Unión Internacional de Telecomunicaciones

UIT-T H.235.3

(09/2005)

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

SERIE H: SISTEMAS AUDIOVISUALES Y MULTIMEDIOS

Infraestructura de los servicios audiovisuales – Aspectos de los sistemas

Marco de seguridad H.323: Perfil de seguridad híbrido

Recomendación UIT-T H.235.3

Unión Internacional de Telecomunicaciones

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.235.3

Marco de seguridad H.323: Perfil de seguridad híbrido

Resumen

El objetivo de esta Recomendación es describir un perfil de seguridad híbrido eficaz y adaptable para la versión 2 y versiones posteriores de la Rec. UIT-T H.235.0, basado en la infraestructura de clave pública (PKI). En él se aprovechan los perfiles de seguridad de las Recs. UIT-T H.235.1 y H.235.2, gracias a la utilización de las firmas digitales de la Rec. UIT-T H.235.2 y del perfil de seguridad básico de la Rec. UIT-T H.235.1.

En versiones anteriores de las subseries H.235, este perfil se incluía en el anexo F/H.235. En los apéndices IV, V y VI de H.235.0 se indica la correspondencia entre las cláusulas, las figuras y los cuadros de las versiones 3 y 4 de H.235.

Orígenes

La Recomendación UIT-T H.235.3 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

Autenticación, certificado, criptación, firma digital, gestión de claves, integridad, perfil de seguridad, seguridad de multimedia.

PREFACIO

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

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

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

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

NOTA

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

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

PROPIEDAD INTELECTUAL

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

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

© 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

Recomendación UIT-T H.235.3

Marco de seguridad H.323: Perfil de seguridad híbrido

1 Alcance

El objetivo de esta Recomendación es describir un perfil de seguridad híbrido eficaz y adaptable para la versión 2 y versiones posteriores de la Rec. UIT-T H.235.0, basado en la infraestructura de claves públicas (PKI, *public key infrastructure*). En él se aprovechan los perfiles de seguridad de las Recs. UIT-T H.235.1 y H.235.2, gracias a la utilización de las firmas digitales de la Rec. UIT-T H.235.2 y del perfil de seguridad básico de la Rec. UIT-T H.235.1.

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 comunicaciones multimedios por paquetes*.

– Recomendación UIT-T H.235, versión 1 (1998), *Seguridad y criptado para terminales multimedios de la serie H (basados en las Recomendaciones H.323 y H.245)*.

– 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.235.0 (2005), *Marco de seguridad H.323: Marco de seguridad para sistemas multimedia 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.235.2 (2005), *Marco de seguridad H.323: Perfil de seguridad de firma*.

– Recomendación UIT-T H.235.6 (2005), *Marco de seguridad H.323: Perfil de criptación vocal con gestión de claves H.323 y H.245 nativa.*

– 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 Q.931 (1998), *Especificación de la capa 3 de la interfaz usuario-red de la red digital de servicios integrados para el control de la llamada básica*.

– Recomendación UIT-T X.509 (2005) | ISO/CEI 9594-8:2005, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marcos para certificados de claves públicas y de atributos*.

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

ISO 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*.

– Recomendación UIT-T X.803 (1994) | ISO/CEI 10745:1995, *Tecnología de la información – Interconexión de sistemas abiertos – Modelo de seguridad de capas superiores*.

– Recomendación UIT-T X.810 (1995) | ISO/CEI 10181-1:1996, *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: Visión general*.

– Recomendación UIT-T X.811 (1995) | ISO/CEI 10181-2:1996, *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: Marco de autenticación*.

– IETF RFC 3280 (2002), *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.

2.2 Referencias informativas

[ISO|CEI 14888-3] ISO/CEI 14888-3:1998, *Information technology – Security techniques – Digital signatures with appendix; Part 3: Certificate-based mechanisms*.

[PKCS] PKCS #1 v2.0: *RSA Cryptography Standard;* RSA Laboratories; October 1, 1998; http://www.rsa.com/rsalabs/pubs/PKCS/index.html.

[PKCS] PKCS #7: *Cryptographic Message Syntax Standard*, An RSA Laboratories Technical Note, version 1.5, Revised November 1, 1993; http://www.rsa.com/rsalabs/pubs/PKCS/index.html.

[RFC1321] IETF RFC 1321 (1992), *The MD5 Message-Digest Algorithm*.

3 Términos y definiciones

A los efectos de esta Recomendación, se aplican las definiciones de esta cláusula junto con las de las cláusulas 3/H.323, 3/H.225.0 y 3/H.245. Algunos de los siguientes términos tienen el sentido de las definiciones de las Recs. UIT-T X.800 | ISO 7498-2, X.803 | ISO/CEI 10745, X.810 | ISO/CEI 10181-1, X.811 | ISO/CEI 10181-2 y H.235.0.

4 Abreviaturas, siglas o acrónimos

En esta Recomendación se utilizan las siguientes abreviaturas, siglas o acrónimos.

ALG Pasarela de nivel de aplicación (*application level gateway*)

ASN.1 Notación de sintaxis abstracta uno (*abstract syntax notation one*)

BRJ Rechazo de anchura de banda (*bandwidth reject*)

BRQ Petición de anchura de banda (*bandwidth request*)

CA Autoridad de certificación (*certification authority*)

CRL Lista de revocación de certificados (*certificate revocation list*)

DB Base de datos (*database*)

DH	Diffie-Hellman
DN	Nombre distinguido (*distinguished name*)
EP	Punto extremo (*endpoint)*
GCF	Confirmación de controlador de acceso (*gatekeeper confirm)*
GK	Controlador de acceso (*gatekeeper)*
GKID	Identificador de controlador de acceso (*gatekeeper identifier*)
GKSP	Procesador de seguridad de controlador de acceso (*gatekeeper security processor*)
GRJ	Rechazo de controlador de acceso (*gatekeeper reject*)
GRQ	Petición de controlador de acceso (*gatekeeper request)*
HMAC	Código de autenticación de mensaje troceado (*hashed message authentication code)*
ICV	Valor de comprobación de integridad (*integrity check value*)
ID	Identificador (*identifier*)
IP	Protocolo Internet (*Internet protocol*)
LDAP	Protocolo ligero de acceso al directorio (*lightweight directory access protocol*)
LRQ	Petición de localización (*location request*)
MCU	Unidad de control multipunto (*multipoint control unit*)
MD5	Message digest 5
NAT	Traducción de dirección de red (*network address translation*)
OID	Identificador de objeto (*object identifier*)
PDU	Unidad de datos de protocolo (*protocol data unit*)
PKI	Infraestructura de claves públicas (*public key infrastructure*)
RAS	Registro, admisión y estado (*registration, admission and status*)
RCF	Confirmación de registro (*registration confirm)*
RRJ	Rechazo de registro (*registration reject*)
RRQ	Petición de registro (*registration request)*
RSA	Algoritmo de criptación de Rivest, Shamir y Adleman
RTP	Protocolo de transporte en tiempo real (*real-time transport protocol*)
SHA	Algoritmo troceado asegurado (*secure hash algorithm*)
UDP	Protocolo de datagrama de usuario (*user datagram protocol*)
URQ	Petición de desregistro (*unregistration request*)
VoIP	Voz sobre el protocolo Internet (*voice-over-IP*)

5 Convenios

En esta Recomendación se utilizan los siguientes convenios en lo relativo al nivel de obligación:

– La obligación firme se expresa con el futuro simple del verbo (futuro de mandato) o expresiones con significado de obligación.

– La conveniencia, es decir una acción aconsejada pero no obligatoria, se expresa con el condicional del verbo modal "deber" o expresiones que indican conveniencia.

– La opción se expresa mediante el presente de indicativo del verbo "poder" o expresiones de posibilidad.

En el perfil de seguridad híbrido se utilizan términos y definiciones provenientes de las Recs. UIT-T H.235.1 y H.235.2.

Si bien el servicio de integridad de mensaje siempre proporciona autenticación de mensaje, lo contrario no siempre es cierto. En el modo sólo autenticación, no puede garantizarse más que la integridad de 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 e integridad utiliza el mismo material de claves sin afectar por ello la seguridad.

Este perfil de seguridad es aplicable en entornos en los cuales puede haber muchos terminales y no pueden asignarse contraseñas estáticas y/o claves simétricas, por ejemplo las implementaciones de cobertura muy grande o mundial. Este perfil de seguridad supone la disponibilidad de una infraestructura de claves públicas con certificados asignados y claves privadas/públicas, directorios, etc. Además, en este perfil de seguridad se utilizan técnicas de criptación simétrica cuando corresponde.

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 y puede señalar, por ejemplo, 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).

6 Consideraciones generales

En esta Recomendación se describe un perfil de seguridad híbrido, basado en la PKI, eficaz y adaptable, en el que se utilizan las firmas digitales de H.235.2 y el perfil de seguridad básico de H.235.1. Esta Recomendación se sugiere como una opción. Las entidades de seguridad H.323 (terminales, controladores de acceso, pasarelas, MCU, etc.) pueden implementarlo 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 la Rec. UIT-T H.235.2 sí se aplican, pero simplificados, y se utilizan firmas digitales conformes a los procedimientos RSA. Sin embargo, las firmas digitales se utilizan sólo cuando es absolutamente necesario, y en otros casos se emplean técnicas de seguridad simétrica sumamente eficientes del perfil de seguridad básico descrito en la Rec. UIT-T H.235.1.

El perfil de seguridad híbrido conviene a la telefonía IP "mundial" adaptable (o "escalable"). Cuando se aplica estrictamente, este perfil de seguridad supera las limitaciones del perfil de seguridad básico simple descrito en H.235.1 y resuelve ciertos inconvenientes de H.235.2, 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. Los usuarios pueden entonces elegir más fácilmente su proveedor VoIP, soportándose así cierto tipo de movilidad de usuario. En él se utiliza

la criptografía asimétrica con firmas y certificados solamente cuando es necesario y en otros casos técnicas simétricas más simples y eficientes. Permite la tunelización de los mensajes H.245 para la integridad de los mismos y también implementa algunas disposiciones para el no repudio de mensajes.

Con el perfil de seguridad híbrido es obligatorio utilizar el modelo con encaminamiento por GK y se utilizan las técnicas de tunelización H.245. Se están estudiando otras disposiciones aplicables a los modelos que no tienen encaminamiento por GK.

Las prestaciones ofrecidas por este perfil incluyen:

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

– La autenticación de usuario (entidad reconocida), sin importar el número de saltos del nivel de aplicación que atraviese el mensaje.

  NOTA 1 – Por salto se entiende un elemento de red H.235 fiable (por ejemplo, GK, GW, MCU, un apoderado (*proxy*), o un cortafuegos (*firewall*)). Es decir, cuando la seguridad salto por salto en el nivel de aplicación se garantiza con técnicas simétricas, no puede garantizarse una verdadera seguridad extremo a extremo entre terminales.

– La integridad de todas las porciones o las porciones críticas (campos) de los mensajes que llegan a una entidad, cualquiera que sea el número de saltos atravesados por el mensaje en el nivel de aplicación. La integridad del propio mensaje obtenida mediante un número aleatorio generado de forma fuerte es también facultativa.

– Las garantías de autenticación, integridad y no repudio (parciales) 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 correcta prestación de estos servicios de seguridad evita varios tipos de ataques, por ejemplo:

– *Ataques por intromisión*: la autenticación e integridad de los mensajes salto por salto en el nivel de aplicación evita tales ataques cuando la entidad entrometida 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.

– *Simulación*: la autenticación del usuario evita estos ataques.

– *Asaltos a la conexión*: la utilización de autenticación/integridad para cada mensaje de señalización evita estos ataques.

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 segura 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 segura 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 transmitir el mensaje FACILITY (FACILIDAD) de actualización de clave, y es útil, por ejemplo, en llamadas de muy larga duración.

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

NOTA 2 – Los certificados RSA con generación MD5 ([RFC 1321]) no forman parte de este perfil de seguridad.

Cabría utilizar, facultativamente, el perfil de seguridad con criptación vocal de H.235.6 (véase 6.1/H.235.6) junto con el perfil de seguridad híbrido. Su uso se negocia como parte de la señalización de establecimiento de la comunicación.

Cuadro 1/H.235.3 – Visión general del perfil de seguridad híbrido

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

La solución de esta Recomendación se puede aplicar para proteger la integridad de todo el mensaje. Para RAS H.225.0, la protección de integridad cubre el mensaje RAS completo; en el caso de la señalización de llamada cubre el mensaje completo de señalización de llamada, H.225.0, incluidos los encabezamientos Q.931.

El usuario debería utilizar un esquema de firma con clave pública/privada para la autenticación. Este esquema generalmente ofrece mejor integridad.

Esta Recomendación no describe procedimientos de registro, certificación y atribución de certificados desde una tercera parte fiable ni 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. Son procedimientos que pueden realizarse por medios que no forman parte de esta Recomendación.

Las entidades de comunicación que intervienen pueden determinar implícitamente la utilización, bien de los perfiles de seguridad básicos H.235.1, del perfil de firma H.235.2, 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 la cláusula 10/H.235.2).

6.1 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.

6.2 Autenticación e integridad

En esta Recomendación se utilizan los siguientes términos para la prestación de servicios de seguridad.

Autenticación e integridad: Un servicio de seguridad combinado que soporta la integridad de los mensajes junto con la autenticación de usuario. El usuario se autentica cuando aplica correctamente la firma digital a algún dato con clave privada, o bien cuando aplica correctamente el secreto compartido pertinente. 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 de los bits de utilización de clave en la clave de firma (en el certificado) (véase también RFC 3280).

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 la utilización 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.

Conforme a 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, proporcionando 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. Lo hacen fijando el motivo de rechazo a **securityDenial** u otro código de error de seguridad apropiado de acuerdo a 11.1/H.235.0. Dependiendo de la capacidad para reconocer un ataque y de la manera más adecuada para reaccionar en estos casos, un controlador de acceso que recibe un **xRQ** protegido, cuyos identificadores de objeto (**tokenOID**, **algorithmOID**) no están definidos, debería responder con un **xRJ** no protegido y con un motivo de rechazo fijado a **securityDenial**, pero también puede descartar este mensaje. El punto extremo descartará el mensaje no protegido recibido y se desconectará, pero puede intentarlo otra vez con otros OID. Muy probablemente, un controlador de acceso que recibe un mensaje SETUP de señalización de llamada H.225.0 protegido, cuyos identificadores de objeto (**tokenOID**, **algorithmOID**) no están identificados, debería responder con un mensaje RELEASE COMPLETE no protegido y con el motivo de rechazo fijado a **securityDenied**, pero también puede descartar este mensaje. Ahora bien, un controlador de acceso que reciba un FACILITY H.225.0 protegido, cuyos identificadores de objeto (**tokenOID**, **algorithmOID**) no están identificados, debería responder con un FACILITY no protegido y con el motivo fijado a **undefinedReason**, pero también puede descartar este mensaje. De igual manera, se debe guardar registro del problema de seguridad encontrado. Como parte de la

respuesta retornada, el emisor puede proporcionar una lista de certificados aceptables en testigos separados, a fin de facilitar al receptor 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 la cláusula 13) y en los campos del mensaje que han sido llenados. En esta Recomendación se hace referencia a los identificadores de objeto mediante letras (por ejemplo, "A").

Este perfil no utiliza los campos ICV H.235. En su lugar, se introducen valores de comprobación de la integridad criptográfica en el campo **signature** del **token** en el **cryptoSignedToken** cuando se hace referencia a H.235.2, o en los campos de troceado del **CryptoToken** cuando se hace referencia a H.235.1.

7 Procedimiento IV

Cuando se emplea el procedimiento IV para la seguridad salto por salto, deberán aplicarse los siguientes procedimientos. El procedimiento IV combina el procedimiento I de la cláusula 7/H.235.1 y el procedimiento II de la cláusula 7/H.235.2.

Para el primer mensaje, incluida la respuesta correspondiente, enviado en cada sentido de transmisión, se utilizará el procedimiento II de H.235.2 (autenticación e integridad salto por salto, véase la cláusula 7/H.235.2) 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 híbrido.

– **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 la cláusula 12/H.235.2).

– **certificate** debería contener el certificado de usuario del emisor si el receptor no lo ha obtenido por otro medio; **type** contendrá OID "W", que indica que se incluye un certificado RSA-SHA1, u OID "P" (véase la cláusula 20/H.235.2), en cuyo caso **certificate** contiene un URL.

En un escenario con un solo dominio administrativo, el "primer mensaje/respuesta" se define como el mensaje/respuesta RAS H.225.0 inicial, 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 es SETUP.

Siempre que se transporte un certificado digital en un mensaje, la entidad receptora verificará si la identidad del emisor coincide con la identidad del certificado, conforme al procedimiento de la cláusula 14/H.235.2, para evitar ataques por intromisión.

El emisor y el receptor intercambian y calculan una cadena de bits secreta Diffie-Hellman autenticada. En el cuadro 4/H.235.6 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 criptación 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 la Rec. UIT-T H.235.1.

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 8.5/H.235.6). 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 H.235.1. 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 8.5/H.235.6).

NOTA 1 – En los entornos de encaminamiento directo hay comunicación entre entidades y terminales emisor/receptor. 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 de H.235.1 (véase la cláusula 7/H.235.1) 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 de H.235.1.

Esta Recomendación se puede utilizar con los sistemas de la versión 1 de H.235, teniendo precaución de utilizar los ID de emisores y generalID como se indica en la cláusula 19/H.235.2.

Cabe esperar que un controlador de acceso reciba de un punto extremo fijo determinado solamente una **RRQ** con testigo DH y firma digital. No obstante, algunos mensajes **RCF**/**RRJ** perdidos o retardados pueden provocar una retransmisión en la que se utilice otro **RRQ** firmado.

Cuando la correspondiente respuesta de registro no llegue a tiempo al punto extremo, éste puede intentarlo de nuevo. En este caso, el punto extremo debe utilizar el testigo DH más reciente, pero el número de secuencia y la indicación de tiempo serán diferentes.

Para un punto extremo fijo determinado, el controlador de acceso ha de utilizar el más reciente de los mensajes **RRQ** firmados recibidos y establecer el secreto compartido a partir del testigo DH, aunque el GK tenga ya un secreto compartido disponible. Es decir, el GK debe reemplazar cualquier secreto compartido existente por el nuevo. El GK tiene que responder con una **RCF** firmada que tenga el testigo DH de respuesta. Conviene que se genere de nuevo el testigo DH de respuesta.

NOTA 2 – El método recomendado y preferido para actualizar la clave es el que utiliza el mensaje FACILITY, como se define en la cláusula 9. No obstante, se reconoce que la clave se puede actualizar mediante otro **RRQ** firmado aditivo con un nuevo testigo DH.

NOTA 3 – Un controlador de acceso que posea un secreto compartido ha de responder a un **RRQ** protegido por HMAC (conforme a la Rec. UIT-T H.235.1) con un mensaje de respuesta por HMAC.

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.

Esto es, la asociación de seguridad abarca todas las llamadas entre un par fijo de entidades mientras esté activo 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 1.

Al contrario, cuando no se valida el indicador **multipleCalls** en SETUP, se calculará de nuevo, individualmente, una clave de enlace para cada llamada.

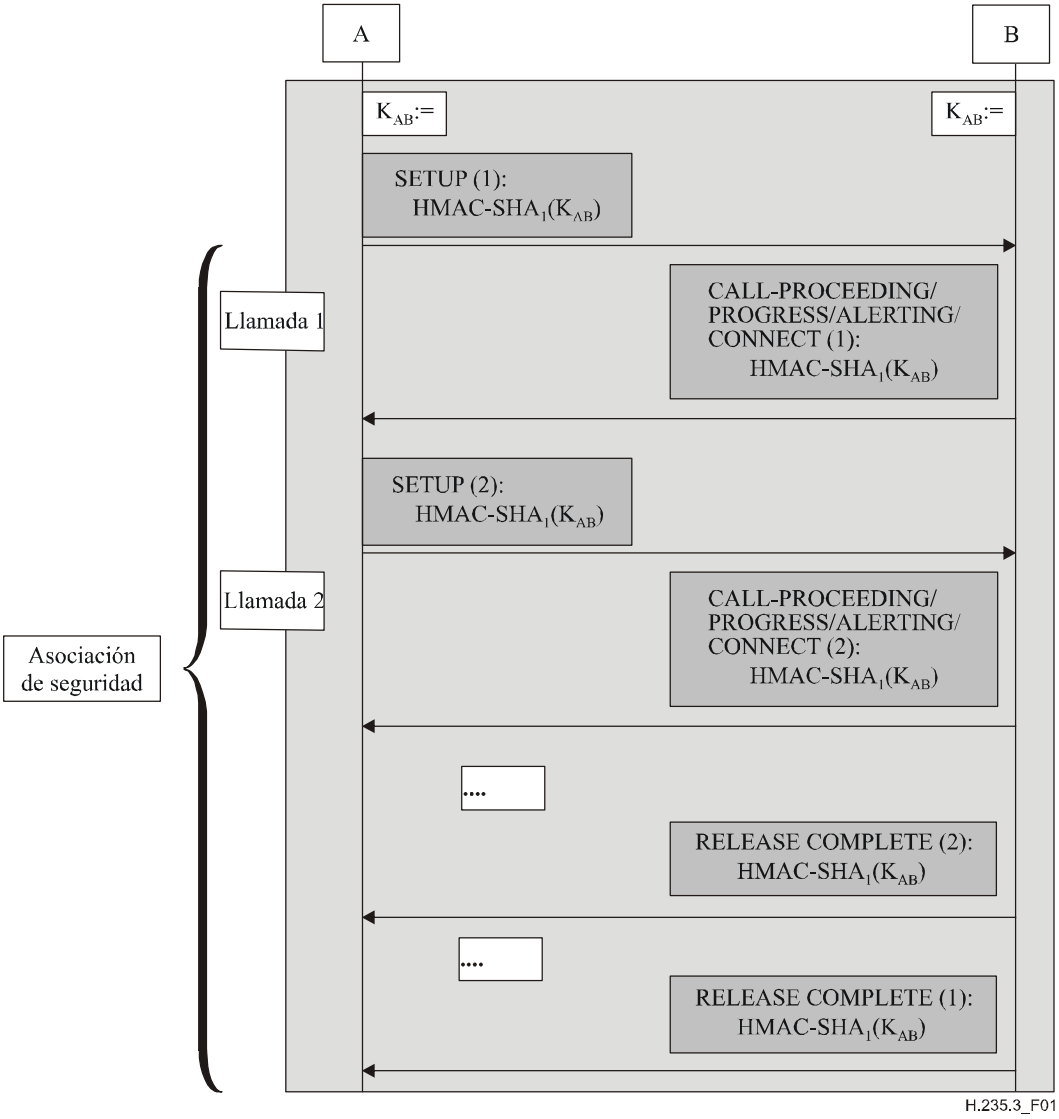


Figura 1/H.235.3 – Asociación de seguridad para llamadas concurrentes

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 debería ser iniciada por cualquier entidad que considere que la necesita. Puede ser conveniente actualizarla cuando la clave de sesión no ofrece todas las garantías, si hay motivos para pensar que ya no es o no será segura, y por 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 receptor contesta con un mensaje FACILITY similar que transporta su testigo Diffie-Hellman, un certificado digital facultativo, y su firma digital. Una vez finalizado el procedimiento de actualización de clave, el iniciador y el receptor 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 8.5/H.235.6).

El mensaje FACILITY para fines de actualización de clave se protegerá de conformidad con el procedimiento II/H.235.2. No se podrán utilizar otros mensajes FACILITY sin el testigo Diffie-Hellman para fines de actualización de clave y deberán protegerse conforme al procedimiento I de la cláusula 7/H.235.1.

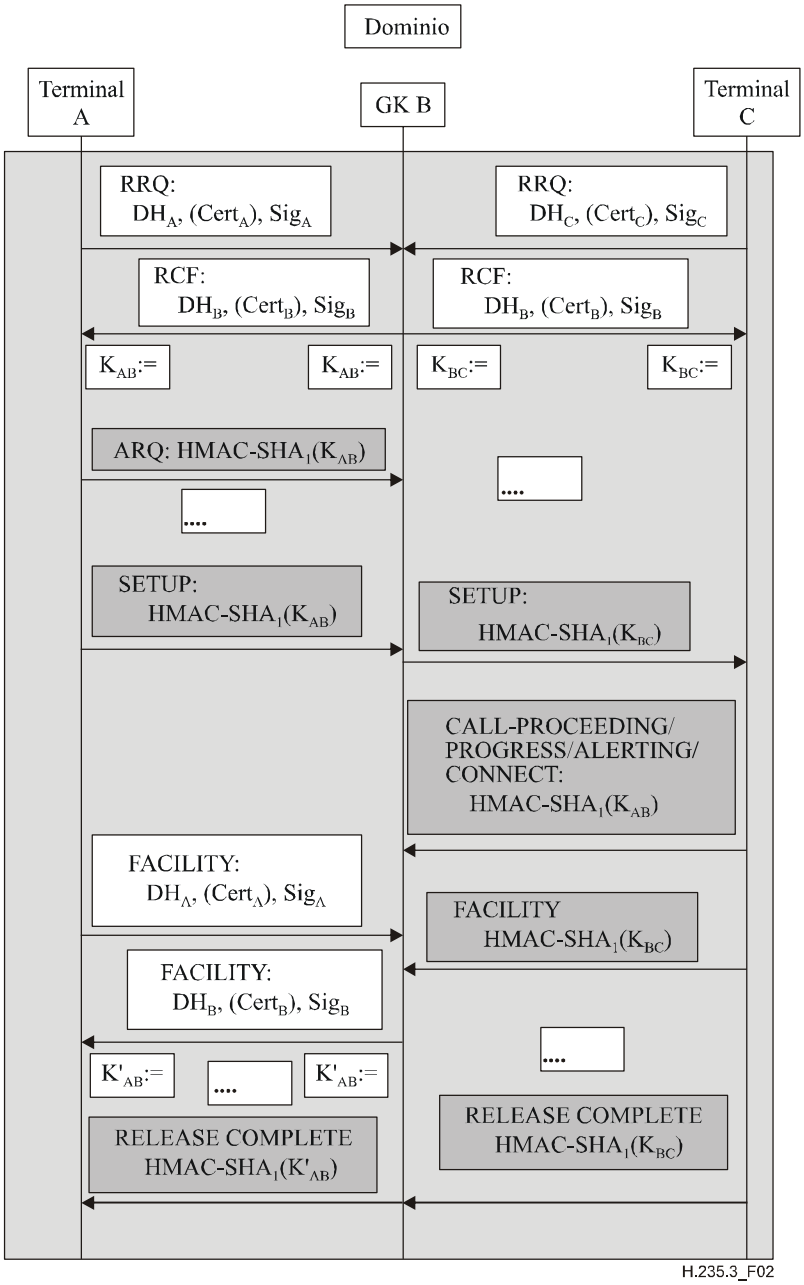
10 Utilización de técnicas basadas en curves elípticas

Queda en estudio.

11 Ejemplos ilustrativos

En los diagramas de flujo de las figuras 2 y 3 se ilustra la utilización de esta Recomendación 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 H.235.2, en tanto que los mensajes en gris oscuro se relacionan con el perfil básico H.235.1. 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 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.



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 2/H.235.3 – Diagrama de flujo en un dominio administrativo simple

NOTA 1 – Las figuras 2 y 3 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 que se trata de un sistema sin arranque rápido de conformidad con 7.3.1/H.323. La figura 2 muestra también el procedimiento de actualización de clave entre el terminal A y el controlador de acceso B mediante FACILITY.

En la figura 3 se muestra un ejemplo de 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 2, también puede aplicarse entre ambos dominios durante la fase de establecimiento de la comunicación.

NOTA 2 – En la figura 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 3 se ilustra también el procedimiento de actualización de clave entre ambos dominios mediante FACILITY.

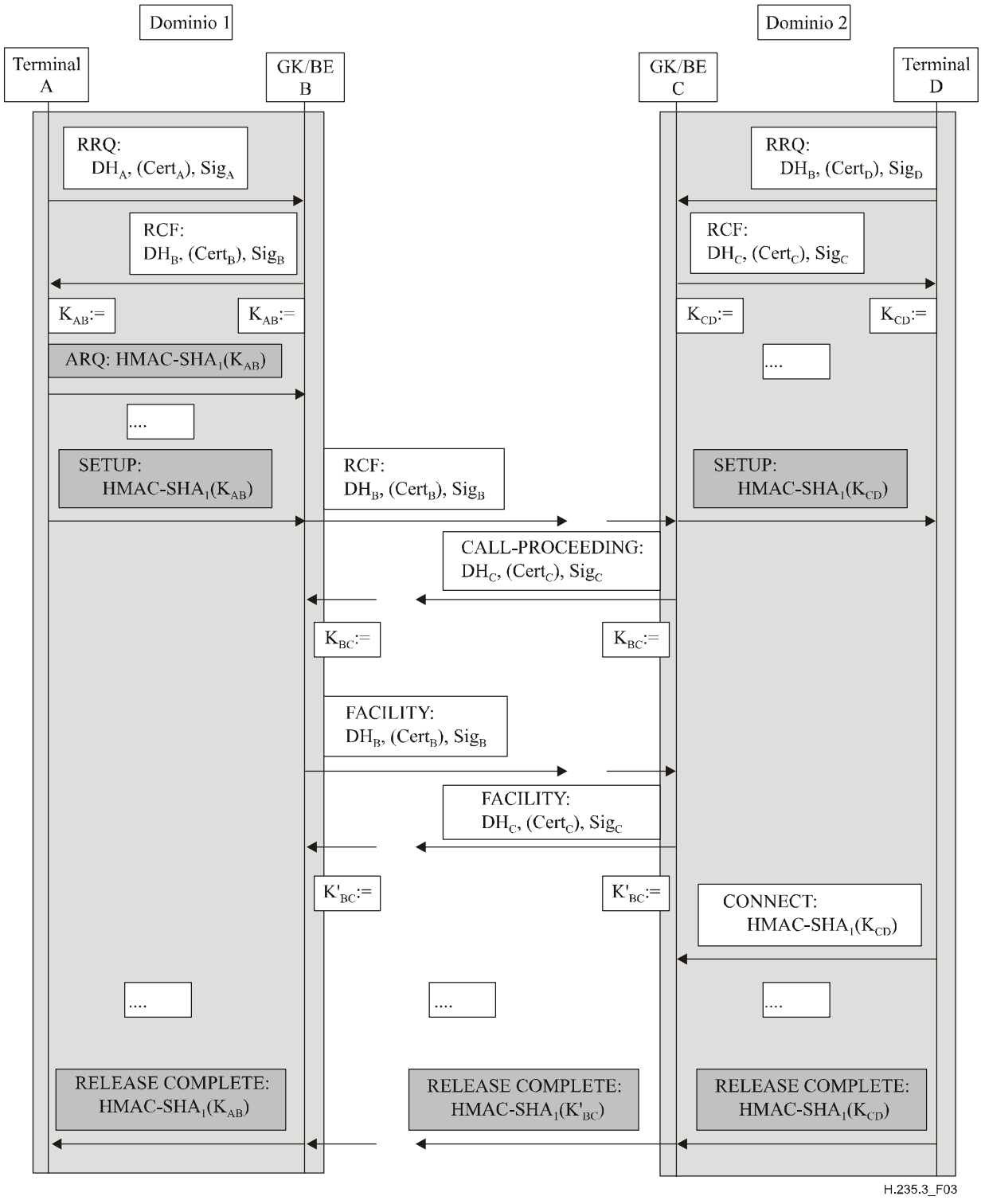


Figura 3/H.235.3 – Diagrama de flujo con varios dominios administrativos

12 Comportamiento multidifusión

Los mensajes multidifusión H.225.0 tales como **GRQ** o **LRQ** incluirán un **CryptoToken** de conformidad con el procedimiento II sin especificación de **generalID**. Cuando dichos mensajes se envían en modo unidifusión, el mensaje incluirá un **CryptoToken** con especificación de **generalID**.

13 Lista de mensajes de señalización seguros

El procedimiento IV despliega el procedimiento I de H.235.1 o el procedimiento II de H.235.2, lo que depende del escenario y del mensaje real, como se indica a continuación.

13.1 RAS H.225.0

Mensaje RAS H.225.0	Campos de señalización H.235	Autenticación e integridad	No repudio
GatekeeperRequest, GatekeeperConfirm, GatekeeperReject if GK discovery is applied RegistrationRequest, RegistrationConfirm, RegistrationReject if GK discovery is not applied	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.			

13.2 Señalización de llamada H.225.0 (un solo dominio administrativo)

Mensaje de señalización de llamada H.225.0	Campos de señalización H.235	Autenticación e integridad	No repudio
Setup-UUIE, Connect-UUIE (nota 1), Facility-UUIE (nota 2), 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 (nota 3)	CryptoToken	Procedimiento II	Procedimiento II
NOTA 1 – Se supone que cualquiera de los dos mensajes es el primero en cada sentido de transmisión. NOTA 2 – No se utiliza para actualización de clave. NOTA 3 – Se utiliza para actualización de clave.			

13.3 Señalización de llamada H.225.0 (varios dominios administrativos)

Mensaje de señalización de llamada H.225.0	Campos de señalización H.235	Autenticación e integridad	No repudio
Setup-UUIE, Connect-UUIE (nota 1), Alerting-UUIE (nota 2), CallProceeding-UUIE, Facility-UUIE (nota 3), Progress-UUIE, Information-UUIE, ReleaseComplete-UUIE	CryptoToken, ClearToken	Procedimiento II	Procedimiento II
Alerting-UUIE (nota 4), CallProceeding-UUIE, Facility-UUIE (nota 5), Progress-UUIE, Information-UUIE, ReleaseComplete-UUIE, Status-UUIE, StatusInquiry-UUIE, SetupAcknowledge-UUIE, Notify-UUIE	CryptoToken, ClearToken	Procedimiento I	Procedimiento I
NOTA 1 – Se supone que cualquiera de los dos mensajes es el primero en cada sentido de transmisión. NOTA 2 – Cualquiera de estos mensajes se transmite como primer mensaje en cualquier sentido. NOTA 3 – Se utiliza para actualización de clave. NOTA 4 – Ninguno de estos mensajes se transmite como primer mensaje en cualquier sentido. NOTA 5 – No se utiliza para actualización de clave.			

14 Lista de identificadores de objeto

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

Cuadro 2/H.235.3 – Identificadores de objeto

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 de la Rec. UIT-T H.235.2 para el CryptoToken-tokenOID e indica que la firma/troceado RSA incluye todos los campos en los mensajes RAS/ o de señalización de llamada 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 de la Rec. UIT-T H.235.2 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.

Apéndice I

Procesador de seguridad de controlador de acceso conforme a H.235.3

En este apéndice informativo se describe un ejemplo de utilización de un procesador de seguridad de controlador de acceso (GKSP) conforme a H.235.3 combinado con un controlador de acceso (GK). El GKSP traspasa desde un GK monolítico hacia una entidad funcional GKSP independiente varias de las tareas de seguridad pertinentes a H.235.3, por ejemplo la ejecución de funciones Diffie-Hellman que consumen muchos recursos, los cálculos y verificaciones de firmas digitales y el tratamiento de los certificados X.509. Si bien hay por lo menos una entidad GKSP por cada GK, uno solo de éstos puede también prestar servicios a varios GKSP, haciendo que se puedan atender más puntos extremos (aumento de la "escalabilidad") y mejorando la robustez de todo el sistema.

En la figura I.1 se presenta una arquitectura de GK fraccionado en la que un GKSP cumple las funciones de seguridad H.235.3.

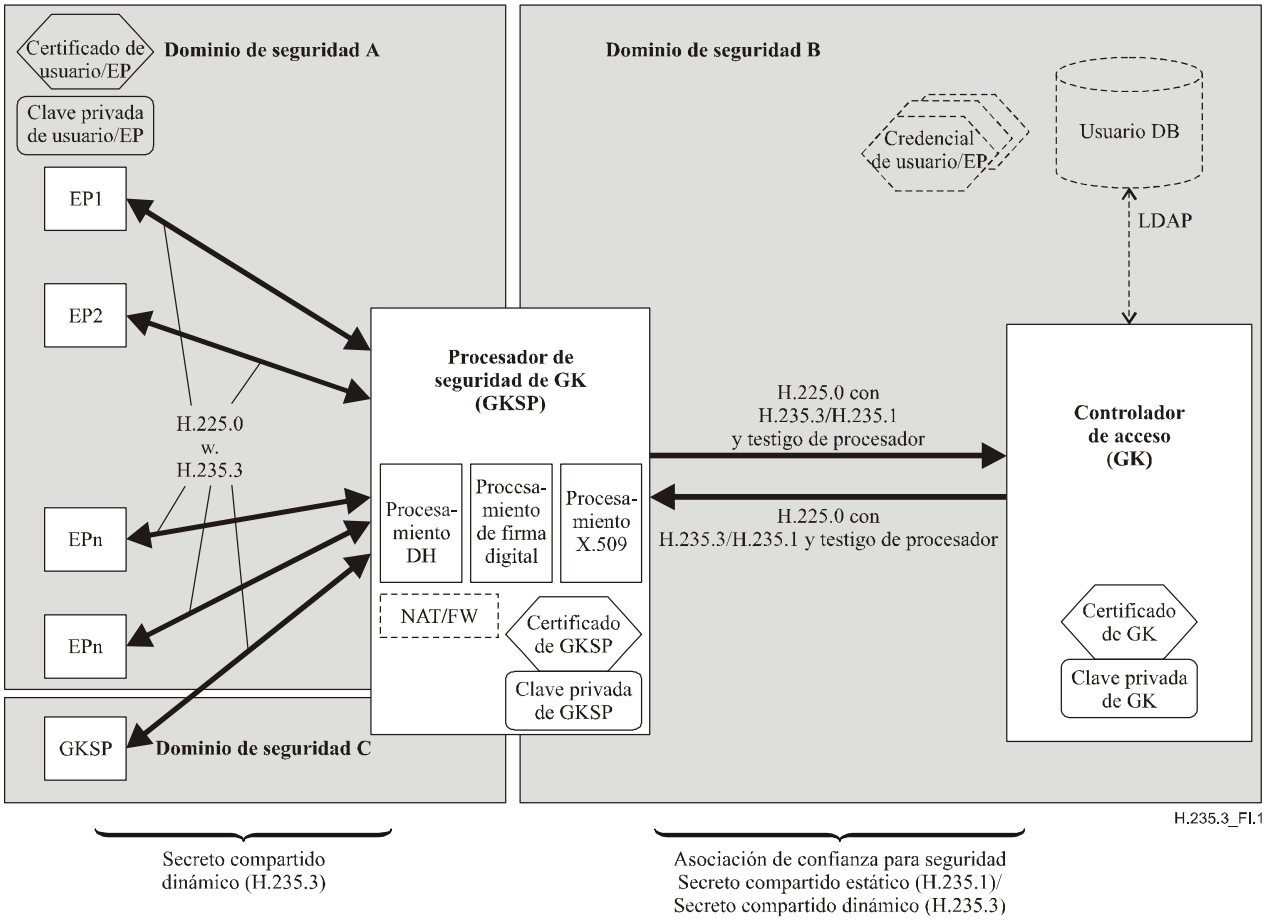


Figura I.1/H.235.3 – Arquitectura de procesador de seguridad de controlador de acceso

NOTA 1 – El GKSP también puede realizar otras funciones útiles, por ejemplo la de traducción de direcciones de red (NAT), de cortafuegos, de pasarela de nivel de aplicación (ALG, *application level gateway*) etc. Estas funciones pueden formar parte del tratamiento de seguridad o ser funciones internas independientes, pero no se describen en esta cláusula y quedan en estudio.

El GKSP está en relación con varios puntos extremos (EP) dentro del dominio administrativo de seguridad A y también puede comunicarse con otro GKSP en un dominio administrativo de seguridad C (que no se indica en la figura).

NOTA 2 – En la práctica no es necesario que los tres dominios administrativos de seguridad sean distintos. Es posible definir enteramente el GKSP dentro del dominio administrativo de seguridad B al que pertenece el GK, definirlo en el dominio A o en un dominio propio independiente (que no se muestra en la figura).

Al utilizar el GKSP, el GK no necesita desempeñar ciertas funciones de seguridad que consumen mucha potencia de cálculo. Ahora bien, el GK sigue encargándose de la autorización y la admisión mediante la verificación de correspondencia de la credencial adecuada (por ejemplo, seudónimo, nombre distinguido (DN), número de serie de certificado, certificado X.509) con la base de datos (interna o externa) en la que figuran los usuarios abonados, sus permisos y credenciales. En la cláusula I.3 se definen las credenciales convenientes para los GKSP conformes a H.235.3.

NOTA 3 – Esta Recomendación no se aplica a una posible interfaz LDAP entre el GK y la base de datos abonado/usuario. También se deja a discreción del GK decidir cuáles son los criterios y credenciales (por ejemplo, seudónimo, DN o número de serie de certificado) necesarios para controlar el acceso. No se especifica cuáles credenciales (por ejemplo, seudónimo, DN y número de serie de certificado) han de almacenarse en dichas bases de datos.

NOTA 4 – El GKSP no tiene que ocuparse de asuntos relativos a la configuración o administración de usuarios o abonados, ni requiere acceder a sus bases de datos.

NOTA 5 – Los EP en los que se utilizan H.235.3 y el GKSP también suelen tener un certificado raíz (este caso no se muestra en la figura I.1), que permite a la entidad verificar el certificado de otra entidad (EP, GKSP).

La comunicación entre el GKSP y su GK, o entre dos GKSP, es segura. Puede ser conforme a H.235.1 cuando se supone que hay un secreto compartido configurado estáticamente o H.235.3 que permite establecer un secreto compartido dinámico. En ambos casos se supone que el GK y el GKSP han establecido una relación de confianza mutua, ya sea a través de una asociación de seguridad estática o dinámica. De tratarse de varios GKSP, es posible concatenar las relaciones de confianza.

En consecuencia, el GK confía en que el GKSP puede efectuar los procedimientos de autenticación de extremo lejano y realizar correctamente los de seguridad. El GKSP informa al GK del resultado del procesamiento de seguridad mediante una simple afirmación de seguridad en el testigo de procesador.

Se supone que cada EP conforme a H.235.3 y el GKSP tienen certificados X.509 que verifican de forma fiable la identidad del propietario legítimo de la clave pública por comparación con una clave privada correspondiente para firma.

NOTA 6 – En la figura I.1 no se muestra explícitamente la clave pública correspondiente a la clave privada; en general, la clave pública certificada se transporta dentro del certificado X.509 de usuario/EP.

NOTA 7 – No se muestran todos los certificados o claves privadas de todos los puntos extremos o GKSP.

NOTA 8 – El certificado GKSP suele ser un certificado de servidor.

Es necesario un certificado distinto y único, y una clave privada para el GK únicamente si se ha implementado H.235.3 para la comunicación con el GKSP.

El GKSP es un apoderado basado en estados que funciona entre los EP y el GK, o entre dos GK. Hay por lo menos una entidad GKSP por cada GK, pero también es posible que un GK comunique con varios GKSP, haciendo que se puedan atender más EP (aumento de la escalabilidad) y mejorando la robustez de todo el sistema. Es posible ordenar los elementos de un GKPS específicos de H.235.3 en una configuración lineal en cadena (figura I.2) o en una arquitectura jerárquica como se muestra en la figura I.3.

Si bien existe como mínimo una entidad genérica GKSP por cada GK, un solo GK puede atender múltiples GKSP genéricos, con lo cual se pueden cubrir más EP y se incrementa la robustez de todo el sistema. Puede haber uno o varios GKSP genéricos entre un EP y un GK. Siendo así, es posible que haya configuraciones en cascada, lineales o jerárquicas, de varios GKSP. Un EP establecerá

siempre una relación de confianza con su GK asociado a través de uno o varios GKSP. Un GK puede tener múltiples relaciones de confianza con diversos EP.

En la figura I.2 se presenta una arquitectura de elementos de GKSP conectados en cadena.

Figura I.2/H.235.3 – Arquitectura GKSP en cadena

En la figura I.2, el GKSP1 autentica el mensaje RRQ recibido del EP1, mientras el GK1 o el GK2 deciden si se autoriza el EP1. El GKSP1 y el GKSP2 (resp. GKSP3 y GKSP4) retransmiten los mensajes de señalización H.323 entre el EP1 y el GK1 (resp. GK1 y GK2).

En la figura I.3 se muestra una arquitectura jerárquica con elementos de GKSP en cascada.

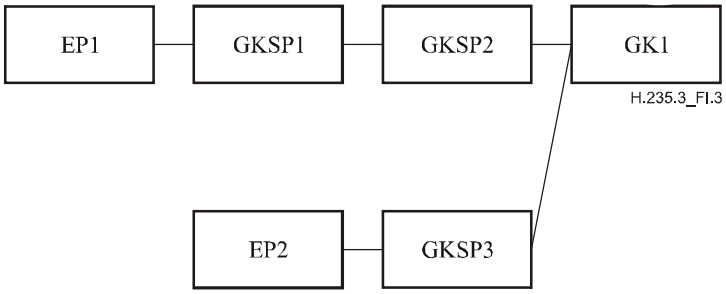


Figura I.3/H.235.3 – Arquitectura GKSP jerárquica

El GKSP tiene por lo menos una dirección IP y es, por regla general, un dispositivo de seguridad de borde que se encuentra en la frontera entre dos dominios administrativos de seguridad diferentes. Por consecuencia, puede poseer dos direcciones IP, una hacia los EP H.323 o el GKSP par (dominios administrativos de seguridad A y C) y otra interna hacia el GK (dominio administrativo de seguridad B).

I.1 Descubrimiento de un procesador de seguridad de controlador de acceso

Se supone que un EP H.323 no necesita saber si hay un GKSP. Es posible que el EP haya configurado la dirección IP del GKSP como punto de contacto del GK. El comportamiento del EP es el mismo con o sin GKSP. El EP puede emplear la fase de descubrimiento de GK y servirse de **GRQ** para ubicar a su GKSP.

Un GKSP que comunique con el EP solicitante debe determinar si el GK correspondiente soporta un procesador de seguridad.

Cuando el GKSP pretenda emplear H.235.1 en su comunicación con el GK pero no se haya configurado un secreto compartido entre ambos, retorna **GRJ** al EP con **reason** puesta a **securityDenial**/**securityDenied**. De lo contrario, reenvía **GRQ** e incluye un ClearToken de procesador y especifica el elemento de perfil atribuyendo el ID 0 conforme al cuadro I.1. Puesto que en este caso el GK soporta el GKSP, retorna un **GCF**/**GRJ** e incluye un testigo de procesador.

Si el GKSP va a emplear H.235.3 en su comunicación con el GK, le reenvía un **GRQ** que contenga un ClearToken de procesador y especifica el elemento de perfil atribuyendo el ID 0 conforme al cuadro I.1. Un GK que acepte los GKSP y sea conforme a este apéndice responderá mediante un **GCF** y un ClearToken de procesador.

Un GK que no soporte procesador de seguridad o que no funcione conforme a este apéndice ignorará el testigo de procesador y responderá con **GCF**/**GRJ**. El GKSP reconoce la situación, pues no hay testigo de procesador en el **GRQ**/**GRJ** recibido, y envía entonces al EP un **GRJ** especificando el motivo (**reason**) **securityDenial**/**securityDenied**.

Sabiendo que existe un GKSP, un GK que reciba un **GRQ** directamente de un EP sin que haya transitado por un GKSP responderá con un **GRJ** y especificará el motivo (**reason**) **securityDenial**/**securityDenied** (sin incluir testigo de procesador).

I.2 Funcionamiento de un procesador de seguridad de controlador de acceso

Un procesador de seguridad desempeña, como mínimo, las siguientes funciones:

– Terminar el protocolo H.235.3 con los EP H.323 o el GKSP par, conforme al procedimiento IV.

– Ejecutar el protocolo H.235.3 Diffie-Hellman con los EP H.323 o el GKSP par; es decir, realizar operaciones de exponenciación modular Diffie-Hellman.

– Verificar las firmas digitales recibidas, que envían los EP H.323 o del GKSP par en mensajes H.235.3 seguros.

– Comprobar la seguridad de los certificados digitales X.509 recibidos, es decir verificar el trayecto, la validez, la CRL, etc.

– Cuando se trate de mensajes reenviados desde el GKSP hacia el GK o hacia otro GKSP, debe generar nuevos testigos H.235 (H.235.1 o H.235.3). El GKSP emplea su identificador de GKSP como **sendersID** y el del GK (GKID) como **generalID** en el ClearToken de H.235 básica.

– Cuando se trate de mensajes recibidos desde un EP H.323, incluye un testigo de procesador. Para el mensaje inicial **RRQ**/**GRQ**, el testigo de procesador tiene un elemento perfil de seguridad cuyo ElementID es 0, que indica cuál es el método de autenticación encontrado. El GKSP también puede incluir un elemento de perfil de seguridad cuyo ElementID es 0 en cualquier otro mensaje RAS y/o de señalización de llamada H.225.0.

Además, el testigo de procesador tiene uno o varios elementos de perfil de seguridad que transportan las credenciales.

En el contexto de este apéndice, las siguientes credenciales se consideran apropiadas:

– ElementID 1, para suministrar el asunto (*subject*) encontrado en un certificado X.509.

– ElementID 2, para suministrar el subjectAltName encontrado en un certificado X.509.

– ElementID 3, para suministrar el número de serie encontrado en un certificado X.509.

– ElementID 4, para suministrar el nombre del emisor encontrado en un certificado X.509.

– ElementID 5, para suministrar el identificador de punto extremo del terminal H.323.

NOTA – El GK también puede interpretar el elemento alias H.323 de mensajes H.225.0 como credencial. Puesto que este elemento siempre está presente en los mensajes, no es necesario definir un elemento alias particular en un elemento de perfil de seguridad.

Asimismo, en el GKSP hay un elemento de perfil de seguridad cuya credencial es ElementID 6, que sirve para indicar que se ha encontrado un error. Si la autenticación entre el EP H.323 y el GKSP ha tenido éxito, este último puede incluir un elemento de perfil de seguridad con ElementID 6: no se ha encontrado error de seguridad.

– Si el GKSP encuentra errores de seguridad (firma digital errónea, fallo en la validación del certificado, etc.) en un mensaje recibido del EP H.323 o del GKSP par, anota el error en un registro cronológico y reenvía el mensaje al GK, incluye un testigo de procesador que tenga un elemento de perfil de seguridad del tipo ElementID 6, con lo cual señala el tipo de error, y deja a discreción del GK la decisión y la correspondiente reacción.

– De encontrar el GKSP errores de seguridad en un mensaje recibido del GK o de otro GKSP, lo anota en un registro cronológico y descarta el mensaje.
– Calcular las firmas digitales para mensajes H.235.3 dirigidos a los EP H.323 o al GKSP par.
– Retransmitir en ambos sentidos todo mensaje H.225.0 entre un EP H.323 y el GK o el GKSP, y efectuar las siguientes operaciones sobre los testigos:
  • Comunica con su GK utilizando el protocolo H.225.0, habiendo retirado los testigos H.235.3 recibidos de los EP H.323 o del GKSP par en la primera toma de contacto.
  • Verifica los testigos H.235.1 incorporados recibidos de los EP H.323 o del GKSP par y los retira antes de retransmitir los mensajes hacia el GK.
  • Termina el protocolo H.235.1/H.235.3 con su GK.
  • Incluye testigos H.235.1/H.235.3 en mensajes salientes hacia los puntos extremos H.323 o el GKSP par.
  • Deja prácticamente intactos los mensajes H.225.0 recibidos de los EP H.323 o del GK; hace solamente los mencionados cambios de testigos.
  • Garantiza la seguridad del protocolo H.225.0 entre el GKSP y su GK utilizando ya sea el perfil de seguridad básico de H.235.1 o el perfil de seguridad híbrido de H.235.3.
– Cuando se utilice el perfil de seguridad híbrido de H.235.3 entre el GKSP y el GK, o entre el GKSP y otro GKSP, el GKSP:
  a) ejecuta el protocolo H.235.3 con el GK o el GKSP, con el fin de establecer una nueva clave dinámica tras la recepción del primer mensaje del primer EP o del GKSP par, o bien;
  b) inicia el protocolo H.235.3 con el GK o el GKSP para establecer una nueva clave dinámica antes de que inicie la comunicación otro EP H.323 o GKSP. Entonces habrá un secreto dinámico compartido listo para la protección de los primeros mensajes de toma de contacto recibidos de un terminal H.323 o de un GKSP par, y se reducirá aún más el tiempo de establecimiento de la asociación global de seguridad.
– El GKSP no reenvía ningún mensaje FACILITY específico de H.235.3 para actualización de clave.
– Cuando se utilice el perfil de seguridad básico de H.235.1 entre el GKSP y el GK, o entre el GKSP y otro GKSP, el GKSP empleará la clave compartida estática para proteger los mensajes RAS y/o de señalización de llamada H.225.0.
– Mantener un registro de las asociaciones de seguridad; establecimiento del secreto compartido DH y mantenimiento de los secretos compartidos dinámicos. Dependiendo de su política de seguridad, el GKSP puede solicitar que se redefinan las claves correspondientes a los secretos compartidos dinámicos que mantiene, utilizando mensajes FACILITY. Al suprimir el registro del terminal H.323 o de un GKSP par, el GKSP debería descartar la clave compartida dinámica y considerar que no hay ninguna asociación de seguridad vigente.
– Crear una correspondencia uno a uno entre puertos de transporte (EP-GKSP y GKSP-GK) para los protocolos RAS y/o de señalización de llamada H.225.0.

I.3 Testigo de procesador

Al recibir un mensaje RAS H.225.0 y/o de señalización de llamada, asegurado conforme a H.235.3, que transporte un certificado X.509 y una firma digital, el GKSP suprime los testigos H.235.3 e incluye un testigo independiente de procesador para el mensaje reenviado a su GK o al próximo GKSP (si lo hubiere).

Junto con el testigo de procesador, el GKSP indica las características encontradas (método de autenticación, identificador de EP, nombre que aparece en el certificado (nombre o subjectAltName), número de serie en el certificado X.509, nombre de emisor del certificado X.509), o da una indicación de error. El testigo de procesador es una simple afirmación de seguridad que atestigua la relación de seguridad confirmada (fructuosa o infructuosa) entre el GKSP y los EP H.323 hacia el GK.

El GK puede detectar la presencia de un GKSP inspeccionando los mensajes recibidos y reconociendo en ellos un testigo de procesador. De no haberlos se supone que no existe ningún GKSP.

El testigo de procesador es un ClearToken en el que se utilizan los siguientes campos:

– **tokenOID**: un OID para "PT"; véase el cuadro I.2.

– **generalID** que puede ser:

  • el identificador del punto extremo H.323, cuando se trate de un mensaje, asegurado conforme a H.235, recibido desde uno de dichos puntos, o bien

  • el identificador de GK, si el mensaje recibido, asegurado conforme a H.235, proviene del GK.

– **certificate**: es facultativo y puede ser el certificado H.235.2/H.235.3 recibido del EP H.323 o del GKSP par. Si se incluye, el GKSP reenvía el mensaje al GK.

  En el campo **certificate** conviene utilizar el subject/subjectAltName, el ID del EP, el número de serie del certificado, o cualquier otra credencial ligera en lugar del certificado completo. El motivo es que los certificados X.509 tienden a ser bastante largos y que podría haber un problema de fragmentación de mensajes cuando se incluían certificados en mensajes H.225.0 transportados mediante el UDP.

– **profileInfo**: por lo menos un elemento de perfil.

  El testigo de procesador puede tener varios elementos de perfil, entre los enumerados en el cuadro I.1.

No se utilizan los demás campos de un ClearToken de procesador de seguridad de GK.

Cuadro I.1/H.235.3 – Especificación de elementos de perfil

Valor de ElementID	Descripción	Especificación
0	Elemento de perfil que indica el método de autenticación. Su utilización sólo es obligatoria durante la toma de contacto inicial (GRQ o RRQ).	• No se utiliza **paramS**. • **element**: se especifica un elemento y en el campo **integer** se utiliza uno de los siguientes valores para indicar cuál es el método de autenticación encontrado en el EP H.323 o el GKSP par: 1) otro método de autenticación, no especificado ni normalizado, 2) ninguno (es decir, no hay autenticación), 3) el secreto compartido H.235.1 (sin definir en este apéndice) 4) H.235.2, 5) H.235.3, 6) H.235.5, (sin definir en este apéndice) 7) H.235.4, (sin definir en este apéndice) 8) H.530 (sin definir en este apéndice).
1	Elemento de perfil que tiene el **subject** del certificado recibido. Su utilización es facultativa.	• No se utiliza **paramS**. • **element**: se especifica un elemento y el **subject** del certificado recibido en los campos **name** u **octets**. NOTA – Es probable que el GKSP tenga que recodificar el **subject** de la representación Name X.509 para convertirlo en una cadena de octetos o en una representación **name** BMP.
2	Elemento de perfil que tiene el **subjectAltName** del certificado recibido. Su utilización es facultativa.	• No se utiliza **paramS**. • **element**: se especifica un elemento y el **subjectAltName** del certificado recibido en los campos **name** u **octets**. NOTA – Es probable que el GKSP tenga que recodificar el **subjectAltName** de la representación Name X.509 para convertirla en una cadena octetos o en una representación **name** BMP.
3	Elemento de perfil que tiene el número de serie del certificado. Su utilización es obligatoria.	• No se utiliza **paramS**. • **element**: se especifica un elemento y el **certificateSerialNumber** del certificado X.509 recibido en el campo **integer**.
4	Elemento de perfil que tiene el emisor del certificado. Su utilización es obligatoria.	• No se utiliza **paramS**. • **element**: se especifica un elemento y el nombre **issuer** del certificado X.509 recibido en los campos **name** u **octets**. NOTA – Es probable que el GKSP tenga que recodificar el emisor de la representación Name X.509 para convertirlo en una cadena de octetos o en una representación **name** BMP.

Cuadro I.1/H.235.3 – Especificación de elementos de perfil

Valor de ElementID	Descripción	Especificación
5	Elemento de perfil que tiene el identificador de EP, del EP o terminal que origina el mensaje. Su utilización es facultativa.	• No se utiliza **paramS**. • **element**: se especifica un elemento y el identificador de EP, del EP o terminal que origina el mensaje en el campo **name**.
6	Elemento de perfil que tiene una indicación de error. Su utilización es obligatoria en cualquier caso de error (> 0) y facultativa cuando se indique que no hay error (0).	• No se utiliza **paramS**. • **element**: se especifica un elemento y uno de los siguientes valores de error codificados en el campo **integer**: 0: no hay error 1: securityDenied 2: securityWrongSyncTime 3: securityReplay 4: securityWrongGeneralID 5: securityWrongSendersID 6: securityMessageIntegrityFailed 7: securityWrongOID 8: securityDHmismatch 9: securityCertificateExpired 10: securityCertificateDateInvalid 11: securityCertificateRevoked 12: securityCertificateNotReadable 13: securityCertificateSignatureInvalid 14: securityCertificateMissing 15: securityCertificateIncomplete 16: securityUnsupportedCertificateAlgOID 17: securityUnknownCA 18: error de seguridad no especificado 19: no se soporta el GKSP.

I.4 Ejemplo de uso de GKSP

En esta cláusula se dan ejemplos de diagramas de flujo de mensajes (véanse la figuras I.4 e I.5) para el caso de un procesador de seguridad de GK que funciona dentro de un dominio administrativo de seguridad. Obsérvese que en las figuras I.4 e I.5 sólo se muestran aquellos mensajes que son esenciales en el contexto de H.235.3; en la práctica, puede haber muchos más mensajes RAS y/o de señalización de llamada H.225.0.

En ambas figuras, tanto el terminal A H.323 como el GKSP conformes a H.235.3, utilizan el perfil de seguridad híbrido H.235.3; en otras palabras, no comparten ningún secreto estático. En la figura I.4, el GKSP y el GK emplean el perfil de seguridad básico H.235.1 para proteger los mensajes RAS y de señalización de llamada H.225.0. K_{BC} indica el secreto que comparten el GKSP B y el GK C.

La figura I.4 representa una llamada completa desde el terminal A, que pasa por el GKSP B y el GK C y se encamina mediante un GK. Al principio, el terminal A y el GKSP B negocian una clave dinámica de enlace, K_{AB}, con arreglo a H.235.3, durante la fase de registro del RAS. Con este fin, el terminal A genera el mensaje **RRQ** que transporta la semiclave Diffie-Hellman, DH_A de A, que tiene el certificado de A (facultativo) y la firma digital de A en todo el mensaje **RRQ** o en alguna de sus partes.

El GKSP B recibe el **RRQ** y verifica la firma digital: compara y verifica el certificado digital X.509 transportado (en su caso) con el certificado raíz de A, verifica el trayecto y la CRL, etc.

El GKSP reenvía el mensaje **RRQ** al GK C, añade un testigo de procesador (PT) que contiene los siguientes elementos de perfil de seguridad:

– 0 para indicar que se trata de H.235.3 (5);

– 2 el subjectAltName del certificado de A;

– 3 el número de serie del certificado de A;

– 5 el ID de EP de A;

y aplica el perfil de seguridad básico de H.235.1 con la clave compartida K_{BC}; se realiza una verificación de integridad HMAC-SHA1 para todo el mensaje **RRQ** o sólo parte de él.

Si el resultado de validación de certificado o firma digital no es satisfactorio, el GKSP B no puede autenticar ni autorizar el terminal A; en este caso, el GKSP anota el error en un registro cronológico y reenvía el RRQ incorrecto al GK C.

El GK C recibe el mensaje **RRQ**, verifica su integridad mediante K_{BC} y procesa el PT con los elementos de perfil incluidos. Si esta validación del **RRQ** es satisfactoria, el GKC autoriza el terminal A y responde enviando un **RCF** al GKSP B.

El GKSP B recibe el **RCF**, reconoce que el GK C ha autorizado el terminal A y reenvía un **RCF** a este terminal: calcula e introduce su semiclave Diffie-Hellman, DH_B y su certificado (facultativo), y firma el **RRQ** (todo o parte de él) con su clave privada. El terminal A valida entonces la autenticidad del mensaje **RCF** recibido.

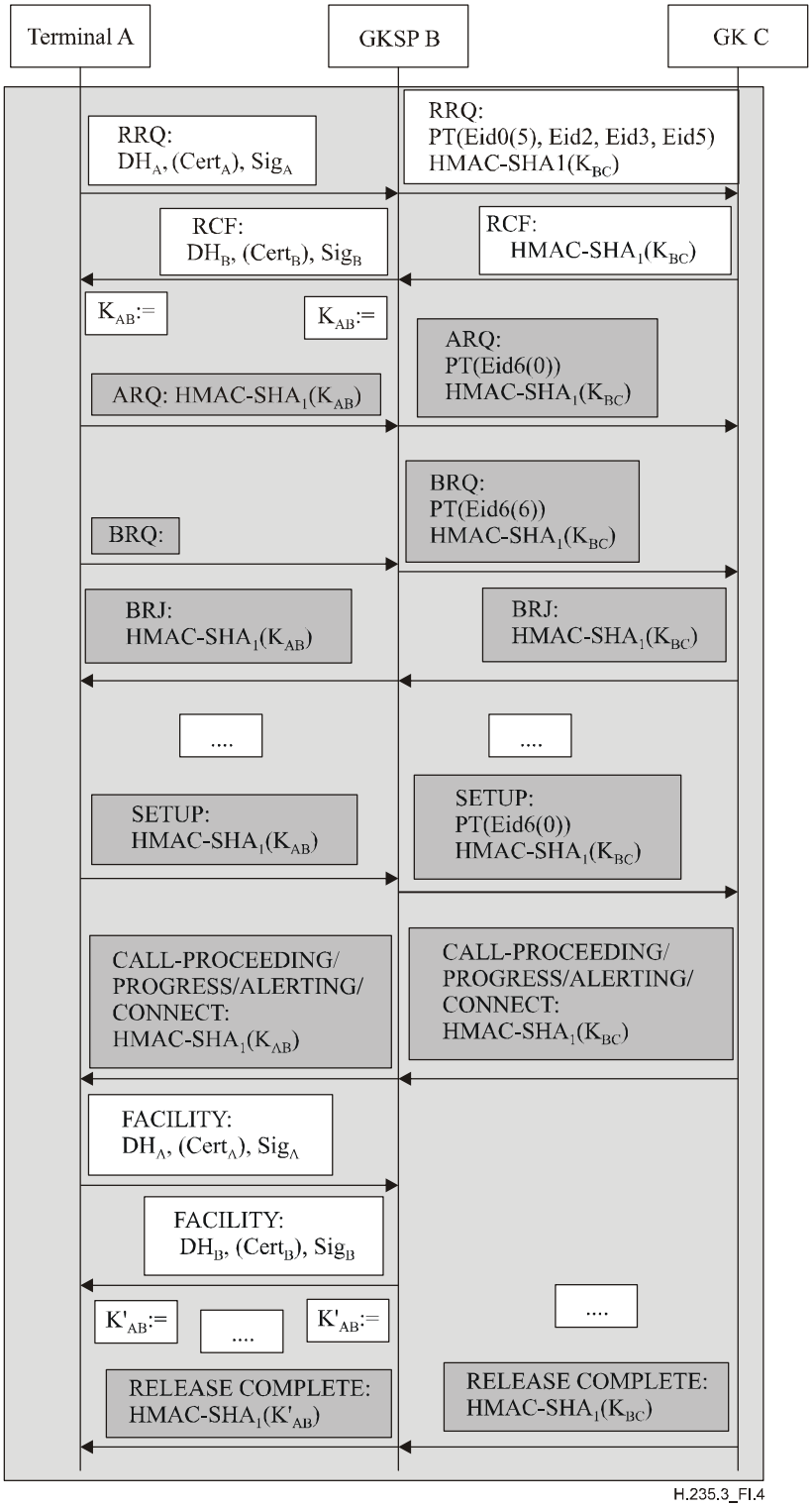
Si el GKSP B ha autenticado satisfactoriamente y ha autorizado el terminal A, ambos calculan el secreto compartido dinámico, K_{AB} que representa la relación de confianza establecida entre los dos. De lo contrario, y en caso de que el GK C no autorice el terminal A, el GKSP B reenvía un **RCF** a dicho terminal A: calcula e introduce su semiclave Diffie-Hellman, DH_B, y su certificado (facultativo), y firma el **RRQ** (todo o parte de él) con su clave privada. Al no estar autorizado el terminal A, el GKSP B no conserva el K_{AB}. El GKSP B puede registrar el **RCF** del fallo en un fichero cronológico.

El terminal A y el GKSP B emplean el secreto compartido dinámico, K_{AB} para proteger a otros mensajes RAS y de señalización de llamada H.225.0 utilizando el perfil de seguridad básico de H.235.1. Por su parte, el GKSP B y el GK C se sirven del perfil de seguridad básico de H.235.1 para la protección de todos los mensajes RAS y de señalización de llamada H.225.0.

Cuando el terminal A recibe un **RCF**, interrumpe el establecimiento de la comunicación.

En la figura I.4 también se muestra un caso de error: el terminal A (u otra entidad) envía al GKSP un mensaje **BRQ** sin protección, que también puede ser el resultado de un ataque en el que de alguna manera se haya suprimido o alterado la protección de seguridad H.235.1. El GKSP detecta el fallo en la verificación de integridad y reenvía al GK el mensaje **BRQ** con un PT, y el elemento de perfil de seguridad indica securityMessageIntegrityFailed (6). El GK reconoce entonces que se ha violado la seguridad y no autoriza la petición de ancho de banda, a través de una respuesta **BRJ**.

Cierto tiempo después del establecimiento de la comunicación, el terminal A actualiza con el GKSP B la clave K_{AB}, siendo K'_{AB} la clave actualizada. Al final de la llamada, el GK C termina la llamada.



Cert	Certificado de usuario	GK	Controlador de acceso
DH_A	Testigo Diffie-Hellman g^a mod p	GKSP	Procesador de seguridad de GK
DH_B	Testigo Diffie-Hellman g^b mod p	HMAC-SHA1	Valor calculado de prueba de integridad
Eid*n*	ElementID de perfil de seguridad con valor *n*	K, K'	Clave de enlace simétrica
		PT	Testigo de procesador
EP	Punto extremo (Terminal)	Sig	Firma digital

Figura I.4/H.235.3 – Flujo de llamada con procesador de seguridad de GK y protección de mensaje H.235.1 (GKSP-a-GK)

En la figura I.5, el GKSP y el GK utilizan el perfil de seguridad híbrido H.235.3 para la protección de los mensajes RAS y de señalización de llamada H.225.0. K_{BC} es el secreto compartido dinámico, que negocian inicialmente el GKSP y el GK y que luego comparten en el contexto del perfil de seguridad básico H.235.1, para la protección de los mensajes RAS y de señalización de llamada H.225.0. En la figura I.5 también se muestra un terminal D H.323, conforme a H.235.1, que comparte un secreto estático K_{DB} con su GKSP B.

La figura I.5 representa una llamada completa desde el terminal A, a través del GKSP B y el GK C, y que se encamina mediante un GK. En la figura I.5, se supone que el terminal A es realmente el primer EP que se inscribe en el GK a través del GKSP.

El terminal A y el GKSP B emplean este secreto compartido dinámico, K_{AB} para proteger otros mensajes RAS y de señalización de llamada H.225.0, utilizando el perfil de seguridad básico H.235.1. El GKSP B y el GK C se sirven del perfil de seguridad básico H.235.1 para proteger otros mensajes RAS y de señalización de llamada H.225.0, utilizando el secreto compartido dinámico K_{BC}.

El terminal A y el GKSP B negocian al principio una clave de enlace dinámica, K_{AB} con arreglo a H.235.3. Durante la primera toma de contacto **RRQ**/**RCF** entre el terminal A y el GKSP, en la que ambas entidades establecen un secreto compartido dinámico, K_{AB}, el GKSP y el GK también se valen de H.235.3 para fijar el secreto compartido dinámico K_{BC}.

El GKSP reenvía el mensaje **RRQ** recibido del terminal A, añade un PT que incluye tres elementos de perfil de seguridad:

– 0 indica que se utiliza H.235.3 (5);

– 3 el número de serie del certificado de A;

– 6 indica que no hay error (0);

y aplica el perfil de seguridad híbrido H.235.3. Como inicialmente no hay ningún secreto compartido, el GKSP B y el GK C ejecutan el protocolo H.235.3 y crean un secreto compartido dinámico K_{BC}.

Más adelante, el terminal D se inscribe en el GKSP B mediante un **RRQ** protegido H.235.1. El GKSP B reenvía este **RRQ** al GK C e incluye un PT que transporta tres elementos de perfil de seguridad, a saber:

– 0, indica que se utiliza H.235.1 (3);

– 5, el identificador del EP D;

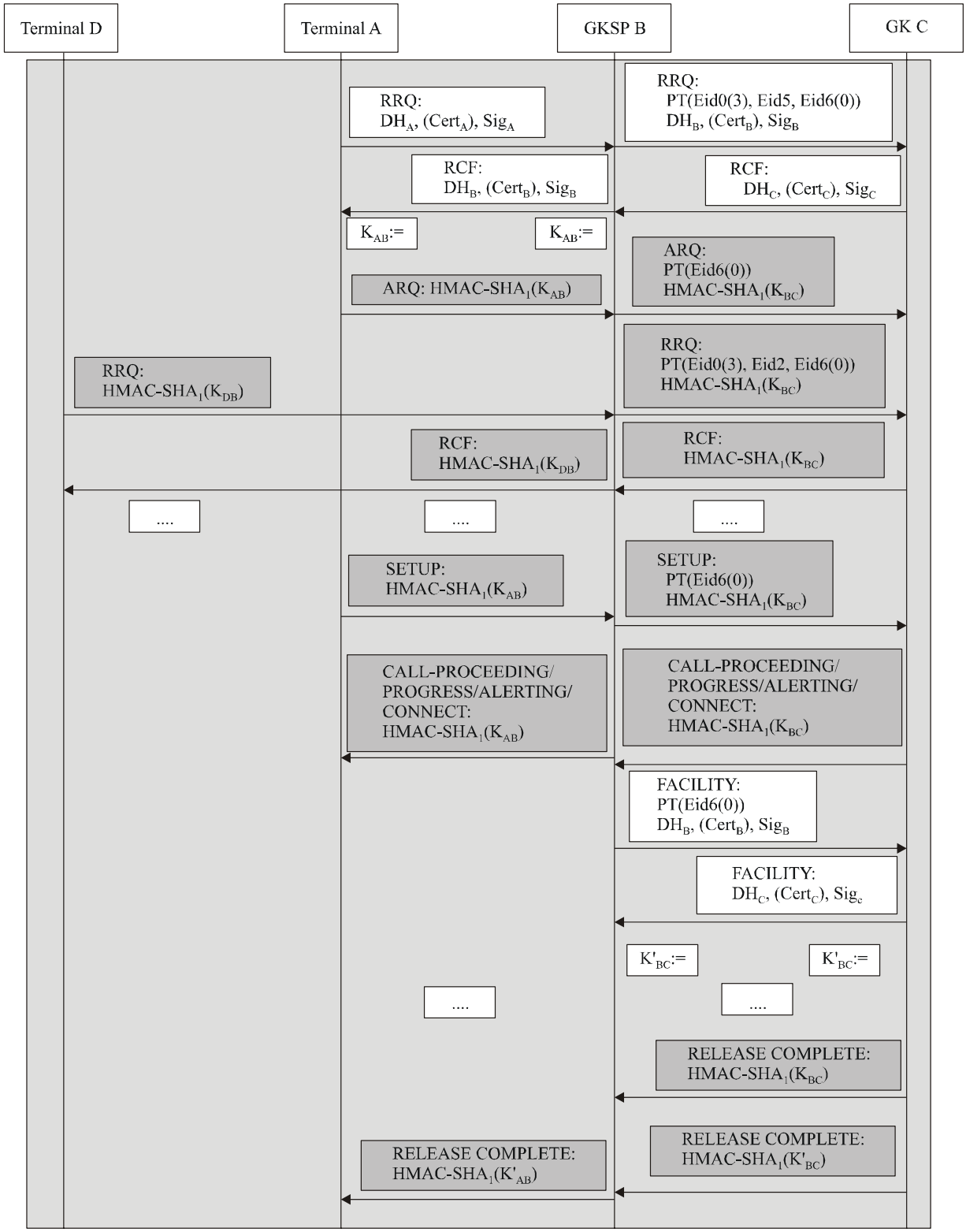
– 6, indica que no hay error (0);

y aplica el perfil de seguridad híbrido H.235.3. Puesto que ya se ha establecido un secreto dinámico compartido K_{BC}, el GKSP protege el mensaje **RRQ** reenviado con H.235.1 utilizando dicho secreto. El GK C autoriza el terminal D y responde con un **RCF**, que el GKSP a su vez reenvía al terminal D.

Cierto tiempo después del establecimiento de la comunicación desde el terminal A a través del GK C, el GKSP B decide renovar la clave K_{BC}, para lo cual efectúa con el GK C un procedimiento de actualización del que resulta la nueva clave: K'_{BC}.

En la figura I.5 también se muestra un caso de error: el GKSP recibe un mensaje RELEASE-COMPLETE del GK. El GKSP B no puede verificar la integridad de este mensaje porque no se usa la clave vigente. El mensaje pudo haber sido reproducido o manipulado por un pirata o bien el GK está utilizando una clave desactualizada que ya ha expirado. El GKSP B anota entonces el evento de seguridad en un registro cronológico y descarta el mensaje sin reenviarlo al terminal A.

Al final, el GK C termina la llamada.



Cert	Certificado de usuario	GK	Controlador de acceso
DH_A	Testigo Diffie-Hellman g^a mod p	GKSP	Procesador de seguridad de GK
DH_B	Testigo Diffie-Hellman g^b mod p	HMAC-SHA1	Valor calculado de prueba de integridad
DH_C	Testigo Diffie-Hellman g^c mod p	K, K'	Clave de enlace simétrica
Eid*n*	ElementID de perfil de seguridad con valor *n*	PT	Testigo de procesador
		Sig	Firma digital
EP	Punto extremo (Terminal)		

Figura I.5/H.235.3 – Flujo de llamada con procesador de seguridad de GK y protección de mensaje H.235.3 (GKSP-a-GK)

I.5 Lista de identificadores de objeto

En el cuadro I.2 se enumeran los OID referenciados que han de utilizarse junto con el cuadro I.1.

Cuadro I.2/H.235.3 – Identificadores de objeto empleados en el apéndice I

Referencia de identificador de objeto	Valor(es) de identificador de objeto	Descripción
"PT"	{itu-t (0) recommendation (0) h (8) 235 version (0) 4 15}	Sirve para señalar el Clear token de procesador de GK en la comunicación desde un GKSP hacia un GK.

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

Impreso en Suiza
Ginebra, 2006