Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

H.235.1

(09/2005)

SERIE H: SISTEMAS AUDIOVISUALES Y MULTIMEDIOS

Infraestructura de los servicios audiovisuales – Aspectos de los sistemas

Marco de seguridad H.323: Perfil de seguridad básico

Recomendación UIT-T H.235.1

RECOMENDACIONES UIT-T DE LA SERIE H

SISTEMAS AUDIOVISUALES Y MULTIMEDIOS

CARACTERÍSTICAS DE LOS SISTEMAS VIDEOTELEFÓNICOS	H.100–H.199
INFRAESTRUCTURA DE LOS SERVICIOS AUDIOVISUALES	
Generalidades	H.200–H.219
Multiplexación y sincronización en transmisión	H.220–H.229
Aspectos de los sistemas	**H.230–H.239**
Procedimientos de comunicación	H.240–H.259
Codificación de imágenes vídeo en movimiento	H.260–H.279
Aspectos relacionados con los sistemas	H.280–H.299
Sistemas y equipos terminales para los servicios audiovisuales	H.300–H.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.235.1

Marco de seguridad H.323: Perfil de seguridad básico

Resumen

La presente Recomendación prevé la protección mediante autenticación e integridad, o sólo autenticación, utilizando técnicas criptográficas de contraseña segura para los mensajes de señalización de llamada y RAS H.225.0, los mensajes H.225.0 y los mensajes H.245 tunelizados que están protegidos por troceado HMAC-SHA1-96 con contraseña en los mensajes de señalización de llamada y RAS H.225.0. El perfil de seguridad es aplicable a las entidades terminales a controlador de acceso H.323, controlador de acceso a controlador de acceso H.323, pasarela a controlador de acceso H.323 y otras entidades H.323 en entornos administrados con claves/contraseñas simétricas asignadas.

En versiones anteriores de la subserie H.235, este perfil estaba comprendido en parte del anexo D/H.235. En los apéndices IV, V, VI a H.235.0 se indica la correspondencia entre el texto, y los cuadros de las versiones 3 y 4 de H.235.

Orígenes

La Recomendación UIT-T H.235.1 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 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 no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB.

ÍNDICE

Recomendación UIT-T H.235.1

Marco de seguridad H.323: Perfil de seguridad básico

1 Alcance

La presente Recomendación prevé la protección mediante autenticación e integridad o sólo autenticación, utilizando técnicas criptográficas con contraseña segura para los mensajes de señalización de llamada y RAS H-225.0, los mensajes H.225.0 y los mensajes H.245 tunelizados que están protegidos por troceado HMAC-SHA1-96 con contraseña en los mensajes de señalización de llamada y RAS H.225.0. El perfil de seguridad es aplicable a las entidades terminal a controlador de acceso H.323 controlador de acceso a controlador de acceso, pasarela a controlador de acceso H.323 y otras entidades H.323.

2 Referencias

2.1 Referencias normativas

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación.

– Recomendación UIT-T H.225.0 (2003), *Protocolos de señalización de llamada y paquetización de trenes de medios para sistemas de comunicación multimedios por paquetes*.

– Recomendación UIT-T H.235 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.235.2 (2005), *Marco de seguridad H.323: Perfil de seguridad de firma*.

– Recomendación UIT-T H.235.4 (2005), *Marco de seguridad H.323: Seguridad de llamada con encaminamiento directo y selectivo*.

– Recomendación UIT-T H.235.6 (2005), *Marco de seguridad H.323: Perfil de criptación vocal con gestión de claves H.235/H.245 nativa*.

– Recomendación UIT-T H.245 versión 10 (2003), *Protocolo de control para comunicación multimedios*.

– Recomendación UIT-T H.323 (2003), *Sistemas de comunicación multimedios basados en paquetes*.

– Recomendación UIT-T H.323 anexo F (1999), *Tipos de punto extremo simples*.

– 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.800 (1991), *Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT*.

ISO/CEI 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*.

ISO/CEI 10118-3:2004, *Information Technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions*.

2.2 Referencias informativas

[FIPSPUB180-2] Federal Information Processing Standard FIPS PUB 180-2, Secure Hash Standard, U. S. Department of Commerce, Technology Administration, National Institute of Standards and Technology, 1 August 2002.

[OIW] Stable Implementation – Agreements for Open Systems Interconnection Protocols: Part 12 – OS Security; Output from the December 1994 Open Systems Environment Implementors' Workshop (OIW); http://nemo.ncsl.nist.gov/oiw/agreements/stable/OSI/12s_9412.txt.

[RFC2104] IETF RFC 2104 (1997), *HMAC: Keyed-Hashing for Message Authentication*.

[WEBOIDs] http://www.alvestrand.no/objectid/top.html.

3 Términos y definiciones

A los efectos de la presente Recomendación, son de aplicación, además de las de esta cláusula, las definiciones de las cláusulas 3/H.323, 3/H.225.0 y 3/H.245. Algunos de los términos se utilizan con la definición que se les da en las Recs. UIT-T X.800 | ISO/CEI 7498-2, X.803 | ISO/CEI 10745, X.810 | ISO/CEI 10181-1 y X.811 | ISO/CEI 10181-2.

La presente Recomendación utiliza los siguientes términos para la prestación de servicios de seguridad:

3.1 autenticación e integridad: Se trata de un servicio de seguridad combinado, parte del perfil básico, que soporta la integridad del mensaje además de la autenticación del usuario. El usuario puede realizar la autenticación aplicando correctamente un procedimiento de clave secreta compartida. Ambos servicios de seguridad son proporcionados por el mismo mecanismo de seguridad.

3.2 sólo autenticación: Este servicio de seguridad, que es una opción del servicio de seguridad básico, soporta únicamente la autenticación de campos seleccionados, pero no la integridad completa del mensaje. El perfil de seguridad de sólo autenticación es aplicable a los mensajes de señalización que atraviesan dispositivos NAT/cortafuegos. El usuario puede realizar la autenticación aplicando correctamente un procedimiento de clave secreta compartida.

Cuando se utilizan técnicas de clave simétrica, los servicios de seguridad de autenticación/integridad sólo se aplicarán salto a salto.

4 Abreviaturas, siglas o acrónimos

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

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

EP Punto extremo (*endpoint*)

EPID Identificador de punto extremo (*endpoint identifier*)

GK Controlador de acceso (*gatekeeper*)

GKID Identificador de controlador de acceso (*gatekeeper identifier*)

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*)

LRQ Petición de localización (*location request*)

MAC Código de autenticación de mensaje (*message authentication code*)

NAT Traducción de dirección de red (*network address translation*)

OID Identificador de objeto (*object identifier*)

RAS Registro, admisión y estado (*registration, admission and status*)

RTP Protocolo en tiempo real (*real-time protocol*)

SHA Algoritmo troceado asegurado (*secure hash algorithm*)

TCP Protocolo de control de transmisión (*transmission control protocol*)

UIT Unión Internacional de Telecomunicaciones

UTC Reloj de tiempo universal (*universal time clock*)

VoIP Voz sobre el protocolo Internet (*voice over Internet protocol*)

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.

Esta Recomendación define el **perfil de seguridad básico**. Este perfil proporciona la seguridad básica por medios sencillos utilizando técnicas criptográficas seguras basadas en contraseñas. El perfil de seguridad básico puede utilizarse combinado con los perfiles de seguridad H.235.3, H.235.4, H.235.5, H.235.6 y H.235.7.

En los procedimientos de esta Recomendación se utilizan los campos H.235 para la prestación de servicios de seguridad de autenticación/integridad en mensajes de señalización H.323. Diferentes identificadores de objeto (véase la cláusula 15) determinan el servicio de seguridad efectivamente seleccionado y la versión de protocolo de la presente Recomendación que se está utilizando.

El procedimiento I especifica el modo de implementar los servicios de seguridad mediante determinados mecanismos de seguridad, como las técnicas simétricas (clave troceada). En el texto se hace referencia a los identificadores de objeto mediante un símbolo (por ejemplo, "A"). Véase también la cláusula 5/H.235.0.

Si bien el servicio de integridad también realiza la autenticación de los mensajes, lo contrario no siempre es cierto. En la práctica, el servicio combinado de autenticación e integridad explota el mismo material de claves sin debilitar la seguridad.

Además, toda la información de seguridad salto por salto se introduce en el elemento **CryptoHashedToken**. Esta información se recalcula en cada salto.

La presente Recomendación aplica determinadas técnicas criptográficas simétricas para lograr la autenticación y la integridad. En este texto se utiliza el término contraseña y secreto compartido en el contexto de estas técnicas simétricas.

Por regla general, la contraseña, la clave de sesión y el secreto compartido tienen en común que todos son utilizados en la criptografía simétrica entre dos (o más) entidades. La diferencia entre una contraseña y un clave de sesión/secreto compartido es el modo en que las claves se aplican realmente, por ejemplo, contraseñas para la autenticación y la autorización, claves de sesión para la criptación. El término "secreto compartido" es en cierto modo neutro, pues de hecho no se refiere a ninguna utilización especifica.

La **contraseña** (que también puede contemplarse como un secreto compartido) se utiliza para la autenticación/integridad de mensajes RAS y H.225.0, puesto que este elemento puede ser introducido por el usuario. Por norma general, las contraseñas son cadenas de caracteres alfanuméricos que los usuarios pueden memorizar. La contraseña tiene normalmente un tiempo de vida largo; la contraseña se conoce *a priori* y puede ser definida como parte del proceso global de abono del usuario. Algunos algoritmos (por ejemplo, la canalización de la contraseña a través de un algoritmo troceado) pueden transformar la contraseña para un procesamiento más conveniente en los protocolos a fin de que tenga una longitud fija.

Es obvio que la utilización de las contraseñas ha de hacerse cuidadosamente, pues sólo pueden proporcionar seguridad suficiente cuando se eligen aleatoriamente a partir de una muestra amplia, cuando su entropía es suficiente para que sean impredecibles, y cuando se modifican periódicamente. Las reglas para escoger y actualizar las contraseñas quedan fuera del alcance de la presente Recomendación.

Un buen método para aprovechar los beneficios de las contraseñas y los secretos compartidos es transformar la cadena de contraseña de usuario en una cadena de bits fija que será el secreto compartido, utilizando una función generadora unidireccional criptográficamente fuerte.

Puede recomendarse, cuando se utilice el perfil de seguridad de la presente Recomendación, la aplicación de troceado SHA1 de cadena de contraseña, con lo que se obtiene un secreto compartido de 20 bytes. La ventaja es que el valor generador resultante no sólo oculta la contraseña real, sino que también define un formato de cadena de bits de longitud fija sin realmente sacrificar entropía.

Por consiguiente,

secreto compartido: = SHA1 (contraseña)

El **ClearToken** (**testigo claro**) H.235 ofrece un campo denominado **random** que contiene un entero de 32 bits. Este campo se utiliza en el siguiente sentido: **random** es realmente un número monotónicamente creciente que arranca en un valor cualquiera y se incrementa con cada mensaje saliente. El campo **random** se utiliza como un valor de "aleatorización" adicional a la entrada de la función de troceo en el caso de que se envíen varios mensajes uno inmediatamente después de otro, que transportan sin embargo identificaciones de tiempo idénticas. Esto puede suceder cuando el reloj UTC no proporciona una resolución de reloj suficiente. En esencia, la función de troceo producido o el valor de comprobación de la integridad parecen diferentes debido al cambio del

valor de **random**. Se trata de contrarrestar los ataques de reproducción. Para simplificar la implementación, aquí se prefiere un contador creciente que una secuencia verdaderamente aleatoria. El recipiente puede guardar las parejas **timestamp/random** recibidas durante el periodo definido por una ventana de tiempo local. Se puede identificar un ataque de reproducción cuando la misma pareja **timestamp/random** ocurre dos veces.

NOTA – La ventana de tiempo compensa las variaciones del tiempo sincronizado y el retardo de tránsito de la red.

La norma de este perfil es "adoptar el identificador del receptor como **generalID** en el **ClearToken**". Esto de hecho significa que, para los mensajes RAS destinados al controlador de acceso, este identificador es el identificador del GK; para los mensajes RAS destinados al punto extremo, es el identificador de punto extremo, y para los mensajes de señalización de llamada H.225.0 destinados al controlador de acceso, éste es el identificador de GK, y para los mensajes de señalización de llamada H.225.0 destinados al punto extremo, es el identificador de punto extremo llamado. Véase también la cláusula 14.

El **sendersID** será fijado a la cadena de identificación del emisor. Esto quiere decir que, para los mensajes RAS destinados al controlador de acceso, éste es el identificador de punto extremo; para los mensajes RAS destinados al punto extremo, éste es el identificador de controlador de acceso; para los mensajes de señalización de llamada H.225.0 destinados al controlador de acceso, éste es el identificador GK y para los mensajes de señalización de llamada H.225.0 destinados al punto extremo, es el identificador de punto extremo llamado. Véase también la cláusula 14.

Esta Recomendación puede aplicar protección de integridad de mensaje que cubra el mensaje completo. Para los RAS H.225.0, la protección de integridad cubre todo el mensaje RAS; para la señalización de llamada, cubre el mensaje completo de señalización de llamada H.225.0, incluidas las cabeceras Q.931.

Esta Recomendación utiliza términos relativos a la seguridad muy conocidos como clave, gestión de claves y SET, que tienen significados distintos en otros contextos (por ejemplo, la tablilla de clave sensible, la gestión de claves de procesos Q.931/Q.932 y los protocolos de transacciones electrónicas seguras).

6 Visión general

La presente Recomendación prevé la protección mediante la autenticación e integridad, o sólo autenticación, utilizando técnicas criptográficas de contraseña segura para los mensajes de señalización de llamada y RAS H.225.0, los mensajes de H.225.0 y los mensajes H.245 tunelizados que están protegidos por troceado HMAC-SHA1-96 con contraseña en los mensajes de señalización de llamada y RAS H.225.0. Este perfil de seguridad es aplicable a las entidades terminal a controlador de acceso H.323, controlador de acceso a controlador de acceso, pasarela a controlador de acceso H.323 y otras entidades H.323 en entornos administrados con claves/contraseñas simétricas asignadas.

6.1 Resumen de las características de seguridad

Las características proporcionadas por estos perfiles incluyen:

– Para mensajes RAS, H.225.0 y H.245 tunelizados:

  • La autenticación de usuario a una entidad deseada con independencia del número de saltos del nivel de aplicación que atraviesa el mensaje.

    NOTA – Salto tiene aquí el sentido de un elemento de red H.235 de confianza (por ejemplo, GK, GW, MCU, servidor intermedio, 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.

- La integridad del propio mensaje de señalización, incluidas las porciones (campos) críticas de los mensajes que llegan a una entidad, con independencia del número de saltos del nivel de aplicación que atraviesa el mensaje.
- La autenticación e integridad del mensaje de señalización salto por salto en el nivel de aplicación proporciona estos servicios de seguridad para el mensaje completo.

Utilizando correctamente estos servicios de seguridad se consigue frustrar varios ataques:

- Los ataques de denegación de servicio: una comprobación rápida de los números generadores criptográficos puede evitar tales ataques.
- Ataques de "intromisión": la autenticación e integridad de los mensajes salto por salto en el nivel de aplicación previene contra tales ataques cuando el ataque intermedio se produce en un salto del nivel de aplicación, es decir, un encaminador hostil.
- Ataques de reproducción: estos ataques se evitan mediante el empleo de indicaciones de tiempo y números secuenciales.
- Engaño: la autenticación del usuario evita tales ataques.
- Asalto a la conexión: la autenticación/integridad de cada mensaje de señalización evita tales ataques.

Otros puntos destacados del perfil de seguridad simple incluyen:

- La utilización de algoritmos robustos, bien conocidos y ampliamente utilizados basados en normas IMTC/ETSI/IETF.
- La capacidad de utilización por fases basado en el requisito de seguridad del modelo comercial.
- Su aplicabilidad en distintos casos, por ejemplo, los grupos cerrados, los entornos escalables y las conferencia multipunto.
- El perfil de seguridad de sólo autenticación se aplica cuando se proporciona un cierto grado de seguridad para el paso a través de un NAT/cortafuegos.

En el cuadro 1 se resumen los procedimientos definidos en esta Recomendación según los perfiles de seguridad para satisfacer los diferentes requisitos de seguridad. El perfil facultativo de seguridad de sólo autenticación corresponde a la diagonal sombreada (color azul en la copia electrónica).

Cuadro 1/H.235 – Resumen de los perfiles de seguridad

Servicios de seguridad	**Funciones de llamada**			
	RAS	**H.225.0**	**H.245 (nota)**	**RTP**
Autenticación	Contraseña HMAC-SHA1-96	Contraseña HMAC-SHA1-96	Contraseña HMAC-SHA1-96	
Sólo autenticación	Contraseña HMAC-SHA1-96	Contraseña HMAC-SHA1-96	Contraseña HMAC-SHA1-96	
No repudio				
Integridad	Contraseña HMAC-SHA1-96	Contraseña HMAC-SHA1-96	Contraseña HMAC-SHA1-96	
Confidencialidad				
Control de acceso				
Gestión de claves	Asignación de contraseña basada en acuerdo			
NOTA – H.245 tunelizado o H.245 insertado en una conexión rápida H.225.0.				

Para la autenticación, el usuario deberá utilizar un esquema basado en contraseñas. El esquema basado en contraseñas está muy recomendado para la autenticación por su simplicidad y facilidad de implementación. La función de troceo de todos los campos en los mensajes RAS y de señalización de llamada H.225.0 es el método recomendado para la integridad de los mensajes (también cuando se utiliza el esquema de contraseñas).

Las entidades H.323 seguras que disponen de este perfil de seguridad verifican la autenticación junto con la integridad utilizando el mismo mecanismo de seguridad común.

Los métodos de control de acceso no se describen explícitamente; estos métodos se pueden implementar localmente tras la recepción de la información transportada en los campos de señalización H.235 (ClearToken, CryptoToken).

La presente Recomendación no describe los procedimientos de gestión para la asignación de claves secretas/contraseñas basada en acuerdo. Tales procedimientos podrían realizarse por medios que están fuera del alcance de esta Recomendación.

Las entidades de comunicación involucradas son capaces de determinar implícitamente la utilización, bien del perfil de seguridad básico o bien del perfil de seguridad de firmas mediante la evaluación de los identificadores de objeto de seguridad señalados de los mensajes (**tokenOID** y **algorithmOID**; véase también la cláusula 15).

6.2 Aplicabilidad del perfil de seguridad básico

El perfil de seguridad básico es aplicable en un entorno que permita asignar claves simétricas/contraseñas acordadas a las entidades H.323 aseguradas (terminales) y elementos de red (GK, servidores intermedios). El perfil proporciona la autenticación e integridad, o la autenticación solamente, del mensaje RAS y de señalización de llamada H.225.0 y H.245 tunelizado utilizando la función de troceo HMAC-SHA1-96 basado en contraseñas especificado por el procedimiento I. El establecimiento de comunicación de H.225.0 utilizando FastStart (GK a GK o terminal a terminal) incluye la gestión de claves integrada de Diffie-Hellman.

Con el perfil de seguridad básico es obligatorio utilizar el procedimiento de conexión rápida y es conveniente utilizar la tunelización H.245 dentro de los mensajes H.225.0.

6.3 Requisitos H.323

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

- Conexión rápida.
- Modelo con encaminamiento por controlador de acceso.

6.4 Visión general de los procedimientos

El siguiente procedimiento es para utilización en este perfil.

El procedimiento I es un mecanismo de autenticación de mensajes de señalización basado en claves simétricas simples que utiliza una contraseña compartida por dos entidades (por ejemplo, controlador de acceso y punto extremo H.323). Este procedimiento proporciona la autenticación e integridad de los mensajes RAS, Q.931 y H.245 (véase la cláusula 7).

El procedimiento IA es un mecanismo de sólo autenticación basado en una clave simétrica simple, y que consta de una contraseña compartida entre dos entidades (por ejemplo, un controlador de acceso y un punto extremo H.323). Este procedimiento proporciona autenticación, mas no integridad completa de mensaje. La opción de autenticación únicamente se aplica en los casos en que los mensajes de señalización H.323 atraviesen NAT/cortafuegos.

Dependiendo de la política de seguridad, la autenticación puede ser unilateral, o mutua (recíproca) si se aplica también la autenticación/integridad en el sentido inverso y se proporciona por tanto mayor seguridad. El controlador de acceso decide si se aplica también la autenticación/integridad en el sentido inverso.

Los controladores de acceso que detectan que ha fallado la autenticación y/o que ha fallado la validación de la integridad en un mensaje de señalización de llamada o RAS recibido de un punto extremo o un controlador de acceso par seguros, responde con un mensaje de rechazo que señala el fallo de seguridad fijando el motivo del rechazo a **securityDenial**, u otros códigos de error de seguridad adecuados, conforme a 11.1/H.235.0. Dependiendo de la capacidad para reconocer un ataque, y de la manera más adecuada para reaccionar ante él, un controlador de acceso que reciba una **xRQ** asegurada con identificadores de objeto indefinidos (**tokenOID**, **algorithmOID**) puede responder con **xRJ** no seguro y con razón de rechazo puesta a **securityDenial**, o puede simplemente descartar este mensaje. Debería incluirse en un registro cronológico el evento de seguridad encontrado. De otra parte, el punto extremo descartará el mensaje no seguro recibido, se desconectará y podrá tratar de nuevo escogiendo otros OID. De la misma forma, un controlador de acceso que reciba un mensaje SETUP H.225.0 seguro con identificadores de objeto indefinidos (**tokenOID**, **algorithmOID**) puede responder con un RELEASE COMPLETE no seguro y la razón de rechazo puesta a **securityDenied**, o puede simplemente descartar ese mensaje. Como antes, el evento de seguridad encontrado debería ser registrado.

Existe una señalización H.235 implícita para indicar el uso del procedimiento I y el mecanismo de seguridad aplicado, según los identificadores de objeto (véase también la cláusula 15) y los campos de mensaje rellenos.

Ese perfil no utiliza los campos ICV H.235; en su lugar, los valores criptográficos de comprobación de la integridad son tratados como números generadores criptográficos e introducidos en los campos generadores de **CryptoToken**.

7 Autenticación e integridad de mensajes señalización basada en claves simétricas (procedimiento I)

Cuando se emplea el procedimiento I deberán seguirse estos pasos:

- El algoritmo HMAC-SHA1-96 genera un valor autenticador de troceado que tiene 12 bytes (96 bits). Si la clave es generada a partir de una contraseña, *deberá* utilizarse el mecanismo descrito en 8.2.4 para el cálculo de dicha clave derivada de la contraseña.

  NOTA 1 – Cuando la clave secreta se deriva de una contraseña introducida por el usuario se debe tener cuidado de garantizar una aleatorización suficiente. Se recomienda, por ejemplo, utilizar secretos verdaderamente aleatorios para la clave secreta, o para garantizar que las contraseñas son suficientemente largas.

- El campo **CryptoH323Token** en cada mensaje RAS/H.225.0 deberá contener los siguientes campos:
  - **nestedCryptoToken** con un **CryptoToken** que a su vez contiene el **cryptoHashedToken** que contiene los campos siguientes:
    - **tokenOID** puesto a: "A", indicando que el cálculo de la autenticación/integridad incluye todos los campos del mensaje RAS o de señalización de llamada H.225.0.
    - **hashedVals**, que contiene el campo **ClearToken** utilizado con los siguientes campos:
      - **tokenOID** puesto a: "T", indicando que se está utilizando, como se muestra a continuación, el **ClearToken** básico para la autenticación del mensaje y protección contra reproducción, así como (facultativamente) para la gestión de

clave Diffie-Hellman descrita en 8.5/H.235.6. Se pueden también usar **ClearTokens** con otros OID en lugar del **ClearToken** básico.

- **timeStamp** que contiene la indicación de tiempo.
- **random**, que contiene un número secuencial monotónicamente creciente. Este número permite la elaboración de dos mensajes con la misma indicación de tiempo única (dentro de la resolución de reloj).
- **generalID**, que contiene el identificador del receptor (sólo en el caso de mensajes unidifusión).
- **sendersID**, que contiene el identificador del emisor.
- **dhkey**, utilizado para pasar los parámetros Diffie-Hellman especificados en esta Recomendación durante **Setup** a **Connect**.
  - **halfkey**, que contiene la clave pública aleatoria de una parte.
  - **modsize**, que contiene el número primo DH (véase el cuadro 4/H.235.6).
  - **generator**, que contiene el grupo Diffie-Hellman (véase el cuadro 4/H.235.6).

NOTA 2 – Cuando el perfil de seguridad básico se utiliza sin el perfil de seguridad de criptación vocal, no deberían enviarse entonces parámetros Diffie-Hellman y tampoco debería haber **dhkey**; los **halfkey**, **modsize** y **generator** pueden fijarse a {'0'B,'0'B,'0'B}.

- **token**, que contiene **HASHED** con los campos:
  - **algorithmOID** puesto a "U", indicando el uso de HMAC-SHA1-96.
  - **params** puesto a NULO (NULL).
  - **hash**, con el autenticador calculado utilizando HMAC-SHA1-96. El autenticador puede calcularse para:
    - todos los campos RAS y de señalización de llamada H.225.0 del mensaje si el valor de **tokenOID** en el **CryptoHashedToken** es "A" (que indica autenticación e integridad).

tokenOID "A" se utiliza para la protección de las UU-PDU-H323 tunelizadas, incluidos todos los contenidos de mensaje H.245; el cálculo de la función de troceo se efectuará sobre el mensaje de señalización de llamada **H.225.0** completo con todos los campos, de conformidad con el procedimiento descrito en 7.3.

- El autenticador se verifica en el extremo de cada rama de terminación de canal (EP1-GK1, GK1-GK2, GK2-EP2, EP1-GK2, GK1-EP2 o EP1-EP2, por ejemplo), y es recalculado antes del envío del mensaje a la rama siguiente.

NOTA 3 – El autenticador se calcula mensaje por mensaje.

NOTA 4 – Deberá utilizarse el método de relleno de la norma SHA1 (ISO/CEI 10118-3).

NOTA 5 – Cuando se utiliza la combinación de autenticación e integridad, el autenticador se calcula sobre el mensaje completo.

NOTA 6 – Para evitar que se puedan producir ataques de reproducción, se recomienda decididamente que las implementaciones garanticen que se cambia la contraseña (clave) antes de una inversión (compleción del ciclo) del número secuencial monotónicamente creciente.

NOTA 7 – El destinatario es capaz de detectar la utilización del procedimiento I mediante la evaluación del **tokenOID** dentro del **EncodedGeneralToken** troceado (detectando la presencia de "A").

7.1 Cálculo de la función de troceo basado en contraseña

Tanto el emisor como el receptor de un mensaje de autenticación/integridad calculan la función de troceo con clave sobre todos los campos del mensaje codificado en ASN.1 (utilizando el OID "A").

Para el caso del perfil de sólo autenticación, tanto el emisor como el receptor calculan una función de troceo con clave en todo el ClearToken codificado mediante ASN.1 (utilizando el OID "B").

7.2 HMAC-SHA1-96

HMAC-SHA1-96 es el valor de troceo criptográfico de 96 bits truncado del cálculo de SHA1 de 160 bits. Los 96 bits más a la izquierda del valor de troceo que representa la red por bytes se utilizarán como resultado. RFC 2104 describe el procedimiento cuando la clave secreta *K* es el secreto compartido (= SHA1-contraseña generada numéricamente) y *text* es el valor de memoria intermedia del mensaje.

7.3 Cálculo y verificación de autenticación e integridad

Para la autenticación y la integridad de los mensajes (en caso de aplicarse un OID "A"), el procedimiento es el siguiente:

El emisor de un mensaje deberá calcular el troceado como sigue:

1) Fijará un determinado valor de troceo por defecto de 96 bits de longitud. El esquema exacto de bits no importa aquí, pero constituye una buena elección un esquema de bits único que no aparezca en el mensaje restante.
2) Codificará en ASN.1 el mensaje completo; para RAS esto incluirá el mensaje completo RAS H.225.0; en el caso de la señalización de llamada incluirá el mensaje completo de señalización de llamada H.225.0.
3) Localizará la estructura de bits por defecto en el mensaje codificado y la reemplazará por 96 bits cero.

   NOTA 1 – Esto puede implicar algunos pasos de prueba y error en el caso poco frecuente de que el esquema por defecto aparezca más de una vez en el mensaje.
4) Calculará el valor de troceo criptográfico en el mensaje codificado en ASN.1 utilizando HMAC-SHA1-96 (véase 7.2).
5) Sustituirá el esquema por defecto en el mensaje codificado por el valor de troceo calculado.

El destinatario recibe el mensaje y procede como sigue:

1) Decodifica el mensaje en ASN.1.
2) Extrae el valor de troceo recibido y lo guarda en un RV variable local.
3) Busca y localiza el valor de troceo RV en el mensaje codificado recibido.

   NOTA 2 – En circunstancias poco frecuentes en que la subcadena del valor de troceo puede aparecer varias veces en el mensaje completo, deberán repetirse los pasos 3-6 sucesivamente arrancando de una posición de búsqueda diferente.
4) Sobrescribe el esquema de bits en el mensaje codificado con 96 bits cero.
5) Calcula el valor de troceo criptográfico en el mensaje codificado utilizando HMAC-SHA1-96 (véase 7.2).
6) Compara RV con el valor de troceo calculado. El mensaje sólo se considera inalterado si los dos valores de troceo son iguales; en este caso, la autenticación ha tenido éxito y el procedimiento se detiene.
7) En los demás casos el destinatario repite los pasos 3-7 escribiendo nuevamente el valor RV en la misma posición y buscando otra concordancia. Si ninguna comprobación de concordancia da como resultado una comparación de valores de troceo correcta, el mensaje ha sido alterado (accidental o deliberadamente) durante el tránsito y no es autenticado.

8 Sólo autenticación (procedimiento IA)

Se puede elegir en cada terminal si se implementa la sola autenticación (utilizando OID "B", véase la cláusula 20/H.235.2). En este caso, se calcula el autenticador en un subconjunto (**ClearToken** dentro de **CryptoToken**) del mensaje RAS/H.225.0. La sola autenticación puede ser útil al atravesar NAT/cortafuegos que cambien direcciones/puertos IP dentro de cabidas útiles H.323.

Puesto que la autenticación cubre solamente una porción muy limitada del mensaje, este procedimiento de sólo autenticación no proporciona integridad de mensaje como sí lo hace el procedimiento I. Es decir, la sola autenticación es menos segura.

En el procedimiento de sólo autenticación se utilizarán los siguientes campos en los mensajes protegidos:

- El campo **CryptoH323Token** en cada mensaje RAS/H.225.0 contendrá los siguientes campos:
  - **nestedCryptoToken**, con un **CryptoToken** que a su vez contiene el **cryptoHashedToken**, que tiene los siguientes campos:
    - **tokenOID**, fijado a:
      - "B" (véase la cláusula 20/H.235.2), lo que indica que el cálculo de sólo autenticación incluye todos los campos en el **ClearToken**.
    - **hashedVals**, que contienen el campo **ClearToken** utilizado con los siguientes campos:
      - **tokenOID**, fijado a:
        - "T" (como en el ejemplo del ClearToken básico para el resto de los contenidos de ClearToken) o cualquier otro OID adecuado para otros propósitos.
      - **timeStamp**, que contiene la indicación de tiempo;
      - **random**, que contiene un número secuencial monótonamente creciente. Este número permite la elaboración de dos mensajes que tengan la misma indicación de tiempo (dentro de la resolución del reloj);
      - **generalID**, que contiene el identificador del recipiente (sólo en el caso de mensajes unidifusión);
      - **sendersID**, que contiene el identificador del emisor;
      - **dhkey**, que se utiliza para hacer pasar los parámetros Diffie-Hellman, como se especifica en la Rec. UIT-T H.235 durante **Setup** a **Connect**.
        - **halfkey**, que contiene la clave pública aleatoria de una parte;
        - **modsize**, que contiene el DH primo (véase el cuadro 4/H.235.6);
        - **generator**, que contiene el grupo DH (véase el cuadro 4/H.235.6).

        NOTA 1 – Cuando se use el perfil de seguridad básico sin el perfil de seguridad de criptación de voz no deberían enviarse parámetros Diffie-Hellman y no debería haber **dhkey**; **halfkey**, **modsize** y **generator** se pueden fijar a {'0'B,'0'B,'0'B}.
  - **token**, que contiene **HASHED** con los campos:
    - **algorithmOID** fijado a "U", que indica la utilización de HMAC-SHA1-96;
    - **params** fijado a NULL;
    - **hash**, que contiene el autenticador calculado mediante HMAC-SHA1-96. El autenticador se calculará para:
      - todos los campos de **ClearToken**, si **tokenOID** en el **CryptoHashedToken** se ha fijado a "B" (lo que indica que se utiliza la sola autenticación).

- Al final de cada tramo de canal de terminación se verifica el autenticador (EP1-GK1, GK1-GK2, GK2-EP2, EP1-GK2, GK1-EP2 o EP1-EP2 según el caso), y se recalcula antes de enviar el mensaje al tramo subsiguiente.

NOTA 2 – El autenticador se calcula para el **ClearToken**.

NOTA 3 – Se utilizará el método de relleno con la norma SHA1 (ISO/CEI 10118-3).

NOTA 4 – Para evitar ataques de reproducción es muy recomendado que las implementaciones garanticen que la contraseña (clave) se cambie antes del incremento (o cuando se complete el ciclo) del número secuencial monótonamente creciente.

NOTA 5 – El receptor debe poder detectar la utilización del procedimiento IA evaluando el **OID** "B" dentro del **tokenOID**.

Se calculará el autenticador sólo para el **ClearToken** dentro del **CryptoH323Token** (es decir **ClearToken**) del **token** del **cryptoHashedToken**. Se calculará el valor de troceo criptográfico en la cadena de bits codificados ASN.1 de **ClearToken**.

Los puntos extremos de las versiones 1 y 2 de H.235 pueden utilizar sólo autenticación, en cuyo caso se utilizarán los OID correspondientes para "B". Los puntos extremos de la versión 1 han de seguir el procedimiento descrito en la cláusula 11.

9 Ilustración de la utilización del procedimiento I

En las figuras 1 a 3 se representa la presencia de claves compartidas en el extremo de canales de comunicación para las diferentes combinaciones de canales H.225.0 con encaminamiento directo y por controlador de acceso. Con independencia del modelo de llamada, una clave secreta está siempre presente entre un EP y su GK a fin de proporcionar la autenticación e integridad del mensaje RAS. Cuando un canal RAS y un canal H.225.0 terminan entre los mismos dos nodos, se puede utilizar la misma clave para proporcionar la autenticación e integridad de ambos mensajes RAS y H.225.0.

En la figura 1 se representa el caso que permite más fácilmente una extensión con los dos puntos extremos dentro de zonas que aplican el modelo con encaminamiento por controlador de acceso. Todos los GK involucrados comparten mutuamente claves. Para que sea extensible, se recomienda el escenario representado en la figura 1.

NOTA 1 – Este escenario no proporciona una verdadera seguridad de extremo a extremo entre puntos extremos; toda la seguridad depende de los controladores de acceso intermedios de confianza.

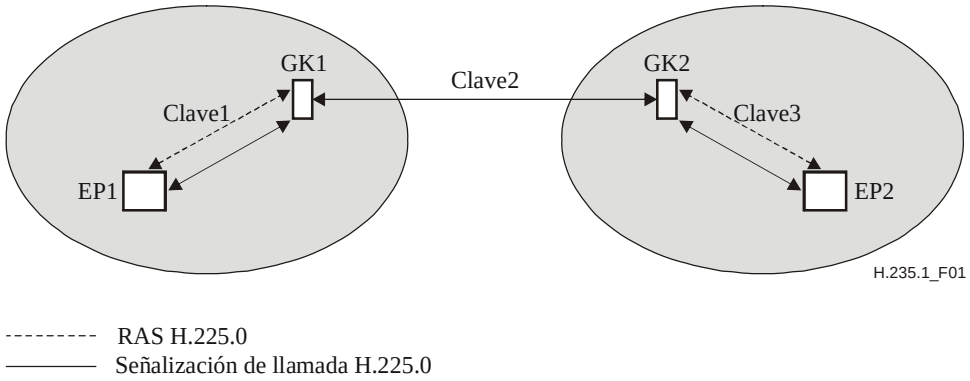

Figura 1/H.235.1 – Ilustración de la utilización del procedimiento I para el caso GK-GK con ambos EP en zonas con encaminamiento por controlador de acceso

En la figura 2 se representa un caso mixto en el cual un EP se encuentra dentro de una zona en la es aplicable el modelo con encaminamiento por controlador de acceso mientras que el otro EP se encuentra en una zona donde es aplicable el modelo de encaminamiento directo. Puede ser el caso de entornos cerrados en los cuales el número de EP2 y de GK1 es limitado.

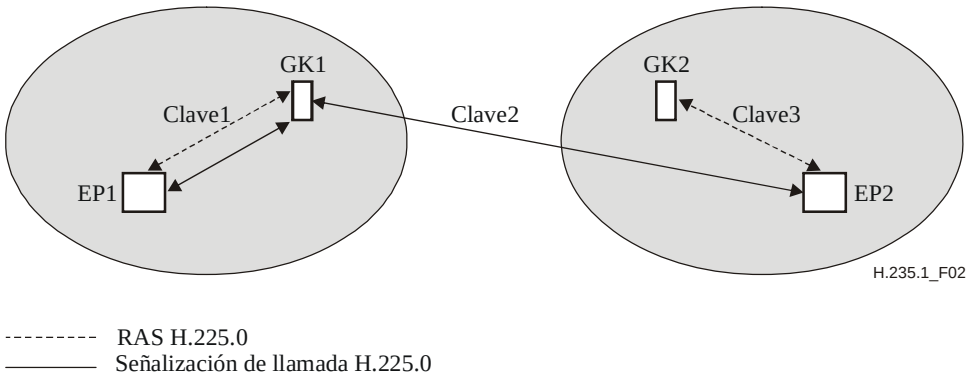

Figura 2/H.235.1 – Ilustración de la utilización del procedimiento I para el caso mixto con EP1 en una zona de encaminamiento por controlador de acceso y EP2 en una zona de encaminamiento directo

En la figura 3 se representa un caso con ambos EP en zonas que aplican el modelo de GK con encaminamiento directo. Este escenario no es muy extensible cuando están implicados muchos EP. En principio, se recomienda la utilización en su lugar de H.235.2 con los procedimientos II/III. Para este escenario específico y los procedimientos I, II o III, se necesitan también medidas de seguridad adicionales (que protejan contra el fraude y la utilización incorrecta de llamadas por medio de la autorización de la llamada con testigos de acceso en controladores de acceso H.323, por ejemplo) las cuales no se describen en esta Recomendación; este tema queda en estudio.

NOTA 2 – Este escenario proporciona una verdadera seguridad de extremo a extremo entre puntos extremos, sin que dependa de nodos intermedios de confianza.

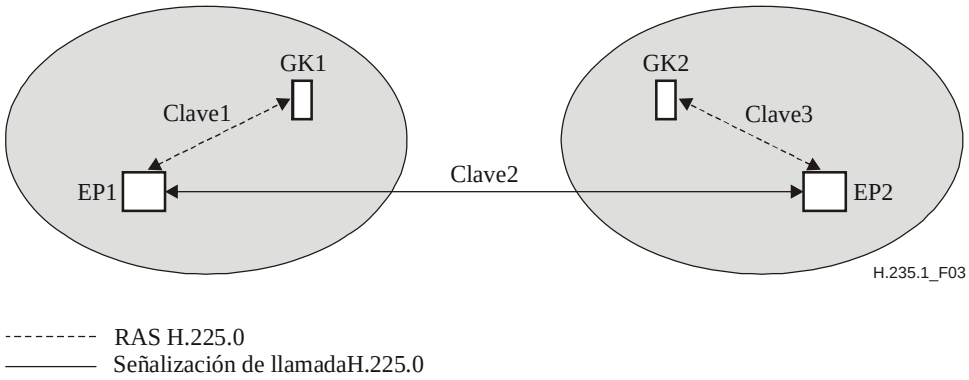

Figura 3/H.235.1 – Ilustración de la utilización del procedimiento I para el caso con ambos EP en zonas que utilizan un modelo de GK con encaminamiento directo

Consideremos el caso de la figura 1 donde tres contraseñas son compartidas por parejas: entre EP1-GK1, entre GK1-GK2 y entre GK2-EP2, respectivamente. A partir de estas contraseñas se generan tres claves de 20 bytes – *Key1 (clave1)*, *Key2 (clave2)* y *Key3 (clave3)* – basándose en el procedimiento descrito en 8.2.4 de H.235.0. Para conseguir una seguridad máxima se recomienda que las tres contraseñas/claves aleatorias sean independientes.

Más adelante se detalla el procedimiento para la autenticación/integridad de los mensajes RAS H.225.0 y H.245. El ejemplo de descripción representa parámetros específicos en un modelo con encaminamiento por controlador de acceso; también son posibles otras combinaciones válidas y útiles de identificadores de objeto en diferentes escenarios.

NOTA 3 – Los escenarios que se muestran en las figuras 1 a 3 no son fácilmente extensibles cuando el número de claves (contraseñas) simétricas compartidas entre GK (figura 1), entre GK y EP distantes (figura 2), o entre los EP (figura 3) es demasiado grande.

9.1 Autenticación e integridad de los mensajes RAS

Consideremos el caso en que EP1 desea enviar un mensaje RAS, por ejemplo, un mensaje **ARQ** (petición de admisiones), a GK1. EP1 genera una indicación de tiempo y un número secuencial y los incluye en los campos **timeStamp** y **random** respectivamente, junto con el alias del GK1 en el campo **generalID** y el ID de EP en el campo **sendersID**. Estos campos están presentes en el campo **ClearToken** del **hashedVals** presente en el **cryptoHashedToken** del campo **CryptoToken** del **cryptoH323Token** del mensaje **ARQ**.

El **tokenOID** dentro del **cryptoHashedToken** se fija a "A", indicando que a todos los campos en el mensaje **ARQ** se les ha aplicado la función de troceo. El **HASHED** dentro de **token** en **cryptoHashedToken** tiene el **algorithmOID** puesto a "U", indicando el uso de HMAC-SHA1-96, y **params** puesto a NULO. EP1 calcula entonces el autenticador basado en el HMAC-SHA1-96 utilizando la clave de 20 bytes *Key1*. El autenticador es calculado sobre el mensaje RAS entero.

EP1 incluye el autenticador calculado dentro de **hash** en el campo **token** del campo **cryptoHashedToken** del **CryptoToken** presente en el **cryptoH323Token** del mensaje **ARQ**. El mensaje **ARQ** es enviado entonces al GK1.

Tras la recepción del mensaje **ARQ**, GK1 verifica el autenticador basándose en varios criterios que incluyen:

- Vida de **timeStamp** y unicidad del **random**.
- Identidad del **generalID** e identificador propio.
- Concordancia del autenticador en el mensaje **ARQ** con el calculado por GK1.

9.2 Autenticación e integridad de los mensajes H.225.0

Consideremos el caso en que EP1 desea enviar un mensaje H.225.0, por ejemplo, un mensaje **Setup**, a EP2. EP1 genera una indicación de tiempo y un número secuencial y los incluye en los campos **timeStamp** y **random** respectivamente, junto con el alias del GK1 en el **generalID** y el ID de EP en el campo **sendersID**. EP1 calcula también media clave Diffie-Hellman e incluye los parámetros Diffie-Hellman **halfkey**, **modsize** y **generator** en el campo **dhkey** del **ClearToken**. Estos campos están presentes en el campo **ClearToken** de **hashedVals** presente en el **cryptoHashedToken** del campo **CryptoToken** del **cryptoH323Token** del mensaje **Setup**.

El **tokenOID** dentro del **cryptoHashedToken** se fija a "A", indicando con ello que se ha aplicado la función de troceo a todos los campos en el mensaje de señalización H.225.0. El **HASHED** dentro de **token** en **cryptoHashedToken** tiene el **algorithmOID** puesto a "U", indicando la utilización de HMAC-SHA1-96, y **params** puesto a NULO. EP1 calcula a continuación el autenticador basado en el algoritmo HMAC-SHA1 utilizando la clave de 20 bytes, *Key1*. El autenticador es calculado de conformidad con el método de troceo elegido (A) tomando en consideración el mensaje de señalización de llamada H.225.0 completo.

EP1 incluye el autenticador calculado dentro de **hash** en el campo **token** del campo **cryptoHashedToken** del **CryptoToken** presente en el **cryptoH323Token** del mensaje **Setup**. A continuación se envía el mensaje **Setup** a GK1.

Tras la recepción del mensaje **Setup**, GK1 verifica el autenticador basándose en varios criterios que incluyen:

- Validez de **timeStamp** y carácter único de **random**.
- La identidad del **generalID** y el identificador propio.
- La verificación de parámetros Diffie-Hellman, por ejemplo, probando si el primo de 1024 bits y el generador son correctos. La prueba de seguridad de los parámetros Diffie Hellman es un proceso que consume tiempo y solamente puede realizarse cuando la política local lo requiere.
- Concordancia del autenticador en el mensaje **Setup** con el calculado por GK1.

Si el autenticador es verificado, GK1 calcula un nuevo autenticador para insertarlo (sustituirlo) en el mensaje **Setup** antes de reenviarlo a GK2 como sigue. GK1 reemplaza los campos **timeStamp**, **random**, **sendersID** y **generalID** en el campo **ClearToken** de **hashedVals** utilizando valores pertinentes a la rama GK1-GK2. El campo **timeStamp** contiene la indicación de tiempo actual, el campo **random** contiene el siguiente número secuencial monotónicamente creciente para la rama GK1-GK2, el campo **generalID** contiene el alias de GK2 y el **sendersID** contiene el alias de GK1. GK1 incluye también los parámetros Diffie-Hellman recibidos en el campo **dhkey** del **ClearToken**.

GK1 calcula después un nuevo autenticador para el mensaje de señalización de llamada H.225.0 utilizando la clave *Key2 (Clave2*) y el algoritmo HMAC-SHA1-96 (**algorithmOID**="U"), lo inserta en **hash** dentro de **token** y pasa el mensaje **Setup** al GK2.

Tras la recepción del mensaje **Setup**, GK2 verifica el autenticador, calcula un nuevo autenticador después de modificar los campos **ClearToken** en **hashedVals** adecuadamente, lo inserta en el campo **hash** y pasa el mensaje **Setup** al EP2.

9.3 Autenticación e integridad de los mensajes H.245

Consideremos el caso en el que EP1 desea enviar un mensaje H.245, por ejemplo, un mensaje **TerminalCapabilitySet**, a EP2. EP1 comprueba si es necesario enviar un mensaje H.225.0 a GK1. En caso afirmativo, el mensaje H.245 es tunelizado dentro de dicho mensaje H.225.0. Los campos dentro del mensaje H.225.0 se fijan del modo descrito anteriormente para la transmisión de un mensaje H.225.0. Puesto que el mensaje H.245 está tunelizado, la **h323-uu-pdu** en el mensaje **h323-UserInformation** tiene sus campos fijados como sigue:

- el valor del campo **h323-message-body** es el tipo de mensaje H.225.0 que está siendo transmitido;
- el valor de **h245Tunnelling** es VERDADERO (TRUE);
- **h245Control** contiene la cadena de octetos PDU H.245.

EP1 genera un **CryptoToken** para el mensaje H.225.0, pone **tokenOID** a "A" indicando autenticación e integridad, fija **timeStamp**, **random**, **sendersID**, **generalID** y **tokenOID** a "T" en el **ClearToken** del **hashedVals**, fija **algorithmOID** a "U" indicando la utilización de HMAC-SHA1-96 y **hash** al autenticador generador calculado sobre todos los campos del mensaje de señalización de llamada H.225.0.

Sin embargo, si no hay ningún mensaje H.225.0 pendiente de transmisión, el mensaje H.245 es tunelizado dentro de un mensaje **facility** H.225.0 ad hoc. La **h323-uu-pdu** en el mensaje **h323-UserInformation** tiene sus campos fijados como sigue:

- el valor del campo **h323-message-body** es **facility** que contiene:
  - **reason**, con el valor **undefinedReason**;
  - **tokens** y **cryptoTokens**, con el valor habitual de mensajes H.225.0;
- el valor de **h245Tunnelling** es VERDADERO (TRUE);

- **h245Control** contiene la cadena de octetos PDU H.245.

Tal como se ha descrito anteriormente, EP1 genera un **CryptoToken** como parte del mensaje **facility** de H.225.0. El mensaje **facility** es a continuación transmitido por EP1 a GK1.

En cualquiera de los dos casos (si está pendiente de transmisión un mensaje H.225.0 o si se utiliza un mensaje **facility** H.225.0 ad hoc), GK1 verifica el autenticador tras la recepción del mensaje. A continuación, si está pendiente de transmisión un mensaje H.225.0 para la rama GK1-GK2, el mensaje H.245 es tunelizado dentro de ese mensaje; en caso contrario, es tunelizado dentro de un mensaje **facility** H.225.0 ad hoc. Al igual que en el caso de la transmisión de un mensaje H.225.0, se calcula un nuevo autenticador para el mensaje H.225.0 antes de su transmisión de GK1 a GK2. El proceso se repite para la rama GK2-EP2.

9.4 Escenario con encaminamiento directo

Las entidades H.323 aseguradas no sólo pueden comunicar dentro del entorno con encaminamiento por controlador de acceso como se señala en esta Recomendación, también pueden utilizar el modo de encaminamiento directo. Este modelo con encaminamiento directo requiere medidas de seguridad adicionales (testigos de acceso) que no son necesarias en los entornos con encaminamiento por controlador de acceso más sencillos. Rec. UIT-T H.235.4 describe como asegurar el modelo con encaminamiento directo.

10 Soporte de los servicios fuera del terminal

La entidades H.323 aseguradas pueden utilizar servicios fuera del terminal de conformidad con el procedimiento descrito en I.1.6/H.235.0.

11 Compatibilidad con la versión 1 de H.235

Aunque estos perfiles de seguridad se han desarrollado pensando en la Rec. UIT-T H.235 versión 2 (Rec. UIT-T H.235 (2000)), se pueden también aplicar a la Rec. UIT-T H.235 versión 1 (Rec. UIT-T H.235 (1998)) con algunas modificaciones menores. El receptor puede detectar la presencia de la versión de protocolo H.235 del emisor mediante la evaluación de los identificadores de objeto de perfil de seguridad (véase cláusula 15).

Las implementaciones de la Rec. UIT-T H.235 versión 1 (Rec. UIT-T H.235 (1998)):

- no fijan ni evalúan el **sendersID** en el **ClearToken**;
- no pueden utilizar los servicios fuera del terminal de la cláusula 10.

12 Funcionamiento en multidifusión

Los mensajes de multidifusión H.225.0, como GRQ o LRQ, no deberán incluir el CryptoToken del procedimiento I. Cuando tales mensajes son enviados en unidifusión, deberán incluir un CryptoToken.

13 Lista de mensajes de señalización seguros

En esta cláusula se presenta un resumen de cómo y por qué medios, esta Recomendación asegura los distintos mensajes de señalización H.323.

13.1 RAS H.225.0

Mensaje RAS H.225.0	Campos de señalización H.235	Autenticación e integridad
Cualquiera	cryptoTokens	Procedimiento I

13.2 Señalización de llamada H.225.0

Mensaje de señalización de llamada H.225.0	Campos de señalización H.235	Autenticación e integridad
UUIE Aviso, UUIE Llamada en curso, UUIE Conexión, UUIE Establecimiento, UUIE Facilidad, UUIE Progresión, UUIE Información, UUIE Liberación completa, UUIE Estado, UUIE Petición de estado, UUIE Acuse de establecimiento, UUIE Notificación	cryptoTokens	Procedimiento I

13.3 Control de llamada H.245

Los mensajes H.245 con destino a, o procedentes de, entidades H.323 aseguradas deberán ser transportados como parte de la conexión rápida segura, o ser tunelizados utilizando el mensaje **UUIE Facilidad** H.225.0.

14 Utilización de sendersID y de generalID

El **ClearToken** tiene los campos **sendersID** (**identificador del emisor**) y **generalID**. Cuando se dispone de información de identificación, el **sendersID** ha de ser el identificador del controlador de acceso (GKID, *gatekeeper identifier*) para los mensajes iniciados por el controlador de acceso, y el identificador de punto extremo (EPID, *endpoint identifier*) para los mensajes iniciados por el punto extremo. Cuando se dispone de información de identificación, el **generalID** ha de ser el GKID para los mensajes iniciados por el punto extremo, y el EPID para los mensajes iniciados por el controlador de acceso. Cuando no se dispone de información de identificación, o cuando la difusión/multidifusión es ambigua, no se incluye el campo o se incluye con una cadena nula. El cuadro 2 resume la situación.

Cuadro 2/H.235.1 – Utilización de sendersID y generalID

Mensaje	sendersID	generalID
GRQ unidifusión	**EPID** si está disponible, en su defecto **NULL**	**GKID**
GRQ multidifusión	**EPID** si está disponible, en su defecto **NULL**	
GCF, **GRJ**	**GKID**	**EPID** si está disponible, en su defecto **NULL**
RRQ inicial	**EPID** si está disponible, en su defecto **NULL**	**GKID**
RCF	**GKID**	**EPID**
RRJ	**GKID**	

Cuadro 2/H.235.1 – Utilización de sendersID y generalID

Mensaje	sendersID	generalID
URQ, UCF, URJ, BRQ, BCF, BRJ, DRQ, DCF, DRJ, NSM, RIP, SCI, SCR, XRS (EP a GK)	**EPID**	**GKID**
URQ, UCF, URJ, BRQ, BCF, BRJ, DRQ, DCF, DRJ, NSM, RIP, SCI, SCR, XRS (GK a EP)	**GKID**	**EPID**
ARQ, IRQ, RAI	**EPID**	**GKID**
ACF, ARJ, BCF, LCF, LRJ, IRR, IRQ, RAC, LCF, LRJ, IACK, INAK	**GKID**	**EPID**
LRQ unidifusión (EP a GK)	**EPID**	**GKID**
LRQ unidifusión (GK a GK)	**GKID**	**GKID**
LRQ multidifusión	**EPID**	
NOTA – GKID es el identificador del controlador de acceso, EPID es el identificador de punto extremo. Un espacio en blanco equivale a una cadena de identificación faltante o nula.		

15 Lista de identificadores de objeto

En el cuadro 3 se listan todos los OID referenciados (véanse también [OIW] y [WEBOIDs]). Hay identificadores de objeto para la versión 1 de H.235 [H.235v1] y la versión 2 de H.235 [H.235v2].

Cuadro 3/H.235.1 – Identificadores de objeto

Referencia de identificador de objeto	Valor(es) de identificador de objeto	Descripción
"A"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 1} {itu-t (0) recommendation (0) h (8) 235 version (0) 1 1}	Utilizado en los procedimientos I para el CryptoToken-tokenOID, indicando que el troceado incluye todos los campos del mensaje RAS y de señalización de llamada H.225.0 (autenticación e integridad).
"E"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 9} {itu-t (0) recommendation (0) h (8) 235 version (0) 2 9}	ClearToken de extremo a extremo que transporta sendersID para la verificación en el lado del receptor.
"T"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 5} {itu-t (0) recommendation (0) h (8) 235 version (0) 1 5}	Utilizado en los procedimientos I e IA como el ClearToken básico para la autenticación de mensaje y protección contra los ataques de reproducción y, como una opción, también para la gestión de clave Diffie-Hellman, como se describe en 8.5/H.235.6.
"U"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 6} {itu-t (0) recommendation (0) h (8) 235 version (0) 1 6}	Utilizado en el procedimiento I para el algoritmo OID, indicando la utilización de HMAC-SHA1-96.

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