman
WT	ClearToken de movilidad (*mobility ClearToken*)
XT	CryptoToken para autenticación de terminal móvil
ZZ	Secreto compartido/contraseña del usuario móvil que es compartido con la correspondiente AuF
ZZMT	Secreto compartido del terminal móvil MT, que es compartido con la AuF correspondiente
ZZ_n	Secreto compartido número *n*
$\oplus$	Operador lógico "O exclusivo" bit a bit (*bitwise XOR*)

6 Referencias

6.1 Referencias normativas

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones, por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes.

[1] Recomendación UIT-T H.225.0 Versión 4 (2000), *Protocolos de señalización de llamada y paquetización de trenes de medios para sistemas de comunicación multimedios por paquetes*.

[2] Recomendación UIT-T H.225.0 anexo G (Proyecto), *Comunicación entre dominios administrativos*.

[3] Recomendación UIT-T H.501 (2002), *Protocolo para gestión de la movilidad y comunicación intradominio/interdominio en sistemas multimedios*.

[4] Recomendación UIT-T H.235 Versión 2 (2000), *Seguridad y criptado para terminales multimedios de la serie H (basados en las Recomendaciones H.323 y H.245)*.

[5] Recomendación UIT-T H.323 Versión 4 (2000), *Sistemas de comunicación multimedios basados en paquetes*.

[6] Recomendación UIT-T H.510 (2002), *Movilidad para sistemas y servicios multimedios H.323*.

[7] Recomendación UIT-T X.800 (1991), *Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT*.

6.2 Referencias no normativas

[8] IETF RFC 1305 (1992), *Network Time Protocol (Version 3) Specification, Implementation and Analysis, Internet Engineering Task Force*.

[9] IETF RFC 2030 (1996), *Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI; Internet Engineering Task Force*.

7 Requisitos y constricciones de seguridad para la movilidad

La gestión de la movilidad multimedios y la aplicación a los entornos de movilidad H.323 están enfrentadas a los siguientes requisitos y constricciones de seguridad:

- Esta Recomendación soportará y facilitará, en materia de seguridad, un mejor interfuncionamiento de los sistemas securizados H.323 cuando dichos sistemas están desplegados en un entorno de movilidad con componentes distribuidos y dominios gestionados separadamente.
- El usuario móvil será autenticado cuando se desplace a través de dominios. La autenticación del usuario móvil servirá de base para conceder acceso al usuario y permiso para el servicio. La autenticación se efectuará mediante la AuF de base cuando se conecte inicialmente a un dominio visitado extranjero. Para toda otra interacción con el dominio visitado, la autenticación del usuario móvil se efectuará a través del dominio visitado sin que sea necesario interrogar a la AuF de base cada vez.

- El terminal móvil debe ser autenticado cuando se desplace a través de dominios. La autenticación del terminal móvil puede utilizarse para detectar y rastrear los terminales móviles (MT) que puedan estar incluidos en lista negra/lista blanca. La autenticación de MT debe llevarse a cabo junto con la autenticación de usuario móvil, y no por separado en un procedimiento adicional.
- Se debe soportar un escenario en el que los MT son mantenidos en una AuF diferente (posiblemente en un dominio diferente) que aquélla a que pertenecen los usuarios móviles. En un escenario tal, el dominio visitado interrogará al dominio de base del usuario con una sola petición de autenticación y no con peticiones de autenticación individuales. La AuF de base del usuario puede entonces delegar interrogaciones para la autenticación del MT, pero esa comunicación no forma arte de esta Recomendación.
- Sobre la base de la relación de confianza entre el dominio visitado y el dominio de base, el dominio visitado autenticará ante el usuario móvil, por ejemplo que el MT está apto para autenticar al controlador de acceso visitado. De la misma forma, el dominio visitado debe autenticar ante la AuF de base.

  NOTA – Puesto que el dominio visitado y el dominio de base generalmente no comparten una relación de seguridad establecida, no se puede esperar obtener una autenticación fuerte entre esos dos dominios, en un sentido estricto. No obstante, se podría alcanzar cierto grado de confianza utilizando enlaces securizados salto por salto entre el dominio visitado y el dominio de base.
- Los protocolos de gestión de la movilidad dentro y a través de los dominios estarán securizados contra impostura, pérdida de integridad y, si es posible, contra pérdida de confidencialidad.
- Los ataques por denegación de servicio deben reducirse al mínimo en la mayor medida posible.
- El perfil de usuario y la información relativa al perfil de usuario, así como toda clave de seguridad deberán transmitirse de manera securizada a través y en el interior de dominios. Esto último exige una gestión securizada de las claves en un entorno de movilidad. Esto incluye el requisito de que una información tan delicada no pueda ponerse a disposición de ninguna entidad ni dominio intermedios, a menos que sea necesario. Esto significa que la contraseña del usuario del MT no deberá ponerse a disposición de ninguna entidad funcional excepto el MT y la AuF. Significa también que el secreto compartido con el MT no se pondrá a disposición de ninguna entidad funcional excepto el MT y la AuF. Además, esto significa que la clave de sesión dinámica negociada para securizar la comunicación entre el MT y el dominio visitado no se pondrá a disposición de otras entidades de red intermedias.
- La clave de sesión dinámica debe ser auténtica y estar vinculada criptográficamente a la autenticación realizada. Para ello es necesario que la clave de sesión haya sido renovada.
- La arquitectura de seguridad global tendrá en cuenta las relaciones de confianza entre dominios. Por una parte, esto requiere que se tengan en cuenta las relaciones de seguridad entre entidades y dominios. Por otra parte, se deberá detectar las entidades tramposas [como podría serlo una que se hiciera pasar por un controlador de acceso visitado (V-GK, *visited gatekeeper*) pero tal impostura también podría realizarla cualquier otra entidad] y reducir al mínimo las probabilidades de engaño.
- Las técnicas de seguridad que habrán de aplicarse tendrán en cuenta la Rec. UIT-T H.235 [4] existente así como otras técnicas de seguridad; sólo se introducirán mejoras si son necesarias.
- La arquitectura de seguridad desplegada debe ser simple y no requerirá que se tomen medidas adicionales relativas a la infraestructura de seguridad tales como tarjetas inteligentes y complejos protocolos de gestión.

8 Seguridad salto por salto con técnicas criptográficas simétricas

Dado que las técnicas de seguridad simétricas se despliegan de acuerdo con el anexo D/H.235 [4] en entornos H.323 casi estáticos de no movilidad, esta Recomendación muestra la arquitectura de seguridad con procedimientos de seguridad en un entorno H.323 de movilidad, que también despliega las mismas técnicas de seguridad. Esencialmente, esta Recomendación describe una arquitectura de seguridad basada en una infraestructura que utiliza solamente secretos compartidos simétricamente. Los secretos compartidos se definen salto por salto, o por pares, entre las entidades comunicantes.

Éste es un modelo de seguridad simple y no requiere, por ejemplo, el empleo de una determinada infraestructura de seguridad de clave pública. La arquitectura de seguridad salto por salto está concebida para desplegar, en gran escala, técnicas simétricas de seguridad del anexo D/H.235 [4] bien diseñadas. Se considera que el rendimiento de las técnicas criptográficas simétricas es relativamente alto, por lo que son también aplicables de manera general en el entorno de movilidad.

La figura 1 representa la arquitectura de seguridad para un entorno de movilidad H.323 de acuerdo con la Rec. UIT-T H.510 [6], que se basa en la Rec. UIT-T H.501 [3]. Muestra la principal relación arquitectural de las entidades funcionales. Muestra también la relación de seguridad de claves entre las entidades, así como el caso en que el terminal móvil (MT) está conectado al controlador de acceso de base en el dominio de base.

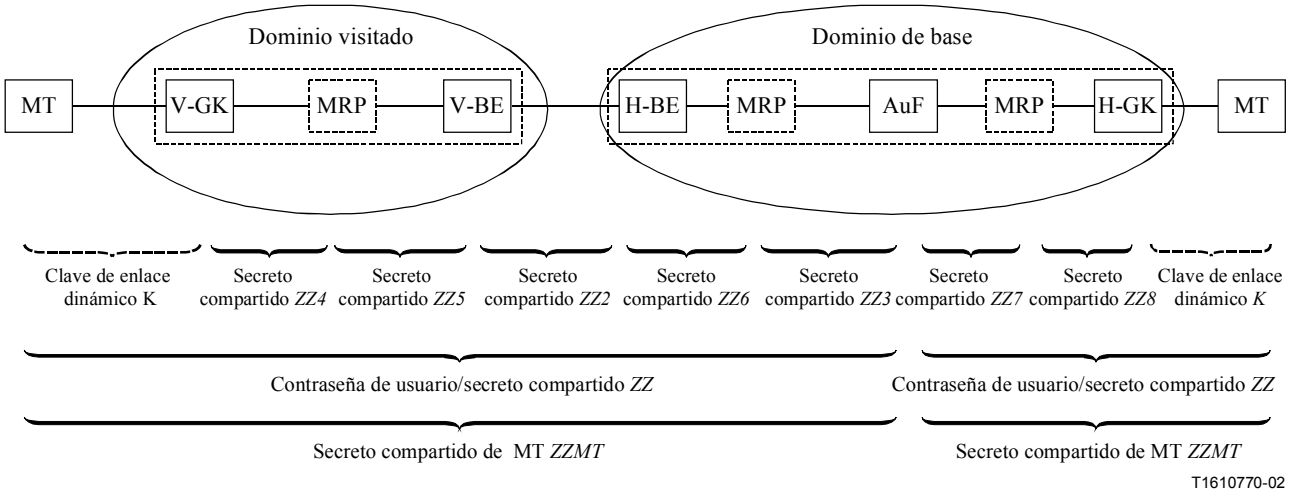

Figura 1/H.530 – Arquitectura de seguridad para un entorno de movilidad H.323

Se supone que el MT y la AuF en el dominio de base comparten una contraseña administrada *ZZ* que se asigna en el proceso de abono de usuario. Además, el V-GK y el elemento funcional siguiente a una distancia de un salto (por ejemplo un MRP) comparten un secreto compartido *ZZ4*, y el MRP comparte con V-BE un secreto compartido *ZZ5*. A modo de ejemplo, si un MRP no aparece en un entorno dado, se supondrá en consecuencia un secreto compartido entre el V-GK y el V-BE y se aplicará por consiguiente la protección de seguridad de los mensajes retransmitidos.

Se supone que el H-BE y un MRP comparten un secreto compartido *ZZ6* y que el MRP comparte un secreto compartido *ZZ3* con la AuF. Entre los dominios, se supone la existencia de un secreto compartido *ZZ2* entre V-BE y H-BE o debe haber el IPSEC u otra protección de seguridad de red adecuada como un medio de seguridad genérico. Los secretos compartidos *ZZ2*-*ZZ6* pueden aplicarse para la protección de seguridad del protocolo de gestión de la movilidad H.501 [3] o pueden servir como un secreto compartido para el IPSEC subyacente. Si bien la contraseña del usuario y los secretos compartidos *ZZ2*-*ZZ6* y *ZZMT* se administran estáticamente, la clave de

enlace *K* se asigna dinámicamente como parte del procedimiento de señalización y autenticación. La clave de enlace dinámico *K* se comparte entre el MT y el V-GK.

Como se describe en 8.5, la AuF y el MRP comparten un secreto compartido *ZZ7* y el MRP y el H-GK comparten un secreto compartido *ZZ8*.

NOTA 1 – Esta arquitectura de seguridad depende de nodos intermedios fiduciarios. Esto significa que cualquier nodo intermedio como un V-BE, un H-BE y posiblemente también un MRP, una AuF y un GK, pueden leer e interceptar información de señalización en tránsito no destinada verdaderamente a ellos. Esto no debe ser una dificultad real mientras se ejerza una plena función fiduciaria dentro de un dominio, así como también una estrecha y mutua relación de confianza entre el dominio visitado y el dominio de base sin que intervengan otros dominios intermedios en la comunicación H.323 [5] entre esos dos dominios.

NOTA 2 – Generalmente, la utilización de secretos compartidos limita la escalabilidad; por tanto, sólo un pequeño número de dominios y nodos BE pueden utilizar este principio en entornos controlados. Por ejemplo, se prevé que la arquitectura de seguridad descrita en esta Recomendación pueda agrandarse hasta alcanzar un número de aproximadamente 500 dominios de red, lo que ha resultado factible en las redes del sistema mundial de comunicaciones móviles (GSM). Se supone que la arquitectura de seguridad aquí descrita no se agrandará a un número de dominios de red apreciablemente mayor que 500. Por tanto, el soporte de un entorno de movilidad securizado en gran escala queda en estudio.

8.1 Supuestos

El protocolo de seguridad desplegado en esta Recomendación, cuando se utiliza junto con la Rec. UIT-T H.501 [3], presupone relojes sincronizados en cada tramo cuando se utilizan técnicas del anexo D/H.235 [4] en la capa de aplicación (es decir, V-GK a MRP, MRP a V-BE, V-BE a H-BE, H-BE a MRP y MRP a AuF). Cuando se aplican técnicas de seguridad de red o de transporte en esos enlaces, no se requieren relojes sincronizado entre las entidades indicadas. La arquitectura de seguridad presupone asimismo relojes sincronizados entre el MT y la AuF en el dominio de base. Esto podría lograrse mediante los protocolos de sincronización de tiempo y de relojes NTP (IETF RFC 1305, [8]) o SNTP (IETF RFC 2030, [9]), por ejemplo.

NOTA – No se supone sincronización de relojes entre el MT y ninguno de los GK visitados. Para una autenticación mutua del MT y el GK visitado se despliegan técnicas de seguridad basadas en desafío-respuesta. No se requiere sincronización de relojes para protección de seguridad IPSEC de la Rec. UIT-T H.501 [3].

El protocolo RAS H.225.0 [1] se aplicará para comunicación de señalización entre MT y V-GK, en tanto que el protocolo de gestión de la movilidad H.501 [3] se aplicará entre cualesquiera de las demás entidades funcionales mostradas. La Rec. UIT-T H.501 [3] utilizará facilidades de señalización H.235 [4] para la protección de seguridad de mensajes y la gestión securizada de la movilidad y, además, podrá utilizar IPSEC para una seguridad potenciada.

8.2 Procedimientos de actualización de ubicación securizada

Si bien el MT y el GK visitado generalmente no habían tenido contacto antes y por tanto no pueden desplegar información común relativa al abono, el GK cuando recibe un mensaje inicial del MT no puede, en un primer momento, autenticar al MT, y viceversa. Por esta razón, el V-GK transfiere la tarea de la autenticación y autorización del usuario MT a la AuF en el dominio en que el usuario MT está abonado. La AuF realizará la autenticación del usuario/MT y tomará una decisión sobre la autorización. La AuF responde con el resultado de la verificación de seguridad y suministra información de seguridad por ejemplo credenciales ante el GK visitado y ante el MT, para la sesión.

Como la indagación con miras a la autenticación y autorización en la AuF generalmente sólo se produce cuando el MT y el usuario se conectan inicialmente al dominio visitado, no hay una necesidad inmediata de ejecutar este procedimiento ulteriormente en el curso de la misma llamada/sesión, a menos que esto se considere adecuado por la política de seguridad del V-GK. Por tanto, el V-GK puede funcionar autónomamente con respecto a la AuF una vez que haya recibido

las credenciales de autorización. Esto hace que el V-GK se comporte como un servidor de seguridad que opera a nivel local.

Esta Recomendación soporta dos procedimientos para una actualización de ubicación securizada.

Ambos procedimientos se ejecutan en el curso de la autenticación inicial: Tanto en uno como en el otro procedimiento la autenticación es la misma cuando se utilizan los mensajes **AuthenticationRequest** y **AuthenticationConfirmation** más allá del GK visitado. La única diferencia es que se aplica el mensaje **GRQ** o el **RRQ**.

- Autenticación en la fase de descubrimiento del V-GK: Este procedimiento es aplicable cuando el MT ya tiene un ID de punto extremo y conoce de antemano el identificador de controlador de acceso visitado. En este caso es posible securizar el mensaje **GRQ** de acuerdo con el anexo D; véase la figura 2.
- Autenticación en la fase de registro del MT y del usuario: Este procedimiento se aplica cuando el MT no conoce el identificador del controlador de acceso visitado y todavía no tiene asignado un identificador de punto extremo. Por tanto, el MT y GK primero ejecutan el procedimiento (no securizado) de descubrimiento, en el curso del cual intercambian sus identificadores. Después de esto, el MT y el usuario se autentican cuando envían el **RRQ** inicial; véase la figura 3.

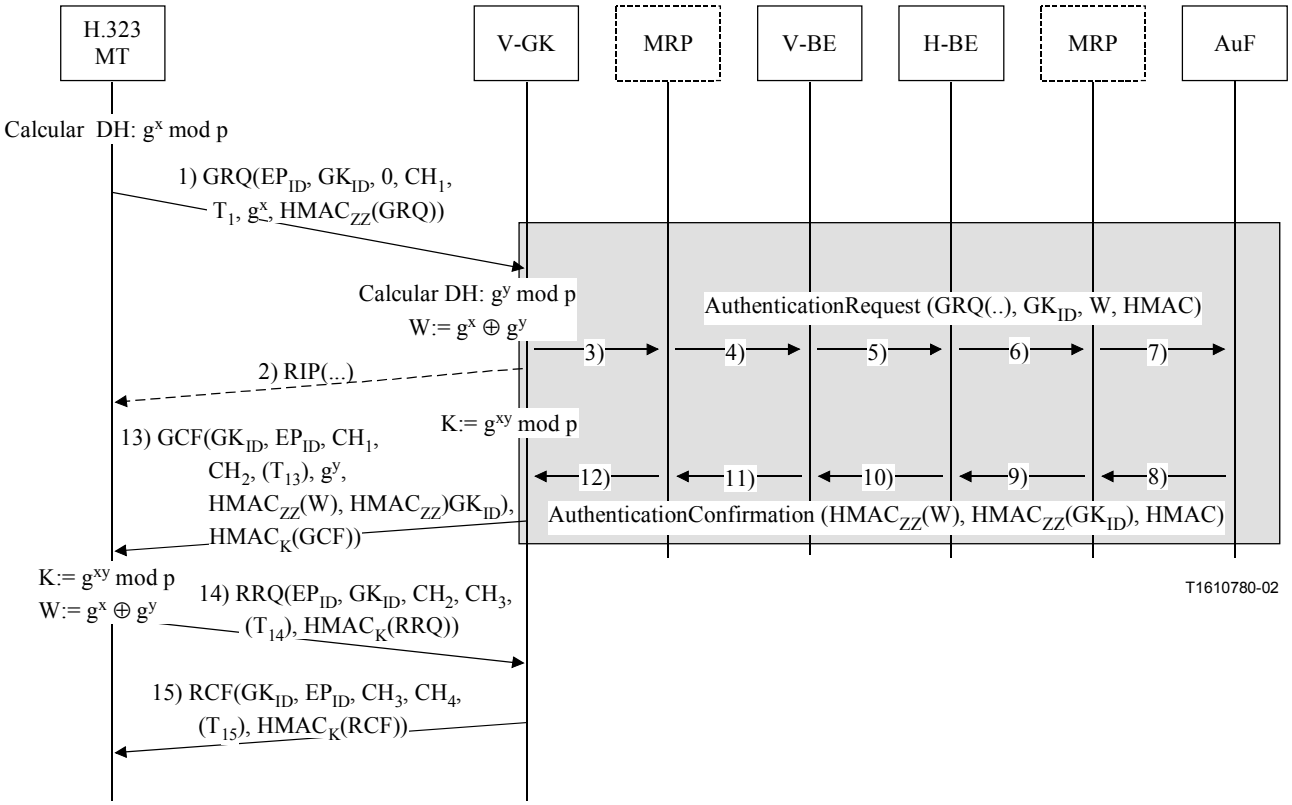

Figura 2/H.530 – Autenticación y gestión de clave en la fase de descubrimiento de GK

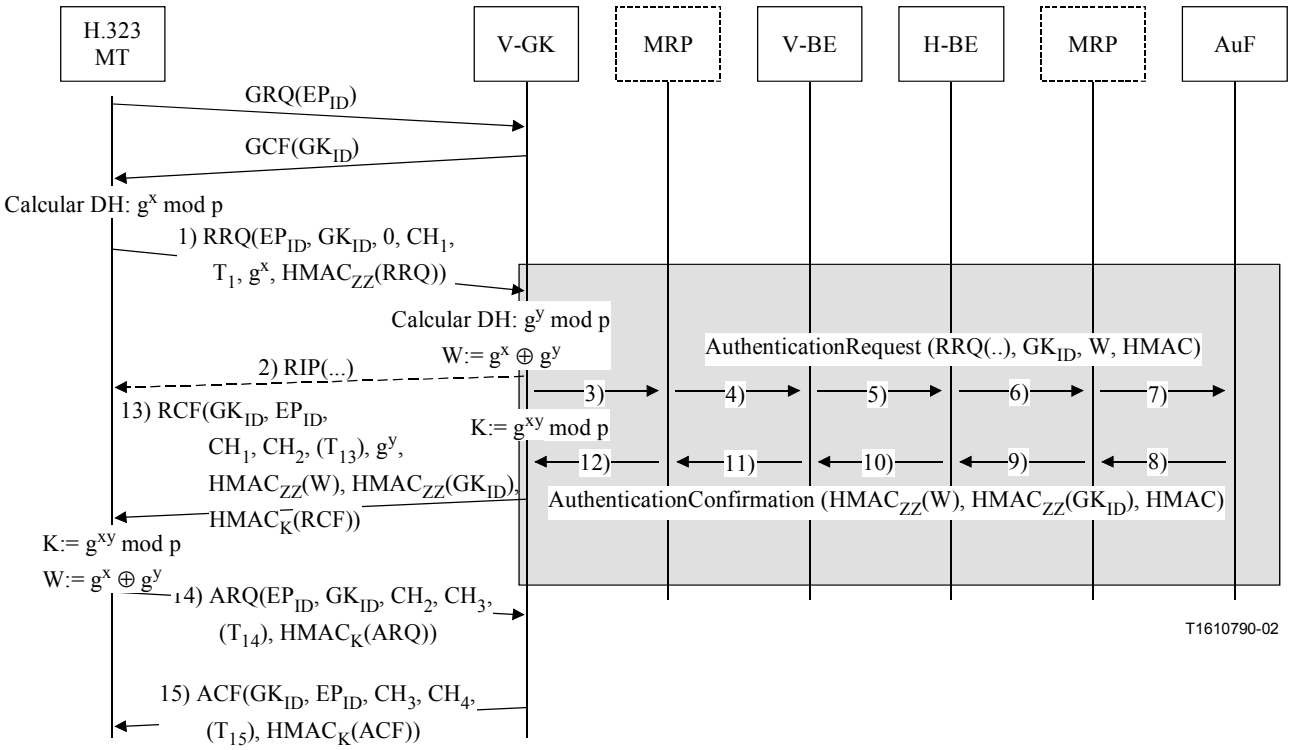

Figura 3/H.530 – Autenticación y gestión de clave en la fase de registro

La actualización de ubicación securizada se produce en uno de estos dos casos:

- cuando un usuario y un MT contactan por primera vez un dominio visitado sin que se disponga de ninguna información previa en el dominio visitado;
- cuando en el dominio visitado ya se dispone de alguna información temporal sobre el MT y el usuario.

En el primer caso se requiere la ejecución completa de los procedimientos de autenticación, en el curso de los cuales el dominio visitado reúne suficiente información de dominio de base para servir al MT. Este procedimiento incluye informes, suministrados por el dominio de base, sobre los resultados de la autenticación, comprobación para la autorización, y credenciales. Este procedimiento puede también conllevar información de perfil de servicio destinada al controlador de acceso visitado. Debe señalarse que tal procedimiento generalmente implica comunicación de red y posiblemente interacción con varias entidades, por lo que su ejecución completa pudiera tomar cierto tiempo.

En el segundo caso, el V-GK no tendría necesidad de contactar al dominio de base, aunque ello no está excluido. El controlador de acceso visitado utilizaría información almacenada localmente sin contactar al dominio de base. Esto podría suceder en el caso de una conexión perdida o restablecida, o cuando ha habido un cambio local del punto de conexión de red. Cuando el MT posee una clave de enlace válida, el MT comenzará por tratar de utilizarla antes de recurrir a efectuar una actualización de ubicación inicial.

Como primer paso, el usuario se autentica explícitamente aplicando la contraseña que obtuvo con ocasión del abono. Sin embargo, en el caso de la autenticación de un terminal móvil, es posible que el MT, facultativamente, se autentique adicionalmente ante la AuF (véase el procedimiento descrito en 8.3).

Esencialmente, el procedimiento de actualización de ubicación securizada se desarrolla de la manera siguiente: El mensaje RAS inicial recibido por el GK visitado se encapsula en un mensaje **AuthenticationRequest** y se transfiere a través de una o varias entidades funcionales a la AuF en el

dominio de base. Esto se hace porque el GK visitado no tiene capacidad para autenticar al MT y al usuario. La AuF verifica la información transferida, autentica al MT/usuario, después de lo cual toma una decisión sobre la autorización del MT/usuario basándose en algún criterio. Como otra posibilidad, la AuF puede recordar al MT/usuario y suministrar el resultado de la autenticación y la comprobación de la autorización mediante credenciales ante el V-GK y el MT utilizando el mensaje **AuthenticationConfirmation**/**AuthenticationRejection**.

El dominio visitado se autentica ante el MT/usuario dando la clave de enlace dinámico en respuesta al desafío del MT. El MT/usuario se autentica con cualquier mensaje RAS subsiguiente hacia el V-GK mediante el empleo de técnicas de desafío y respuesta. De la misma manera, el MT se puede autenticar ante el V-GK.

Debido al principio de seguridad salto por salto, todo nodo intermediario o apoderado tiene que verificar la seguridad H.235 [4] aplicada en cada tramo y recalcular el **CryptoToken** (**testigo criptográfico**) con el digesto de mensaje, de nuevo, mientras no se disponga de un medio de seguridad de red o de transporte. Si se dispone de un medio de seguridad de red o de transporte se pueden omitir las repeticiones del cálculo del digesto de mensaje en el **CryptoToken**.

Puesto que la ejecución de los procedimientos de autenticación de la comunicación de red entre V-GK y AuF puede tomar cierto tiempo, es posible que el V-GK tenga que enviar un mensaje **RIP** al MT para indicarle que el registro está en curso.

Los diagramas de las figuras 4 a 10 representan el flujo de mensajes y destacan la seguridad H.235 [4]. El flujo de mensajes representa el escenario en el que la autenticación se produce en la fase de registro. Una descripción similar es aplicable a los procedimientos cuando la actualización de la ubicación securizada se produce en la fase de descubrimiento de V-GK; en este caso, el **RRQ** encapsulado se sustituye por un **GRQ**. Los elementos de señalización para la autenticación de MT facultativa se definen en 8.3 y por razones de seguridad no se muestran en la mayor parte de las figuras. Por razones de espacio y claridad, el flujo de mensajes se ha dividido en varias fases, cada una de las cuales se representa en una figura distinta, pero su conjunto debe entenderse como un todo. Cuando los mensajes numerados se leen en secuencia se obtiene como resultado un flujo lógico de mensajes de extremo a extremo.

8.2.1 MT a V-GK

La figura 4 muestra la fase de registro inicial entre el MT y el GK visitado. Cada mensaje RAS conlleva un nuevo desafío y el valor del desafío anterior. Con excepción del primer mensaje, el valor de comprobación de integridad de mensaje HMAC sirve como respuesta calculada al anterior desafío; dicho HMAC se calculará de acuerdo con el anexo D/H.235 [4] utilizando la clave de enlace dinámico *K* como secreto compartido. El cálculo del HMAC se ajustará al procedimiento I en D.6.3.2/H.235 [4], sin utilizar el campo **timeStamp**. Si, de todas formas, el MT o el GK visitado incluyen indicaciones de tiempo (tales como T_{13}, T_{14} y T_{15}), estas indicaciones de tiempo no deben comprobarse porque no se puede suponer sincronización de relojes entre MT y V-GK.

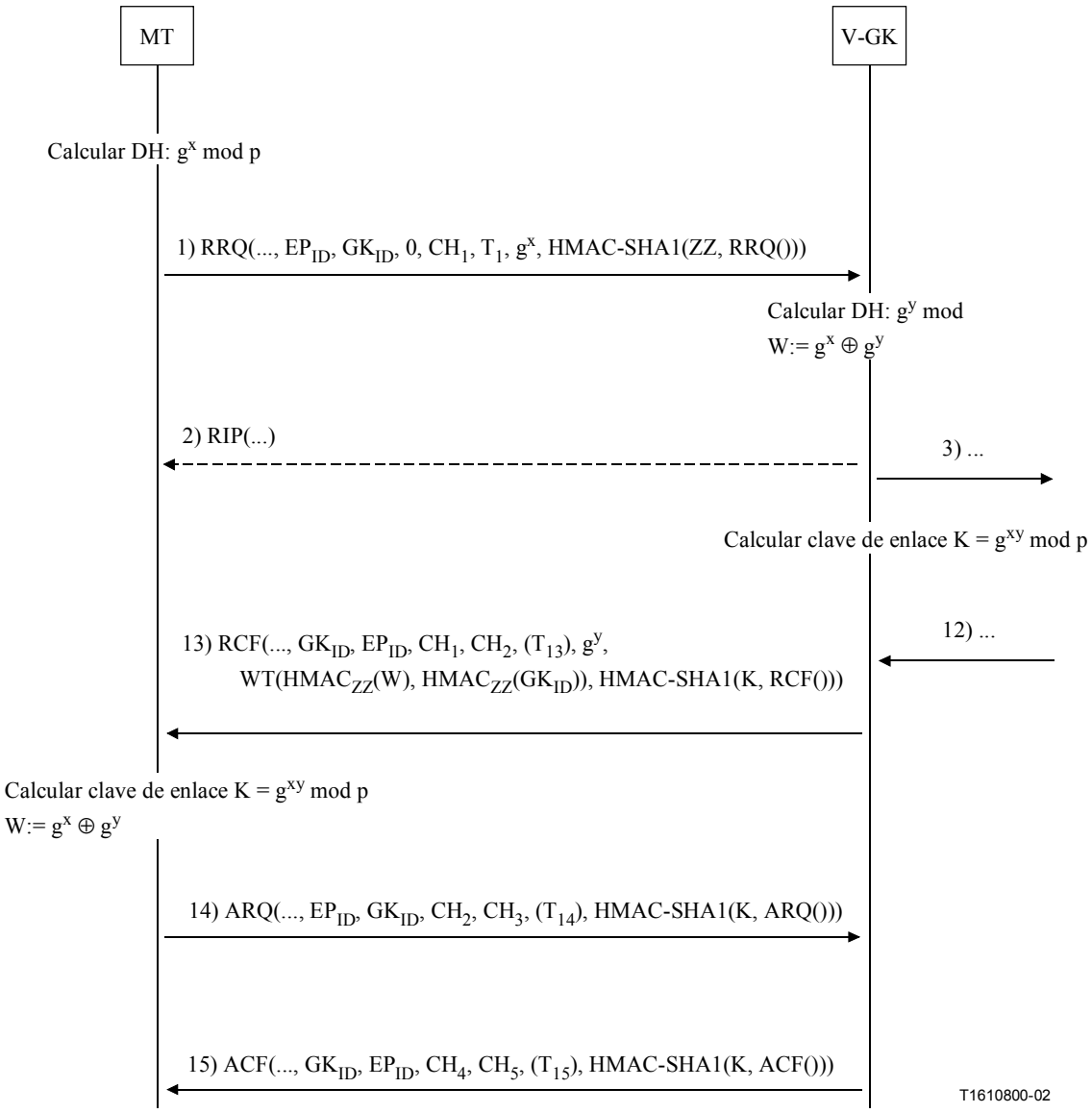

Figura 4/H.530 – Fase de registro inicial y ulteriores mensajes RAS entre MT y V-GK

En caso de registro inicial, el MT generará un nuevo desafío CH_1 y lo incluirá en el campo **challenge** en el **ClearToken** del **RRQ**; véase el mensaje 1). El campo **password** en el **ClearToken** conllevará el valor del anterior desafío. Para el **RRQ**/**GRQ** inicial, el anterior desafío no se fijará a todos ceros.

Además, el MT generará una nueva semiclave Diffie-Hellman $g^x \ mod \ p$ con *x* aleatoria mantenida secreta e incluirá la semiclave en el campo **halfkey** o en el campo **dhkey** con el **ClearToken** del mensaje. El número primo aplicado se incluirá en **modsize** mientras que el generador Diffie-Hellman se incluirá en **generator** de ese **ClearToken**. Para los parámetros de sistema Diffie-Hellman (DH) se tomarán los parámetros tal como figuran en el cuadro D.4/H.235 [4], donde Generator es *2* y se recomiendan números primos mod-P de *1024* bits designados por "Z".

El V-GK recibe el **RRQ** desafiado y lo encapsula en un **applicationMessage** dentro de un **AuthenticationRequest**, véase el mensaje 3) y lo envía al salto siguiente (por ejemplo, MRP).

El V-GK generará una nueva semiclave Diffie-Hellman $g^y \ mod \ p$ con *y* aleatoria mantenida secreta. Para los parámetros sistema Diffie-Hellman se tomarán los parámetros disponibles que figuran en el cuadro D.4/H.235 [4], donde Generator es *2* y se recomiendan los números primos mod-P de *1024* bits mod-P designados por "Z".

Tomando la semiclave Diffie-Hellman $g^x \ mod \ p \ recibida$ y su propia semiclave Diffie-Hellman $g^y \ mod \ p$, el V-GK calculará un valor compuesto *W* aplicando el operador lógico O exclusivo (XOR) bit por bit a ambos valores.

Este valor compuesto *W* se incluirá en el campo **halfkey** del campo **dhkey** dentro de un **ClearToken** de movilidad separado, del mensaje **AuthenticationRequest**. El **generalID** de ese **ClearToken** conllevará el GK_{ID}. El **tokenOID** de ese **ClearToken** de movilidad se fijará a "G2". No se utilizará ningún otro parámetro en ese **ClearToken** de movilidad. La AuF autenticará esta información de **ClearToken** y calculará las credenciales correspondientes. El **ClearToken** de movilidad se muestra como **WT**().

El mensaje **AuthenticationRequest** conllevará integridad de protección de acuerdo con el anexo D/H.235 [4], a menos que el enlace entre el V-GK y el siguiente salto (por ejemplo, MRP) esté securizado por IPSEC.

NOTA 1 – Como el **ClearToken** de movilidad es parte integrante del mensaje **AuthenticationRequest**, la protección de integridad de mensaje completa ya abarca la integridad de cualquier **Clear** y/o **CryptoToken**. Por tanto, no se necesita ninguna protección del **ClearToken** de movilidad por separado.

El V-GK puede depositar un mensaje **RIP** no securizado en el MT para indicar procesamiento de mensaje en curso; véase el mensaje 2). Debido al hecho de que el MT y el GK visitado todavía no comparten un secreto común, el V-GK no tiene capacidad para autenticar este mensaje **RIP** inmediato y proteger su integridad.

NOTA 2 – El MT no debe confiar en mensajes **RIP** no protegidos, pues pudieran no ser auténticos, o haber sido reproducidos fraudulentamente, o provenir de un ataque por denegación de servicio. El MT debe estar preparado para tratar mensajes **RIP** reproducidos fraudulentamente y hacer frente a potenciales inundaciones de mensajes. El tratamiento de tales mensajes **RIP** no protegidos incumbe a la política de seguridad del MT.

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 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 **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).

Además de la comprobación de autorización realizada por la AuF, el GK visitado puede decidir, basándose en su propio criterio, si autoriza o desautoriza al MT. Por tanto, el GK visitado puede rechazar un **GRQ**/**RRQ** incluso si la AuF confirmó la autenticación y autorización. En tal caso, el GK visitado responderá con un **GRJ**/**RRJ** que indica el **motivo** (**reason**) de acuerdo con B.2.2/H.235 [4].

El MT recibe el **RCF** protegido junto con desafíos, semiclave Diffie-Hellman y credenciales, tales como el valor compuesto autenticado *W* y GK_{ID} autenticado; véase el mensaje 13). El MT extrae estos parámetros del **ClearToken** de movilidad. El MT calculará la clave de enlace dinámico *K* de manera análoga a aquélla en que lo hizo el V-GK y como se ha descrito antes. El MT verificará el HMAC como respuesta a la totalidad del mensaje **RCF** utilizando la clave de enlace *K*. El MT calculará el valor compuesto *W* aplicando el operador lógico O exclusivo (XOR) bit por bit al $g^y \bmod p$ recibido y a su propio $g^x \bmod p$. El MT verificará la calidad de correcto del valor compuesto autenticado *W* en el campo **halfkey** del **ClearToken** de movilidad aplicando el secreto compartido *ZZ*. El MT verificará la calidad de correcto del GK_{ID} autenticado en el campo **generator** del **ClearToken** de movilidad aplicando el secreto compartido *ZZ*. Si la autenticidad de cualquiera de estos dos valores no puede probarse, tampoco se puede suponer que la clave de enlace *K* o el V-GK sean auténticos. Esto puede indicar la existencia de entidades de red fraudulentas o el fracaso de la autenticación en general. En este caso, El MT no tendrá en cuenta el RCF y rearrancará con un nuevo **RRQ**.

Cuando el V-GK recibe un mensaje **AuthenticationRejection** con **reason** indicada, enviará un **RRJ** al MT; véase el mensaje 13). El **reason** de seguridad indica un error de seguridad, pues la AuF probablemente no estaba apta para identificar el MT/usuario. El V-GK reenviará entonces este error en **RRJ reason**.

Puesto que MT V-GK no comparten relojes sincronizados, no se tendrán en cuenta las indicaciones de tiempo facultativas transportadas con un mensaje RAS.

NOTA 3 – Dado que el V-GK no puede autenticar un mensaje **GRQ**/**RRQ** inicial no protegido, dichos mensajes pudieran haber sido reproducidos fraudulentamente o provenir de ataques por denegación de servicio. Los contoladores de acceso visitados que reciban un número inesperadamente grande de mensajes RAS protegidos o no protegidos pueden suponer que se trata de un ataque por denegación de servicio y rechazar inmediatamente el procesamiento de ulteriores mensajes.

8.2.2 V-GK a MRP

La comunicación entre el V-GK y el siguiente elemento funcional de salto (por ejemplo, MRP) tiene los siguientes fines:

- Transfiere la autenticación y autorización del MT y usuario hacia la AuF.
- Transfiere la confirmación de autorización de la AuF hacia el MT.

La figura 5 muestra el flujo de mensajes del protocolo. El **AuthenticationRequest**, mensaje 2) transporta completamente el mensaje RAS RRQ/GRQ tal como se recibió del MT. Además, el mensaje **AuthenticationRequest** transporta un **ClearToken** de movilidad que conlleva el valor compuesto *W* y el GK_{ID}. El **ClearToken** de movilidad se muestra como **WT()**. Si se efectúa la autenticación del MT, el V-GK incluye un **CryptoToken** separado para este fin; véase 8.3.

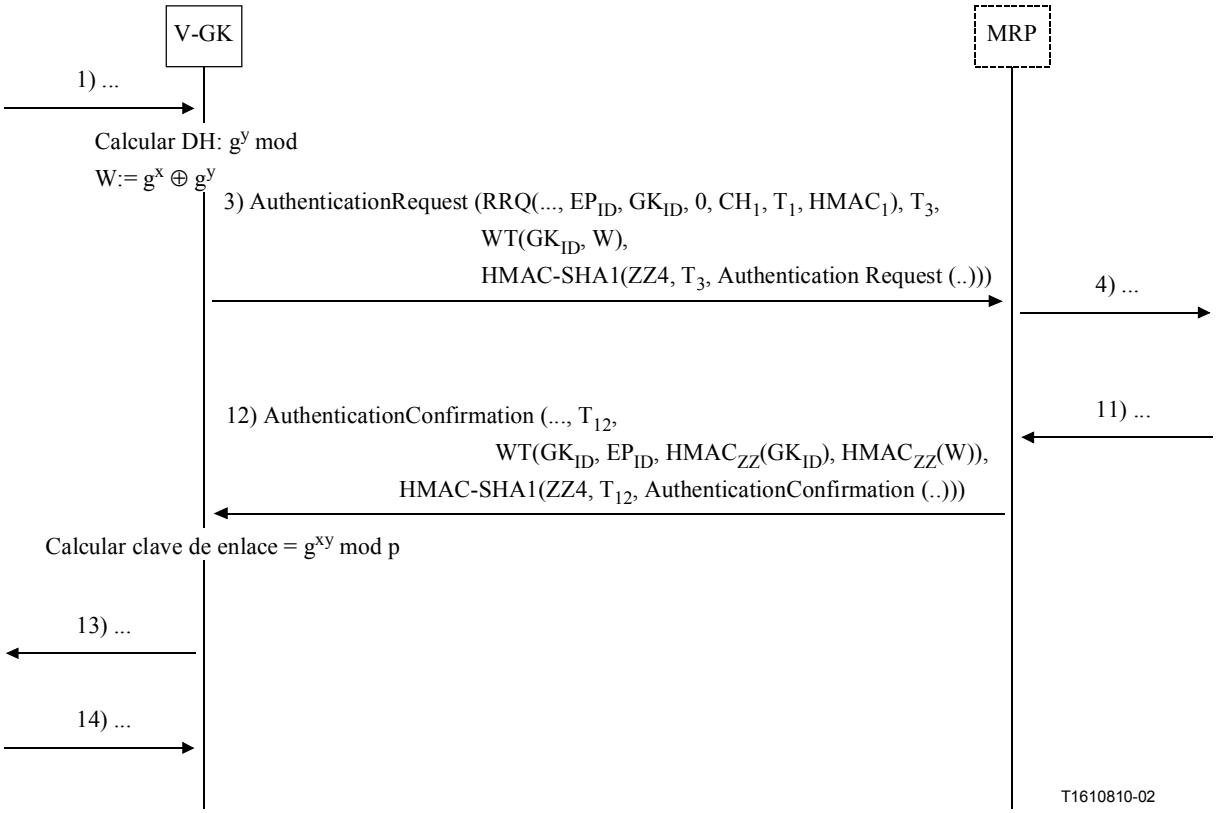

Figura 5/H.530 – Transmisión de información de autenticación entre V-GK y MRP

En caso de que el enlace entre V-GK y MRP no esté protegido por seguridad de red (por ejemplo IPSEC), el mensaje **AuthenticationRequest** será securizado de acuerdo al anexo D/H.235 [4] con una nueva indicación de tiempo T_3 y HMAC calculado con la clave *ZZ4*. De lo contrario, el mensaje **AuthenticationRequest** puede que no necesite protección de seguridad según el anexo D/H.235 [4].

AuthenticationConfirmation o **AuthenticationRejection** en el mensaje 12) transportan los valores autenticados procedentes de la AuF como credenciales en un **ClearToken** de movilidad separado que se muestra como **WT()**. Si el enlace entre V-GK y MRP no está protegido por seguridad de red (por ejemplo IPSEC), **AuthenticationConfirmation** será securizado de acuerdo al anexo D/H.235 [4] con una nueva indicación de tiempo T_{12} y HMAC con la clave *ZZ4*. De lo contrario, **AuthenticationConfirmation**/**AuthenticationRejection** puede que no necesite protección de seguridad según el anexo D/H.235 [4].

El GK_{ID} y EP_{ID} transportados dentro del **ClearToken** de movilidad permiten al V-GK asociar el mensaje **AuthenticationConfirmation**/**AuthenticationRejection** recibido con el correspondiente mensaje **AuthenticationRequest**.

En caso de que el V-GK no tenga una relación de servicio con el MRP (por ejemplo falta la clave *ZZ4*), el V-GK no enviará un **AuthenticationRequest** sino que responderá con **AuthenticationRejection** y **reason** fijado a **noServiceRelationship**.

8.2.3 MRP a V-BE

Un MRP (si está presente y la cuenta de saltos transportada no está excedida, y si una relación de servicio está presente en el V-BE) reenviará al V-BE el mensaje **AuthenticationRequest** recibido; véase el mensaje 4) en la figura 6. El mensaje reenviado será securizado de acuerdo al anexo D/H.235 [4] con una nueva indicación de tiempo T_4 y HMAC calculado con la clave *ZZ5*. De lo contrario, el mensaje **AuthenticationRequest** puede que no necesite protección de seguridad según el anexo D/H.235 [4].

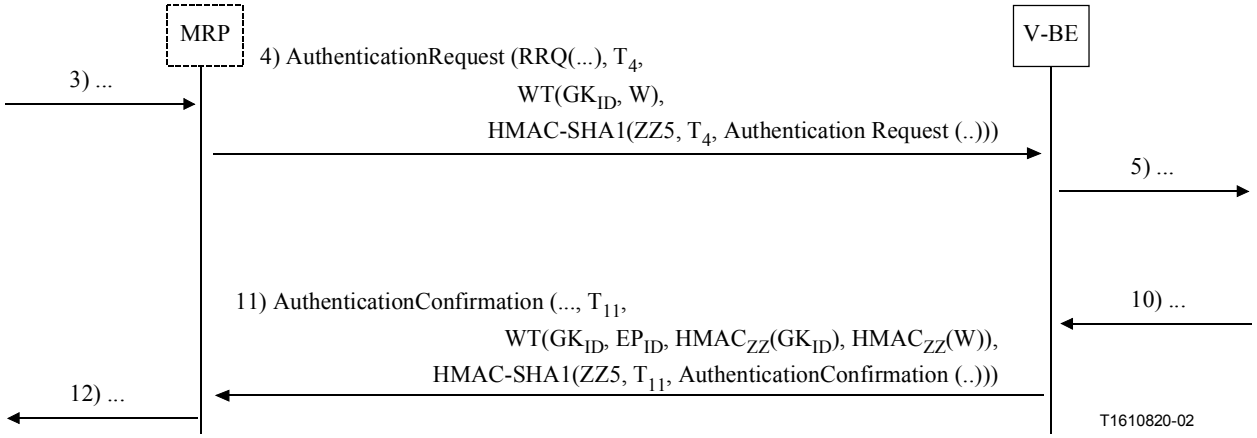

Figura 6/H.530 – Transmisión de información de autenticación entre MRP y V-BE

Un V-BE reenviará un mensaje **AuthenticationConfirmation** o **AuthenticationRejection** al MRP.

AuthenticationConfirmation o **AuthenticationRejection** en el mensaje 11) transportan los valores autenticados como credenciales desde la AuF. Si el enlace entre V-BE y MRP no está protegido por seguridad de red (por ejemplo IPSEC), **AuthenticationConfirmation**/**AuthenticationRejection** serán securizados de acuerdo al anexo D/H.235 [4] con una nueva indicación de tiempo T_{11} y HMAC con la clave *ZZ5*. De lo contrario, **AuthenticationConfirmation**/**AuthenticationRejection** puede que no necesiten protección de seguridad según el anexo D/H.235 [4].

Si se excede la cuenta de saltos, el MRP no enviará un mensaje **AuthenticationRequest**, sino que responderá con el mensaje **AuthenticationRejection** y **reason** fijada a **hopCountExceeded**; véase el mensaje 12).

En caso de que el MRP no tenga una relación servicio con el V-BE (por ejemplo falta la clave *ZZ5*), el V-GK no enviará un **AuthenticationRequest**, sino que responderá con **AuthenticationRejection** y **reason** fijada a **noServiceRelationship**; véase el mensaje 12).

8.2.4 V-BE a H-BE

La figura 7 representa el flujo de mensajes entre dos BE de dos dominios adyacentes en el momento del registro inicial. La seguridad puede haberse realizado mediante IPSEC de acuerdo con la Rec. UIT-T H.501 [3] o mediante el secreto compartido *ZZ2* que es compartido entre V-BE y H-BE. En este último caso, el mensaje H.501 [3] será securizado de acuerdo con el anexo D/H.235 [4].

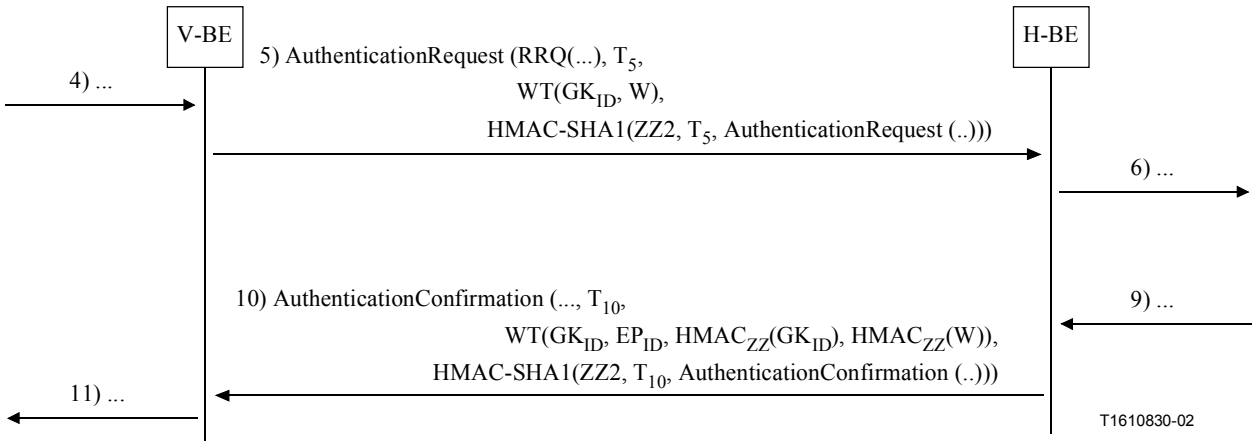

Figura 7/H.530 – Transmisión de información de autenticación entre dos BE

Si la cuenta de saltos transportada no está excedida y está presente una relación de servicio con el H-BE, El mensaje **AuthenticationRequest** H.501 [3] transporta el **RRQ** completo incluidos los correspondientes Clear y CryptoToken; véase el mensaje 5). Esto se hace para dejar que la AuF valide el mensaje **RRQ** y autentique al usuario/MT. Se securiza un mensaje H.501 [3] de manera que el mensaje completo goce de una protección de integridad similar a la descrita en el anexo D/H.235, donde el troceado calculado se almacena en el **CryptoToken** de la **MessageCommonInfo**. Los BE insertarán nuevas indicaciones de tiempo (T_5, T_{10}) para cada mensaje H.501 [3].

El mensaje **AuthenticationConfirmation**/**AuthenticationRejection** transporta los valores autenticados como credenciales procedentes de la AuF en un **ClearToken** de movilidad mostrado como **WT()**.

En caso de que el usuario del MT no esté autorizado para utilizar el servicio H.323 móvil, la AuF debe enviar **AuthenticationRejection** con **reason** fijada a seguridad. En caso de cualquier otro fallo de seguridad, la AuF fijará **reason** a un error, de acuerdo con B.2.2/H.235 [4].

Si la cuenta de saltos está excedida, el V-BE no enviará un mensaje **AuthenticationRequest**, sino que responderá con **AuthenticationRejection** y **reason** fijada a **hopCountExceeded**; véase el mensaje 11).

En caso de que el V-BE no tenga una relación de servicio con el H-BE (por ejemplo falta la clave *ZZ2*), el V-BE no enviará un mensaje **AuthenticationRequest**, sino que responderá con **AuthenticationRejection** y **reason** fijada a **noServiceRelationship**; véase el mensaje 11).

8.2.5 H-BE a MRP

Si está presente un MRP, el flujo de mensajes tiene lugar de acuerdo con la figura 8.

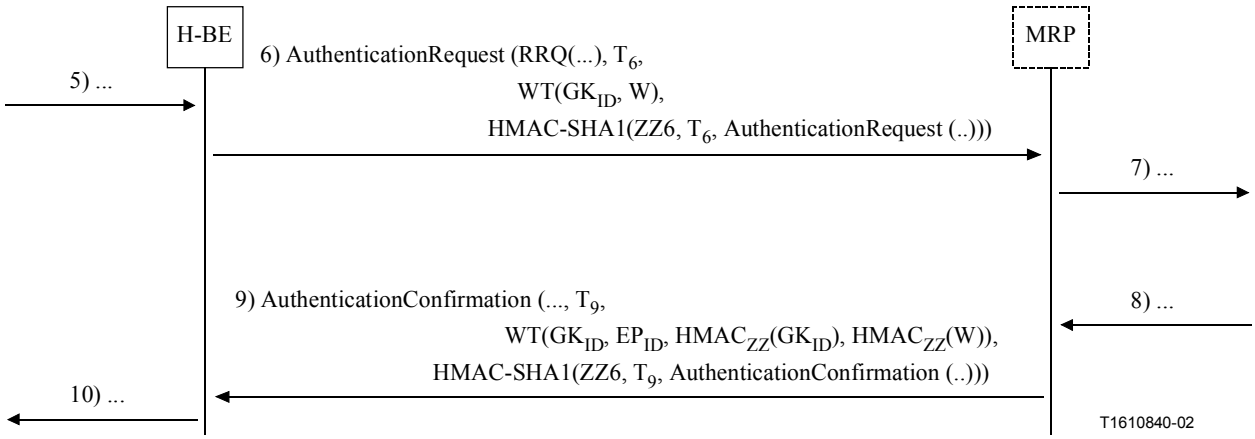

Figura 8/H.530 – Transmisión de información de autenticación entre H-BE y MRP

8.2.6 MRP a AuF

La figura 9 muestra el flujo de mensajes entre el MRP (si existe, si la cuenta de saltos no está excedida y si existe una relación de servicio) y la AuF. Si no existe MRP será sustituido por la anterior entidad de red. Al igual que en las anteriores figuras, el secreto compartido *ZZ3* securiza los mensajes transmitidos.

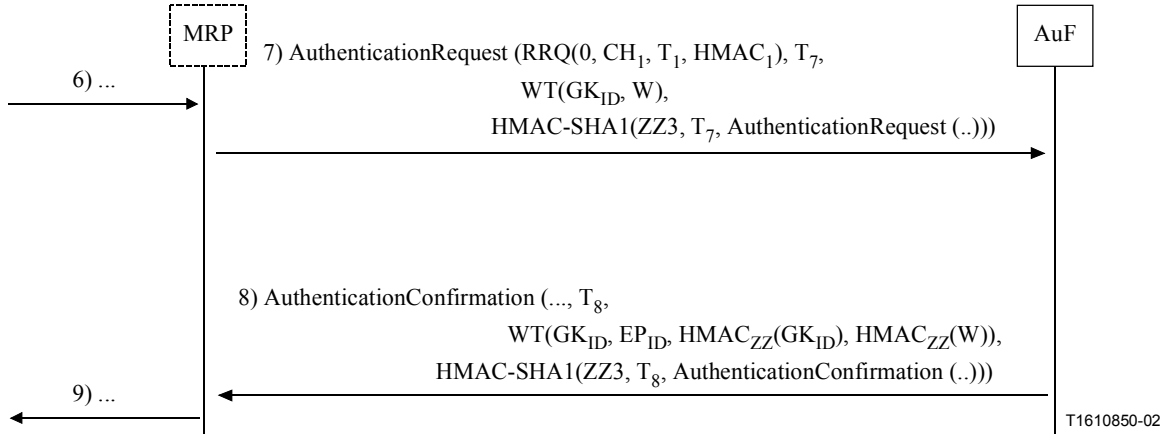

Figura 9/H.530 – Transmisión de información de autenticación entre MRP y AuF

Tras la recepción del mensaje **AuthenticationRequest**, la AuF puede introducir sucesivamente las otras entidades funcionales en la cadena de confianza para preservar la integridad del **RRQ** transportado; véase el mensaje 7). La AuF verificará el **AuthenticationRequest** transportado y después verificará el **RRQ** encapsulado como se describe en el procedimiento I del anexo D/H.235 [4]. La indicación de tiempo T_1 señala que se trata de un **RRQ** y que se deberá comprobar.

Si el MT/usuario es conocido por la AuF y está autorizado, la AuF responderá con **AuthenticationConfirmation**; véase el mensaje 8). Además, si se desea la autenticación del MT, la AuF verificará el correspondiente **CryptoToken** transportado. De lo contrario, cuando el MT/usuario no puede autenticarse o la AuF no lo conoce, se depositará un mensaje **AuthenticationRejection** con **reason** fijada a un error adecuado como se define en B.2.2/H.235 [4].

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**. 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).

Si la cuenta de saltos está excedida, el MRP no enviará un mensaje **AuthenticationRequest**, sino que responderá mediante un mensaje **AuthenticationRejection** con **reason** fijada a **hopCountExceeded**; véase el mensaje 9).

Si el MRP no tiene una relación de servicio con la AuF (por ejemplo falta la clave *ZZ3*), el MRP no enviará un mensaje **AuthenticationRequest**, sino que responderá con **AuthenticationRejection** y **reason** fijada a **noServiceRelationship**; véase el mensaje 9).

NOTA – En un sentido estricto, la AuF no tiene capacidad para autenticar completamente al V-GK. Esto se explica porque el V-GK no tiene capacidad para probar criptográficamente su identidad. Sin embargo, la AuF certifica mediante las credenciales la identidad de V-GK depositada, cualquiera que ésta sea. De esta manera, el usuario/MT tiene la seguridad de que el V-GK con quien está hablando sigue siendo siempre el mismo que ha sido certificado en el procedimiento de autenticación.

8.3 Autenticación del terminal

La autenticación del terminal móvil (MT, *mobile terminal*) es una prestación facultativa adicional, soportada además de la autenticación de usuario móvil. La autenticación del MT se utilizará cuando la sola autenticación del usuario móvil no se considera suficiente y cuando el MT tiene un secreto compartido *ZZMT* correspondiente. Se supone que el terminal móvil posee un secreto compartido *ZZMT* asignado, que comparte con la AuF. La asignación y distribución de este secreto está fuera del ámbito de esta Recomendación.

De hecho, para la autenticación de MT están soportados dos escenarios:

- La AuF a la que está abonado el usuario móvil es idéntica a la AuF que mantiene los terminales móviles abonados. En este caso, la AuF tiene capacidad para autenticar y tomar decisiones sobre la autorización tanto en relación con el usuario como con el MT.
- La AuF a la que está abonado el usuario móvil es diferente de la AuF a la que está abonado el MT. En este caso, hay que enviar primeramente el mensaje **AuthenticationRequest** a la AuF del usuario. Incumbe a la AuF del usuario localizar y contactar la AuF de MT adecuada que se encarga del MT. Esa AuF de MT puede estar ubicada en un dominio diferente. Toda comunicación de este tipo y la necesaria protección de seguridad más allá de la AuF o entre las AuF están fuera del ámbito de esta Recomendación.

La autenticación del terminal móvil se realiza conjuntamente con la autenticación del usuario. Para la autenticación del terminal se utiliza un **CryptoToken** XT() separado. Este **CryptoToken** se transporta dentro de los campos de seguridad del mensaje de autenticación de usuario **GRQ** o del mensaje **RRQ**, lo que dependerá de que la autenticación del usuario y del terminal se produzcan en la fase de descubrimiento del GK visitado o en la fase de registro; véase 8.2.

El terminal móvil se autentica a sí mismo ante la AuF probando que tiene conocimiento o está en posesión del secreto compartido *ZZMT*. Esto permite a la AuF verificar la calidad de correcto del **CryptoToken** proporcionado y reconocer, en retorno al dominio visitado, que esta propiedad forma parte de la respuesta de autorización (**AuthenticationConfirmation**/**AuthenticationRejection**). Después de esto, el dominio visitado puede tomar una decisión sobre la autorización del MT.

El algoritmo HMAC-SHA1-96 introducido se utiliza como la función autenticación criptográfica. El procedimiento que se aplica es esencialmente el procedimiento I del anexo D/H.235 [4] con la salvedad de que la comprobación de la integridad se calcula simplemente sobre el **CryptoToken** del terminal móvil de que se trate, y no sobre el mensaje completo como en realidad se describe en el procedimiento I del anexo D/H.235 [4].

El **CryptoH323Token** concreto para autenticación de terminal móvil contendrá los siguientes campos:

- **NestedCryptoToken** que contiene un **CryptoToken**, que a su vez contiene el **cryptoHashedToken** que contiene los siguientes campos:
  - **TokenOID** fijado a:
    - "G1" que indica que el cálculo de la autenticación/integridad sólo incluye el contenido de este **CryptoToken**.
- **HashedVals** que contiene el campo **ClearToken** con los siguientes campos:
  - **TokenOID** fijado a:
    - "T" que indica que **ClearToken** se está utilizando para autenticación/integridad (véase D.11/H.235 [4]).
    - **timestamp** que contiene la indicación de tiempo.
    - **random** que contiene un número secuencial monótonamente creciente. Este número permite hacer que dos mensajes con la misma indicación de tiempo (dentro de la resolución del reloj) sean únicos.
    - **generalID** que contiene el identificador del recibiente (sólo en el caso de mensajes unidifusión). En este escenario, este es el identificador del dominio de base.
    - **sendersID** que contiene el identificador del emisor. En este escenario, este es el identificador del punto extremo del MT.
- **Token** que contiene **HASHED** con los campos:
  - **algorithmOID** fijado a "U" que indica HMAC-SHA1-96; (véase D.11/H.235 [4]).
  - **params** fijado a NULL.
  - **hash** que contiene el autenticador calculado mediante HMAC-SHA1-96. El autenticador se calculará sobre el **CryptoH323Token** completo.

La AuF receptora verificará el **CryptoToken** encontrado, que está transportando la autenticación del MT. Si la verificación fracasa, la AuF considerará al MT como no autorizado. En este caso, la AuF responderá con el mensaje **AuthenticationRejection** y **reason** fijada a **security**. Para cualquier otro fallo de seguridad, la AuF fijará **reason** a un error de acuerdo con B.2.2/H.235 [4].

La figura 10 muestra el flujo de mensajes en el caso de autenticación del terminal móvil en la fase de registro del terminal móvil. El **CryptoToken** concreto para autenticación del MT se muestra como XT().

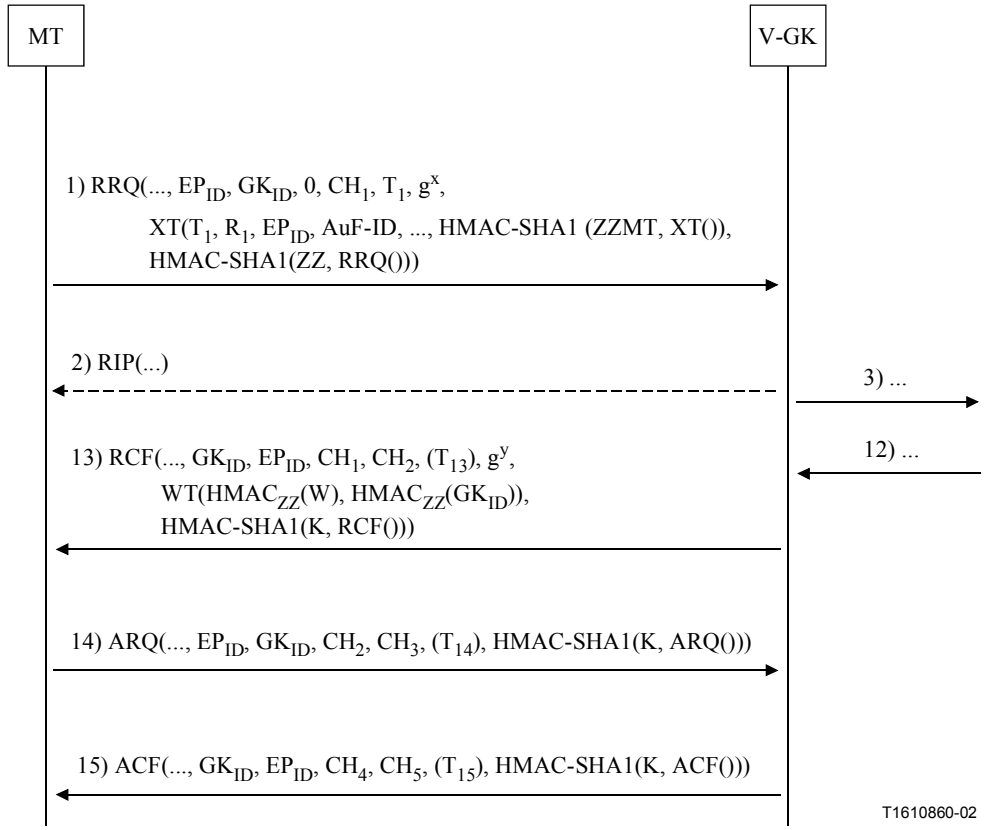

Figura 10/H.530 – Autenticación del MT

El procedimiento de autenticación del MT se aplicará explícitamente sólo durante **GRQ** o **RRQ**. En cualquier otro ulterior mensaje RAS que se intercambie entre el MT y el V-GK, la autenticación del MT se efectúa implícitamente dentro del proceso de autenticación de usuario e integridad de mensaje que se encuentra en curso. No se necesitan medios particulares para una ulterior autenticación del MT.

8.4 Desregistro

Un MT o V-GK tras la recepción de **UCF** liberará la clave de enlace *K*.

8.5 Aplicación del protocolo de seguridad simétrico en el dominio de base

Si bien el protocolo de seguridad para entornos de movilidad descrito en esta Recomendación se aplicará por lo general a terminales móviles (MT) conectados a dominios visitados extranjeros, en esta cláusula se describe la forma en que este protocolo de seguridad para entornos de movilidad puede aplicarse a MT conectados al dominio de base. Esto permite que la aplicación de este protocolo sea independiente del dominio a que el MT esté efectivamente conectado. Se incluye también el caso de los entornos que no son de movilidad pero que, no obstante, soportan H.530.

La figura 11 representa el escenario en el que un MT está conectado al GK de base en el dominio de base y la autenticación y autorización se producen en la fase de registro. Es posible también un escenario similar, que no se muestra, en el que la autenticación y autorización se producen en la fase de descubrimiento de controlador de acceso.

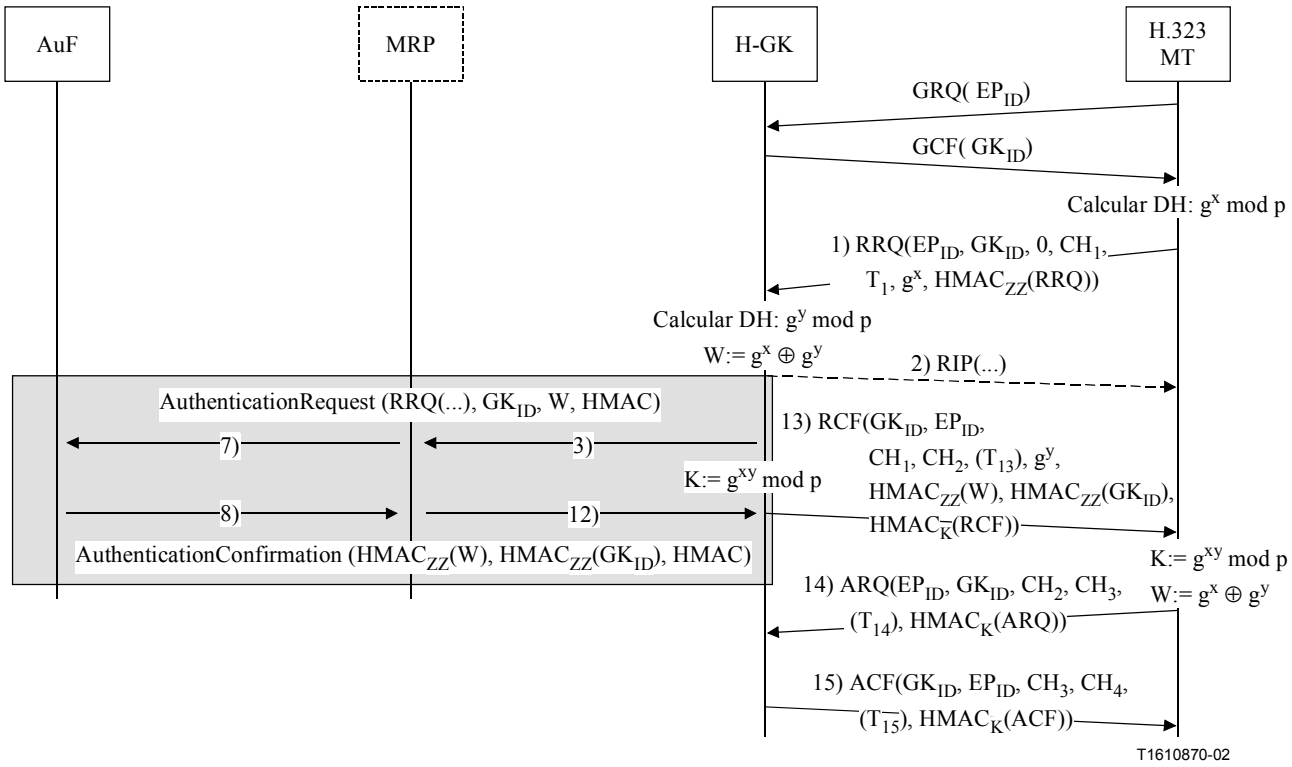

Figura 11/H.530 – Autenticación de MT en el dominio de base en la fase de registro

En cualquier caso, el H-GK se comportará exactamente como un V-GK en el dominio visitado como se muestra en la figura 11 y se aplicarán los respectivos procedimientos de seguridad antes descritos. El secreto compartido *ZZ4* se sustituirá por *ZZ8*, y *ZZ3* por *ZZ7*, respectivamente.

El MRP que aparece en la figura es una entidad facultativa. Cuando no está presente, AuF y H-GK tienen establecida una relación de seguridad directa. Como un caso especial, AuF y H-GK podrían estar coubicadas, y en tal situación la comunicación entre ambas entidades sería un asunto local.

8.6 Identificadores de objeto

En el cuadro 1 se indican todos los identificadores de objeto a que se hace referencia en esta Recomendación.

Cuadro 1/H.530 – Identificadores de objeto utilizados en H.530

Referencia de identificador de objeto	Valor(es) de identificador de objeto	Descripción
"G1"	{itu-t (0) Recommendation (0) h (8) 235 version (0) 2 10}	Se utiliza para indicar un **CryptoToken** de movilidad para la autenticación del MT.
"G2"	{itu-t (0) Recommendation (0) h (8) 235 version (0) 2 11}	Se utiliza para indicar un **ClearToken** de movilidad que mantiene el GK_{ID} y el valor compuesto *W* dentro de **AuthenticationRequest**, o los valores correspondientes autenticados por la AuF, dentro de **AuthenticationConfirmation**/ **AuthenticationRejection** o GCF/GRJ, RCF/RCF.

9 Seguridad de extremo a extremo

Una arquitectura de seguridad de extremo a extremo en un entorno de movilidad H.323 que se basa en conceptos de infraestructura de clave pública (PKI, *public-key infrastructure*) queda en estudio.

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

Impreso en Suiza
Ginebra, 2002