

Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

H.235.7

(09/2005)

SERIE H: SISTEMAS AUDIOVISUALES Y
MULTIMEDIOS

Infraestructura de los servicios audiovisuales – Aspectos
de los sistemas

**Marco de seguridad H.323: Utilización del
protocolo de gestión de claves MIKEY para el
protocolo de transporte en tiempo real seguro
en H.235**

Recomendación UIT-T H.235.7

UIT-T



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.349
Arquitectura de servicios de directorio para servicios audiovisuales y multimedios	H.350–H.359
Arquitectura de la calidad de servicio para servicios audiovisuales y multimedios	H.360–H.369
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.235.7

Marco de seguridad H.323: Utilización del protocolo de gestión de claves MIKEY para el protocolo de transporte en tiempo real seguro en H.235

Resumen

La finalidad de esta Recomendación es describir los procedimientos de seguridad de los sistemas basados en H.323/H.235 de manera que puedan utilizar el protocolo de gestión de claves MIKEY conjuntamente con el protocolo de transporte en tiempo real seguro.

En las versiones anteriores de la subserie H.235, este perfil figuraba en el anexo G/H.235. Los apéndices IV, V, VI de la H.235.0 contienen una tabla de correspondencia de cláusulas, cuadros y figuras entre las versiones 3 y 4 de la H.235.

Orígenes

La Recomendación UIT-T H.235.7 fue aprobada el 13 de septiembre de 2005 por la Comisión de Estudio 16 (2005-2008) del UIT-T por el procedimiento de la Recomendación UIT-T A.8.

Palabras clave

Criptación de medios, gestión de claves MIKEY, perfil de seguridad, protocolo de transporte en tiempo real seguro, seguridad de multimedia, SRTP.

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 no 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.

© UIT 2006

Reservados todos los derechos. Ninguna parte de esta publicación puede reproducirse por ningún procedimiento sin previa autorización escrita por parte de la UIT.

ÍNDICE

	Página
1 Alcance	1
2 Referencias	1
2.1 Referencias normativas	1
2.2 Referencias informativas y Bibliografía.....	2
3 Definiciones.....	2
4 Abreviaturas y símbolos	2
5 Convenios	4
6 Introducción.....	5
7 Panorama general y escenarios.....	6
7.1 Funcionamiento de MIKEY en el "nivel de sesión".....	7
7.2 Funcionamiento de MIKEY en el "nivel de medios"	8
7.3 Negociación de capacidad MIKEY	9
8 Perfil de seguridad utilizando técnicas de seguridad simétricas.....	10
8.1 Terminación de una llamada H.323.....	16
8.2 Creación de nuevas claves TGK y actualización del CSB	17
8.3 Soporte de tunelización H.245	18
8.4 Algoritmos SRTP	18
8.5 Lista de identificadores de Objetos	19
9 Perfil de seguridad que utiliza técnicas de seguridad asimétricas	19
9.1 Terminación de una llamada H.323.....	23
9.2 Creación de nuevas claves TGK y actualización del CSB	24
9.3 Soporte de tunelización H.245	25
9.4 Algoritmos SRTP	25
9.5 Lista de identificadores de objeto.....	26
Apéndice I – Opción MIKEY-DHMAC	26
I.1 Terminación de una llamada H.323.....	30
I.2 Creación de nuevas claves TGK y actualización del CSB	31
Apéndice II – Utilización de la H.235.4 para establecer un secreto precompartido.....	33
II.1 Terminación de una llamada H.323.....	35
II.2 Creación de nuevas claves TGK y actualización del CSB	35

Introducción

La finalidad de esta Recomendación es formular recomendaciones sobre procedimientos de seguridad de manera que los sistemas basados en H.323/H.235 puedan utilizar el protocolo de gestión de claves MIKEY del IETF conjuntamente con el protocolo de seguridad SRTP del IETF.

Esta Recomendación ha sido redactada como un perfil de seguridad de la Rec. UIT-T H.235 que se ofrece como una opción y puede servir de complemento a las otras características de seguridad de medios de la Rec. UIT-T H.235.6.

Esta Recomendación posibilita el despliegue de seguridad de medios SRTP cuando la gestión de claves MIKEY suministra las claves necesarias y los parámetros de seguridad entre los correspondientes puntos de extremo a extremo. Esta Recomendación puede aplicarse en un dominio H.323 entre sistemas H.323 habilitados para funcionar conforme a la H.235.7. Esta Recomendación define las extensiones del protocolo de seguridad para el protocolo de registro, admisión y estado (RAS) y la señalización de llamada H.225.0, así como para H.245, junto con los procedimientos correspondientes. Además, esta Recomendación presenta las capacidades necesarias para soportar el interfuncionamiento con las entidades del protocolo de iniciación de sesión (SIP) del IETF que hayan implementado la gestión de claves MIKEY y SRTP.

Recomendación UIT-T H.235.7

Marco de seguridad H.323: Utilización del protocolo de gestión de claves MIKEY para el protocolo de transporte en tiempo real seguro en H.235

1 Alcance

El objetivo de esta Recomendación es formular recomendaciones sobre procedimientos de seguridad para que los sistemas basados en H.323/H.235 puedan utilizar el protocolo de gestión de claves MIKEY conjuntamente con el protocolo de seguridad SRTP.

Este perfil de seguridad se ofrece como una opción que puede complementar a las otras características de seguridad de medios de H.235.6.

2 Referencias

2.1 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. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación.

- Recomendación UIT-T H.225.0 (2003), *Protocolos de señalización de llamada y paquetización de trenes de medios para sistemas de comunicación multimedios por paquetes*.
- Recomendación UIT-T H.235.0 (2005), *Marco de seguridad H.323: Marco de seguridad para sistemas multimedios de la serie H (H.323 y otros basados en H.245)*.
- Recomendación UIT-T H.235.1 (2005), *Marco de seguridad H.323: Perfil de seguridad básico*.
- Recomendación UIT-T H.235.3 (2005), *Marco de seguridad H.323: Perfil de seguridad híbrido*.
- Recomendación UIT-T H.235.4 (2005), *Marco de seguridad H.323: Seguridad de llamada con encaminamiento directo y selectivo*.
- Recomendación UIT-T H.245 (2005), *Protocolo de control para comunicación multimedia*.
- Recomendación UIT-T H.323 (2003), *Sistemas de comunicación multimedios basados en paquetes*.
- Recomendación UIT-T X.800 (1991), *Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT*.
- ISO/CEI 10118-3:2004, *Information Technology – Security techniques – Hash functions – Part 3: Dedicated hash functions*.
- IETF RFC 3550 (2003), *RTP: A Transport Protocol for Real-Time Applications*.
- IETF RFC 3711 (2004), *The Secure Real Time Transport Protocol (SRTP)*.

- IETF RFC 3830 (2004), *MIKEY: Multimedia Internet KEYing*.

2.2 Referencias informativas y bibliografía

- IETF RFC 1305 (1992), *Network Time Protocol (Version 3) Specification, Implementation and Analysis*.
- IETF RFC 2327 (1999), *SDP: Session description protocol*.
- IETF RFC 2631 (1999), E. Rescorla: *Diffie-Hellman Key Agreement Method*.
- IETF RFC 3261 (2002), *SIP: Session Initiation Protocol*.
- IETF RFC 3264 (2002), *An Offer/Answer Model with the Session Description Protocol (SDP)*.
- IETF RFC ssss (2005), M. Handley, Van Jacobson, C. Perkins: *SDP: Session Description Protocol*, draft-ietf-mmusic-sdp-new-24.txt.
- IETF RFC www (2005), J. Arkko, E. Carrara et al: *Key Management Extensions for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP)*, Internet Draft draft-ietf-mmusic-kmgmt-ext-14.txt, Work in Progress.
- IETF RFC zzzz (2005), M. Euchner: *HMAC-authenticated Diffie-Hellman for MIKEY*, Internet Draft draft-ietf-msec-MIKEY-DHHMAC-11.txt, Work in Progress.

3 Definiciones

Ninguna.

4 Abreviaturas y símbolos

En esta Recomendación se utilizan las siguientes abreviaturas y símbolos.

a, b, e, d	Clave DH privada de EP A, EP B, GK E, GK D (<i>private DH key of EP A, EP B, GK E, GK D</i>)
Cert	Certificado digital (<i>digital certificate</i>) (véase RFC 3830)
CP/C	Llamada en curso a conexión (<i>CallProceeding-to-connect</i>)
CSB	Agrupamiento de sesiones criptadas (<i>crypto session bundle</i>) (véase RFC 3830)
CT _B , CT _A	ClearToken (testigo despejado) del punto extremo B, ClearToken del punto extremo A (<i>ClearToken for endpoint B, ClearToken for endpoint A</i>) (véase la Rec. UIT-T H.235.4)
DRC1	Llamada con encaminamiento directo (<i>direct-routed Call</i>) (véase H.235.4)
ENC _k (x)	Criptación de X utilizando la clave k (<i>encryption of X using key k</i>)
env_key	Clave de envoltorio (RFC 3830) entre el punto extremo B y el punto extremo A (<i>envelope key (RFC 3830) between endpoint B and endpoint A</i>)
EP	Punto extremo (<i>endpoint</i>)
ESC	Instrucción para cerrar la sesión H.245 (<i>H.245 EndSessionCommand</i>)
DH	Diffie-Hellman
DH _A	Media clave DH del punto extremo A (<i>DH half-key of endpoint A</i>)
DH _B	Media clave DH del punto extremo B (<i>DH half-key of endpoint B</i>)
g^a, g^b	Media clave Diffie-Hellman de EP A, EP B (<i>Diffie-Hellman half-key of EP A, EP B</i>)
g^e, g^d	Media clave Diffie-Hellman de GK E, GK D (<i>Diffie-Hellman half-key of GK E, GK D</i>)

GK	Controlador de acceso (<i>gatekeeper</i>)
HDR	Cabida útil de cabecera MIKEY (<i>MIKEY header payload</i>) (véase RFC 3830)
ID _A , ID _B	Identidad (ID) del punto extremo A; identidad del punto extremo B (<i>identity (i.e. endpoint ID) of endpoint A, identity of endpoint B</i>)
IETF	Grupo de tareas especiales de ingeniería en Internet (<i>Internet engineering task force</i>)
Imsg	Mensaje MIKEY del iniciador (<i>MIKEY message of the initiator</i>) (véase RFC 3830)
KEMAC	Mensaje de cabida útil KEMAC de MIKEY (<i>MIKEY KEMAC payload message</i>) (véase RFC 3830)
MAC(<i>k</i> , <i>x</i>)	MAC codificada en <i>x</i> utilizando la clave <i>k</i> (<i>keyed MAC on x using key k</i>)
<i>Ma</i>	Clave de autenticación MIKEY (<i>MIKEY authentication key</i>) (véase RFC 3830)
<i>Me</i>	Clave de criptación MIKEY (<i>MIKEY encryption key</i>) (véase RFC 3830)
MIKEY	Claves Internet de multimedia (<i>multimedia Internet keying</i>)
NTP	Protocolo de señales horarias de red (<i>network time protocol</i>)
PKI	Infraestructura de claves públicas (<i>public-key infrastructure</i>)
Rmsg	Mensaje MIKEY del respondedor (<i>MIKEY message of the responder</i>) (véase RFC 3830)
PKE	Mensaje de cabida útil PKE de MIKEY (<i>MIKEY PKE payload message</i>) (véase RFC 3830)
PRF	Función pseudoaleatoria (MIKEY-PRF) (véanse las secciones 4.1.2–4.1.4 de RFC 3830) (<i>pseudo-random function (MIKEY-PRF)</i>)
Rand	Nonce (parámetro temporal aleatorio) (<i>random nonce</i>) (véase RFC 3830)
rand()	Valor aleatorio (<i>random value</i>)
RSA	Rivest, Shamir y Adleman (algoritmo de clave pública) (<i>Rivest, Shamir and Adleman (public key algorithm)</i>)
<i>sa</i> , <i>sb</i>	Secreto compartido entre el punto extremo A y el GK, secreto compartido entre el punto extremo B y el GK (<i>shared secret among endpoint A and GK, shared secret among endpoint B and GK</i>)
<i>sl</i>	Secreto compartido entre controladores de acceso (<i>shared secret among gatekeepers</i>)
SDP	Protocolo de descripción de sesión (<i>session description protocol</i>)
SHA1	Algoritmo de generación numérica seguro N.º 1 (ISO/CEI 10118-3) (<i>secure hash algorithm 1 (ISO10118-3)</i>)
SIP	Protocolo de iniciación de sesión (<i>session initiation protocol</i>)
SP	Política de seguridad (<i>security policy</i>) (véase RFC 3830)
SRTCP	Protocolo de control de transporte en tiempo real seguro (<i>secure real-time transport control protocol</i>)
SRTP	Protocolo de transporte en tiempo real seguro (<i>secure real-time transport protocol</i>) (véase [RFC 3711])
SSRC	Fuente de sincronización (RTP) (<i>synchronization source (RTP)</i>)
T	Indicación de tiempo (<i>timestamp</i>) (véase RFC 3830)

TGK	Clave de generación de tráfico (véase RFC 3830) entre el punto extremo A y el punto extremo B (<i>traffic generating key between endpoint A and endpoint B</i>)
V	Campo de mensaje de verificación (<i>verification message field</i>) (véase RFC 3830)
ZZ _{AB}	Secreto H.323 compartido dinámico ZZ _{AB} (<i>dynamic shared H.323 secret ZZ_{AB}</i>)
{}	Cero, una o más veces presente (<i>zero, one or more occurrences</i>)
[]	Elemento facultativo (<i>optional element</i>)

5 Convenios

Los identificadores de objeto son señalados mediante una referencia simbólica en el texto (por ejemplo, "G1"), y en las cláusulas 8.5 y 9.5 se enumeran los valores numéricos efectivos de estos identificadores simbólicos; para más información, véase también la cláusula 5/H.235.0.

En el cuadro 1 se definen los cinco protocolos de gestión de claves MIKEY a los que se hace referencia en esta Recomendación:

Cuadro 1/H.235.7 – Protocolos de gestión de claves MIKEY

Protocolo MIKEY	Descripción	Valor OID	Identificador de parámetro	Implementación
MIKEY	Cualquier protocolo MIKEY	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 76}	76	Obligatoria
MIKEY-PS	Protocolo de distribución de claves simétricas que emplea claves simétricas precompartidas y HMAC; (véase RFC 3830).	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 72}	72	Obligatoria
MIKEY-DHMAC	Protocolo de convenio de claves Diffie-Hellman que utiliza claves simétricas precompartidas y HMAC; (véase RFC zzzz).	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 73}	73	Facultativa
MIKEY-PK-SIGN	Protocolo de distribución de claves públicas (basadas en RSA) que utiliza firmas digitales; (véase RFC 3830).	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 74}	74	Obligatoria
MIKEY-DH-SIGN	Protocolo de convenio de claves Diffie-Hellman que utiliza firmas digitales; (véase RFC 3830).	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 75}	75	Facultativa

MIKEY (primera fila del cuadro 1) se refiere a la familia de protocolos MIKEY en general sin indicar específicamente ninguna variante del protocolo de gestión de claves MIKEY particular como MIKEY-PS, MIKEY-DHMAC, MIKEY-PK-SIGN o MIKEY-DH-SIGN. La implementación correspondiente de MIKEY englobará el procesamiento de los mensajes MIKEY tales como la cabida útil de la cabecera común MIKEY (sección 6.1 de RFC 3830), pero no necesariamente exige la implementación de un protocolo de gestión de claves MIKEY particular o la implementación de una cabida útil de información MIKEY determinada. El identificador de objeto (OID, *object identifier*) y el identificador de parámetros correspondientes se utilizarán en los

casos en que un punto extremo H.323 no conoce la verdadera variante del protocolo MIKEY que se está utilizando. En cualquier otro caso, por el contrario, se recomienda emplear el OID y el identificador de parámetros específicos de la variante real del protocolo de gestión de claves MIKEY.

6 Introducción

Se ha manifestado interés en utilizar las características de seguridad del "protocolo de transporte en tiempo real seguro" (SRTP) del IETF dentro de la Rec. UIT-T H.235. Aunque las versiones previas de H.235 ya ofrecen varias características de seguridad de medios tales como la criptación vocal utilizando cifrado de bloques y la autenticación limitada del protocolo de transporte en tiempo real (RTP, *real time transport protocol*) (opción antibombardeo publicitario), hay muy buenos motivos para adoptar SRTP:

- utilización de cifrado de trenes para mejorar la calidad de funcionamiento, la robustez y la seguridad;
- compatibilidad con otros terminales SRTP, como los terminales de medios basados en SIP.
NOTA – Esta Recomendación no especifica los procedimientos de interfuncionamiento de seguridad con SIP (RFC 3261); ese tema queda en estudio.
- proporcionar seguridad mejorada para la protección de protocolo de control de transporte en tiempo real (RTCP, *real time transport control protocol*);
- lograr una mayor integridad que abarque todo el paquete RTP/RTCP;
- desplegar el algoritmo de criptación de la norma de criptación avanzada (AES, *advanced encryption standard*) más perfeccionado;
- utilizar claves de criptación/autenticación de sesión deducidas de una función pseudoaleatoria en ambos extremos.

Por otro lado, se ha identificado la necesidad de disponer de una gestión de claves basada en el algoritmo de clave pública de Rivest, Shamir y Adleman (RSA), además de los esquemas de convenio de claves Diffie-Hellman propuestos en H.235. De manera similar, se reconoce que son útiles las técnicas de gestión de claves distintas de la infraestructura de clave pública (PKI, *public key infrastructure*), en los casos en que se considera que las infraestructuras de clave pública no son una opción. También hay interés en abordar las cuestiones de la interceptación legal en el contexto de la gestión de claves.

El IETF también ha consagrado esfuerzos para definir un esquema de gestión de claves que pueda funcionar en tiempo real y que se denomina MIKEY (RFC 3830). Este esquema de gestión de claves genérico puede interfuncionar satisfactoriamente con SRTP para proporcionar claves maestras (TGK), así como claves de tráfico de sesión, ya sea extremo a extremo o probablemente entre un extremo y un punto medio/salto por salto. MIKEY es un protocolo de gestión de claves optimizado que completa su función con un máximo de dos mensajes, lo que lo hace recomendable para el arranque rápido del establecimiento de la comunicación en H.323.

Esta Recomendación presenta procedimientos de seguridad para desplegar los protocolos de gestión de claves MIKEY desde dentro de H.323/H.235, a fin de soportar la seguridad de medios SRTP. Obsérvese que podría haber otros modos facultativos para soportar SRTP en H.323/H.235, pero esas medidas no se abordan en esta Recomendación y quedan en estudio.

En esta Recomendación se exponen los protocolos de gestión de claves MIKEY de un modo conceptualmente similar al método descrito en RFC www, a tenor del cual el protocolo de iniciación de sesión (SIP) (RFC 3261) transporta MIKEY dentro del protocolo de descripción de sesión (SDP, *session description protocol*) (RFC 2327, RFC ssss y RFC 3264).

En esta Recomendación se especifican dos perfiles de seguridad con los procedimientos correspondientes para dos infraestructuras de seguridad totalmente distintas:

- la infraestructura de seguridad basada en clave simétrica que puede soportar múltiples controladores de acceso (véase la cláusula 8); y
- la infraestructura de seguridad basada en clave asimétrica (PKI) que puede soportar múltiples controladores de acceso (véase la cláusula 9).

7 Panorama general y escenarios

En la figura 1 se presenta el escenario general que aborda esta Recomendación. Al menos dos puntos extremos distintos A y B de H.323 forman parte de este caso. Los puntos extremos pueden ser terminales H.323 o pasarelas de medios H.323, esta última con una posible interfaz a otras redes basadas en paquetes o en otras tecnologías. Adicionalmente, se supone que al menos un controlador de acceso forma parte del entorno. En el caso de que sólo haya un controlador de acceso simple disponible, se supondrá que todos los puntos extremos H.323 se encuentran únicamente dentro de la zona de ese controlador de acceso. En caso de que se utilicen múltiples controladores de acceso encadenados, los puntos extremos H.323 pueden estar situados dentro de distintas zonas de controlador de acceso. Además, se supone que los puntos extremos H.323 se comunican directamente extremo a extremo a través del protocolo de medios RTP.

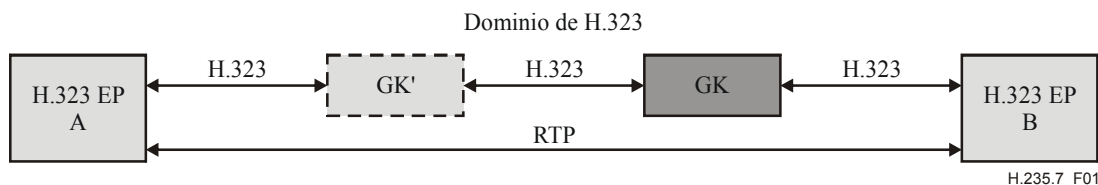


Figura 1/H.235.7 – Escenario

En la figura 2 se ilustra el escenario de seguridad general en el que se señala la utilización de protocolos de gestión de claves MIKEY y el protocolo de seguridad de medios SRTP. Los protocolos de gestión de claves MIKEY funcionan entre los puntos extremos A y B de H.323; dichos protocolos están encapsulados en contenedores dentro de las tomas de contacto de señalización H.245 (conjunto de capacidades de terminal, modo de petición, tomas de contacto de canal lógico abierto y MiscellaneousCommand (instrucciones diversas)) y son transparentes a cualquier controlador(es) de acceso intermedio).

Obsérvese que un punto extremo H.323 puede ser en realidad una pasarela. Por ejemplo, la pasarela puede ofrecer capacidades de interfuncionamiento para poder establecer la interfaz con sistemas basados en SIP, en cuyo caso, la pasarela no terminaría necesariamente los protocolos MIKEY sino que podría retransmitirlos y ampliarlos para lograr una verdadera gestión de claves de extremo a extremo entre los terminales multimedia participantes, soportando así la seguridad de medios extremo a extremo con SRTP. Este método permitiría soportar el interfuncionamiento de seguridad entre sistemas basados en H.323/H.235 y SIP. La funcionalidad o la especificación de interfuncionamiento específicas de dichas pasarelas no es un tema de esta Recomendación y queda en estudio.

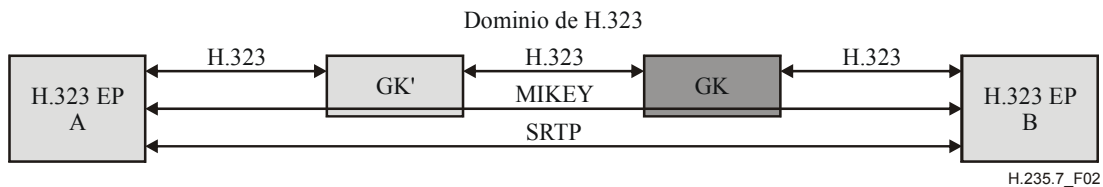


Figura 2/H.235.7 – Escenario de seguridad con MIKEY y SRTP

Todos los protocolos de gestión de claves que se describen en esta Recomendación constan de dos etapas:

- La etapa 1 se produce durante la fase de protocolo RAS y de señalización de llamada H.225.0. Para los protocolos MIKEY de clave simétrica (MIKEY-PS o MIKEY-DHHMAC) en esta etapa se establece un ZZ_{AB} compartido extremo a extremo entre los puntos extremos A y B, que se despliega como un secreto precompartido para MIKEY. Para los protocolos MIKEY asimétricos (MIKEY-PK-SIGN y MIKEY-DH-SIGN) en esta etapa se establecen secretos compartidos dinámicos entre el punto extremo y su próximo salto (por lo general su controlador de acceso de servicio); el secreto compartido dinámico no está relacionado con MIKEY pero es útil para garantizar la señalización de llamada H.225.0 entre el punto extremo y su próximo salto.
- La etapa 2 se produce durante las fases de señalización de llamada H.225.0/protocolo H.245. Esta etapa permite establecer la negociación y activar el protocolo MIKEY (MIKEY-PS, MIKEY-DHHMAC, MIKEY-PK-SIGN o MIKEY-DH-SIGN) entre los puntos extremos A y B y establecer el protocolo MIKEY TGK. Durante la etapa 2, los puntos extremos MIKEY también pueden hacer funcionar el protocolo de creación de nuevas claves MIKEY y de actualización de claves para renovar o actualizar la TGK. Además, durante la etapa 2 puede producirse la terminación de una llamada y el descarte de material de claves (TGK).

7.1 Funcionamiento de MIKEY en el "nivel de sesión"

Los protocolos de gestión de claves MIKEY pueden funcionar en un "nivel de sesión", es decir, se aplica la TGK de MIKEY a más de un tren de medios. Durante la toma de contacto **TerminalCapability** se recomienda utilizar MIKEY en el "nivel de sesión".

TerminalCapabilitySet utilizará **h235SecurityCapability** y para la **genericH235SecurityCapability** se especificará **encryptionAuthenticationAndIntegrity** como se indica a continuación:

- **capabilityIdentifier** indicará uno de los OID de MIKEY dentro de **standard**;
- **maxbitRate** y **collapsing** tampoco se utilizan aquí;
- **nonCollapsing** con los siguientes **GenericParameters** cuando se ejecuta MIKEY en un "nivel de sesión" para todos los canales lógicos:
 - **parameterIdentifier**: en **standard** utilizando el valor 0 para señalar que MIKEY está en un "nivel de sesión";
 - **parameterValue** con el mensaje codificado en binario MIKEY (I o R) dentro de **octetString**;
 - **supersedes** permanece vacío/sin utilizarse;
- **nonCollapsingRaw** tampoco se utiliza aquí;
- **transport** (no se utiliza, o los parámetros de transporte por defecto).

OpenLogicalChannel y **OpenLogicalChannelAck** no utilizarán **encryptionSync** durante el funcionamiento de MIKEY en el "nivel de sesión". De manera similar, **RequestMode** no empleará **genericModeParameters** de **ModeElement** para MIKEY cuando éste se encuentra funcionando en el "nivel de sesión".

MiscellaneousCommand utilizará **encryptionUpdate**, se especificará **genericParameter** así:

- **parameterIdentifier**: en **standard** utilizando el valor 0 para señalar que la creación de nuevas claves TGK de MIKEY y la actualización del CSB se encuentran en el "nivel de sesión";
- **parameterValue** con el mensaje codificado en binario MIKEY (I o R) en **octetString**;
- **supersedes** permanece vacío/sin utilizarse.

LogicalChannelNumber no se tomará en cuenta para MIKEY en el nivel de sesión y puede mantener cualquier valor.

RequestMode utilizará **capabilityIdentifier** en **genericModeParameters** de **ModeElement** como se indica a continuación:

- **capabilityIdentifier** indicará uno de los OID de MIKEY en **standard**;
- **maxbitRate** y **collapsing** tampoco se utilizan aquí;
- **nonCollapsing** con los siguientes **GenericParameters** cuando se ejecuta MIKEY en el "nivel de sesión" de un canal lógico particular:
 - **parameterIdentifier**: en **standard** utilizando el valor 0 para señalar que MIKEY se encuentra en el "nivel de sesión";
 - **parameterValue** con el mensaje codificado en binario de MIKEY (I o R) en **octetString**;
 - **supersedes** permanece vacío/sin utilizarse;
- **nonCollapsingRaw** tampoco se utiliza aquí;
- **transport** (no se utiliza, o los parámetros de transporte por defecto).

7.2 Funcionamiento de MIKEY en el "nivel de medios"

De manera similar, los protocolos de gestión de claves MIKEY pueden funcionar facultativamente en un "nivel de medios", es decir, la TGK de MIKEY se aplica sólo a un canal lógico específico en un tren de medios. La toma de contacto **TerminalCapability** debe aprovecharse para negociar el protocolo MIKEY mientras que **OpenLogicalChannel/Ack** permitirá transportar el mensaje MIKEY codificado.

TerminalCapabilitySet utilizará **h235SecurityCapability** y para la **genericH235SecurityCapability** se especificará **encryptionAuthenticationAndIntegrity** así:

- **capabilityIdentifier** indicará uno de los OID de MIKEY en **standard**;
- **maxbitRate**, **nonCollapsing** y **collapsing** tampoco se utilizan aquí;
- **nonCollapsingRaw** tampoco se utiliza aquí;
- **transport** (no se utiliza, o los parámetros de transporte por defecto).

OpenLogicalChannel u **OpenLogicalChannelAck** utilizarán el **genericParameter** en **encryptionSync** de la siguiente manera:

- **parameterIdentifier**: en **standard** utilizando el valor del identificador de parámetro (véase el cuadro 1) correspondiente al protocolo MIKEY negociado;
- **parameterValue** con el mensaje codificado en binario MIKEY (I o R) en **octetString**;
- **supersedes** permanece vacío/sin utilizarse;

- **synchFlag** en **encryptionSync** se fijará al número de cabida útil dinámico. **h235key** no será utilizada en esta Recomendación y será una cadena de octetos vacía. **escrowentry** no será empleada.

MiscellaneousCommand utilizará **encryptionUpdate** cuando **genericParameter** en **encryptionSync** se emplee de la siguiente manera:

- **parameterIdentifier**: en **standard** utilizando el valor del identificador de parámetro (véase el cuadro 1) correspondiente al protocolo MIKEY negociado;
- **parameterValue** con el mensaje codificado en binario MIKEY (I o R) en **octetString**;
- **supersedes** permanece vacío/sin utilizarse.

RequestMode utilizará **capabilityIdentifier** en **genericModeParameters** de **ModeElement** de la siguiente manera:

- **capabilityIdentifier** indicará uno de los OID de MIKEY en **standard**;
- **maxbitRate** y **collapsing** permanecen sin utilizarse;
- **nonCollapsing** con el siguiente **GenericParameters** fijado cuando se ejecuta MIKEY en un "nivel de medios" para un canal lógico particular:
 - **parameterIdentifier**: en **standard** utilizando el valor del identificador de parámetro (véase el cuadro 1) correspondiente al protocolo MIKEY negociado;
 - **parameterValue** con el mensaje codificado en binario MIKEY (I o R) en **octetString**;
 - **supersedes** permanece vacío/sin utilizarse;
- **nonCollapsingRaw** permanece sin utilizarse;
- **transport** (no se utiliza, o los parámetros de transporte por defecto).

7.3 Negociación de capacidad MIKEY

Si se transportan protocolos MIKEY tanto en el conjunto de capacidades del terminal/modo de petición, como en la toma de contacto del canal lógico abierto, el protocolo MIKEY de esta toma de contacto tendrá precedencia y suprimirá la información de gestión de claves anterior obtenida durante el conjunto de capacidades del terminal/modo de petición.

Como existe la posibilidad de que los puntos extremo no implementen todo el conjunto de protocolos de gestión de claves MIKEY o incluso no implementen ninguno de ellos (es decir, puntos extremo que posiblemente no están en absoluto en consonancia con esta Recomendación), los puntos extremo que generan la llamada pueden no conocer las capacidades MIKEY soportadas en el punto extremo llamado. Por lo tanto, se recomienda que la negociación de las capacidades de gestión de claves MIKEY se realice utilizando tomas de contacto del conjunto de capacidades de terminal.

Durante dicha negociación, el punto extremo llamante debe señalar sus protocolos de gestión de claves MIKEY soportados y aceptables. Para ello, el punto extremo llamante debe indicar sus capacidades de seguridad MIKEY soportadas. En **genericH235SecurityCapability**, el punto extremo llamante fijará **capabilityIdentifier** al valor del OID (véase el cuadro 1) conforme al perfil de seguridad preferido y a la gestión de claves MIKEY. El punto extremo llamante debería utilizar también otros protocolos MIKEY soportados, en orden de preferencia decreciente conforme a su política y limitaciones de seguridad.

Un punto extremo llamado que no soporte esta Recomendación debe rechazar la llamada utilizando **ReleaseComplete** con **ReleaseCompleteReason** fijado a **securityDenied** o puede continuar sin seguridad si lo permiten sus reglas de política de seguridad. El llamante puede deducir que el llamado no soporta la capacidad MIKEY solicitada (en la capacidad devuelta no se indican capacidades MIKEY).

Un punto extremo llamado que soporta esta Recomendación pero que no soporta una capacidad de protocolos MIKEY solicitada debe señalar sus protocolos MIKEY soportados y aceptables durante la toma de contacto de negociación de conjunto de capacidades de terminal.

Un punto extremo llamado que soporta esta Recomendación y un protocolo MIKEY solicitado pero que no soporta una combinación particular de algoritmos y parámetros de seguridad MIKEY/SRTP (es decir, política de seguridad MIKEY, SP) debe transmitir como respuesta un mensaje de error MIKEY (véase RFC 3830 secciones 5.1.1, 5.1.2 y 6.1.2). El punto extremo llamado debe incluir su política de seguridad (SP) MIKEY soportada y aceptable con los algoritmos y parámetros de seguridad MIKEY/SRTP.

En esta Recomendación se utilizará la tunelización de los mensajes H.245 en el marco de la señalización de llamada H.225.0 con la finalidad de asegurar los mensajes de señalización de llamada de H.225.0. En esta Recomendación se puede incluso evitar la utilización de tunelización de los mensajes H.245, aunque en ese caso se requiere el empleo de al menos un transporte seguro que proteja la integridad (TLS, seguridad de nivel de transporte (*transport level security*); IP protocolo de seguridad (IPsec, *Internet security protocol*)) para asegurar los mensajes H.245. En esta Recomendación no se ha especificado esta opción.

De preferencia, en esta Recomendación se utilizará también la conexión rápida, a tenor de la cual los mensajes H.245 tunelizados se encapsulan dentro de los mensajes de establecimiento de señalización de la llamada y de llamada en curso a conexión H.225.0. Esto permitirá completar las tomas de contacto MIKEY en un máximo de dos viajes de ida y vuelta.

Para conferir protección contra ataques por degradación durante la negociación de la capacidad, un punto extremo conforme a esta especificación debe observar estrictamente el procedimiento que se describe en la sección 6.15 de RFC 3830 donde el llamante crea una lista de identificadores de protocolos de gestión de claves MIKEY ofrecidos (KMID, *MIKEY key management protocol identifiers*), véase la sección 8.3 RFC www, y la incluye en la cabida útil de la extensión general MIKEY de cada protocolo MIKEY ofrecido.

En el caso de un canal dúplex completo, SRTP se utiliza dos veces, una vez en cada sentido, pero sólo se negocia una clave maestra MIKEY dinámica (TGK) entre los puntos extremo H.323. Los puntos extremo utilizan claves de sesión SRTP direccionales aplicando identificadores de sesión de criptación MIKEY específicos a la función de cálculo de claves MIKEY y SRTP.

8 Perfil de seguridad utilizando técnicas de seguridad simétricas

Esta cláusula describe un perfil de seguridad de esta Recomendación en el que sólo se despliegan técnicas de seguridad simétricas.

En la figura 3 se muestra un escenario en el que se suponen secretos compartidos salto por salto (administrados o configurados) entre las entidades H.323 en el dominio H.323 (*sa*, *sb* y *sl*), lo que permite desplegar seguridad básica conforme a la H.235.1 (autenticación y/o integridad de mensaje) a los protocolos RAS y de señalización de llamada H.225.0. Para garantizar la autenticidad (es decir, la integridad) de los mensajes de señalización intercambiados entre EP B y EP A, se requiere el despliegue de la seguridad básica de la H.235.1 en la modalidad salto por salto.

Se supone que el punto extremo B está sincronizado en el tiempo de forma flexible con el resto de los puntos extremos H.323; de lo contrario MIKEY no puede funcionar de modo seguro.

NOTA – Esta Recomendación no describe ningún medio (seguro) para sincronizar los relojes entre las entidades participantes. Por lo general, se supone que la sincronización de tiempo puede lograrse en las redes corporativas.

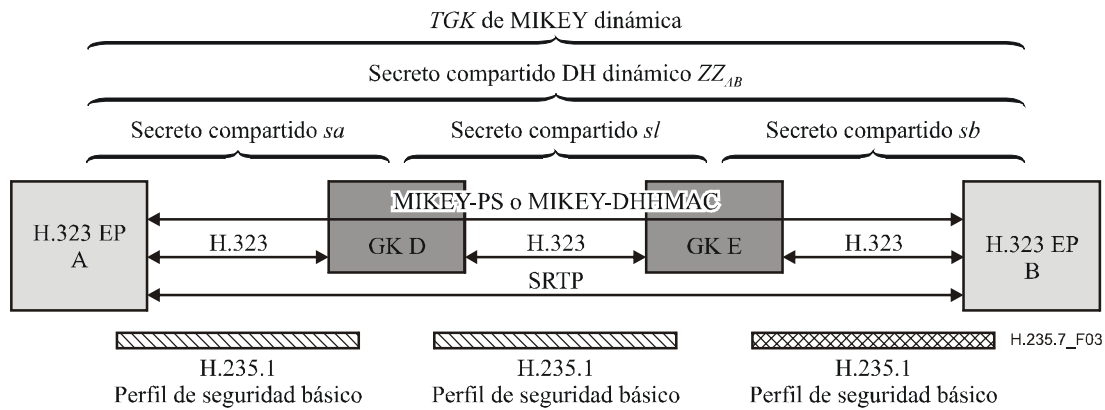


Figura 3/H.235.7 – Caso salto por salto sólo con secretos compartidos

El enfoque básico de este escenario es el despliegue, en el dominio de H.323, del protocolo de distribución de claves MIKEY-PS (simétrico con la utilización de secretos precompartidos) o, cuando hay que garantizar un secreto absoluto hacia adelante, el protocolo de convenio de claves MIKEY-DHHMAC (Diffie-Hellman utilizando HMAC). RFC zzzz se ofrece como una opción que complementa a MIKEY, véase el apéndice I.

Cuando EP B (iniciador de MIKEY) llama a EP A (respondedor de MIKEY), se establece un secreto compartido dinámico ZZ_{AB} entre EP A y EP B como parte del protocolo RAS de H.225.0 y del establecimiento de una comunicación. El secreto compartido dinámico ZZ_{AB} se utiliza más adelante como el secreto precompartido MIKEY, a partir del cual MIKEY en EP A y en EP B deduce la criptación simétrica y las claves de autenticación (no se muestran en esta figura).

El EP B llamante genera la *TGK* de MIKEY (se trata en realidad de una clave maestra) para el EP A par. El EP B crea los mensajes de protocolo MIKEY y encapsula todo el mensaje MIKEY en un contenedor dentro del mensaje tunelizado **TerminalCapabilitySet/OpenLogicalChannel**. El GK E, en un entorno encaminado por GK, simplemente retransmitirá el contenedor MIKEY hacia el otro punto extremo A sin ninguna decodificación del propio MIKEY. El EP A termina el protocolo MIKEY en el dominio H.323.

Así, el EP B y el EP A establecen una *TGK*.

El protocolo MIKEY-PS o MIKEY-DHHMAC funciona entre EP B y EP A. De esta manera, los puntos extremo obtienen la *TGK* y pueden deducir las claves de sesión SRTP/SRTCP. Los protocolos SRTP y SRTCP aplican estas claves de sesión extremo a extremo.

NOTA 1 – MIKEY suministra todos los parámetros necesarios para SRTP (algoritmos, longitudes de clave, tiempo de vida de clave, etc.) como parte de las políticas MIKEY.

Los controladores de acceso no participan activamente en el procesamiento MIKEY y actúan como memorias y retransmisores de los mensajes MIKEY encapsulados.

Cuando el EP A origina un establecimiento de comunicación, el procedimiento es similar en el sentido inverso con EP A como el iniciador y EP B como el destinatario.

NOTA 2 – El escenario que se ilustra en la figura 3 también soporta el modelo de señalización de llamada encaminada directamente con controladores de acceso sin encaminamiento. En ese entorno con encaminamiento directo, los mensajes de señalización de llamada H.225.0 (establecimiento, etc.) serán enviados extremo a extremo dentro del dominio H.323 sin ser retransmitidos por el controlador de acceso. Véanse las ilustraciones en el apéndice II sobre la utilización de H.235.4 para esa finalidad.

NOTA 3 – MIKEY utiliza indicaciones de tiempo dentro del protocolo de seguridad como un medio para garantizar la protección de la reproducción del mensaje de gestión de claves. Esto exige que los relojes de los puntos extremos estén sincronizados flexiblemente en el tiempo (con cierta desviación aceptable de reloj). Se considera que esa sincronización de tiempo puede alcanzarse utilizando relojes configurados manualmente o

algún protocolo de sincronización de tiempo de la red (por ejemplo NTP RFC 1305). De esta manera, la sincronización de tiempo dentro del dominio H.323 debe ser viable al menos en las redes empresariales; véanse también las secciones 5.4 y 9.3 de RFC 3830.

NOTA 4 – No se recomienda la combinación de inicio rápido y medios anticipados junto con el protocolo MIKEY-DHMAC. En caso de que se necesiten, los puntos extremos no deben utilizar MIKEY-DHMAC sino MIKEY-PS.

NOTA 5 – El escenario con un solo controlador de acceso es un caso especial del escenario descrito con múltiples controladores de acceso. En este caso, no se necesita el descubrimiento de controlador de acceso/punto extremo de extremo distante utilizando la petición de localización (LRQ, location request)/confirmación de localización (LCF, location confirmation).

A continuación se presentan flujos de mensaje más detallados para el escenario de la figura 3. Según este escenario, hay uno o varios controladores de acceso con encaminamiento en el dominio H.323, donde los mensajes H.245 se tunelizan dentro de H.225.0 y se aplica el inicio rápido.

NOTA 6 – Los diagramas de flujo cubren también un caso encaminado directamente (con controladores de acceso sin encaminamiento) donde los mensajes de señalización de llamada H.225.0 se intercambian directamente entre los puntos extremos sin ser retransmitidos por ningún controlador de acceso, (véase el apéndice II).

El procedimiento que se describe en esta cláusula permite establecer un secreto compartido extremo a extremo ZZ_{AB} entre los puntos extremos EP A y EP B de H.323 durante la etapa 1 utilizando el convenio de claves Diffie-Hellman, el cual se activa durante la fase de registro y admisión de RAS de H.225.0, y en el caso de múltiples controladores de acceso, durante el intercambio de mensajes LRQ/LCF entre los controladores de acceso. El secreto compartido Diffie-Hellman generado sirve como una clave de autenticación de extremo a extremo y permanece durante la llamada. El protocolo MIKEY-PS (o MIKEY-DHMAC) se activa durante el establecimiento de la comunicación de la etapa 2 de manera independiente y establece los secretos basados en llamada MIKEY para el canal portador.

En el apéndice II se describe un procedimiento alternativo y facultativo utilizando el procedimiento DRC1 de la H.235.4, que permite al controlador de acceso generar y distribuir un secreto compartido a EP A y EP B.

El diagrama de la figura 4 también muestra el perfil de seguridad básico H.235.1 en el que cada mensaje se asegura completamente (autenticación e integridad). No obstante, se producen flujos de mensajes similares cuando se aplica la opción de sólo autenticación del perfil de seguridad básica (no se muestra). En este caso, no se calculará el código de autenticación de mensaje troceado (HMAC, *hashed message authentication code*) sino únicamente de un subconjunto (**ClearToken** dentro de **CryptoToken**) del mensaje RAS/H.225.0.

El ejemplo del flujo del mensaje muestra el caso de EP B (iniciador de MIKEY) llamando a EP A (respondedor de MIKEY) utilizando el arranque rápido (véase la figura 4). Inicialmente, los puntos extremos A y B H.323 se registran con el controlador de acceso utilizando una petición de registro (RRQ, *registration request*) y enviando su media clave DH (g^a y g^b). El **ClearToken** (en **CryptoHashedToken**) se utilizará para transportar la media clave Diffie-Hellman durante RRQ y ACF. Para este fin, no debe utilizarse el campo **challenge**.

La media clave Diffie-Hellman será transportada en **dhkey** como parte de **ClearToken**. Éste utilizará el OID "TG" (véase 8.5) en lugar del OID "T" del ClearToken básico H.235.1, señalando que se está empleando este perfil de seguridad junto con la H.235.1. El controlador de acceso mantendrá cada media clave mientras el punto extremo esté registrado. Al enviar mensajes de actualización de validez (*keep alive*) o hacer un nuevo registro simplificado (re-RRQ), los puntos extremos no deben incluir ninguna media clave DH. La confirmación de registro (RCF, *registration confirm*) debe utilizar el OID "TG" en el **ClearToken** para indicar que el controlador de acceso soporta este perfil de seguridad.

Cuando el EP B trata de llamar al EP A, solicita admisión al controlador de acceso D (petición de admisión (**ARQ**, *admission request*)). La **ARQ** utilizará el OID "TG" en el **ClearToken**. Este OID se utilizará también en cualquier otro mensaje RAS dentro del **ClearToken**.

Este escenario abarca controladores de acceso múltiples, encadenados, aunque también puede soportar igualmente un solo controlador de acceso. El descubrimiento del punto en el extremo distante debe realizarse conforme a 8.1.6/H.323 relativa a "Señalización opcional del punto extremo llamado" utilizando **LRQ/LCF**. Así es como el punto extremo iniciador localiza la zona del GK de extremo distante y obtiene por consiguiente la media clave Diffie-Hellman del punto extremo llamado objetivo. Si el GK E necesita localizar la zona del GK de extremo distante, debe enviar un mensaje **LRQ**. En el caso de la multidifusión, no debe utilizarse el **generalID** en el **CryptoToken** de **LRQ**. Si el GK D no soporta este perfil tendrá que devolver el mensaje de rechazo de localización (**LRJ**, *location reject*), de lo contrario, devolverá **LCF** que incluye la media clave Diffie-Hellman de EP A. A continuación, el GK E contestará con el mensaje de confirmación de admisión (**ACF**, *admission confirm*) incluyendo la media clave Diffie-Hellman del EP A. Si el GK E no puede localizar el punto extremo A del extremo distante, el GK E devolverá el mensaje de rechazo de admisión (**ARJ**, *admission reject*).

La comunicación entre dos controladores de acceso será asegurada conforme a la H.235.1. Para ello, se supone la disponibilidad de un secreto compartido común *sl*. Dado que **LRQ** entre los controladores de acceso normalmente es un mensaje multidifusión, por lo general el secreto compartido *sl* no puede ser un secreto compartido por pares sino que se supone que es en realidad un secreto compartido basado en grupos dentro del posible grupo de controladores de acceso. Este escenario limita la modularidad en el caso general, y no proporciona autenticación del origen. No obstante, se considera que dichas limitaciones de seguridad son aceptables en las redes empresariales con un número pequeño y limitado de controladores de acceso bien identificados. Al asegurar la comunicación multidifusión entre los controladores de acceso mediante el uso de firmas digitales pueden superarse esas limitaciones; no obstante, esto queda en estudio.

El EP B obtiene la media clave Diffie-Hellman del EP A (**ACF**). La **ACF** indicará la clave Diffie-Hellman del punto extremo llamado en **dhkey** dentro de **ClearToken** básico de la H.235.1, pero utilizando el OID "TG" en lugar del "T". Este perfil de seguridad no modificará ningún otro campo dentro de **ClearToken**.

NOTA 7 – Los puntos extremos funcionan con una media clave DH, que es estática durante todo el tiempo de registro y para todas las llamadas. Esto no debe considerarse como una debilidad de seguridad mientras cada punto extremo aplique medias claves verdaderamente aleatorias.

No obstante, los puntos extremos proporcionarán un nuevo valor aleatorio de 512 bits (es decir, 64 octetos) dentro de **challenge** junto con su media clave DH, (véase la sección 2.3 de RFC 2631). Estos valores **challenge** están basados en la llamada e introducen la aleatoriedad y la modularidad de tiempo necesarias en la generación de claves DH.

A continuación el EP B originador podrá calcular g^{ab} y el secreto compartido dinámico ZZ_{AB} utilizando un **challenge** aleatorio con el resultado obtenido a partir de MIKEY-PRF (g^{ab} , $0x12F905FE || \text{challenge}$) (véanse las secciones 4.1.2–4.1.4 de RFC 3830). Luego MIKEY podrá deducir la criptación (*Me*) y las claves de autenticación (*Ma*) empleando MIKEY-PRF (véanse las secciones 4.1.2–4.1.4 de RFC 3830).

Durante la etapa 2, el EP B de originador generará una nueva **TGK** de MIKEY y creará el mensaje **I_message** de MIKEY conforme al protocolo MIKEY-PS utilizando *Me* y *Ma*; además, las claves de sesión SRTP podrán deducirse de la **TGK**, como se describe en la sección 4.3 de RFC 3711 (no se muestra en las figuras).

El mensaje **I_message** de MIKEY se codificará en binario.

El EP B originador siempre debe incluir su media clave DH dentro de **dhkey** en un **ClearToken**, habilitando así el modelo de encaminamiento directo soportado por GK. El **ClearToken** debe

incluirse como parte del mensaje de establecimiento y transmitirse hacia el EP A par. Un controlador de acceso de encaminamiento retransmitirá el **ClearToken** transportado (sin modificar los mensajes MIKEY) al siguiente salto.

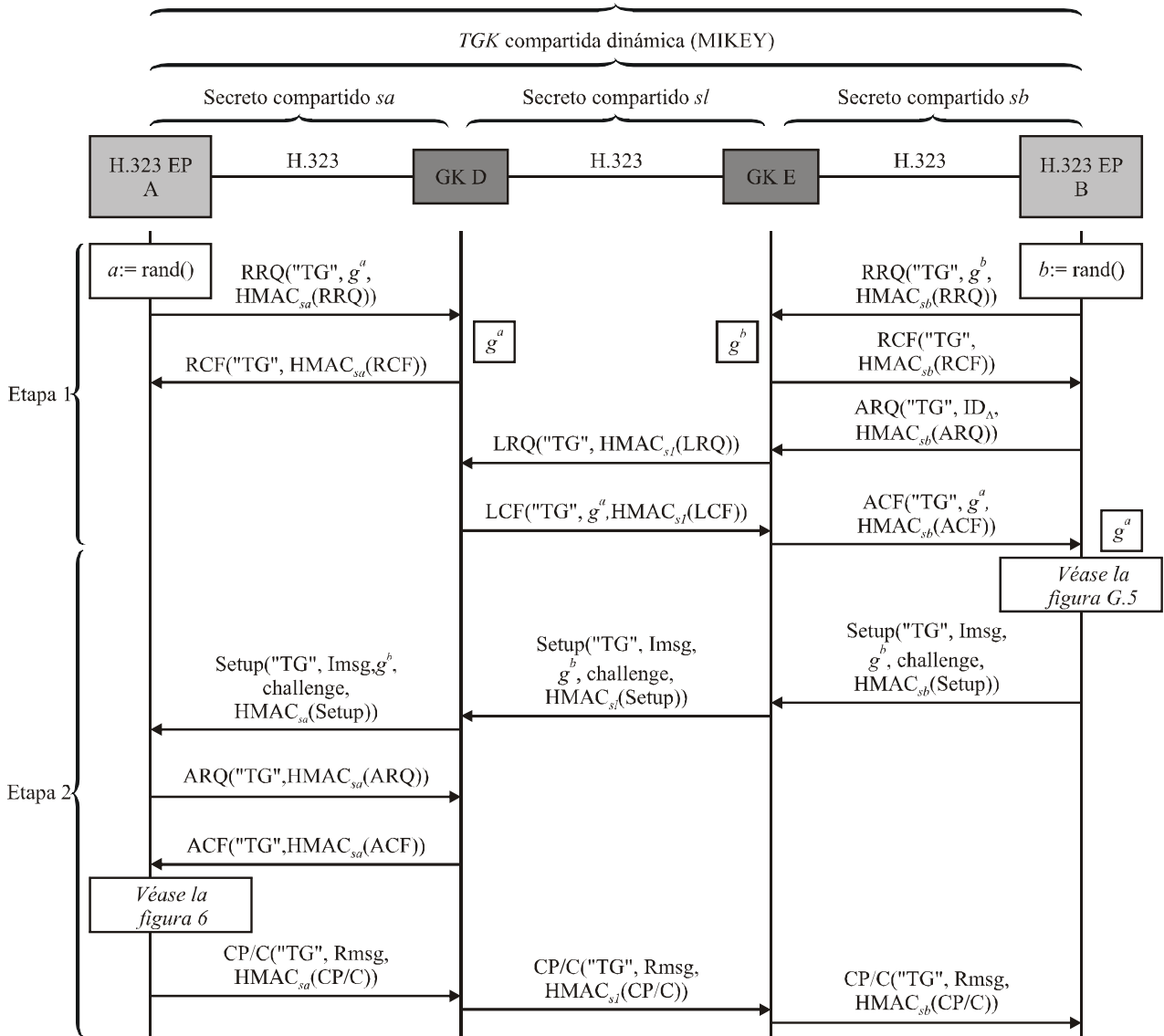
El EP A receptor calculará g^{ab} y el secreto compartido dinámico ZZ_{AB} a partir de MIKEY-PRF (g^{ab} , $0x12F905FE$ || **challenge**) (véanse las secciones 4.1.2–4.1.4 de RFC 3830). Luego MIKEY deduce la criptación (Me) y las claves de autenticación (Ma) utilizando MIKEY-PRF (véanse las secciones 4.1.2–4.1.4 de RFC 3830). A continuación pueden recuperarse las TKG transportadas.

El EP A receptor puede deducir las claves de sesión SRTP a partir de la TKG como se describe en la sección 4.3 de RFC 3711 (no se muestra en las figuras).

El EP A puede crear un mensaje Rmsg R_message similar pero únicamente a petición del EP B o si resulta necesario (DH). Dicho R_message se transporta dentro del mensaje llamada en curso a conexión (CP/C).

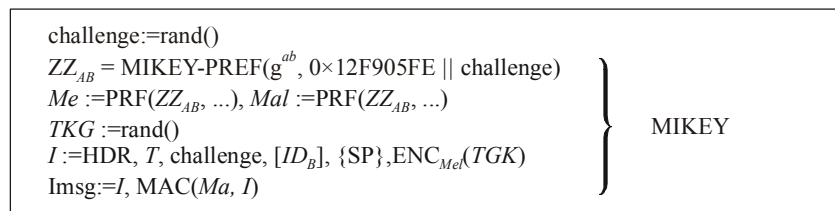
El mensaje llamada en curso a conexión CP/C se envía hacia el EP B.

Secreto compartido dinámico de H.323 $ZZ_{AB} = \text{MIKEY-PRF}(g^{ab}, 0 \times 12F905FE \parallel \text{challenge})$.
 Clave Me de criptación compartida dinámica MIKEY.
 Clave Ma de autenticación compartida dinámica MIKEY



H.235.7_F04

Figura 4/H.235.7 – Ejemplo del punto extremo B llamando al punto extremo A (llamada encaminada por GK) con procesamiento precompartido MIKEY



H.235AnnG_FG.5

Figura 5/H.235.7 – Procesamiento precompartido MIKEY en el EP B

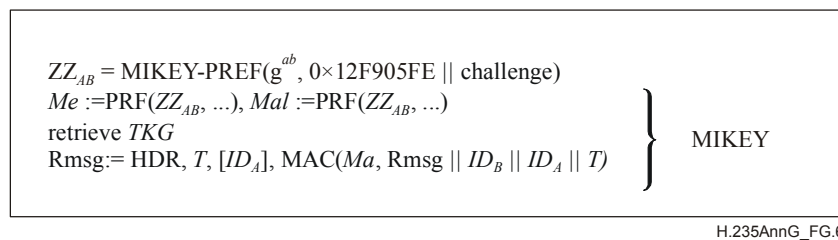


Figura 6/H.235.7 – Procesamiento precompartido MIKEY en el EP A

8.1 Terminación de una llamada H.323

Como los puntos extremos participantes mantienen un estado para MIKEY y SRTP, resulta esencial disponer de un procedimiento adecuado de terminación. La figura 7 muestra un ejemplo de flujos de mensaje en el caso de que el EP B (iniciador de MIKEY) termine una llamada. Básicamente el flujo es conforme a 8.5/H.323 relativa a "Fase E – Terminación de la llamada".

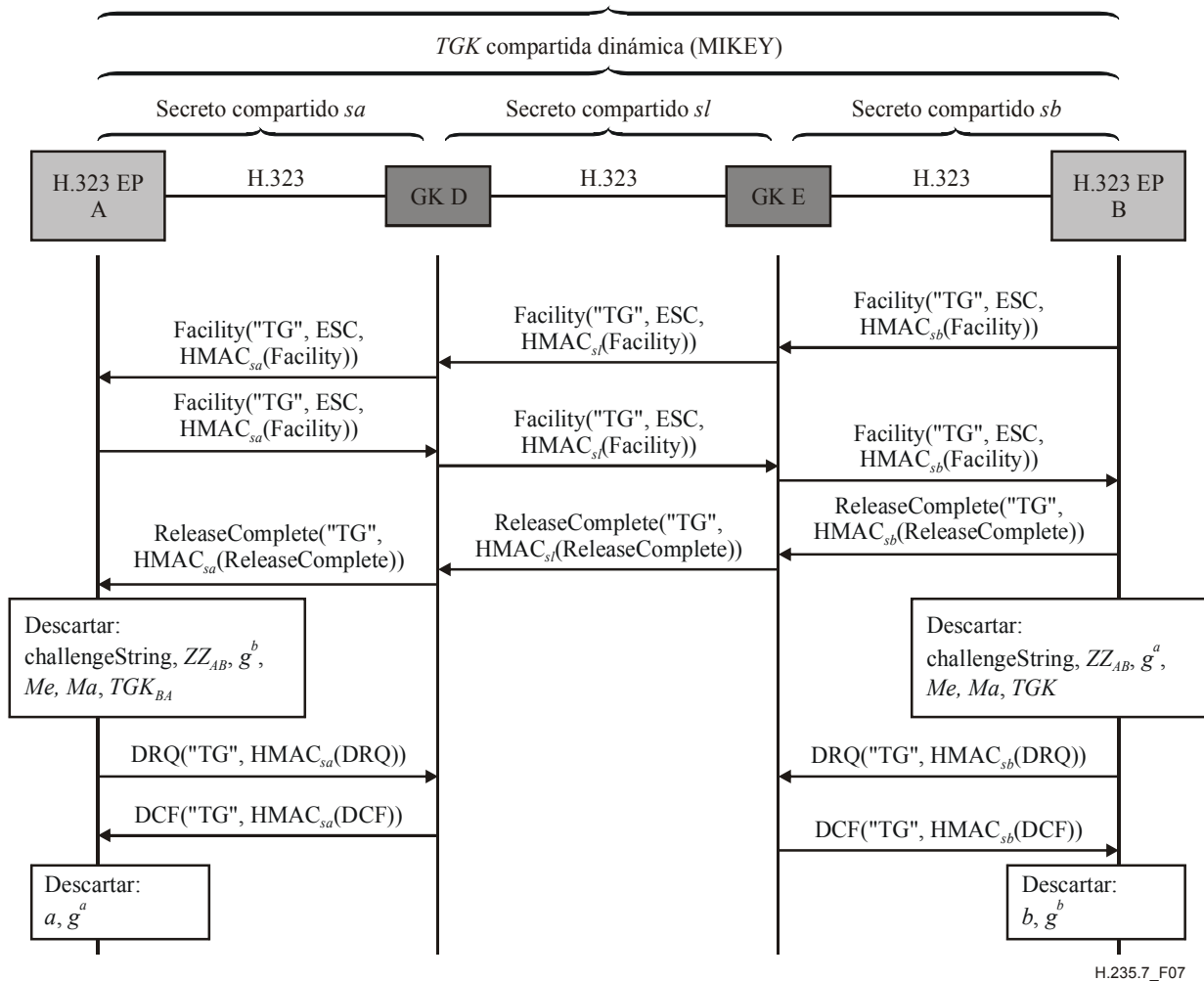
NOTA – La figura muestra también los procedimientos de desconexión facultativos para el caso en que los puntos extremos cancelan su registro completamente. A continuación los puntos extremo deben descartar también la clave DH privada (*a* o *b*) y la media clave DH pública (g^a o g^b).

Como el procedimiento de terminación de una llamada es independiente de este perfil de seguridad, puede utilizarse cualquier OID aplicable del perfil de seguridad subyacente (H.235.1, H.235.3, etc.); por consiguiente, en la figura 7 no se muestra ningún OID.

Si el punto extremo ha de registrarse nuevamente con el controlador de acceso, tendrán que generarse nuevas medias claves DH. Ahora bien, no es necesaria una anulación completa del registro en ninguna circunstancia sólo por la terminación de la llamada. Si el punto extremo decide permanecer registrado con el controlador de acceso, puede seguirse utilizando las medias claves DH estáticas.

Si los puntos extremos permanecen registrados y no se aplica el proceso de desconexión, descartarán únicamente la información relacionada con la llamada incluida la media clave DH del par, el **challenge**, las claves *Me*, *Ma*, de MIKEY, la *TKG* y la información de sesión SRTP relacionada.

Secreto compartido dinámico de H.323 $ZZ_{AB} = \text{MIKEY-PRF}(g^{ab}, 0x12F905FE || \text{challenge})$,
 Clave Me de criptación compartida dinámica de MIKEY,
 Clave Ma de autenticación compartida dinámica de MIKEY



H.235.7_F07

Figura 7/H.235.7 – Ejemplo del punto extremo B terminando una llamada

8.2 Creación de nuevas claves TGK y actualización del CSB

MIKEY dispone de un soporte integrado para la creación de nuevas claves TGK y/o la actualización de información del CSB. El perfil de esta Recomendación utilizará el procedimiento MIKEY-PS de la sección 4.5 de RFC 3830, o cuando hay que garantizar un secreto absoluto hacia adelante, la sección 3.1 de RFC zzzz para esta finalidad, lo que permitirá la actualización de la TGK antes de su expiración o la actualización de otra información sin modificar la TGK.

El mecanismo de creación de nuevas claves TGK y de actualización del CSB es útil para proteger un agrupamiento de canales lógicos con arreglo a la misma política de seguridad. Para ello, se recomienda activar el protocolo precompartido MIKEY (completo) como se describe en la cláusula 8 únicamente para el primer canal lógico. Cualquier canal lógico subsiguiente que tenga que aplicar la misma política de seguridad MIKEY o la misma TGK, deberá utilizar el mecanismo de actualización del CSB sin el mecanismo de creación de nuevas claves TGK de esta cláusula, haciendo referencia al CSB-ID inicial y omitiendo los datos TGK actualizados. Esto permite establecer canales lógicos o sesiones criptadas MIKEY de una manera más eficiente que haciendo funcionar todo el protocolo MIKEY en cada canal lógico.

Los mensajes de creación de nuevas claves TGK de MIKEY o de actualización del CSB serán encapsulados y transportados en una **MiscellaneousCommand** en un mensaje Facility. El **tokenOID** del **ClearToken** se fijará a "TG".

Si el protocolo MIKEY funciona en "nivel de medios", el EP B tendrá que determinar por cuál canal lógico deberá aplicarse la creación de nuevas claves TGK y/o la actualización del CSB. El EP A, en su calidad de respondedor, deberá emplear igualmente **MiscellaneousCommand** en Facility para transportar el mensaje R_message de MIKEY (si lo hubiera).

Para la creación de nuevas claves TGK (véase la figura 8), el EP B, en su calidad de iniciador de MIKEY, tendrá que generar una nueva TGK.

El EP A, en su calidad de respondedor, puede confirmar el mensaje de creación de nuevas claves TGK obtenido, si es necesario a petición del EP B. El EP A creará mensajes R_messages similares. El EP B envía R_message en el mensaje Facility hacia el EP A.

Para la actualización del CSB, el procedimiento antes descrito es similar excepto que el mensaje MIKEY no mantendrá ninguna TGK.

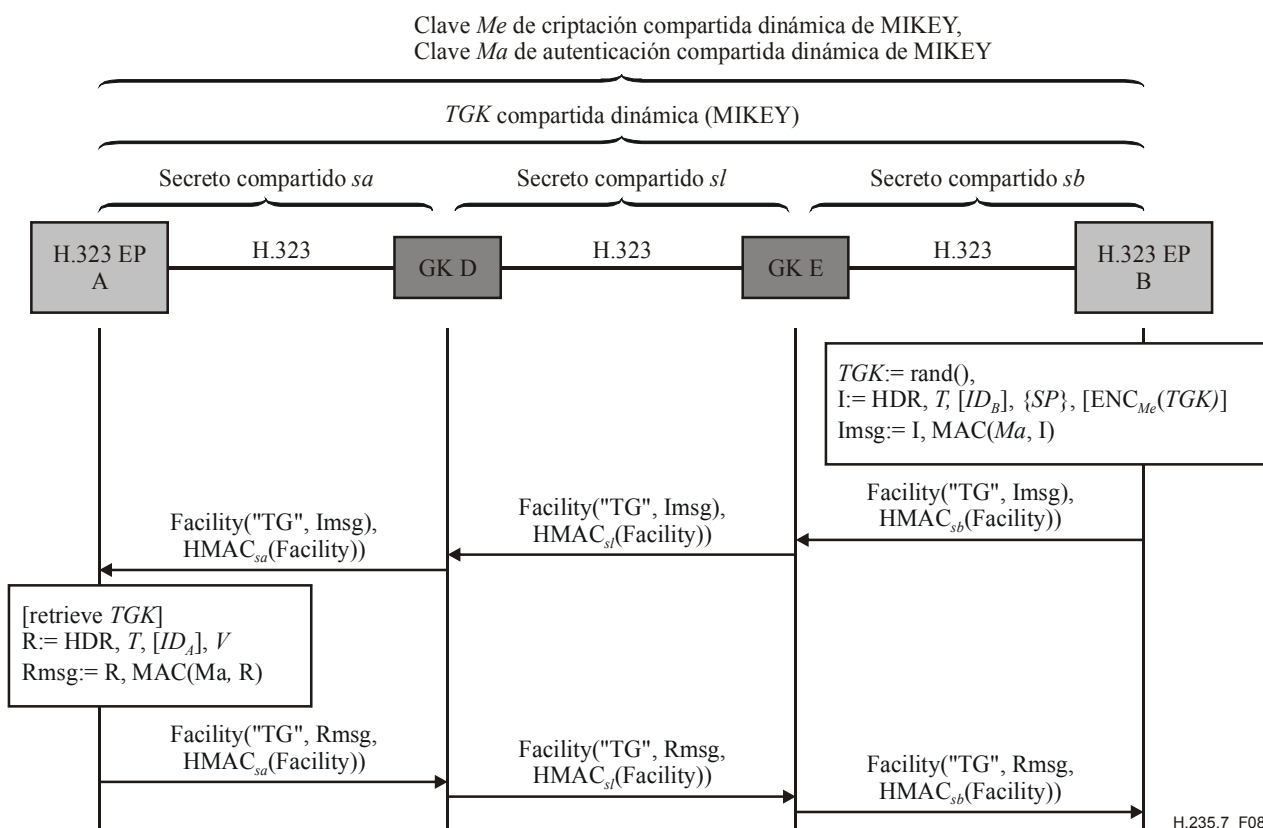


Figura 8/H.235.7 – Ejemplo del punto extremo B actualizando una clave

NOTA – El mensaje Facility de confirmación del EP A al EP B es facultativo y sólo es necesario cuando el EP B también ha solicitado un mensaje de verificación R_message de MIKEY fijando la bandera V en MIKEY HDR.

Esta Recomendación no describe ningún procedimiento para la creación de nuevas claves TGK y/o la actualización del CSB invocado por el respondedor; esto queda en estudio.

8.3 Soporte de tunelización H.245

Si es necesario que se añadan más canales lógicos durante una sesión, se utilizará el modo de tunelización H.245; los mensajes H.245 tunelizados se transportan en un mensaje Facility.

8.4 Algoritmos SRTP

Este perfil de seguridad utilizará el HMAC-SHA1-32 truncado con una longitud de etiqueta de autenticación n_tag igual a 32 bits como algoritmo de autenticación por defecto para RTP. También

podrán soportarse otras longitudes de etiqueta de autenticación como las definidas en RFC 3711, que podrán negociarse a través del parámetro de política de seguridad (SP) MIKEY, según proceda.

8.5 Lista de identificadores de Objetos

"TG"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 70}	Indica un ClearToken básico de la H.235.1 en el contexto de esta Recomendación. Este OID también indica que el protocolo MIKEY-PRF se utiliza para calcular el secreto compartido ZZ _{AB} .
------	--	---

9 Perfil de seguridad que utiliza técnicas de seguridad asimétricas

En esta cláusula se describe un perfil de seguridad de esta Recomendación con técnicas de seguridad asimétricas. Este escenario ofrece mayor modularidad.

No siempre se acepta la existencia de entidades intermediarias (es decir, controladores de acceso) que pueden interceptar las TGK de MIKEY y/o las claves de sesión SRTP. La figura 9 a continuación ilustra un escenario en el que se despliega una infraestructura de claves públicas (PKI) para establecer claves de medios SRTP extremo a extremo.

Postulados: Se supone que tanto EP A como EP B poseen una clave privada (*SK*), así como una clave pública certificada (*cert*). Sin embargo, EP A y GK E, así como EP B y GK D, pueden intercambiar secretos compartidos (administrados/configurados) cuando se utilice H.235.1 para la seguridad del protocolo RAS y la señalización de la llamada H.225.0. Además, se supone que EP A y EP B se sincronizan flexiblemente en tiempo, ya que de lo contrario MIKEY no podría funcionar de modo seguro.

La autenticación/integridad de los mensajes puede lograrse utilizando secretos compartidos salto por salto preconfigurados (*sa*, *sb* y *sl*) y el perfil de seguridad básico de H.235.1 o, de manera más general, empleando PKI para establecer secretos compartidos dinámicos con el perfil de seguridad híbrido H.235.3.

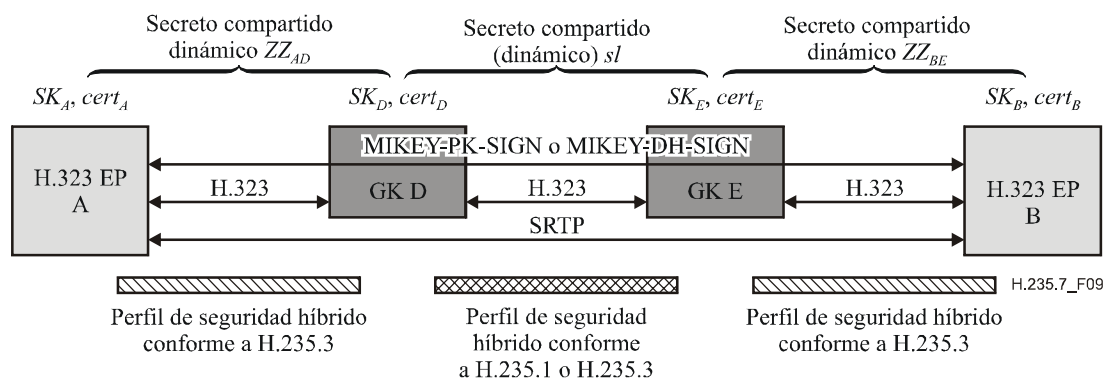


Figura 9/H.235.7 – Escenario de extremo a extremo utilizando PKI (múltiples GK)

EP A y EP B aplican MIKEY-PK-SIGN o MIKEY-DH-SIGN de extremo a extremo y de ese modo establecen la TGK de MIKEY a partir de la cual los sistemas de extremo deducen las claves de sesión SRTP.

NOTA 1 – MIKEY-PK-SIGN satisface el requisito de una gestión de claves basada en RSA.

NOTA 2 – El entorno H.323 más general que se caracteriza por múltiples controladores de acceso encadenados en una hilera, estará mejor protegido sin lugar a duda al utilizar técnicas PKI en lugar de arquitecturas limitadas y con menor capacidad evolutiva que emplean técnicas de seguridad simétricas.

NOTA 3 – No se recomienda combinar el arranque rápido y los medios anticipados en conjunto con el protocolo MIKEY-DH-SIGN, pero si éstos son necesarios, los puntos extremos no deben utilizar MIKEY-DH-SIGN sino MIKEY-PK-SIGN.

En los siguientes párrafos se presentan flujos de mensajes más detallados conformes al escenario de la figura 9. En éste se muestran múltiples controladores de acceso en el dominio de H.323.

En las siguientes figuras se supone nuevamente un controlador de acceso de encaminamiento (modelo encaminado por GK) donde el mensaje H.245 se tuneliza dentro de H.225.0 (arranque rápido).

NOTA 4 – Los diagramas de flujo abarcan también un caso encaminado directamente (con un controlador de acceso sin encaminamiento), en el cual los mensajes de señalización de llamadas H.225.0 son intercambiados directamente entre los puntos extremos sin necesidad de ser retransmitidos por ningún controlador de acceso.

Los diagramas también muestran el perfil de seguridad híbrido H.235.3 con protección integral de los mensajes RAS iniciales (autenticación e integridad) utilizando firmas digitales y certificados facultativos. Esto permite establecer secretos compartidos dinámicos ZZ_{BE} y ZZ_{AD} entre los puntos extremos y el controlador de acceso del salto siguiente, con lo cual los secretos compartidos estáticos resultan innecesarios. No obstante, se producen flujos de mensajes similares cuando se aplica la opción de sólo autenticación del perfil de seguridad de firma (no se muestra).

El ejemplo del flujo de mensajes ilustra el caso en el que EP B (iniciador de MIKEY) llama al EP A (respondedor de MIKEY) (véase la figura 10).

Durante la etapa 1, los puntos extremos H.323 se registran inicialmente con el controlador de acceso del siguiente salto y envían sus medias claves DH (g^a y g^b).

Cuando el EP B está tratando de llamar al EP A, solicita la admisión al controlador de acceso E. El EP B puede pedir el certificado del par *certC* incluyendo un elemento del perfil de seguridad en el **ClearToken**, en caso de que la información del certificado aún no esté disponible para el EP. Este elemento de perfil de seguridad debe utilizar los siguientes campos:

- **elementID** con el valor 7 para señalar un elemento de petición de certificado; la figura 10 lo muestra como certFlag;
- **paramS** no se utiliza;
- **element** indica un elemento con **flag** fijada a VERDADERO.

El mensaje ARQ y cualquier mensaje posterior RAS y de señalización de llamada H.225.0 se protegen mediante el secreto compartido dinámico ZZ_{BE} utilizando el perfil de seguridad básico H.235.1. Si el EP B solicita consultar el certificado, el GK E recoge el certC de un depósito local o de otro depósito de certificados y entrega el (los) resultado(s) como parte de la ACF dentro de **certificate** del **ClearToken** e incluye un elemento de perfil de seguridad. Este elemento empleará los siguientes campos:

- **elementID** con el valor 8 para señalar un elemento de respuesta de certificado; la figura 10 lo muestra como certFlag;
- **paramS** no se utiliza;
- **element** indica un elemento donde **flag** se fija a VERDADERO.

Si el controlador de acceso obtiene múltiples certificados para un punto extremo/UA par, el mensaje ACF contendrá en realidad múltiples ClearTokens, cada uno transportando un certificado simple dentro de **certificate**. A continuación, el punto extremo seleccionará el más apropiado. No obstante, puede suceder que la consulta de certificado tome demasiado tiempo, por ejemplo, cuando se trata de depósitos externos. Si el controlador de acceso no puede aportar el certificado(s) oportuna o definitivamente, el mensaje ACF es devuelto con un **certificate** vacío en el ClearToken, que indica un elemento de perfil de seguridad con las siguientes características:

- **elementID** con el valor 8 para indicar un elemento de respuesta de certificado;

- **paramS** no se utiliza;
- **element** indica un elemento donde **flag** se fija a FALSO.

El punto extremo tendrá la tarea de suspender el intento y tratar de localizar el certificado apropiado por medios no especificados en esta Recomendación. Si el controlador de acceso es capaz de recibir el certificado fuera del límite temporal de respuesta necesario, debe indicarlo dejando **certificate** vacío e incluyendo un elemento de perfil de seguridad dentro de ClearToken donde:

- **elementID** con el valor 8 para indicar un elemento de respuesta de certificado;
- **paramS** no se utiliza;
- **element** indica un elemento donde **flag** se fija a VERDADERO;

En este caso, el GK devolverá este ClearToken dentro de ACF.

Durante la etapa 2, el EP B originador (iniciador de MIKEY) puede generar la nueva TGK de MIKEY, y calcular el mensaje Imsg I_message de MIKEY aplicando el protocolo de gestión de claves MIKEY-PK-SIGN (véanse las figuras 11 y 12); cuando hay que garantizar un secreto absoluto hacia adelante se aplica el protocolo de convenio de claves MIKEY-DH-SIGN (Diffie-Hellman empleando firmas digitales), a título de opción.

Las claves de sesión SRTP pueden deducirse de la TGK como se describe en la sección 4.3 de RFC 3711 (no se muestra en las figuras).

NOTA 5 – Las figuras 11 y 12 no muestran todos los detalles de MIKEY, y algunas partes no se muestran en el cuadro.

El mensaje I_message de MIKEY se codifica en binario y se encapsula en el **OpenLogicalChannel** de H.245.

El **ClearToken** se incluye como parte del mensaje de establecimiento y se envía hacia el EP A. Un controlador de acceso de encaminamiento retransmite el mensaje I_message de MIKEY (sin modificar el mensaje MIKEY) al siguiente salto.

Si hay múltiples controladores de acceso de encaminamiento, los mensajes de señalización de llamada entre los controladores de acceso pueden obtenerse aplicando un secreto compartido administrado y utilizando la H.235.1 o la H.235.3 y claves privadas/públicas.

El EP A puede deducir las claves de sesión SRTP a partir de la TGK como se describe en la sección 4.3 de RFC 3711 (no se muestra en las figuras).

El EP A, en su calidad de respondedor de MIKEY, puede compilar el mensaje Rmsg R_message de MIKEY utilizando la clave *Ma* de MIKEY e incluyendo el mensaje R_message de MIKEY en el mensaje llamada en curso a conexión (CP/C).

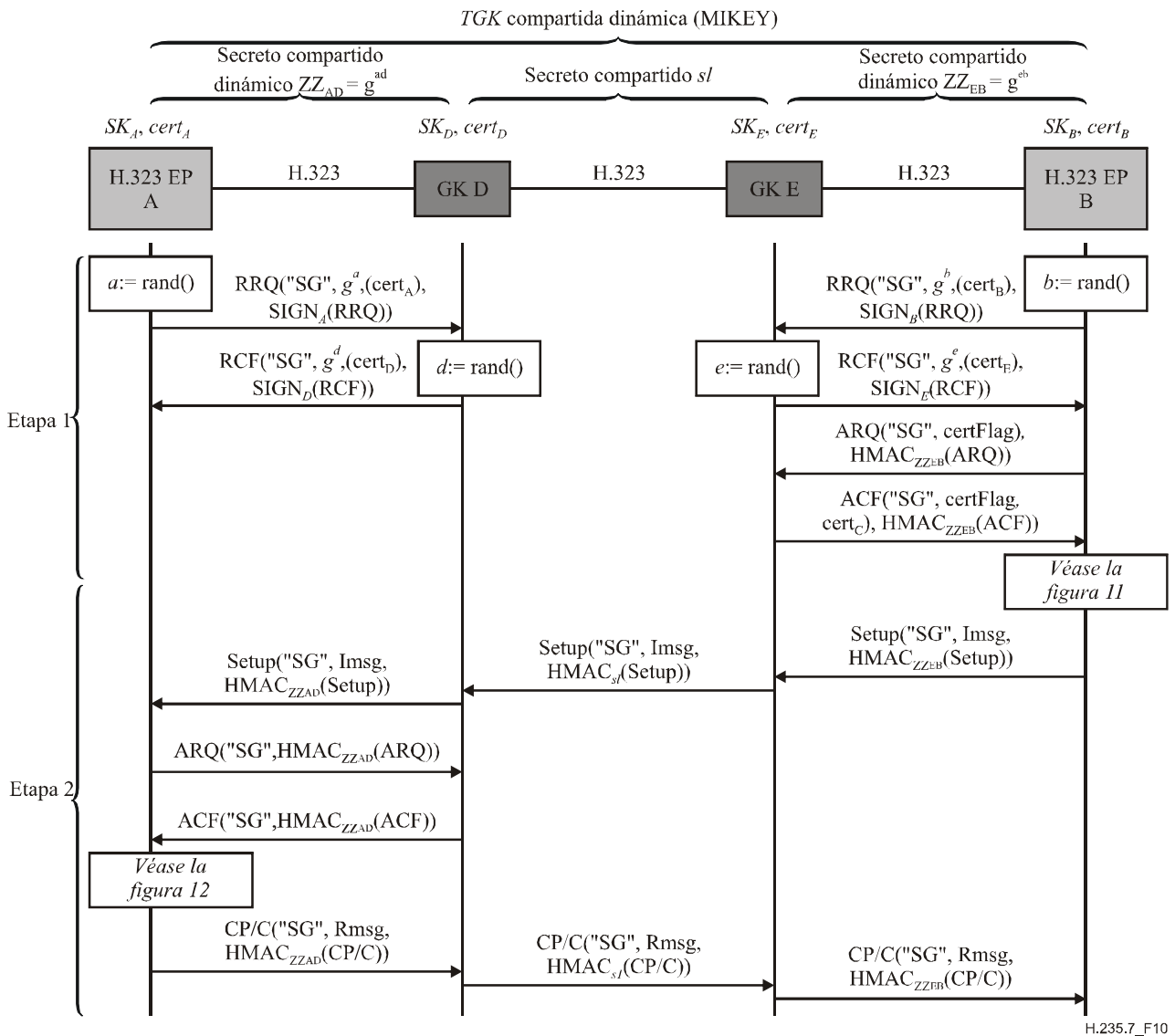


Figura 10/H.235.7 – Ejemplo del EP B llamando al EP A (llamada encaminada por múltiples GK) con protocolo MIKEY-PK-SIGN

```

TGK := rand()
env-key := rand()
Me, Ma := PRF(env-key, ... || Rand)
PKE := ENCPK-A(env-key, ... || Rand)
K := ENCMe(IDB || [TGK])
KEMAC := ENCMe(IDB || [TGK])
M := HMAC-SHA1(Ma, K)
I := HDR, T, rand(), [IDB | CertB], {SP}, [chash], KEMAC, PKE
Imsg := I, SignSK-B(I)

```

Figura 11/H.235.7 – Procesamiento del protocolo MIKEY-PK-SIGN por el EP B

Retrieve env-key, T_{GK}
 $Ma := \text{PRF}(\text{env-key}, \dots \| \text{Rand}),$
 $\text{Rmsg} := \text{HDR}, T, [\text{ID}_A], \text{HMAC-SHA1}(Ma, \text{Rmsg} \| \text{ID}_A \| \text{ID}_B \| T)$

Figura 12/H.235.7 – Procesamiento del protocolo MIKEY-PK-SIGN por el EP A

Un escenario con un solo controlador de acceso representa un caso especial del escenario con múltiples controladores de acceso. En este caso, no es necesario el descubrimiento del controlador de acceso/punto extremo de extremo distante utilizando LRQ/LCF.

9.1 Terminación de una llamada H.323

Como los puntos extremos participantes mantienen el estado MIKEY y SRTP, resulta esencial un procedimiento adecuado de terminación. La figura 13 muestra un ejemplo de flujos de mensajes en el caso en que el EP B (iniciador de MIKEY) termina una llamada. Básicamente, el flujo es conforme a 8.5/H.323 relativa a "Fase E – Terminación de la llamada".

NOTA – En la figura 13 se muestran también los procedimientos de desconexión facultativos para el caso en el que los puntos extremos cancelan su registro completamente. En tal caso, los puntos extremos deben descartar también la media clave DH privada (a o b) y la media clave DH pública (g^a o g^b).

Como el procedimiento de terminación de una llamada es independiente de este perfil de seguridad, podrá utilizarse cualquier OID aplicable del perfil de seguridad subyacente; por esta razón, la figura 13 no muestra ningún OID.

Si el punto extremo requiere registrarse nuevamente con el controlador de acceso, deberán generarse nuevas medias claves DH. No obstante, no se requiere una anulación de registro completa bajo ninguna circunstancia simplemente para la terminación de la llamada. Si el punto extremo decide permanecer registrado con el controlador de acceso, puede seguir utilizando las medias claves DH estáticas.

Si los puntos extremos permanecen registrados y no se aplica la desconexión, éstos deben descartar solamente la información relacionada con la llamada, incluida la media clave DH par, el **challenge**, las claves MIKEY Me , Ma , la TGK y la información de sesión SRTP relacionada.

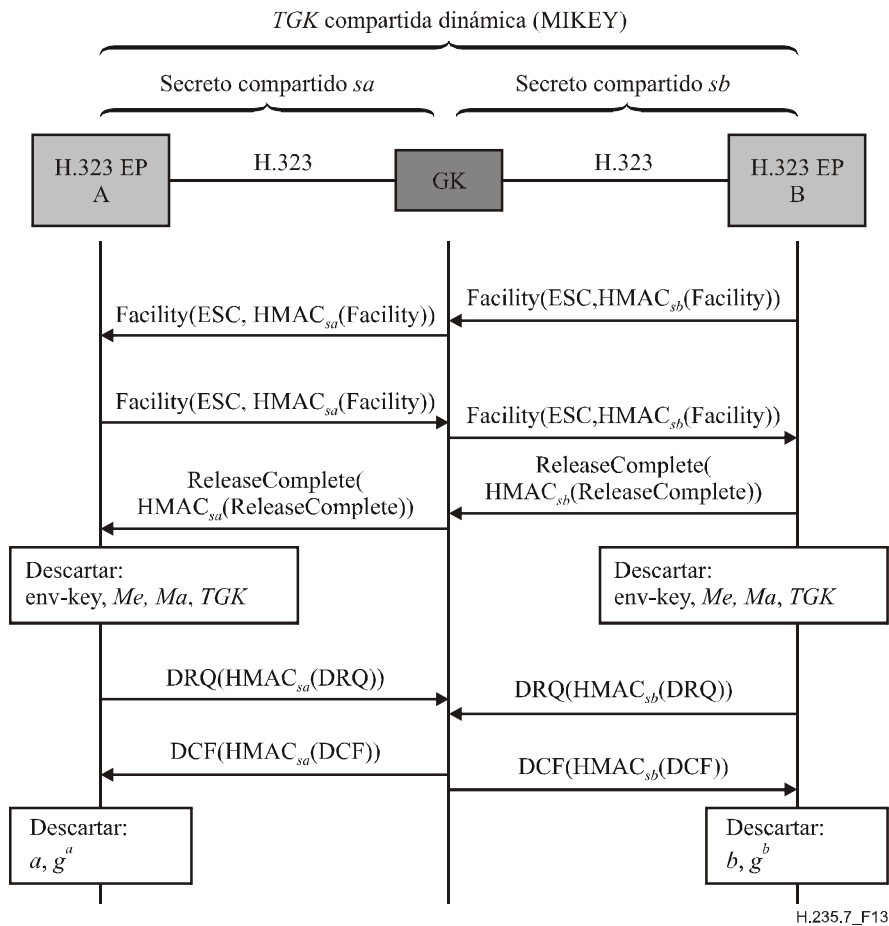


Figura 13/H.235.7 – Ejemplo de terminación de llamada por el punto extremo B

9.2 Creación de nuevas claves TGK y actualización del CSB

MIKEY dispone de soporte integrado para la creación de nuevas claves TGK y/o la actualización de información del CSB. Esta Recomendación utilizará el procedimiento MIKEY-PK-SIGN de la sección 4.5 de RFC 3830 para esta finalidad, que permite actualizar la TGK antes de la expiración o actualizar otra información (CSB) sin modificar la TGK.

El mecanismo de creación de nuevas claves TGK y de actualización del CSB resulta útil para proteger un agrupamiento de canales lógicos conforme a la misma política de seguridad. Para ello, se recomienda activar el protocolo MIKEY-PK-SIGN (completo) como se describe en la cláusula 8 sólo para el primer canal lógico. Cualquier canal lógico subsiguiente al que se aplique la misma política de seguridad MIKEY o la misma TGK, debe utilizar el mecanismo de actualización del CSB sin el mecanismo de creación de nuevas claves TGK de dicha cláusula, haciendo referencia al CSB-ID inicial y omitiendo los datos de la TGK actualizada. Esto permite establecer canales lógicos o sesiones criptadas MIKEY de una manera más eficiente que haciendo funcionar el protocolo MIKEY completo en cada canal lógico.

Los mensajes de creación de nuevas claves TGK de MIKEY o de actualización del CSB estarán incluidos en **MiscellaneousCommand** de un mensaje Facility. El **tokenOID** del **ClearToken** se fijará a "SG".

Cuando el protocolo MIKEY funciona en el "nivel de medios", el EP B ha de determinar en qué canal lógico debe aplicar la creación de nuevas claves TGK y/o la actualización del CSB. El EP A, en su calidad de respondedor, debe utilizar del mismo modo **MiscellaneousCommand** en el mensaje Facility para transportar el mensaje R_message de MIKEY (si lo hubiere).

Para la creación de nuevas claves TGK (véase la figura 14), el EP B, como iniciador de MIKEY, debe generar una nueva TGK. **mikey** mantendrá el mensaje I_message de MIKEY correspondiente.

El respondedor (EP A) puede confirmar el mensaje de creación de claves TGK recibido cuando resulte necesario o cuando lo solicite el EP B. El EP A crea un mensaje Rmsg R_message similar, el cual se transporta en el mensaje Facility. Rmsg es el mensaje de respuesta MIKEY correspondiente y debe transportarse en **octetString** del **GenericParameter**. El EP A envía el mensaje Facility al EP B.

En el caso de una actualización del CSB activada por el iniciador, el procedimiento antes descrito será similar excepto que el mensaje MIKEY no mantendrá ninguna TGK (véase la figura 14).

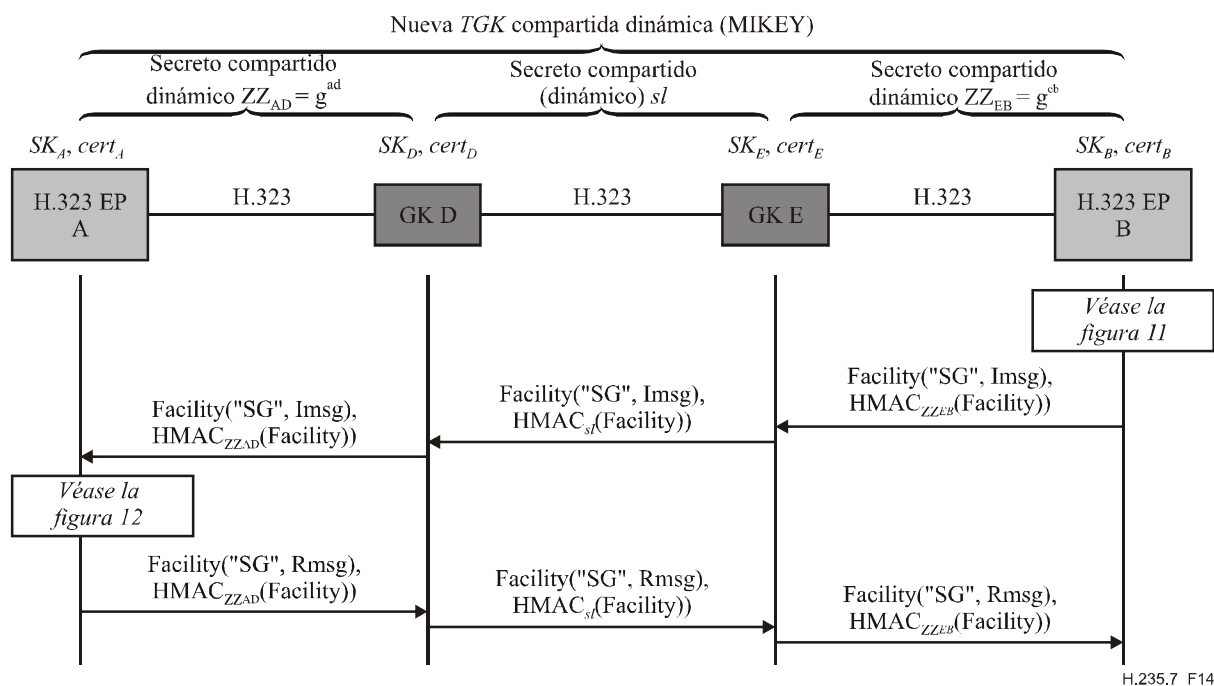


Figura 14/H.235.7 – Ejemplo de iniciación de la creación de nuevas claves TGK y actualización de claves por el EP B (iniciador)

NOTA – El mensaje Facility de confirmación del EP A al EP B es facultativo y sólo es necesario cuando el EP B también solicita un mensaje de verificación R_message de MIKEY fijando la bandera V en MIKEY HDR.

En esta Recomendación no se define ningún procedimiento para la creación de nuevas claves TGK y/o la actualización del CSB invocado por el respondedor; esto queda en estudio.

9.3 Soporte de tunelización H.245

Si durante una sesión deben añadirse más canales lógicos, se utilizará el modo de tunelización H.245; los mensajes H.245 tunelizados se transportan en un mensaje Facility.

9.4 Algoritmos SRTP

Este perfil de seguridad utilizará el método HMAC-SHA1-32 truncado con una longitud de etiqueta de autenticación n_{tag} de 32 bits como algoritmo de autenticación por defecto para RTP. Podrán soportarse otras longitudes de etiqueta de autenticación como las definidas en RFC 3711 y negociarse también a través del parámetro de política de seguridad (SP) de MIKEY según proceda.

9.5 Lista de identificadores de objeto

"SG"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 71}	Indica un ClearToken básico de la H.235.3 en el contexto de esta Recomendación.
------	---	---

Apéndice I

Opción MIKEY-DHHMAC

En este apéndice se describe la manera en la que se debe desplegar la opción de gestión de claves MIKEY-DHHMAC en este perfil de seguridad.

Esta opción supone sólo una infraestructura de seguridad con claves compartidas. MIKEY-DHHMAC (RFC zzzz) ofrece la propiedad de seguridad de secreto absoluto hacia adelante (PFS, *perfect-forward secrecy*) gracias a la capacidad inherente del mecanismo Diffie-Hellman. Así pues, esta opción de gestión de claves puede aplicarse cuando se necesita una garantía PFS y no se dispone de PKI ni de certificados digitales.

En este escenario se suponen controladores de acceso en el dominio H.323.

El procedimiento que se describe en esta cláusula permite establecer un secreto compartido extremo a extremo entre los puntos extremos EP A y EP B de H.323 utilizando un esquema de convenio de claves Diffie-Hellman. Éste se establece durante la fase de registro y admisión de RAS H.225.0, y en el caso de múltiples controladores de acceso, durante el intercambio de mensajes LRQ/LCF entre los controladores de acceso. El secreto compartido Diffie-Hellman generado sirve como una clave de autenticación extremo a extremo que permanece durante toda la llamada. El protocolo MIKEY-DHHMAC se activa durante el establecimiento de la comunicación de modo independiente y permite establecer los secretos basados en llamada de MIKEY para el canal portador.

La figura I.1 es un ejemplo en el cual el punto extremo B llama al punto extremo A través de un GK de encaminamiento. El flujo es similar al de la figura 4, excepto que se despliega el protocolo MIKEY-DHHMAC. El escenario supone uno o varios controladores de acceso de encaminamiento (modelo encaminado por GK) donde los mensajes H.245 son tunelizados dentro de H.225.0 (arranque rápido). La señalización de la llamada puede pasar a través de un controlador de acceso, o no hacerlo; así pues, no es necesario un controlador de acceso de encaminamiento para soportar este caso.

NOTA 1 – El diagrama de flujo abarca también un caso de encaminamiento directo (con controladores de acceso sin encaminamiento) donde los mensajes de señalización de llamada H.225.0 son intercambiados directamente entre los puntos extremos sin necesidad de retransmitirlos a través de ningún controlador de acceso.

El diagrama de la figura I.1 también muestra el perfil de seguridad básico H.235.1, en el que cada mensaje se asegura completamente (autenticación e integridad). No obstante, se producen flujos de mensajes similares cuando se aplica la opción de sólo autenticación del perfil de seguridad básico (no mostrado). En este caso, el HMAC no será calculado para todo el mensaje, sino únicamente para un subconjunto (**ClearToken** dentro de **CryptoToken**) del mensaje RAS/H.225.0.

El ejemplo del flujo de mensaje muestra el caso de un EP B (iniciador de MIKEY) que llama al EP A (respondedor de MIKEY) utilizando el arranque rápido (véase la figura I.1). Durante la etapa 1, los puntos extremos A y B H.323 se registran inicialmente ante el controlador de acceso utilizando **RRQ** y envían sus medias claves DH (g^a y g^b). El **ClearToken** (en **CryptoHashedToken**) será empleado para transportar la media clave Diffie-Hellman durante **RRQ** y **ACF**. Para esta finalidad, no debe utilizarse el campo **challenge**.

La media clave Diffie-Hellman será transportada en **dhkey** como parte del **ClearToken**. Este último utilizará el OID "TG" (véase 8.5) en lugar del OID "T" del ClearToken básico H.235.1, para indicar que este perfil de seguridad se está utilizando junto con la H.235.1. El controlador de acceso mantendrá cada media clave mientras el punto extremo esté registrado. Cuando los puntos extremos envían mensajes de actualización de validez (*keep-alive*) o hacen un nuevo registro simplificado (re-RRQ) no incluirán ninguna media clave DH. La **RCF** utilizará el OID "TG" en el ClearToken para indicar que el controlador de acceso soporta este perfil de seguridad.

Si el EP B trata de llamar al EP A, solicita admisión al controlador de acceso D (**ARQ**). La **ARQ** utilizará el OID "TG" en el ClearToken. Este OID será empleado en cualquier otro mensaje RAS también dentro de ClearToken.

El escenario abarca múltiples controladores de acceso encadenados. El descubrimiento del punto extremo distante debe llevarse a cabo conforme a 8.1.6/H.323 relativa a "Señalización opcional del punto extremo llamado" utilizando **LRQ/LCF**. Así, el punto extremo iniciador localiza la zona del GK de extremo distante y obtiene por consiguiente la media clave Diffie-Hellman del punto extremo llamado tomado como objetivo. Si el GK E necesita localizar la zona del GK del extremo distante, enviará un mensaje **LRQ**. Para el caso de multidifusión, no debe utilizarse el generalID en el CryptoToken de **LRQ**. Si el GK D no soporta este perfil devolverá el mensaje **LRJ**. De lo contrario, devolverá la **LCF** que incluye la media clave Diffie-Hellman del EP A. A continuación, el GK E contestará con **ACF** incluyendo la media clave Diffie-Hellman del EP A. Si el GK E no ha podido localizar el punto extremo distante A, devolverá el mensaje **ARJ**.

La comunicación entre dos controladores de acceso se establecerá conforme a H.235.1. Para ello, se supone que está disponible un secreto compartido común *sl*. Como **LRQ** entre los controladores de acceso es normalmente un mensaje multidifusión, el secreto compartido *sl* por lo general no puede ser un secreto compartido entre un par sino que se supone que es en realidad un secreto compartido por un grupo de los posibles controladores de acceso. Este postulado limita la capacidad evolutiva en el caso general y no proporciona autenticación del origen. No obstante, se considera que en las redes corporativas con un número pequeño y limitado de controladores de acceso conocidos serán aceptables dichas limitaciones de seguridad. Proteger la comunicación multidifusión entre los controladores de acceso utilizando firmas digitales podría superar esas limitaciones; no obstante, esto queda en estudio.

El EP B obtiene la media clave Diffie-Hellman del EP A (**ACF**). La **ACF** mantendrá la clave Diffie-Hellman del punto extremo llamado en **dhkey** dentro del **ClearToken** básico H.235.1, pero utilizando el OID "TG" en lugar del "T". Este perfil de seguridad no modificará ningún otro campo del **ClearToken**.

NOTA 2 – Los puntos extremos funcionan con una media clave DH que se mantiene estática durante todo el tiempo de registro y para todas las llamadas. Esto no representa una debilidad de la seguridad siempre que cada punto extremo aplique medias claves verdaderamente aleatorias.

No obstante, los puntos extremos proporcionarán un nuevo valor aleatorio de 512 bits (es decir, 64 octetos) en **challenge** junto con su media clave DH (véase la sección 2.3 de RFC 2631). Estos valores **challenge** están basados en la llamada e introducen la aleatoriedad y modularidad temporal necesarias para la generación de la clave DH.

El EP B originador podrá entonces calcular g^{ab} y el secreto compartido dinámico ZZ_{AB} utilizando un **challenge** aleatorio con el resultado obtenido a partir de MIKEY-PRF (g^{ab} , $0x12F905FE || \text{challenge}$) (véanse las secciones 4.1.2–4.1.4 de RFC 3830). A continuación, MIKEY podrá deducir la clave de autenticación (Ma) empleando el protocolo MIKEY-PRF (véanse las secciones 4.1.2–4.1.4 de RFC 3830).

Durante la etapa 2, el EP B originador generará nuevos valores aleatorios de MIKEY y con la g^y correspondiente y creará el mensaje Imsg I_message de MIKEY conforme al protocolo MIKEY-DHMAC utilizando Ma .

El mensaje `I_message` de MIKEY estará codificado en binario.

El EP B originador debe incluir siempre su media clave DH en **dhkey** dentro de un **ClearToken**, habilitando también por consecuencia el modelo encaminado directamente y soportado por GK. El **ClearToken** debe incluirse como parte del mensaje establecimiento y enviarse al EP A par. Un controlador de acceso de encaminamiento retransmitirá el ClearToken (sin modificación de los mensajes MIKEY) al siguiente salto.

El EP A receptor calcula g^{ab} y el secreto compartido dinámico ZZ_{AB} a partir de MIKEY-PRF (g^{ab} , `0x12F905FE || challenge`) (véanse las secciones 4.1.2–4.1.4 de RFC 3830). A continuación, MIKEY deduce la clave de autenticación (Ma) utilizando MIKEY-PRF (véanse las secciones 4.1.2–4.1.4 de RFC 3830). El EP A genera un valor w aleatorio de MIKEY y calcula g^w . El EP A calcula la TGK empleando las medias claves DH recibidas.

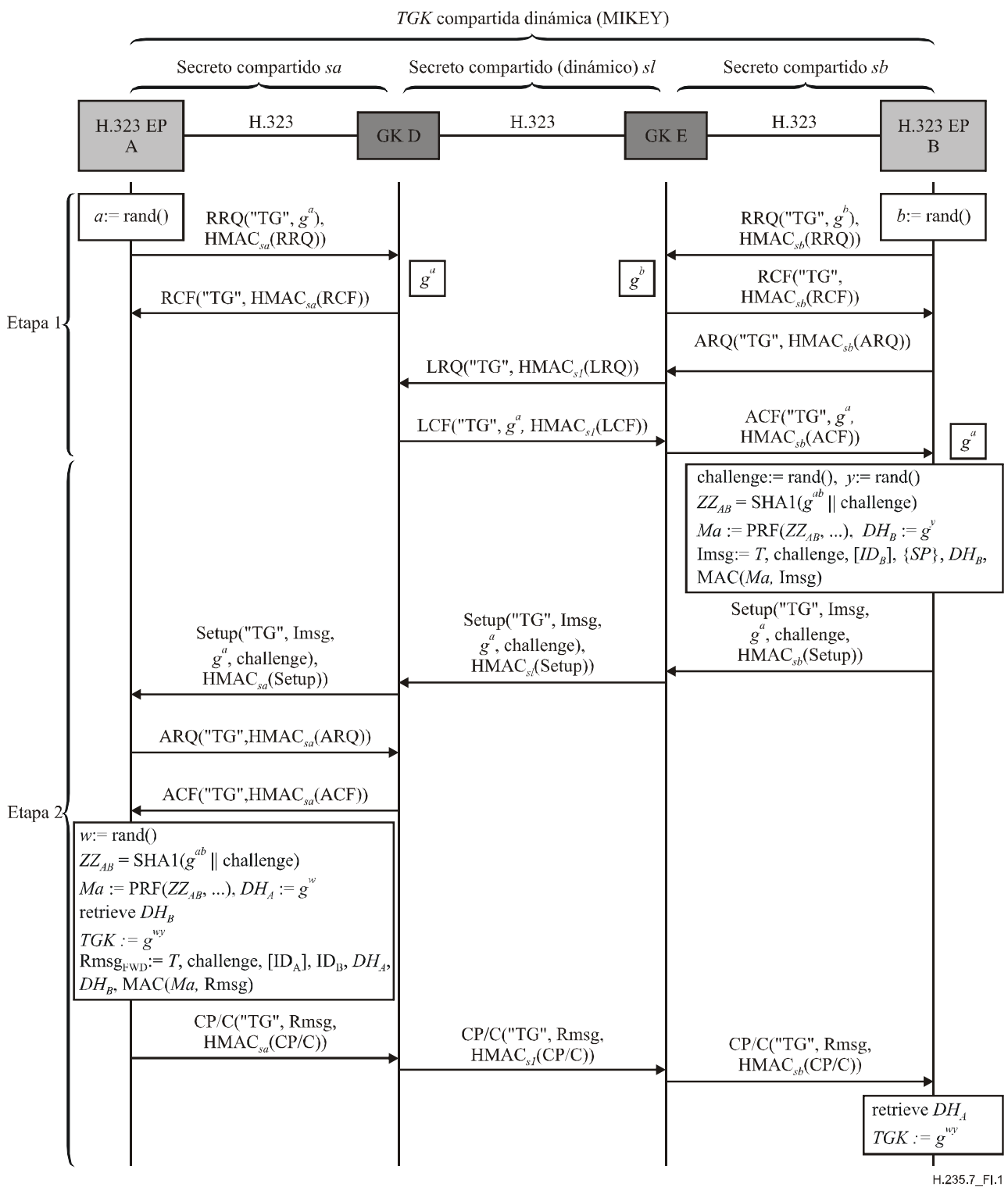
El EP A de recepción puede deducir las claves de sesión SRTP a partir de la TGK , tal como se describe en la sección 4.3 de RFC 3711 (no se muestra en la figura).

El EP A crea un mensaje `Rmsg R_message` similar que se transporta en el mensaje llamada en curso de conexión (CP/C). `Rmsg` es el mensaje de respuesta MIKEY correspondiente que se envía al EP B en el mensaje llamada en curso de conexión (CP/C).

El mensaje de llamada en curso de conexión (CP/C) se envía al EP B.

El EP B recupera la media clave DH y calcula la TGK . A continuación, el EP B deduce las claves de sesión SRTP a partir de las TGK , como se describe en la sección 4.3 de RFC 3711 (no se muestra en la figura).

Secreto compartido dinámico de H.323 $ZZ_{AB} = \text{MIKEY-PRF}(g^{ab}, 0x12F905FE || \text{challenge})$,
 Clave Ma de autenticación compartida dinámica de MIKEY



H.235.7_F1.1

Figura I.1/H.235.7 – Ejemplo del punto extremo B llamando al punto extremo A (llamada encaminada por GK) con el protocolo MIKEY-DHMAC

I.1 Terminación de una llamada H.323

Como los puntos extremos participantes mantienen un estado MIKEY y SRTP, resulta esencial un procedimiento de terminación apropiado. La figura I.2 muestra un ejemplo de flujos de mensajes en el caso de que el EP B (iniciador de MIKEY) termine una llamada. Básicamente, el flujo es conforme a 8.5/H.323 relativa a "Fase E – Terminación de la llamada".

NOTA – La figura I.2 muestra también los procedimientos de desconexión facultativos del caso cuando los puntos extremos cancelan su registro completamente. En ese caso, los puntos extremos también deben descartar la clave DH privada (a o b) y la media clave DH pública (g^a o g^b).

Como el procedimiento de terminación de una llamada es independiente de este perfil de seguridad, podrá utilizarse cualquier OID aplicable del perfil de seguridad subyacente (H.235.1, H.235.3, etc.); por esa razón, la figura I.2 no muestra ningún OID.

Si el punto extremo desea registrarse nuevamente ante el controlador de acceso, deberán generarse nuevas medias claves DH. No obstante, no es necesaria bajo ningún concepto la anulación definitiva del registro simplemente por la terminación de la llamada. Si el punto extremo decide permanecer registrado ante el controlador de acceso, podrá seguir utilizando las medias claves DH estáticas.

Si los puntos extremos permanecen registrados y no se aplica la desconexión, éstos descartarán sólo la información relacionada con la llamada, incluida la media clave DH par, el **challenge**, las claves Me , Ma , de MIKEY, la TGK y la información de sesión SRTP conexas.

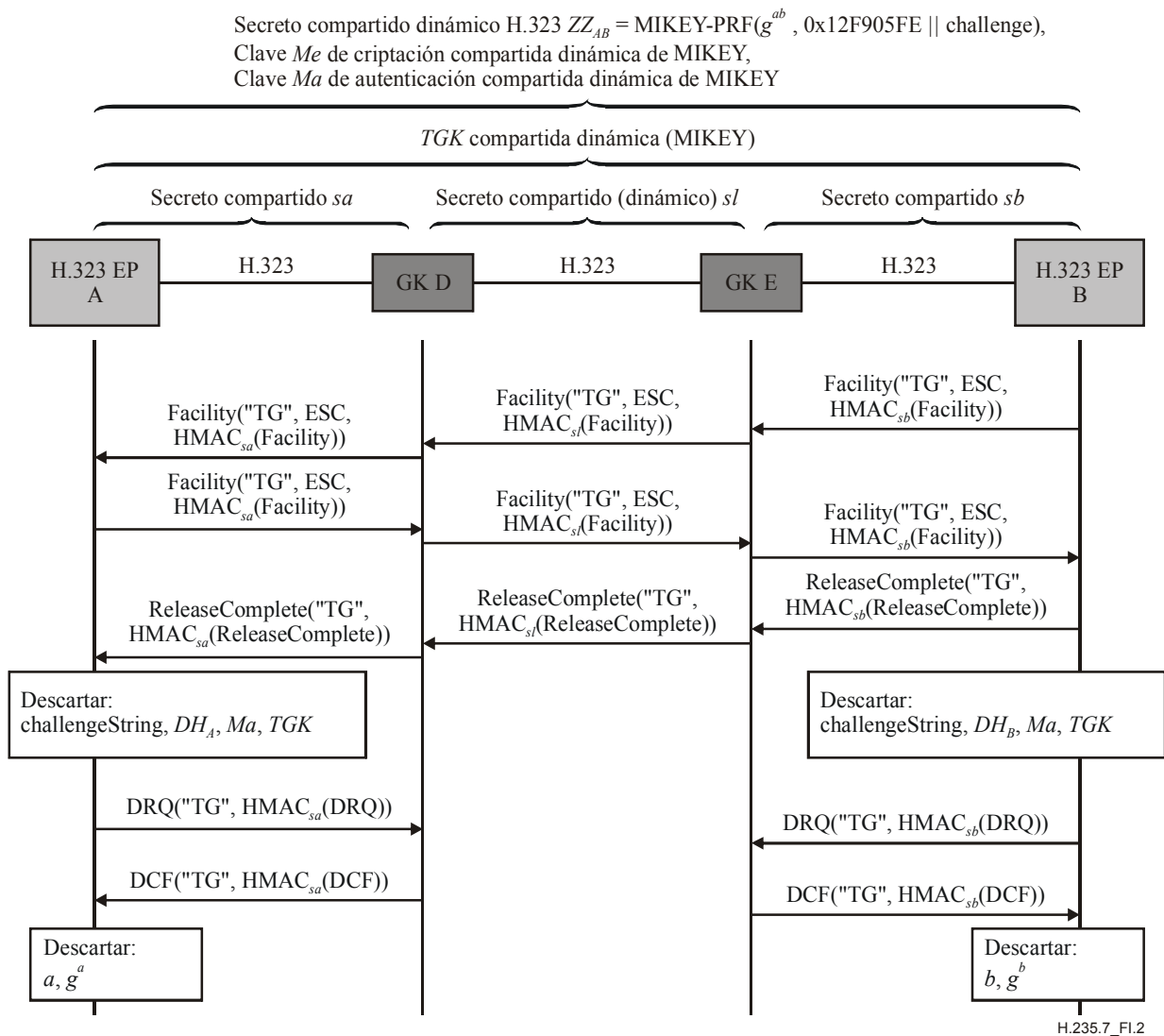


Figura I.2/H.235.7 – Ejemplo de terminación de una llamada por el punto extremo B

I.2 Creación de nuevas claves TGK y actualización del CSB

MIKEY dispone de soporte integrado para la creación de nuevas claves TGK y/o la actualización de información del CSB. En el perfil de esta Recomendación se utiliza el procedimiento MIKEY-DHHMAC de la sección 3.1 de RFC zzzz para este fin, lo que permite actualizar la TGK antes de su expiración o actualizar otra información sin modificar la TGK.

El mecanismo de creación de nuevas claves TGK y de actualización del CSB es útil para proteger un agrupamiento de canales lógicos conforme a la misma política de seguridad. Para ello, se recomienda activar el protocolo MIKEY-DHHMAC (completo), como se describió anteriormente, sólo para el primer canal lógico. Cualquier canal lógico subsiguiente que tenga que aplicar la misma política de seguridad MIKEY o la misma TGK, debe emplear el mecanismo de actualización del CSB sin el mecanismo de creación de nuevas claves TGK, haciendo referencia al CSB-ID inicial y omitiendo las claves Diffie-Hellman actualizadas. Esto permite establecer canales lógicos o sesiones criptadas MIKEY de manera más eficiente que activando el protocolo MIKEY completo en cada canal lógico.

Los mensajes de creación de nuevas claves TGK de MIKEY o de actualización del CSB deben encapsularse y transportarse en **MiscellaneousCommand** dentro de un mensaje Facility. El **tokenOID** del **ClearToken** se debe fijar a "TG".

Cuando MIKEY funciona en "nivel de medios", el EP B tiene que determinar en qué canal lógico debe aplicar la creación de nuevas claves TGK y/o la actualización del CSB. El EP A, como respondedor, utilizará de manera similar **MiscellaneousCommand** en el mensaje Facility para transportar el mensaje R_message de MIKEY (si lo hubiere).

Para la creación de nuevas claves TGK (véase la figura I.3), el EP B, como iniciador de MIKEY, generará una nueva TGK. **parameterValue** incluirá el mensaje I_message de MIKEY codificado en binario.

El EP A, como respondedor, puede confirmar el mensaje recibido de creación de nuevas claves TGK si resulta necesario o si lo solicita el EP B. El EP A crea un mensaje R_message similar, que se transporta en el mensaje Facility. El EP B envía el mensaje Facility al EP A.

Para la actualización del CSB, el procedimiento es similar al antes descrito, excepto que el mensaje MIKEY no mantendrá ninguna TGK.

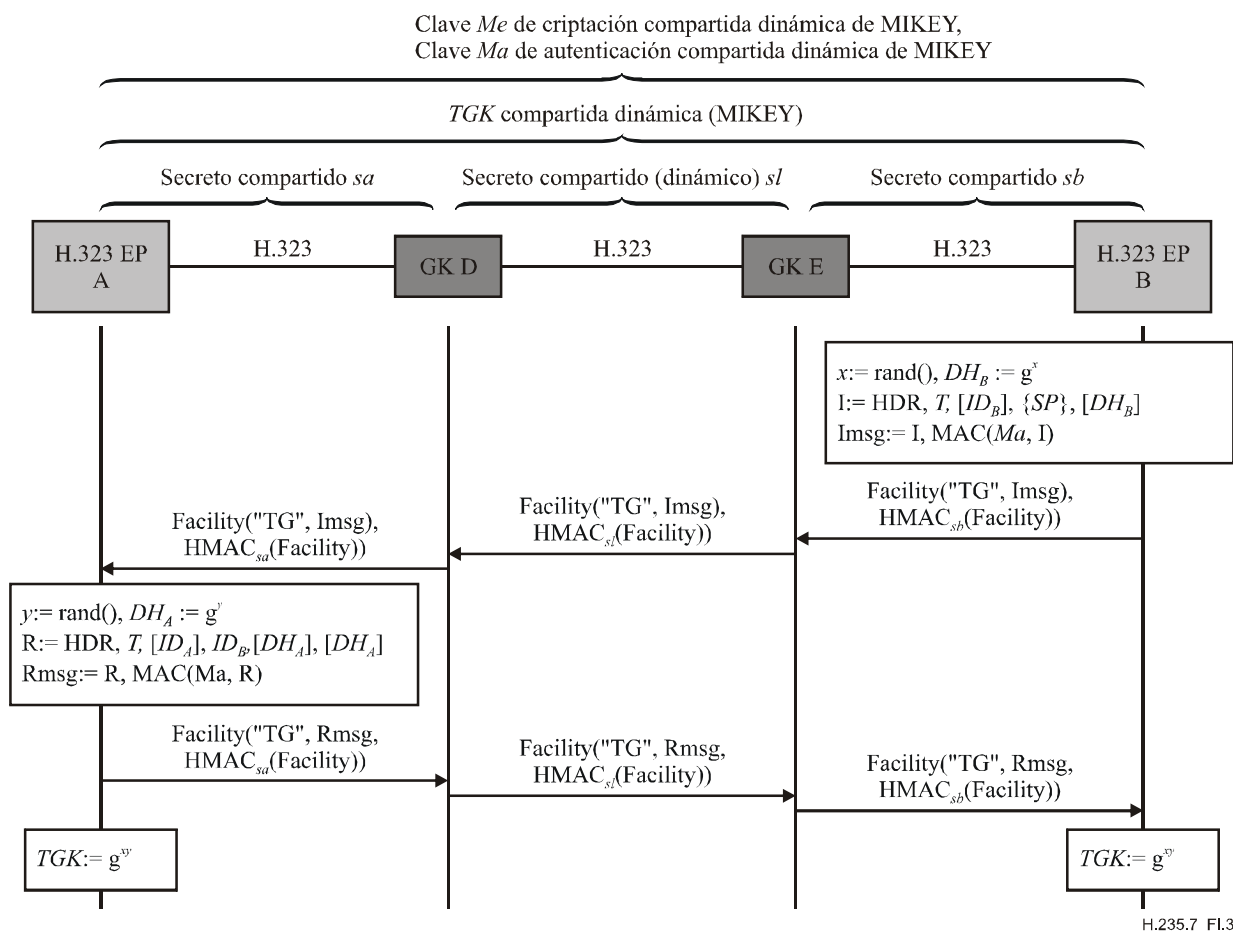


Figura I.3/H.235.7 – Ejemplo del punto extremo B actualizando una clave

Esta Recomendación no define ningún procedimiento para la creación de nuevas claves TGK y/o la actualización del CSB activado por el respondedor; ese tema queda en estudio.

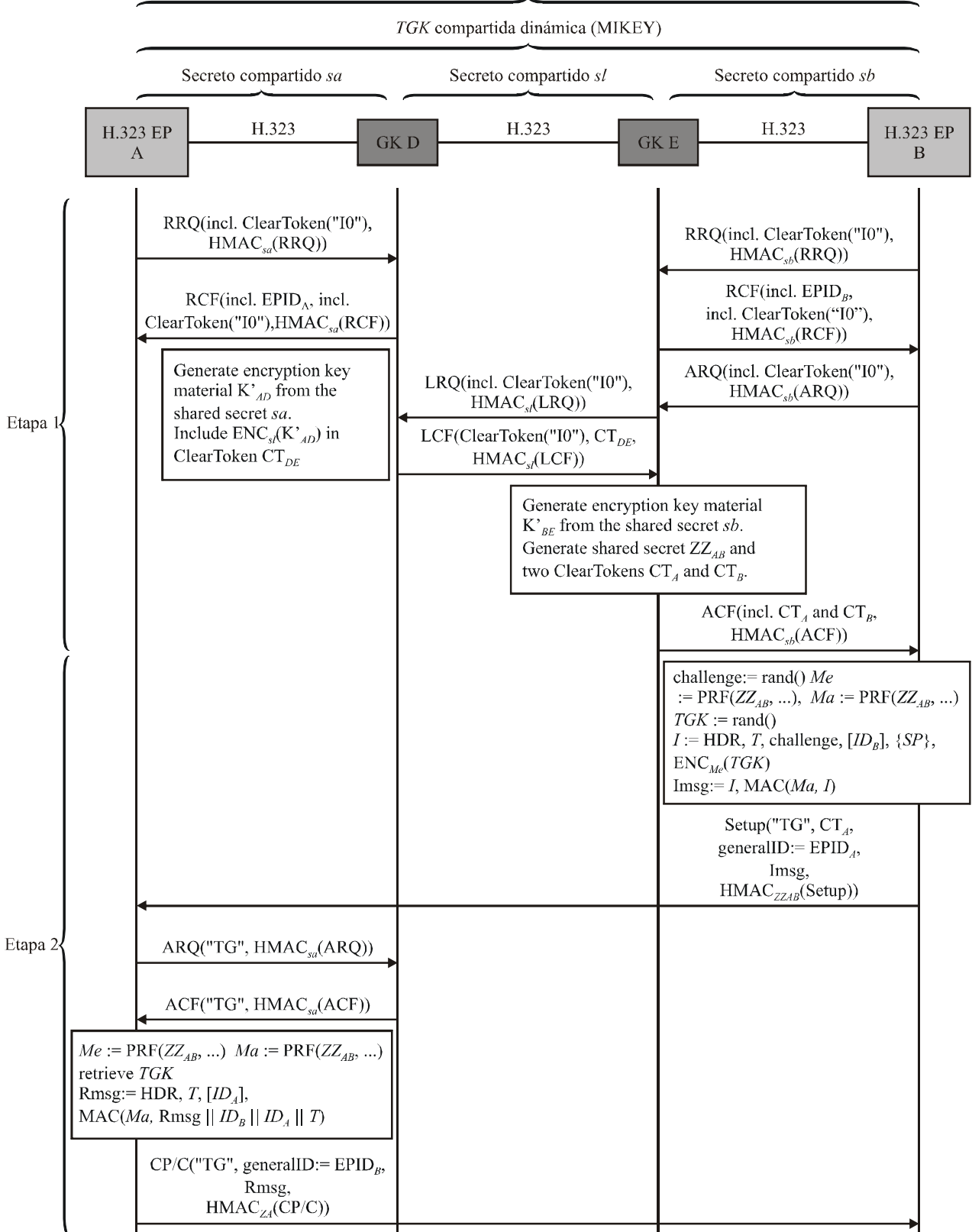
Apéndice II

Utilización de la H.235.4 para establecer un secreto precompartido

Este apéndice define cómo aplicar el procedimiento DRC1 de la Rec. UIT-T H.235.4 para establecer un secreto precompartido ZZ_{AB} entre el punto extremo B y el punto extremo A, suponiendo que dicho secreto extremo a extremo no existe *a priori*. El método que se describe en este apéndice puede aplicarse al caso de un solo controlador de acceso o de múltiples controladores de acceso. El procedimiento en este apéndice no supone cálculos de DH durante el registro o la admisión RAS, sino acciones de criptografía simétrica.

La figura II.1 muestra el ejemplo de un diagrama de flujo cuando el punto extremo B llama al punto extremo A.

Secreto compartido dinámico de H.323 $ZZ_{AB} = \text{MIKEY-PRF}(g^{ab}, 0x12F905FE || \text{challenge})$
 Clave Ma de autenticación compartida dinámica de MIKEY



H.235.7_Fil.1

Figura II.1/H.235.7 – Ejemplo del punto extremo B llamando al punto extremo A (sin encaminamiento por GK) con secreto precompartido MIKEY y DRC1 H.235.4

II.1 Terminación de una llamada H.323

El procedimiento para la terminación de una llamada H.323 será el descrito en 8.1.

II.2 Creación de nuevas claves TGK y actualización del CSB

El procedimiento de creación de nuevas claves TGK y/o actualización del CSB será el descrito en 8.2.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
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	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
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, comunicaciones de sistemas abiertos y seguridad
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet y Redes de la próxima generación
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación