UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T H.235

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

Anexo F
(03/2002)

SERIE H: SISTEMAS AUDIOVISUALES Y MULTIMEDIOS

Infraestructura de los servicios audiovisuales – Aspectos de los sistemas

---

Seguridad y criptado para terminales multimedios de la serie H (basados en las Recomendaciones H.323 y H.245)

Anexo F: Perfil de seguridad híbrido

Recomendación UIT-T H.235 – Anexo F

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.235

Seguridad y criptado para terminales multimedios de la serie H (basados en las Recomendaciones H.323 y H.245)

Anexo F

Perfil de seguridad híbrido

Resumen

Este anexo tiene por finalidad describir un perfil de seguridad híbrido basado en una infraestructura de clave pública (PKI), eficiente y escalable, para la versión 2 de H.235. Este perfil de seguridad híbrido aprovecha los perfiles de seguridad descritos en los anexos D y E/H.235 desplegando firmas digitales del anexo E/H.235 y desplegando el perfil de seguridad básica del anexo D/H.235.

Orígenes

El anexo F a la Recomendación UIT-T H.235, preparado por la Comisión de Estudio 16 (2001-2004) del UIT-T, fue aprobado por el procedimiento de la Resolución 1 de la AMNT el 29 de marzo de 2002.

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.235

Seguridad y criptado para terminales multimedios de la serie H (basados en las Recomendaciones H.323 y H.245)

Anexo F

Perfil de seguridad híbrido

F.1 Visión general

En este anexo se describe un perfil de seguridad híbrido basado en una infraestructura de clave pública (PKI, *public key infrastructure*), eficiente y escalable, que despliega firmas digitales del anexo E/H.235 y que despliega el perfil de seguridad básica del anexo D/H.235. El presente anexo se sugiere como una opción. Las entidades de seguridad H.323 (terminales, controladores de acceso, pasarelas, MCU, etc.) pueden implementar este perfil de seguridad híbrido para mejorar la seguridad o cuando sea necesario.

La noción de "híbrido" en este texto significa que los procedimientos de seguridad del perfil de firmas en el anexo E/H.235 se aplican realmente en un sentido ligero y las firmas digitales son aún conformes con los procedimientos RSA. Sin embargo, las firmas digitales se despliegan sólo cuando ello es absolutamente necesario; de lo contrario, se utilizan técnicas de seguridad simétrica sumamente eficientes del perfil de seguridad básico descrito en el anexo D/H.235.

El perfil de seguridad híbrido es aplicable a la telefonía IP "mundial" escalable. Cuando se aplica estrictamente este perfil de seguridad supera las limitaciones del perfil de seguridad básico simple descrito en el anexo D/H.235. Además, cuando se aplica estrictamente este perfil de seguridad resuelve ciertos inconvenientes del anexo E/H.235 tales como la necesidad de mayor anchura de banda y de una mejor calidad para el procesamiento. Por ejemplo, el perfil de seguridad híbrido no depende de la administración (estática) de los secretos compartidos mutuos de los saltos en diferentes dominios. Así, los usuarios pueden elegir mucho más fácilmente su proveedor VoIP. Por tanto, este perfil de seguridad soporta además cierto tipo de movilidad del usuario. Aplica criptografía asimétrica con firmas y certificados solamente cuando es necesario y en otro caso utiliza técnicas simétricas más simples y eficientes. Proporciona tunelización de los mensajes H.245 para la integridad de los mismos y también implementa algunas disposiciones para el no repudio de mensajes.

El perfil de seguridad híbrido determina el modelo con encaminamiento por GK y se basa en las técnicas de tunelización H.245. Se encuentra en estudio el soporte para los modelos con encaminamiento no efectuado por GK.

Las prestaciones ofrecidas por este perfil incluyen:

Para los mensajes RAS, H.225.0 y H.245:

- La autenticación de usuario a una entidad deseada cualquiera que sea el número de saltos[1] del nivel de aplicación que atraviesa el mensaje.
- La integridad de todas o las porciones críticas (campos) de los mensajes que llegan a una entidad cualquiera que sea el número de saltos del nivel de aplicación atravesados por el

[1] Salto tiene aquí el sentido de un elemento de red H.235 de confianza (por ejemplo, GK, GW, MCU, apoderado o cortafuegos). Por tanto, la seguridad salto por salto en el nivel de aplicación, cuando se utiliza con técnicas simétricas, no proporciona una verdadera seguridad de extremo a extremo entre terminales.

mensaje. La integridad del propio mensaje obtenida mediante un número aleatorio generado de forma fuerte es también facultativa.

- La autenticación, integridad y (algún) no repudio del mensaje salto por salto en el nivel de aplicación proporcionan estos servicios de seguridad para el mensaje completo.
- Utilizando la infraestructura disponible de claves públicas, los usuarios pueden elegir su proveedor de servicio. La gestión de claves para la distribución de claves de la sesión está bien integrada en el perfil de seguridad híbrido.

La provisión adecuada de los servicios de seguridad antes descritos evita varios tipos de ataques, incluyendo:

- *Ataques por intermediarios*: la autenticación e integridad de los mensajes salto por salto en el nivel de aplicación evita tales ataques cuando el intermediario es un salto en el nivel de aplicación, es decir un encaminador hostil.
- *Ataques por reproducción*: La utilización de indicaciones de tiempo y números secuenciales evita estos ataques.
- *Piratería*: la autenticación del usuario evita estos ataques.
- *Asaltos a la conexión*: la utilización de autenticación/integridad para cada mensaje de señalización evita estos ataques.

F.2 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.

– 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*.

– Recomendación UIT-T H.323, versión 4 (2000), *Sistema de comunicación multimedios basados en paquetes*.

– 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)*.

– Recomendación UIT-T H.245, versión 8 (2001), *Protocolo de control para comunicación multimedios*.

– IETF RFC 2459 (1999), *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*.

F.3 Acrónimos

Este anexo utiliza los siguientes acrónimos.

GCF Confirmación de controlador de acceso (*gatekeeper confirm*)

GK Controlador de acceso (*gatekeeper*)

GRQ Petición de controlador de acceso (*gatekeeper request*)

ICV Valor de comprobación de integridad (*integrity check value*)

LRQ Petición de localización (*location request*)

OID Identificador de objeto (*object identifier*)

RAS Registro, admisión y situación

RCF Confirmación de registro (*registration confirm*)

RRQ Petición de registro (*registration request*)

RSA Algoritmo de criptación Rivest, Shamir y Adleman (*Rivest, Shamir and Adleman encryption algorithm*)

SHA Algoritmo troceado asegurado (*secure hash algorithm*)

URQ Petición de desregistro (*unregistration request*)

F.4 Convenios de especificación

El perfil de seguridad híbrido utiliza términos y definiciones de los anexos D y E/H.235.

Si bien el servicio de integridad de mensaje siempre proporciona autenticación de mensaje, lo inverso no siempre es cierto. En el modo sólo autenticación, la integridad asegurada abarca solamente un determinado subconjunto de campos del mensaje. Esto se aplica a los servicios de integridad realizados por medios asimétricos (por ejemplo, firmas digitales). Por tanto, en la práctica, un servicio combinado de autenticación y seguridad explota el mismo material de claves sin que con ello introduzca una debilidad en la seguridad.

Este perfil de seguridad es aplicable en ambientes en los cuales puede haber muchos terminales y donde no es factible la asignación de contraseñas estáticas y/o claves simétricas, por ejemplo, en los escenarios a gran escala o a escala global. En cambio, este perfil de seguridad supone la disponibilidad de una infraestructura de claves públicas con certificados asignados y claves privadas/públicas, directorios, etc. Además, este perfil de seguridad despliega criptotécnicas simétricas cuando sean aplicables.

Este perfil de seguridad introduce los términos "primer" mensaje y "último" mensaje enviados. La protección de seguridad del primer mensaje (y probablemente también del último) es diferente de la protección de seguridad de los mensajes restantes.

Por "primer mensaje" enviado se entiende un mensaje que se transmite entre dos entidades H.323 y establece un contexto de seguridad. Pone a disposición de ambas entidades el material de claves simétricas disponible y por ejemplo señala el comienzo de una llamada. En el caso de RAS H.225.0, el primer mensaje es el RRQ y el mensaje de respuesta conexo. Para la señalización de llamada H.225.0 mediante arranque rápido, el primer mensaje es SETUP (establecimiento) y CONNECT (conexión).

El "último mensaje" termina el contexto de seguridad establecido. El material de claves establecido será destruido. Para RAS H.225.0, el último mensaje es el URQ y el mensaje de respuesta conexo, en tanto que para la señalización de llamada H.225.0 el último mensaje es RELEASE-COMPLETE (liberación completa).

Este perfil de seguridad supone el modelo de llamada con encaminamiento por GK, en el que se aplica el método de señalización de llamada con conexión rápida. Los mensajes de control de llamada H.245 se tunelizan en forma securizada en mensajes de señalización de llamada H.225.0 y heredan por consecuencia el esquema de protección de seguridad H.225.0.

El perfil de seguridad de firma permite tunelizar en forma securizada las PDU de control de llamada H.245 dentro de mensajes de facilidad H.225.0. Los mecanismos de actualización y sincronización de claves H.245 necesitan la tunelización para señalar el mensaje FACILITY (facilidad) de actualización de clave y es útil por ejemplo en las llamadas de muy larga duración.

La zona sombreada de gris claro en el cuadro F.1 representa los mecanismos de seguridad utilizados por el perfil de seguridad híbrido.

NOTA – Los certificados RSA con troceado MD5 no son parte de este perfil de seguridad.

El perfil de seguridad con criptación de voz del anexo D de H.235 (véase D.7) podría ser utilizado facultativamente junto con el perfil de seguridad híbrido. Su utilización se negocia como parte de la señalización de establecimiento de la comunicación.

Cuadro F.1/H.235 – Visión general del perfil de seguridad híbrida

Servicios de seguridad	**Funciones de llamada**			
	RAS	**H.225.0**	**H.245 (nota 3)**	**RTP**
Autenticación	Firma digital RSA (SHA1)	Firma digital RSA (SHA1)	Firma digital RSA (SHA1)	
	HMAC-SHA1-96	HMAC-SHA1-96	HMAC-SHA1-96	
No repudio	(sólo es posible en el primer mensaje)	(sólo es posible en el primer mensaje)		
Integridad	Firma digital RSA (SHA1)	Firma digital RSA (SHA1)	Firma digital RSA (SHA1)	
	HMAC-SHA1-96	HMAC-SHA1-96	HMAC-SHA1-96	
Confidencialidad				
Control de acceso				
Gestión de claves	Atribución de certificado	Atribución de certificado		
	Intercambio de claves Diffie-Hellman autenticadas	Intercambio de claves Diffie-Hellman autenticadas		

NOTA 1 – El perfil de seguridad híbrido tiene que ser soportado también por otras entidades H.235 (por ejemplo, controladores de acceso, pasarelas y apoderados H.235).

NOTA 2 – Los bits de utilización de clave disponibles en el certificado podrían también determinar el servicio de seguridad proporcionado por un terminal (por ejemplo, aseveración de no repudio).

NOTA 3 – H.245 tunelizado o H.245 incorporado dentro de conexión rápida H.225.0.

Para la autenticación, el usuario debe utilizar un esquema de firma con clave pública/privada. Tal esquema generalmente ofrece mejor integridad.

Esta Recomendación no describe procedimientos de registro, certificación y atribución de certificados desde un centro fiduciario y la asignación de claves privadas/públicas, servicios de directorio, parámetros CA específicos, revocación de certificados, actualización/recuperación de pares de claves y otros procedimientos operacionales y de gestión relativos a los certificados, tales como procedimientos para la entrega de certificados o claves públicas/privadas y la instalación de dichos procedimientos en los terminales. Tales procedimientos pueden aplicarse por medios que no forman parte del presente anexo.

Las entidades de comunicación que intervienen son capaces de determinar implícitamente la utilización, bien de los perfiles de seguridad básicos del anexo D/H.235, del perfil de firma del anexo E/H.235, o bien de este perfil de seguridad híbrido mediante la evaluación de los

identificadores de objeto de seguridad señalados en los mensajes (**tokenOID**, y **algorithmOID**; véase también E.8).

F.5 Requisitos relativos a H.323

Se supone que las entidades H.323 que implementan este perfil de seguridad híbrido soportan las siguientes prestaciones H.323:

- conexión rápida;
- tunelización H.245; y
- modelo con encaminamiento por GK.

F.6 Autenticación e integridad

En este anexo se utilizan los siguientes términos para la prestación de servicios de seguridad.

- **Autenticación e integridad**: Éste es un servicio de seguridad combinado que soporta la integridad de los mensajes junto con la autenticación de usuario. El usuario autentica cuando aplica correctamente la firma digital a algún dato con clave privada, o bien cuando aplica correctamente un secreto compartido, conexo. Además de esto, el mensaje es protegido contra la manipulación fraudulenta. Ambos servicios de seguridad son proporcionados por el mismo mecanismo de seguridad. La autenticación e integridad combinadas sólo son posibles sobre la base de salto por salto.

NOTA – Cuando se aplican firmas digitales se puede soportar un servicio de seguridad de no repudio; esto depende también de los valores fijados a los bits de utilización de clave de la clave de firma en el certificado (véase también RFC 2459).

Se describen los siguientes procedimientos para su utilización en este perfil.

El procedimiento IV se basa en firmas digitales que utilizan un par de claves privada/pública y en el despliegue de criptotécnicas simétricas para proveer autenticación e integridad de mensajes RAS, Q.931 y H.245. Los terminales pueden utilizar este método si se necesita una seguridad eficiente y escalable.

En dependencia de la política de seguridad, la autenticación puede ser unilateral, o mutua (es decir, el caso en el que la autenticación/integridad también se aplica en el sentido inverso, por lo que se proporciona una seguridad superior). El modo de seguridad preferido es el de autenticación mutua.

Los controladores de acceso que detectan el fallo de la validación de la autenticación y/o de la integridad en un mensaje RAS/de señalización de llamada recibido de un terminal/controlador de acceso par responderán con un mensaje de rechazo correspondiente que indica un fallo de seguridad. Esto se efectúa fijando el motivo de rechazo a **securityDenial** o a otro código de error de seguridad apropiado de acuerdo a la cláusula B.2/H.235. Como parte de la respuesta retomada, el emisor puede proporcionar una lista de certificados aceptables en testigos separados, a fin de facilitar al recibiente la selección de un certificado adecuado.

Hay una señalización H.235 implícita para indicar la utilización del procedimiento IV y el mecanismo de seguridad aplicado basándose en el valor de los identificadores de objeto (véase también F.12) y en los campos del mensaje que han sido llenados. En este texto se hace referencia a los identificadores de objeto mediante letras (por ejemplo, "A").

Este perfil no utiliza los campos ICV de H.235. En su lugar, los valores de comprobación de la integridad criptográfica se introducen en el campo **signature** del **token** en el **cryptoSignedToken** cuando se hace referencia al anexo E, o los valores de comprobación de la identidad se introducen en los campos de troceado del **CryptoToken** cuando se hace referencia al anexo D.

F.7 Procedimiento IV

Cuando se emplea el procedimiento IV para la seguridad salto por salto, deberán aplicarse los siguientes procedimientos. El procedimiento IV une el procedimiento I del anexo D (véase D.6.3.2) y el procedimiento II del anexo E (véase E.5).

Para el primer mensaje, incluida la respuesta correspondiente, enviado en cada sentido de transmisión, se utilizará el procedimiento II del anexo E (autenticación e integridad salto por salto, véase E.5) para el que se fijarán los siguientes valores:

- OID "A1" en lugar de OID "A" y OID "S1" en lugar de OID "S". La utilización de estos OID permite identificar el perfil de seguridad híbrida.
- **algorithmOID** en **tokenOID** se fijará a "W", que indica la utilización de la firma RSA-SHA1.
- **signature** contendrá una firma RSA codificada en ASN.1 (véase E.10/H.235).
- **certificate** debe contener el certificado de usuario del emisor si el receptor no lo ha obtenido por otro medio.

En un escenario con un solo dominio administrativo, el primer mensaje/respuesta se define como el mensaje/respuesta RAS H.225.0 inicial; éste es generalmente GRQ/GCF o RRQ/RCF. En un escenario de múltiples dominios administrativos, el primer mensaje/respuesta dentro de cada dominio se define como en el caso anterior; el primer mensaje entre los dominios se define como SETUP.

El emisor y el recibiente intercambian y calculan una cadena de bits secreta Diffie-Hellman autenticada. En el cuadro D.4/H.235 se presenta un ejemplo de los parámetros de grupo Diffie-Hellman y se recomienda tomar el número primo de 1024 bits siempre que sea posible, por razones de seguridad. El secreto Diffie-Hellman será calculado para cada tramo, independientemente de que se despliegue o no el perfil de encripción de voz.

A partir de la cadena de bits común que ambas partes calculan, ambas partes derivan un secreto de 160 bits tomando los 160 bits menos significativos. El secreto de 160 bits resultante actúa como la contraseña/secreto compartido que se utiliza en el anexo D.

En un escenario con controladores de acceso en distintos dominios administrativos, el emisor y el receptor utilizarán dos testigos en cada sentido de transmisión para la señalización de llamada H.225.0:

- Un **ClearToken** dentro de **CryptoToken**, que se utiliza para calcular la clave de medios que se comparte entre los terminales (véase D.7.1). Esto es necesario solamente si se va a desplegar criptación de voz.
- Se utiliza un **ClearToken** separado para calcular una clave de enlace que se comparte entre las entidades emisor y receptor para protección del enlace de señalización. Esta clave de enlace sustituye la contraseña compartida entre los controladores de acceso en el anexo D. El **tokenOID** de ese **ClearToken** se fijará a "Q", que indica la utilización de Diffie-Hellman y un perfil de seguridad híbrido. El cálculo de la clave de enlace prosigue de la misma manera que el cálculo de la clave de medios (véase D.7.1).

NOTA – En los entornos encaminados directamente, las entidades y los terminales emisor/receptor corresponden unos con otros. En los entornos con encaminamiento por controlador de acceso, la clave de enlaces se comparte salto por salto entre cada par de controladores de acceso pares, mientras que la clave de medios se comparte de extremo a extremo.

En los entornos con encaminamiento por controlador de acceso, el controlador de acceso reenviará al salto siguiente el testigo Diffie-Hellman recibido del punto extremo.

Se debe utilizar el procedimiento I del anexo D (véase D.6.3.2) para todos los mensajes/respuestas enviados en cada sentido, salvo el primero. Esto se aplica también en un escenario con múltiples controladores de acceso situados dentro de un dominio administrativo. En este caso no hay necesidad de gestión de claves asimétricas y basta con la aplicación del anexo D/H.235.

Se puede utilizar este anexo con los sistemas de la versión 1 de H.235, teniendo precaución de utilizar, en forma limitada, los ID de los emisores y generalID descritos en la cláusula E.17/H.235.

F.8 Asociación de seguridad para llamadas concurrentes

Se proporciona una optimización para el caso en que un par fijo de entidades procesen varias llamadas independientes, en paralelo, utilizando un solo canal de señalización de llamada. En lugar de establecer varias claves de enlace con Diffie-Hellman para cada llamada, se define una asociación de seguridad que abarca múltiples llamadas concurrentes.

Dicho sea en una forma más precisa, la asociación de seguridad abarca todas las llamadas entre un par fijo de entidades mientras esté vivo el canal de señalización de llamada. Las entidades utilizan la bandera **multipleCalls** dentro de Setup para indicar la capacidad de señalización de múltiples llamadas por una sola conexión de señalización de llamada (véase 7.3/H.323).

Si se utiliza una sola conexión de señalización de llamada, sólo se necesita establecer una clave de enlace común; véase la figura F.1.

Por otro lado, si la bandera **multipleCalls** dentro de SETUP no está fijada, se calculará de nuevo, individualmente, una clave de enlace para cada llamada.

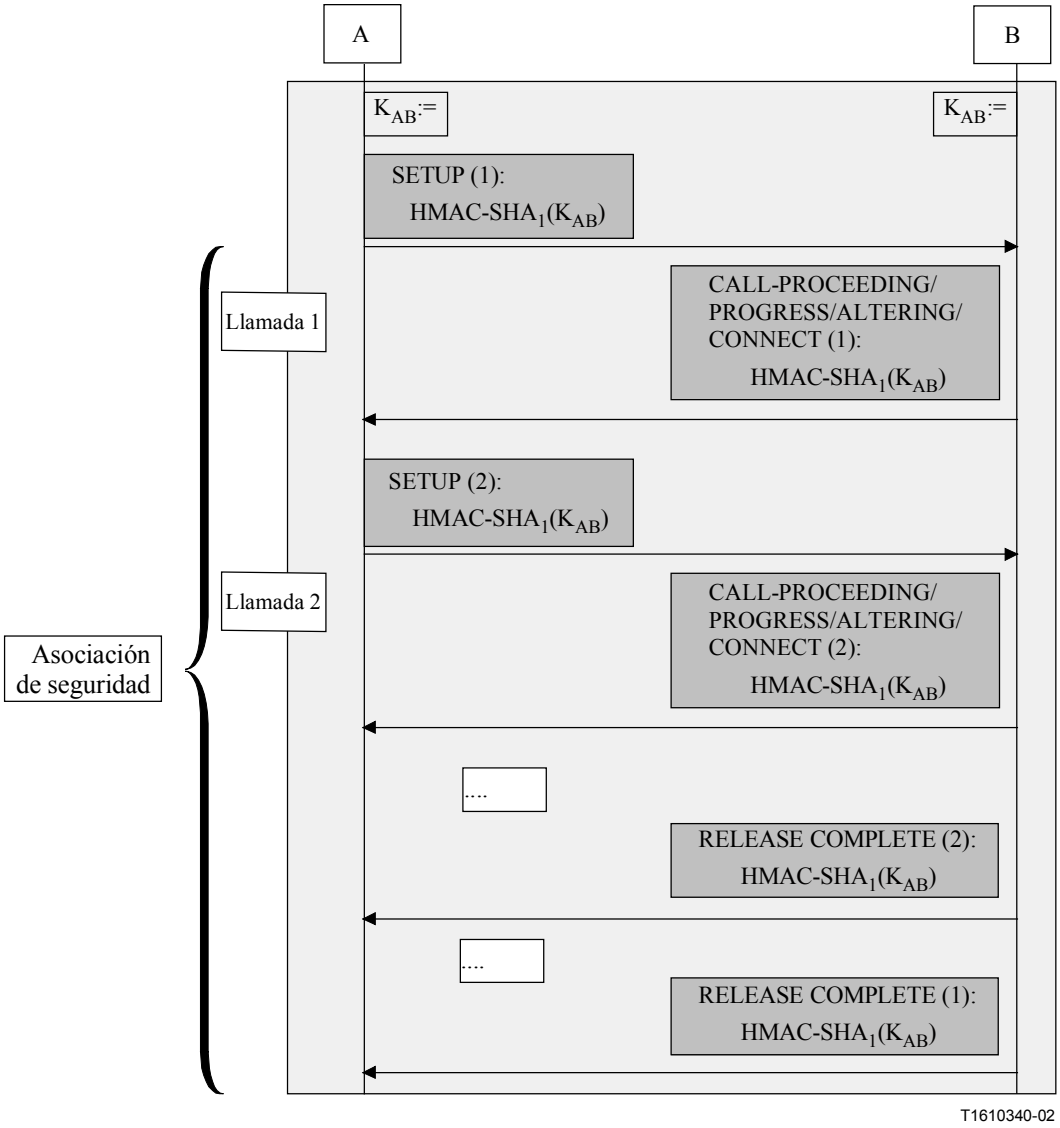


Figura F.1/H.235 – Asociación de seguridad para llamadas concurrentes

F.9 Actualización de clave

Un procedimiento facultativo de actualización de clave permite que cada entidad de comunicación (GK o terminal) renueve la clave de sesión que está utilizando en ese momento, sustituyéndola por una nueva. Tal actualización de clave debe ser iniciada por cualquier entidad que considere que la necesita. Una actualización de clave puede ser motivada por una clave de sesión comprometida, el hecho de considerar que la clave de sesión se ha vuelto, o se volverá, insegura, u otros criterios de políticas de seguridad. Estos aspectos están fuera del alcance de esta Recomendación.

El iniciador invoca la actualización de clave utilizando el mensaje FACILITY. Este mensaje transporta un nuevo testigo Diffie-Hellman, un certificado digital facultativo, y una firma digital del iniciador. Al recibir el mensaje FACILITY, el recibiente contesta con un mensaje FACILITY similar que transporta su testigo Diffie-Hellman, un certificado digital facultativo, y una firma digital del recibiente. Una vez finalizado el procedimiento de actualización de clave, el iniciador y el respondedor utilizarán la nueva clave de enlace calculada.

- El **tokenOID** del **ClearToken** dentro de FACILITY se fijará a "Q", que indica la utilización de Diffie-Hellman y el perfil de seguridad híbrido. El cálculo de la clave de enlace prosigue de la misma manera que el cálculo de la clave de sesión de medios (véase D.7.1).

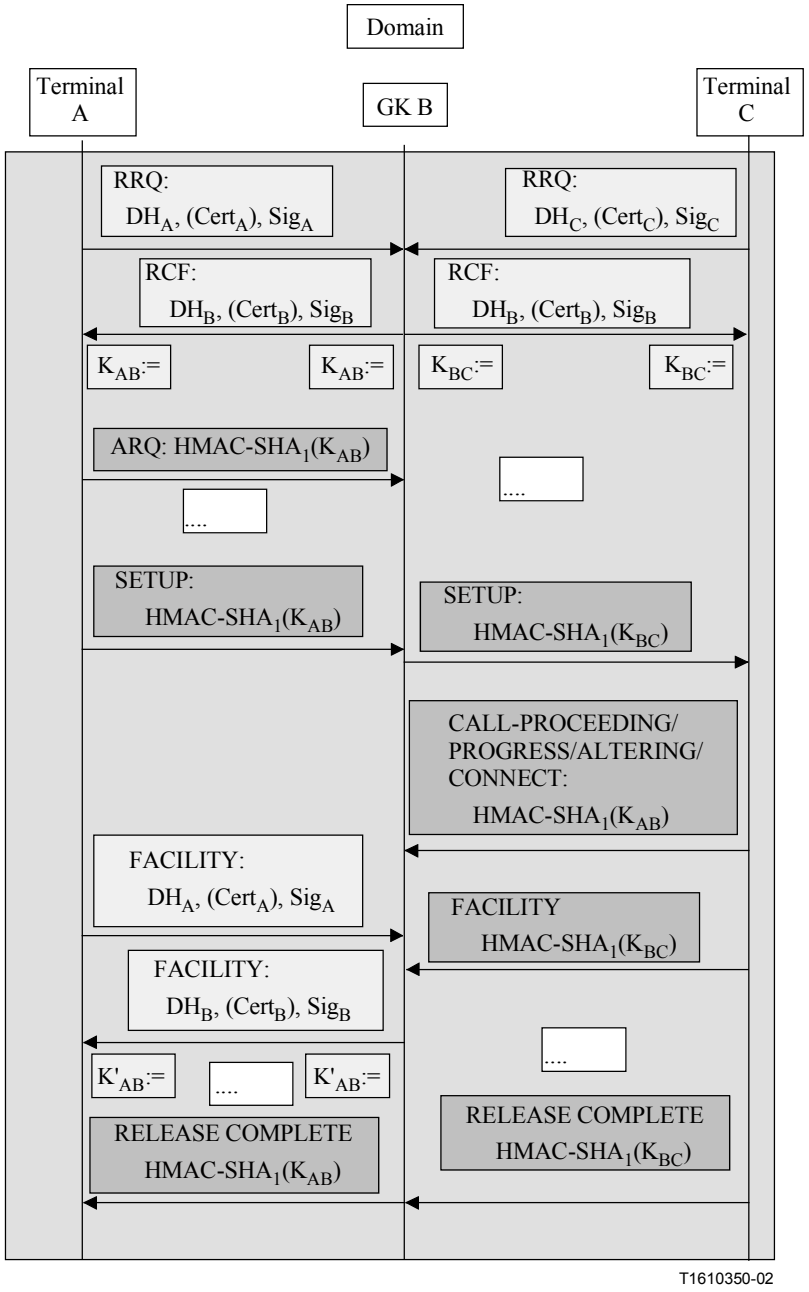
El mensaje FACILITY para fines de actualización de clave se protegerá de conformidad con el procedimiento II del anexo E/H.235. Todo otro mensaje FACILITY sin el transporte del testigo Diffie-Hellman no se desplegará para fines de actualización de clave y se protegerá de conformidad con el procedimiento I del anexo D/H.235.

F.10 Ejemplos ilustrativos

En los diagramas de flujo de las figuras F.2 y F.3 se ilustra la utilización del anexo F en un flujo de mensaje básico. Se debe observar que los diagramas no muestran el flujo de mensaje completo y que por razones de simplicidad se omiten varios mensajes. Los mensajes resaltados en gris claro se relacionan con el perfil de firma del anexo E/H.235, en tanto que los mensajes en gris oscuro se relacionan con el perfil básico del anexo D/H.235. Las figuras destacan las partes de seguridad (más importantes) de cada mensaje (CryptoTokens H. 235, testigos) pero se omiten los detalles.

En el diagrama de flujo de la figura F.2 se ilustra el flujo de mensaje básico en un escenario con un controlador de acceso dentro de un dominio administrativo simple. Suponiendo que el certificado del controlador de acceso es conocido por todos los terminales participantes y que los terminales conocen el certificado del controlador de acceso de la misma manera, no hay necesidad de transmitir los certificados dentro de banda durante el procedimiento de registro.

NOTA 1 – Las figuras F.2 y F.3 a continuación comprenden también el procedimiento de arranque rápido cuando los mensajes de señalización de llamada SETUP y CALL PROCEEDING/PROGRESS/ALERTING/CONNECT incluyen el testigo faststart (véase 8.1.7/H.323). En otro caso, se supone un modo no faststart de conformidad con 7.3.1/H.323. La figura F.2 muestra también el procedimiento de actualización de clave entre el terminal A y el controlador de acceso B mediante FACILITY.



Cert	Certificado de usuario	K, K'	Clave de enlace simétrica
DH_A	Testigo Diffie-Hellman g^a mod p	Sig	Firma digital
DH_B	Testigo Diffie-Hellman g^b mod p		
EP	Punto extremo (Terminal)		
GK	Controlador de acceso		

Figura F.2/H.235 – Diagrama de flujo en un dominio administrativo simple

En la figura F.3 se muestra un ejemplo de un flujo de mensaje en un escenario con diferentes dominios administrativos. Si bien el perfil de seguridad híbrido se aplica dentro de cada dominio entre el terminal y el controlador de acceso como se ilustra en la figura F.2, también puede aplicarse entre ambos dominios durante la fase de establecimiento de la comunicación.

NOTA 2 – En la figura F.3 se han omitido todas las comunicaciones entre los elementos de frontera (BE, *border elements*) y todas las comunicaciones entre GK y BE. En la figura F.3 se ilustra también el procedimiento de actualización de clave entre ambos dominios mediante FACILITY.

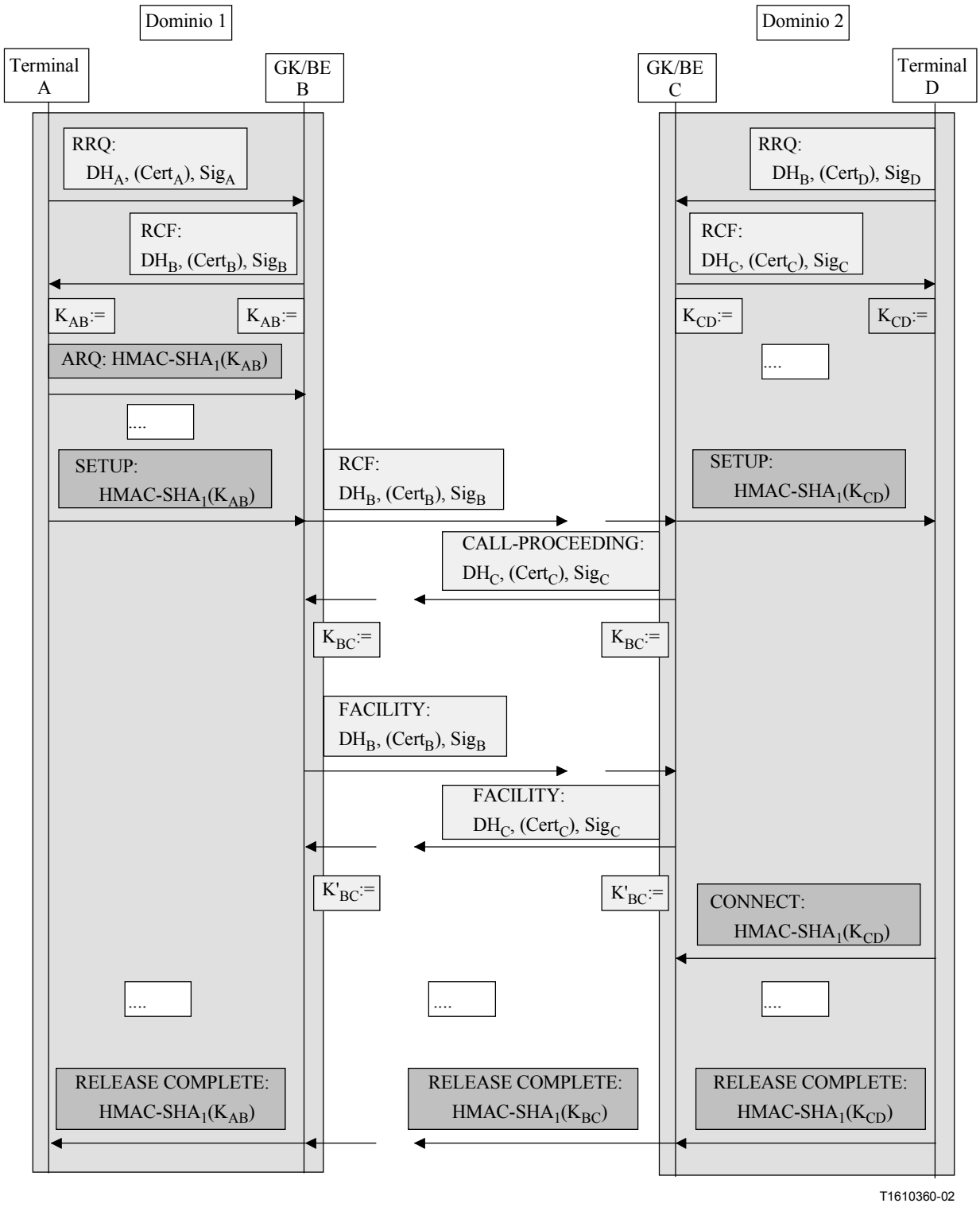


Figura F.3/H.235 – Diagrama de flujo en un dominio administrativo múltiple

F.11 Comportamiento multidifusión

Los mensajes multidifusión H.225.0 tales como **GRQ** o **LRQ** incluirán un **CryptoToken** de conformidad con el procedimiento II en el que no está fijado el **generalID**. Cuando dichos mensajes se envían en modo unidifusión, el mensaje incluirá un **CryptoToken** con el **generalID** fijado.

F.12 Lista de mensajes de señalización securizados

El procedimiento IV despliega el procedimiento I del anexo D o el procedimiento II del anexo E, lo que depende del escenario y del mensaje real, como se indica a continuación.

F.12.1 RAS H.225.0

Mensaje RAS H.225.0	Campos de señalización H.235	Autenticación e integridad	No repudio
GatekeeperRequest, GatekeeperConfirm, GatekeeperReject si se aplica el descubrimiento de GK RegistrationRequest, RegistrationConfirm, RegistrationReject si no se aplica el descubrimiento de GK	CryptoToken, ClearToken	Procedimiento II	Procedimiento II
Cualquier otro mensaje RAS (nota 2)	CryptoToken	Procedimiento I	
NOTA 1 – Para mensajes de unidifusión se aplicarán procedimientos II con los campos seguridad en el **CryptoToken** utilizado. NOTA 2 – No se envían los mensajes de descubrimiento de GK y multidifusión.			

F.12.2 Señalización de llamada H.225.0 (dominio administrativo simple)

Mensaje de señalización de llamada H.225.0	Campos de señalización H.235	Autenticación e integridad	No repudio
Setup-UUIE, Connect-UUIE[a)], Facility-UUIE[b)], Alerting-UUIE, CallProceeding-UUIE, Facility-UUIE, Progress-UUIE, Information-UUIE, ReleaseComplete-UUIE, Status-UUIE, StatusInquiry-UUIE, SetupAcknowledge-UUIE, Notify-UUIE	CryptoToken, ClearToken	Procedimiento I	
Facility-UUIE[c)]	CryptoToken	Procedimiento II	Procedimiento II
a) Se supone que cualquiera de los dos mensajes es el primero en cada sentido de transmisión. b) No se utiliza para actualización de clave. c) Se utiliza para actualización de clave.			

F.12.3 Señalización de llamada H.225.0 (dominio administrativo múltiple)

Mensaje de señalización de llamada H.225.0	Campos de señalización H.235	Autenticación e integridad	No repudio
Setup-UUIE, Connect-UUIE[a)], Alerting-UUIE[b)], CallProceeding-UUIE, Facility-UUIE[c)], Progress-UUIE, Information-UUIE, ReleaseComplete-UUIE	CryptoToken, ClearToken	Procedimiento II	Procedimiento II
Alerting-UUIE[d)], CallProceeding-UUIE, Facility-UUIE[e)], Progress-UUIE, Information-UUIE, ReleaseComplete-UUIE, Status-UUIE, StatusInquiry-UUIE, SetupAcknowledge-UUIE, Notify-UUIE	CryptoToken, ClearToken	Procedimiento I	Procedimiento I

a) Se supone que cualquiera de los dos mensajes es el primero en cada sentido de transmisión.

b) Cualquiera de estos mensajes se transmite como primer mensaje en cualquier sentido.

c) Se utiliza para actualización de clave.

d) Ninguno de estos mensajes se transmite como primer mensaje en cualquier sentido.

e) No se utiliza para actualización de clave.

F.13 Lista de identificadores de objeto

En el cuadro F.2 se indican todos los OID a que se hace referencia.

Cuadro F.2/H.235 – Identificadores de objeto utilizados en el anexo F

Referencia de identificador de objeto	Valor(es) de identificador de objeto	Descripción
"A1"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 20}	Se utiliza como sustituto de OID "A" en el procedimiento II del anexo E para el CryptoToken-tokenOID e indica que la firma/troceado RSA incluye *todos* los campos en el mensaje RAS/H.225.0 (autenticación e integridad).
"S1"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 21}	Se utiliza como sustituto de OID "S" en el procedimiento II del anexo E para el ClearToken-tokenOID e indica que el ClearToken se está utilizando para autenticación e integridad de mensaje. Este OID en el CryptoToken de extremo a extremo también indica, implícitamente, la utilización de DH durante el arranque rápido.
"Q"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 22}	Se utiliza en el procedimiento IV e indica que el ClearToken en el enlace salto por salto transporta un testigo Diffie-Hellman.
"W"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 23}	Se utiliza en el procedimiento IV como un algoritmo OID e indica la utilización de una firma digital basada en SHA1 de RSA.

SERIES DE RECOMENDACIONES DEL UIT-T

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

Ginebra, 2002