Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

H.235.0

(09/2005)

SERIE H: SISTEMAS AUDIOVISUALES Y MULTIMEDIOS

Infraestructura de los servicios audiovisuales – Aspectos de los sistemas

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.235.0

UIT-T

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.235.0

Marco de seguridad H.323: Marco de seguridad para sistemas multimedia de la serie H (H.323 y otros basados en H.245)

Resumen

Esta Recomendación describe mejoras dentro del marco de las especificaciones de las Recomendaciones de la serie H.3xx para incorporar servicios de seguridad tales como *autenticación* y *privacidad* (criptación de datos). El esquema propuesto es aplicable a conferencias punto a punto y multipunto para cualesquiera terminales que utilicen la Rec. UIT-T H.245 como su protocolo de control; también los sistemas H.323 que utilicen los protocolos RAS y/o de señalización de llamada.

Por ejemplo, los sistemas H.323 funcionan por redes de paquetes que no proporcionan una calidad de servicio garantizada. Por la misma razón técnica de que la red de base no proporciona la calidad de servicio, la red no proporciona un servicio seguro. La comunicación en tiempo real segura por redes inseguras plantea generalmente dos problemas importantes: *autenticación* y *privacidad*.

Esta Recomendación describe la infraestructura de seguridad y técnicas de privacidad específicas que han de emplear los terminales multimedia de la serie H.3xx. Esta Recomendación aborda los aspectos relacionados con la conferencia interactiva, entre los que cabe citar la autenticación y privacidad de todos los trenes de medios en tiempo real que son intercambiados en la conferencia, aunque no está limitado estrictamente a éstos. Esta Recomendación proporciona el protocolo y algoritmos necesarios entre las entidades H.323.

Esta Recomendación utiliza las facilidades generales soportadas en la Rec. UIT-T H.245 y como tal, cualquier norma que funcione junto con este protocolo de control puede utilizar este marco de seguridad. Se prevé que siempre que sea posible otros terminales de la serie H puedan interfuncionar y utilizar directamente los métodos descritos en esta Recomendación, en el que inicialmente no se prevé la implementación completa en todos los campos, sino que destacará específicamente la autenticación de puntos extremos y la privacidad de los medios.

Esta Recomendación incluye la capacidad de negociar servicios y funcionalidades de una manera genérica, y la selectividad en relación con técnicas criptográficas y capacidades utilizadas. La manera específica en que éstas se utilizan se relaciona con las capacidades de los sistemas, requisitos de aplicación y restricciones específicas de la política de seguridad. Esta Recomendación soporta diversos algoritmos criptográficos, con opciones variadas apropiadas para diferentes fines, por ejemplo, longitudes de claves. Ciertos algoritmos criptográficos pueden ser asignados a servicios de seguridad específicos (por ejemplo, uno para criptación rápida de tren de medios y otro para criptación de señalización).

Cabe señalar también que algunos algoritmos criptográficos o mecanismos pueden estar reservados para exportación u otros aspectos nacionales (por ejemplo, con longitudes de claves restringidas). Esta Recomendación soporta la señalización de algoritmos bien conocidos además de la señalización de algoritmos criptográficos no normalizados o privados. No hay algoritmos específicamente obligatorios, aunque se aconseja decididamente que los puntos extremos soportan el mayor número posible de algoritmos para lograr el interfuncionamiento. Esto es paralelo al concepto de que el soporte de la Rec. UIT-T H.245 no garantiza el interfuncionamiento entre códecs de dos entidades.

La versión 4 de la Rec. UIT-T H.235 divide la versión 3 anterior de la Rec. UIT-T H.235 en una subserie de Recomendaciones H.235.x reestructurada. Se han añadido dos nuevas Recomendaciones a la subserie, las Recs. UIT-T H.235.8 y H.235.9 y se han ampliado otras con nuevas funcionalidades (Recs. UIT-T H.235.3 y H.235.5). La Rec. UIT-T H.235.0 contiene el marco de seguridad para los sistemas H.323. Es un texto común y de referencia para las Recomendaciones de la subserie H.235.x.

En los nuevos apéndices IV, V y VI se indica la relación entre la nueva disposición y el texto, las figuras y los cuadros de la versión 3 de la Rec. UIT-T H.235 (2003), incluyendo el corrigendum 1 y las enmiendas que se han hecho.

Orígenes

La Recomendación UIT-T H.235.0 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 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

Página

Recomendación UIT-T H.235.0

Marco de seguridad H.323: Marco de seguridad para sistemas multimedia de la serie H (H.323 y otros basados en H.245)

1 Alcance

La finalidad primaria de esta Recomendación es proporcionar un marco de seguridad para la autenticación, privacidad e integridad en el contexto de los protocolos vigentes de la serie H. El texto actual de esta Recomendación proporciona detalles sobre la implementación con la Rec. UIT-T H.323. Se prevé que este marco funcione junto con otros protocolos de la serie H que utilizan como protocolo de control la Rec. UIT-T H.245 y/o los protocolos RAS y/o de señalización de llamada de la Rec. UIT-T H.225.0.

Entre los objetivos adicionales de esta Recomendación cabe citar:

1) Crear una arquitectura de seguridad como un marco extensible y flexible para aplicar un sistema de seguridad para los terminales de la serie H y otros sistemas basados en la H.323. Esto se debe proporcionar mediante servicios flexibles e independientes y la funcionalidad que éstos suministran, e incluye la posibilidad de negociar y seleccionar las técnicas criptográficas empleadas, así como la manera en la cual éstas se utilizan.
2) Proporcionar seguridad para todas las comunicaciones establecidas como resultado de la aplicación de los protocolos H.3xx. Esto incluye los aspectos relativos al establecimiento de la conexión, control de la llamada e intercambio de medios entre todas las entidades. Este requisito comprende la utilización de comunicación confidencial (privacidad) y puede explotar funciones para autenticación de pares así como protección del entorno del usuario contra ataques.
3) Esta Recomendación no excluye la integración de otras funciones de seguridad en entidades H.3xx que puedan protegerlas contra ataques de la red.
4) Esta Recomendación no debe limitar la posibilidad de ampliar según proceda cualesquiera especificaciones de la Recomendación de la serie H.3xx. Esto puede incluir el número de usuarios seguros y los niveles de seguridad proporcionados.
5) Cuando proceda, todos los mecanismos y facilidades deben ser proporcionados independientemente de cualquier transporte o topologías subyacentes. Para contrarrestar estas amenazas se pueden necesitar otros medios que están fuera del ámbito de esta Recomendación.
6) Se prevé el funcionamiento en un entorno mixto (entidades seguras e inseguras).
7) Esta Recomendación debe proporcionar facilidades para distribuir claves de sesión asociadas con la criptografía utilizada. (Esto no supone que la gestión de certificados basada en claves públicas deba ser parte de esta Recomendación.)
8) Esta Recomendación proporciona dos perfiles de seguridad que facilitan la compatibilidad. En la H.235.1 se describe un perfil de seguridad sencillo basado en contraseñas, que es sencillo pero seguro, mientras que en la H.235.2 se presenta un perfil de seguridad de firmas, con firmas digitales, certificados y una infraestructura de claves públicas que superan las limitaciones de la H.235.1.

La arquitectura de seguridad, descrita en esta Recomendación, no supone el conocimiento entre los participantes. Sin embargo, supone que se han tomado precauciones adecuadas para asegurar físicamente los puntos extremos de la serie H. Por consiguiente, se considera que la principal amenaza a la seguridad de las comunicaciones es la intromisión en la red o algún otro método de desviar los trenes de medios.

La Rec. UIT-T H.323 proporciona los medios para conducir una conferencia de audio, vídeo y datos entre dos o más partes, pero no el mecanismo para que cada participante pueda autenticar la identidad de los otros participantes, ni los medios para salvaguardar la privacidad de comunicaciones (es decir, criptado de los trenes).

Las Recs. UIT-T H.323, H.324 y H.310 utilizan los procedimientos de señalización de canal lógico de la Rec. UIT-T H.245, en los cuales se describe el contenido de cada canal lógico cuando se abre el canal. Se proporcionan procedimientos para indicar las capacidades del receptor y del transmisor, las transmisiones están limitadas a lo que pueden decodificar los receptores, y los receptores pueden pedir a los transmisores un modo deseado. Las capacidades de seguridad de cada punto extremo son indicadas de la misma manera que cualquier otra capacidad de comunicación.

Algunos terminales de la serie H (H.323) pueden ser utilizados en configuraciones multipunto. El mecanismo de seguridad descrito en esta Recomendación permitirá el funcionamiento seguro en estos entornos, incluido el funcionamiento de unidades de control multipunto (MCU) centralizadas y descentralizadas.

1.1 Estructura de la subserie de Recomendaciones H.235.x

Esta Recomendación relativa al marco de seguridad es una referencia para la subserie de Recomendaciones H.235.x que se ilustra en la figura 1. Esta Recomendación contiene texto común e información general que resulta útil para todas las Recomendaciones de la serie H.235.x.

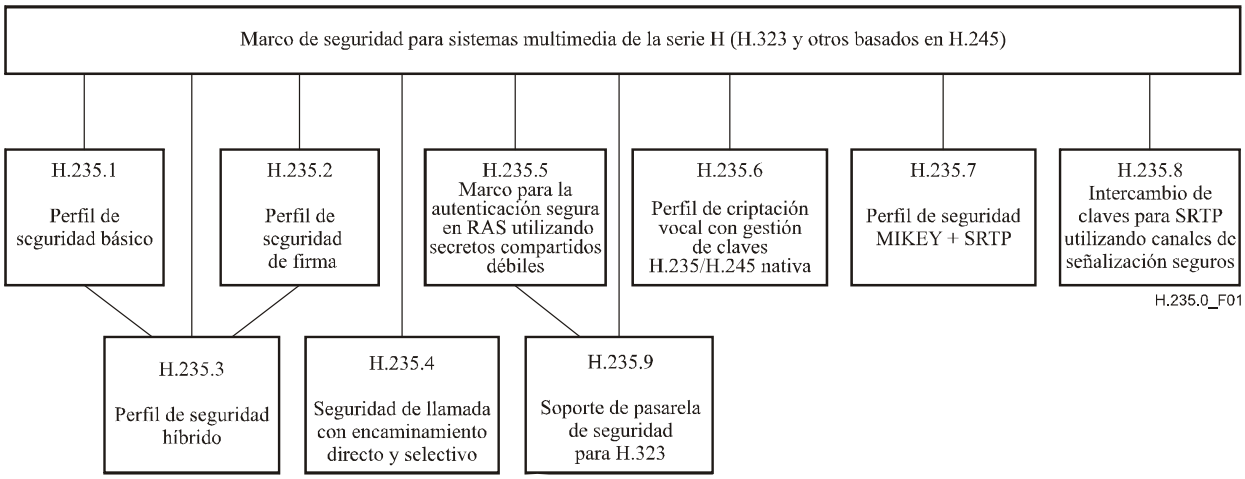


Figura 1/H.235.0 – Estructura de la subserie de Recomendaciones H.235.x

La línea vertical de la figura 1 indica una dependencia directa con el texto principal de la H.235.0; puede haber más dependencias indirectas de otras Recomendaciones de la serie H.235.x. Pueden utilizarse varias Recomendaciones conjuntamente y de manera complementaria; véase también 6.9.

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 (2003), *Seguridad y criptado para terminales multimedios de la serie H (basados en las Recomendaciones H.323 y H.245)*, más enmienda 1 (2004), más corrigendum 1 (2005).

– 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.235.3 (2005), *Marco de seguridad H.323: Perfil de seguridad híbrido*.

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

– Recomendación UIT-T H.235.5 (2005), *Marco de seguridad H.323: Marco para la autenticación segura en RAS utilizando secretos compartidos débiles*.

– 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.235.7 (2005), *Marco de seguridad H.323: Utilización del protocolo de gestión de claves MIKEY para el protocolo de transporte en tiempo real seguro en H.235*.

– Recomendación UIT-T H.235.8 (2005), *Marco de seguridad H.323: Intercambio de claves para el protocolo de transporte en tiempo real seguro utilizando canales de señalización seguros*.

– Recomendación UIT-T H.235.9 (2005), *Marco de seguridad H.323: Soporte de pasarela de seguridad para H.323*.

– 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 H.530 (2003), *Procedimientos de seguridad simétricos para movilidad de sistemas H.323 según la Recomendación H.510*, más corrigendum 1 (2003).

– 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 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 9798-2:1999, *Information technology – Security techniques – Entity authentication – Part 2: Mechanisms using symmetric encipherment algorithms*.

– ISO/CEI 9798-3:1998, *Information technology – Security techniques – Entity authentication – Part 3: Mechanism using digital signature techniques*.

– ISO/CEI 9798-4:1999, *Information technology – Security techniques – Entity authentication – Part 4: Mechanisms using a cryptographic check function*.

– ISO/CEI 15946-1:2002, *Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General*.

– ISO/CEI 15946-2:2002, *Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures*.

– ATM Forum: af-sec-0100.002 (2001), *ATM Security Specification Version 1.1*.

– IETF RFC 2246 (1999), *The TLS Protocol Version 1.0*.

– IETF RFC 2401 (1998), *Security Architecture for the Internet Protocol*.

– IETF RFC 2407 (1998), *The Internet IP Security Domain of Interpretation for ISAKMP*.

– IETF RFC 2408 (1998), *Internet Security Association and Key Management Protocol (ISAKMP)*.

– IETF RFC 2865 (2000), *Remote Authentication Dial In User Service (RADIUS)*.

– IETF RFC 3546 (2003), Transport Layer Security Protocol (TLS) Extensions.

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

2.2 Referencias informativas

[Daemon] DAEMON (J.), *Cipher and Hash function design*, Ph.D. Thesis, Katholieke Universiteit Leuven, March 1995.

[ESP] IETF RFC 2406 (1998), *IP Encapsulating Security Payload (ESP)*.

[OAKLEY] IETF RFC 2412 (1998), *The OAKLEY Key Determination Protocol*.

[IKE] IETF RFC 2409 (1998), *The Internet Key Exchange (IKE)*.

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

[J.170] ITU-T Recommendation J.170 (2005), *IPCablecom security specification*.

[RTP] IETF RFC 3550 (2003), *RTP: A transport Protocol for Real-Time Applications*.

[Schneier] SCHNEIER (B.), *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd Edition, John Wiley & Sons, Inc., 1995.

[SRTP] IETF RFC 3711 (2004), *The Secure Real-time Transport Protocol (SRTP)*.

3 Términos y definiciones

En esta Recomendación se aplican las definiciones que figuran en la cláusula 3/H.323, cláusula 3/H.225.0 y cláusula 3/H.245 junto con las de esta cláusula. Algunos de los siguientes términos se utilizan como se define en las Recs. UIT-T X.800 | ISO 7498-2, X.803 | ISO/CEI 10745, X.810 | ISO/CEI 10181-1 y X.811 | ISO/CEI 10181-2.

3.1 control de acceso: Prevención del uso no autorizado de un recurso, incluida la prevención del uso de un recurso de una manera no autorizada (Rec. UIT-T X.800).

3.2 autenticación: Provisión de seguridad de la identidad alegada de una entidad (Rec. UIT-T X.811 | ISO/CEI 10181-2).

3.3 autorización: Concesión de permisos sobre la base de identificación autenticada.

3.4 ataque: Actividades realizadas para obviar los mecanismos de seguridad de un sistema o aprovechar sus deficiencias. Los ataques directos a un sistema aprovechan las deficiencias en los algoritmos, principios o propiedades subyacentes de un mecanismo de seguridad. Los ataques indirectos obvian el mecanismo, o hacen que el sistema utilice el mecanismo incorrectamente.

3.5 certificado: Conjunto de datos relativos a la seguridad emitidos por una autoridad de seguridad o tercero de confianza, junto con información de seguridad que se utiliza para proporcionar los servicios de integridad y autenticación de origen de datos para los datos (Rec. UIT-T X.810 | ISO/CEI 10181-1). En esta Recomendación, el término se relaciona con certificados de "clave pública" que son valores que representan una clave pública patentada (y otra información facultativa) verificada y firmada por una autoridad de confianza en un formato infalsificable.

3.6 cifra: Algoritmo criptográfico, una transformada matemática.

3.7 confidencialidad: Propiedad que impide la revelación de información a individuos, entidades o procesos no autorizados.

3.8 algoritmo criptográfico: Función matemática que calcula un resultado a partir de uno o varios valores de entrada.

3.8 *bis* EC-GDSA: Firma digital de curva elíptica con apéndice análoga al algoritmo de firma digital NIST (DSA, *digital signature algorithm)*]; (véase también ISO/CEI 15946-2, capítulo 5).

3.8 *ter* criptosistema de curva elíptica (ECC, *elliptic curve cryptosystem*): Un criptosistema de claves públicas (véase la sección 8.7 del Foro *ATM Security Specification Version 1.1*).

3.8 *quat* esquema de convenio de claves de curva elíptica – Diffie-Hellman (ECKAS-DH, *elliptic curve key agreement scheme Diffie-Hellman*): El esquema de convenio de claves Diffie-Hellman que utiliza criptografía de curva elíptica.

3.9 cifrado: Cifrado (criptación) es el proceso que hace que los datos sean ilegibles para entidades no autorizadas aplicando un algoritmo criptográfico (un algoritmo de criptación). El descifrado (descriptación) es la operación inversa por la cual el texto cifrado se transforma en texto claro.

3.10 integridad: Propiedad de que los datos no han sido alterados de una manera no autorizada.

3.11 gestión de claves: Generación, almacenamiento, distribución, supresión, archivado y aplicación de claves de acuerdo con una política de seguridad (Rec. UIT-T X.800).

3.12 tren de medios: Un tren de medios puede ser del tipo audio, vídeo o datos, o una combinación de cualquiera de ellos. Los datos de trenes de medios transportan datos de usuario o de aplicación (cabida útil) pero no datos de control.

3.13 no repudio: Protección contra la negación por una de las entidades que participan en una comunicación de haber participado en toda la comunicación o parte de ésta.

3.14 privacidad: Modo de comunicación en el cual sólo las partes habilitadas explícitamente pueden interpretar la comunicación. Esto se logra en general mediante criptación y claves compartidas para el cifrado.

3.15 canal privado: Para esta Recomendación, un canal privado es el resultante de negociación previa por un canal seguro. En este contexto, puede ser utilizado para manipular trenes de medios.

3.16 criptografía de claves públicas: Sistema de criptación que utiliza claves asimétricas (para criptación/descriptación) en el cual las claves tienen una relación matemática entre sí, que no puede ser calculada razonablemente.

3.17 perfil de seguridad: Conjunto (subconjunto) de características y procedimientos coherentes y con capacidad de interfuncionamiento entre sí que caen fuera del alcance de la Rec. UIT-T H.235 y que son útiles para proporcionar seguridad a las comunicaciones multimedia H.323 entre las entidades involucradas en un escenario específico.

3.18 inundación: Ataque de denegación de servicio que tiene lugar cuando se envían en exceso a un sistema datos no autorizados. Un caso especial es la inundación de medios que se produce cuando se envían paquetes RTP en puertos UDP. Normalmente el sistema es inundado con paquetes; su procesamiento consume recursos preciosos del sistema.

3.19 algoritmo criptográfico simétrico (**basado en claves secretas**): Un algoritmo para realizar el cifrado o el algoritmo correspondiente para realizar el descifrado en el cual se requiere la misma clave para ambas operaciones (Rec. UIT-T X.810 | ISO/CEI 10181-1).

3.20 amenaza: Posible violación de la seguridad (Rec. UIT-T X.800 | ISO/CEI 7498-2).

4 Abreviaturas, siglas o acrónimos

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

3DES	DES triple (*triple DES*)
AES	Algoritmo de criptación avanzado (*advanced encryption algorithm*)
ALG	Pasarela de capa de aplicación (*application layer gateway*)
ASN.1	Notación de sintaxis abstracta uno (*abstract syntax notation No. 1*)
BES	Servidor fuera del terminal (*back-end server*)
CA	Autoridad de certificación (*certificate authority*)
CBC	Concatenación de bloques cifrados (*cipher block chaining*)
CFB	Retroalimentación cifrada (*cipher feedback*)
CRL	Lista de revocación de certificados (*certificate revocation list*)
DES	Norma de criptación de datos (*data encryption standard*)
DH	Diffie-Hellman
DNS	Sistema de nombres de dominio (*domain name system*)
DSS	Norma sobre firmas digitales (*digital signature standard*)
DTMF	Multifrecuencia bitono (*dual tone multi-frequency*)
ECB	Libro de código electrónico (*electronic code book*)
ECC y EC	Criptosistema de curva elíptica (*elliptic curve cryptosystem*) (véase la sección 8.7 *ATM Forum Security Specification Versión 1.1*). Un criptosistema de claves públicas

EC-GDSA	Firma digital de curva elíptica con apéndice análoga al algoritmo de firma digital NIST (DSA) [*elliptic curve digital signature with appendix analog of the NIST digital signature algorithm (DSA)*]; (véase también ISO/CEI 15946-2, capítulo 5)
ECKAS-DH	Esquema de convenio de claves de curva elíptica – Diffie-Hellman (*elliptic curve key agreement scheme – Diffie-Hellman*) – El esquema de convenio de claves Diffie-Hellman que utiliza criptografía de curva elíptica
EOFB	Modo OFB mejorado (*enhanced OFB mode*)
EP	Punto extremo (*endpoint*)
GK	Controlador de acceso (*gatekeeper*)
GW	Pasarela (*gateway*)
ICV	Valor de comprobación de integridad (*integrity check value*)
ID	Identificador (*identifier*)
IETF	Grupo de tareas especiales de ingeniería en Internet (*Internet engineering task force*)
IPsec	Seguridad del protocolo Internet (*Internet protocol security*)
ISAKMP	Protocolo de gestión de clave con asociación de seguridad en Internet (*Internet security association key management protocol)*
ISO	Organización Internacional de Normalización (*international standards for standardization*)
IV	Vector de inicialización (*initialization vector)*
LDAP	Protocolo ligero de acceso al directorio (*lightweight directory access protocol*)
MAC	Código de autenticación de mensaje (*message authentication code*)
MC	Controlador multidifusión (*multicast controller*)
MCU	Unidad de control multipunto (*multipoint control unit*)
MPS	Tren de cabida útil múltiple (*multiple payload stream*)
NAT	Traducción de dirección de red (*network address translation*)
OCSP	Protocolo en línea del estado del certificado (*online certificate status protocol*)
OFB	Modo realimentación de salida (*output feedback mode*)
OID	Identificador de objeto (*object identifier*)
PDU	Unidad de datos de protocolo (*protocol data unit*)
PKI	Infraestructura de claves públicas (*public key infrastructure*)
POTS	Servicio telefónico tradicional (*plain old telephone service*)
PRF	Función seudoaleatoria (*pseudo-random function*)
Q&A	Preguntas y respuestas (*question and answer*)
QoS	Calidad de servicio (*quality of service*)
RAS	Registro, admisión y estado (*registration, admission and status*)
RSA	Rivest, Shamir y Adleman (algoritmo de clave pública)
RTCP	Protocolo de control de transporte en tiempo real (*real-time transport control protocol*)

RTP	Protocolo de transporte en tiempo real (*real-time transport protocol*)
SASET	Tipo de punto extremo de audio simple de seguridad (*secure audio simple endpoint type*)
SDU	Unidad de datos de servicio (*service data unit*)
SHA1	Algoritmo de generación numérica seguro N.º 1 (*secure hash algorithm No. 1*)
SRTP	Protocolo de transporte en tiempo real seguro (*secure real-time transport protocol*)
SSL	Capa de zócalo segura (*secure socket layer*)
TLS	Seguridad de nivel de transporte (*transport level security*)
TSAP	Punto de acceso al servicio de transporte (*transport service access point*)
TTP	Tercera parte fiable (*trusted third party*)
UDP	Protocolo de datagrama de usuario (*user datagram protocol*)
XOR, ⊕	O exclusivo (*exclusive OR*)

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.

Las referencias a cláusulas, subcláusulas, anexos y apéndices se refieren a esta Recomendación, a menos que se indique explícitamente otra Recomendación. Por ejemplo, "1.4" hace referencia a la cláusula 1.4 de esta Recomendación; "6.4/H.245" hace referencia a la cláusula 6.4 de la Rec. UIT-T H.245.

Esta Recomendación describe el uso de "n" tipos de mensajes diferentes: H.245, RAS, Q.931, etc. Para distinguir entre los diferentes tipos de mensajes, se sigue el siguiente convenio: los nombres de mensajes y parámetros H.245 están formados por varias palabras unidas y en negritas (**maximumDelayJitter)**. Los nombres de mensajes RAS se representan con abreviaturas de tres letras (**ARQ**). Los nombres de mensajes Q.931 están formados por una o dos palabras cuyas letras iniciales aparecen en mayúsculas **(Call Proceeding)**.

En esta Recomendación puede indicarse que se ponga en NULL una estructura de datos ASN.1 compuesta, por ejemplo, "**paramS** puesto a NULL" (véanse las cláusulas 7, 8, 9.1 y 9.2/H.235.1, las cláusulas 7, 9, 15.1 y 15.2/H.235.2). Significa que no hay ninguno de los elementos opcionales en esa SECUENCIA (esto es, **Params**).

En esta Recomendación se definen diversos identificadores de objeto (OID) para la señalización de capacidades de seguridad, procedimientos o algoritmos de seguridad. Estos identificadores están relacionados con un árbol jerárquico de valores atribuidos que puede provenir de una fuente externa o ser parte del árbol de OID mantenido por el UIT-T. En particular, aquellos OID relativos a la Rec. UIT-T H.235 se presentan en el texto de la siguiente manera:

"OID" = {itu-t (0) recommendation (0) h (8) 235 version (0) **V** **N**}, donde **V** representa simbólicamente una única cifra decimal que indica la versión correspondiente de la Rec. UIT-T H.235, por ejemplo, 1, 2, 3 ó 4. **N** representa simbólicamente una cifra decimal que

identifica unívocamente el ejemplar del OID y, por tanto, el procedimiento, algoritmo o capacidad de seguridad.

Es decir, el OID codificado ASN.1 consta de una secuencia de números. Por comodidad, se utiliza una notación de abreviaturas nemotécnicas de texto para cada OID, por ejemplo "OID". Se suministra una correspondencia entre cada cadena OID y una secuencia de números ASN.1. Las implementaciones conformes a la Rec. UIT-T H.235 utilizarán únicamente los números codificados ASN.1.

6 Presentación del sistema

En la figura 2 se ha ilustrado el alcance de esta Recomendación en el marco de la Rec. UIT-T H.323.

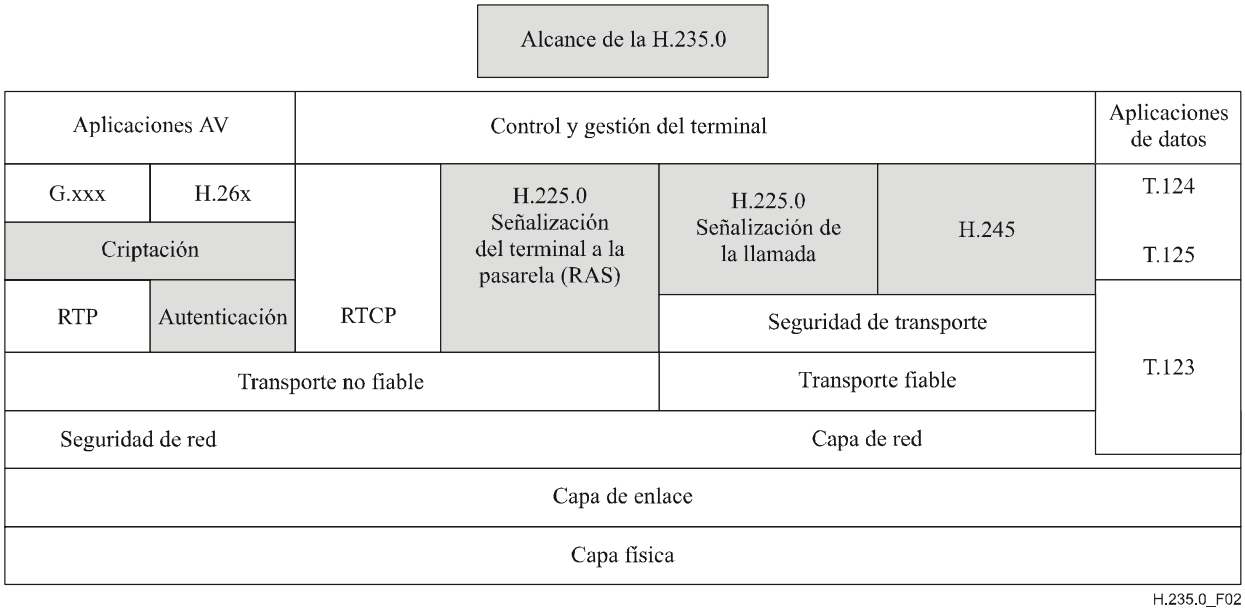


Figura 2/H.235.0 – Descripción general

Para la Rec. UIT-T H.323, la señalización para indicar que se utiliza TLS (RFC 2246, RFC 3546), IPsec o un mecanismo de marca en el canal de control H.245 se realizará en el canal H.225.0, con o sin seguridad, durante el intercambio inicial de mensajes Q.931.

6.1 Resumen

1) El canal de señalización de llamada se puede proteger utilizando TLS (RFC 2246, RFC 3546) o IPsec (RFC 2401, [ESP]) en un puerto conocido seguro (Rec. UIT-T H.225.0).

2) Los usuarios pueden ser autenticados durante la conexión de llamada inicial, en el proceso de proporcionar seguridad el canal H.245 y/o mediante el intercambio de certificados por el canal H.245.

3) Las capacidades de criptación de un canal de medios son determinadas por extensiones del mecanismo de negociación de capacidades existente.

4) La distribución inicial de material de claves del terminal director se efectúa mediante mensajes H.245 **OpenLogicalChannel** (**Apertura canal lógico**) u **OpenLogicalChannelAck** (**Acuse apertura canal lógico**).

5) El recifrado se puede realizar mediante las instrucciones H.245: **EncryptionUpdateCommand** (**Instrucción actualización criptación**), **EncryptionUpdateRequest** (**Petición actualización criptación**), **EncryptionUpdate** (**Actualización criptación**) y **EncryptionUpdateAck** (**Acuse actualización criptación**).

6) La distribución de material de claves se protege haciendo funcionar el canal H.245 como un canal privado o protegiendo específicamente el material de claves mediante el uso de certificados intercambiados seleccionados.

7) Los protocolos de seguridad presentados se conforman con las normas publicadas de la ISO o con las normas propuestas de IETF.

6.2 Autenticación

El proceso de autenticación verifica que los respondedores son, de hecho, quienes dicen ser. La autenticación se puede realizar junto con el intercambio de certificados basados en claves públicas. Se puede efectuar también por un intercambio que utiliza un secreto compartido entre las entidades participantes. Éste puede ser una contraseña estática o alguna otra pieza previa de información.

Esta Recomendación describe el protocolo para intercambiar los certificados, pero no especifica los criterios por los cuales éstos son verificados y aceptados mutuamente. En general, los certificados dan cierta seguridad al verificador de que el presentador del certificado es quien dice ser. La intención del intercambio de certificados es autenticar al *usuario* del punto extremo, no simplemente al punto extremo físico. Cuando se utilizan certificados digitales, un protocolo de autenticación prueba que los respondedores poseen las claves privadas correspondientes a las claves públicas contenidas en los certificados. Esta autenticación protege contra ataques intermedios, pero no prueba automáticamente quiénes son los respondedores. Para esto se requiere normalmente que haya alguna política relativa a otro contenido de los certificados. Por ejemplo, para los certificados de autorización, el certificado contendría normalmente la identificación del proveedor de servicio junto con alguna forma de identificación de cuenta de usuario prescrita por el proveedor de servicio.

El marco de autenticación de esta Recomendación no prescribe el contenido de los certificados (es decir, no especifica una política de certificado) además de lo requerido por el protocolo de autenticación. Sin embargo, una aplicación que utiliza este marco puede imponer requisitos de política de alto nivel, tales como presentar el certificado al usuario para aprobación. Esta política de alto nivel puede ser automatizada dentro de la aplicación o requerir la interacción humana.

Para la autenticación que no utiliza certificados digitales, esta Recomendación proporciona la señalización para completar distintos casos de presentación/admisión. Este método de autenticación requiere la coordinación previa por las entidades comunicantes de modo que se pueda obtener un secreto compartido. Un ejemplo de este método sería un cliente de un servicio basado en abono.

La tercera opción de autenticación es utilizar el contexto de un protocolo de seguridad distinto, tal como TLS (RFC 2246, RFC 3546) o RFC 2409 [IKE].

Entre entidades pares puede haber autenticación bidireccional y unidireccional, en algunos o en todos los canales de comunicación.

Todos los mecanismos de autenticación específicos descritos en esta Recomendación son idénticos a los algoritmos desarrollados por la ISO, o derivados de éstos, como se especifica en las Partes 2 a 3 de ISO/CEI 9798, o están basados en protocolos IETF.

6.2.1 Certificados

La normalización de certificados, incluida su generación, administración y distribución, está fuera del alcance de esta Recomendación. Los certificados utilizados para establecer canales seguros (señalización de llamada y/o control de llamada) se conformarán a los prescritos por cualquier protocolo que haya sido negociado para asegurar el canal.

Cabe señalar que para la autenticación que utiliza certificados de clave pública, los puntos extremos tienen que proporcionar firmas digitales utilizando el valor de clave privada asociado. El intercambio de certificados de clave pública por sí solo no protege contra ataques intermedios. Los protocolos H.235 cumplen este requisito.

6.3 Seguridad de establecimiento de la comunicación

Hay por lo menos dos razones para proporcionar seguridad al canal de establecimiento de la comunicación (por ejemplo, H.323 que utiliza Q.931). La primera es la autenticación simple, antes de aceptar la llamada. La segunda razón es tener en cuenta la autorización de la llamada. Si esta funcionalidad se desea en el terminal de la serie H, se debe utilizar un modo seguro de comunicación (tal como TLS/IPsec para H.323) antes del intercambio de mensajes de conexión de la llamada. Como otra posibilidad, la autorización se puede proporcionar sobre la base de una autenticación específica del servicio. Las condiciones de una política de autorización específica del servicio están fuera del alcance de esta Recomendación.

6.4 Seguridad de control de la llamada (H.245)

También hay que hacer seguro de alguna forma el canal de control de llamada (H.245) para proporcionar privacidad de los medios subsiguientes. El canal H.245 se asegurará utilizando cualquier mecanismo de privacidad negociado (esto incluye la opción "ninguno"). Los mensajes H.245 se utilizan para señalizar algoritmos de criptación y claves de criptación utilizados en los canales de medios privados compartidos. La capacidad de hacer esto, canal lógico por canal lógico, permite que diferentes canales de medios sean criptados por diferentes mecanismos. Por ejemplo, en conferencias multipunto centralizadas, es posible utilizar diferentes claves para los trenes a cada punto extremo. Esto puede permitir que los trenes de medios sean privados para cada punto extremo en la conferencia. Para utilizar los mensajes H.245 de una manera segura, todo el canal H.245 (canal lógico 0) se debe abrir de una manera segura negociada.

El mecanismo utilizado para hacer seguro el canal H.245 depende de los terminales de la serie H participantes. El único requisito en todos los sistemas que utilizan esta estructura de seguridad es que cada uno tenga alguna manera de negociar y/o señalizar que el canal H.245 ha de funcionar de una manera particularmente segura antes de que sea iniciado realmente. Por ejemplo, H.323 utilizará los mensajes de señalización de conexión H.225.0 para realizar esto.

6.5 Privacidad de trenes de medios

Esta Recomendación describe la privacidad de medios para trenes de medios enviados por transportes basados en paquetes. Estos canales pueden ser unidireccionales con respecto a las caracterizaciones de canal lógico H.245. Los canales no tienen que ser unidireccionales en un nivel físico o de transporte.

Un primer paso para obtener la privacidad de los medios debe ser la provisión de un canal de control privado por el cual establecer material de claves criptográficas y/o establecer los canales lógicos que transportarán los trenes de medios criptados. Para esto, cuando se funciona en una conferencia segura, cualesquiera puntos extremos participantes pueden utilizar un canal H.245 criptado. De esta manera, la selección del algoritmo criptográfico y las claves de criptación transferidas en la instrucción **OpenLogicalChannel** H.245 están protegidas.

El canal seguro H.245 puede funcionar con características diferentes de las de los canales de medios privados mientras proporcione un nivel de privacidad mutuamente aceptable. Esto prevé mecanismos que protegen los trenes de medios y los canales de control para funcionar de una manera completamente independiente, proporcionando niveles totalmente diferentes de robustez y complejidad.

Si se requiere que el canal H.245 funcione de una manera no criptada, las claves de criptación de medios específicos pueden ser criptadas separadamente de la manera señalizada y acordadas por las partes participantes. Se puede utilizar un canal lógico del tipo **h235Control** (**Control h235**) para proporcionar el material que ha de proteger las claves de criptación de medios. Este canal lógico puede funcionar en un modo negociado adecuadamente.

La privacidad (criptación) de los datos transportados por canales lógicos tendrá la forma especificada por **OpenLogicalChannel**. La información de encabezamiento específica de transporte no será criptada. La privacidad de datos se ha de basar en la criptación de extremo a extremo.

6.6 Elementos de confianza

La base para la autenticación (confianza) y la privacidad es definida por los terminales del canal de comunicación. Para un canal de establecimiento de conexión, ésta puede estar entre el llamante y un componente de la red anfitriona. Por ejemplo, un teléfono "confía" en que el conmutador de red lo conectará con el teléfono cuyo número ha marcado. Por este motivo, toda entidad que termina un canal de control H.245 criptado o cualesquiera canales lógicos del tipo **encryptedData** (**Datos criptados**) será considerada un elemento de confianza de la conexión; esto incluye las unidades de control multipunto y las pasarelas. El resultado de confiar en un elemento es la confianza para revelar el mecanismo de privacidad (algoritmo y clave) a ese elemento.

Dado lo anterior, corresponde a los participantes en el trayecto de comunicación autenticar cualquiera y todos los elementos "de confianza". Esto se hará normalmente mediante el intercambio de certificados como se haría para la autenticación de extremo a extremo "normalizada". Esta Recomendación no requiere ningún nivel específico de autenticación, sino que aconseja que dicho nivel sea aceptable para todas las entidades que utilizan el elemento de confianza. Los detalles de un modelo de confianza y de una política de certificados quedan en estudio.

La privacidad se puede asegurar entre dos puntos extremos solamente si las conexiones entre elementos de confianza han demostrado estar protegidas contra ataques intermedios.

6.6.1 Depósito de claves

Aunque no se requiere específicamente para el funcionamiento, esta Recomendación contiene disposiciones para que las entidades que utilizan el protocolo H.235 soporten la facilidad conocida como tercera parte confiable (TTP, *trusted third party*) dentro de los elementos de señalización.

Se debería soportar la posibilidad de recuperar las claves de criptación de medios perdidas en aquellas instalaciones en las que esta funcionalidad es deseada o requerida.

El depósito de claves es una facilidad a menudo denominada tercera parte confiable (TTP). Esta facilidad queda en estudio.

6.7 No repudio

Queda en estudio.

6.8 Seguridad en entorno de movilidad

Es posible utilizar los sistemas basados en la H.323 en un entorno de movilidad conforme a la Rec. UIT-T H.510. En la Rec. UIT-T H.530 se describen los procedimientos y protocolos de seguridad para dichos sistemas, y se presentan protocolos y procedimientos de esta Recomendación.

6.9 Perfiles de seguridad

Esta Recomendación hace referencia a varios perfiles de seguridad de H.235 (es decir, H.235.1, H.235.2, H.235.3, H.235.4, H.235.5, H.235.6, H.235.7, H.235.8 y H.235.9). En un perfil de seguridad se especifica la utilización particular de H.235 o un subconjunto de funcionalidades de esa Recomendación para entornos bien definidos, con un alcance de aplicabilidad preciso.

Dependiendo del entorno y de la aplicación, se pueden implementar los perfiles de seguridad bien sea de una manera selectiva o todos al tiempo. Con frecuencia, en los sistemas en que se ha habilitado la H.235 se indica dentro de los identificadores de objeto, como parte de los mensajes de señalización, qué perfiles de seguridad utilizan. En estos sistemas se debería escoger el perfil de seguridad conforme a sus propias necesidades.

Por otra parte, los puntos extremos pueden también ofrecer inicialmente múltiples perfiles de seguridad simultáneamente, en mensajes **RRQ/GRQ**, y después esperar a que el controlador de acceso escoja el más adecuado a través de una respuesta a ellos en un mensaje **RCF/GCF**. Las transacciones **LRQ/LCF** entre controladores de acceso también pueden transportar varios perfiles de seguridad. Al calcular firmas digitales o números generados para proporcionar integridad de mensaje, en primer lugar se deberían calcular los números generadores y signaturas digitales que no proporcionen dicha integridad en el subconjunto de campos y ponerlos en el mensaje, poner a cero en la memoria intermedia de mensaje todos aquellos que sí lo hagan, y sólo entonces se deberían calcular las firmas digitales y los números generadores utilizando esta memoria, para después ponerlos en el mensaje.

Cada una de las Recomendaciones de la subserie describe un perfil de seguridad de la H.235.0. Por regla general, cada perfil de seguridad de la H.235.0 consta de un caso de utilización específico de la H.235.0 para un determinado caso particular y/o contiene una determinada especificación de característica de seguridad o una combinación de mecanismos de seguridad y perfiles de seguridad.

Todos los perfiles de seguridad en el ámbito de la H.235.0 son facultativos.

La figura 3 ilustra combinaciones típicas y posibles de perfiles de seguridad. Las líneas continuas indican que la combinación de perfiles de seguridad está definida y es posible. Las líneas discontinuas indican que la combinación es en general posible, aunque no resulte muy útil. Cuando no hay una línea, esa determinada combinación no está aún definida.

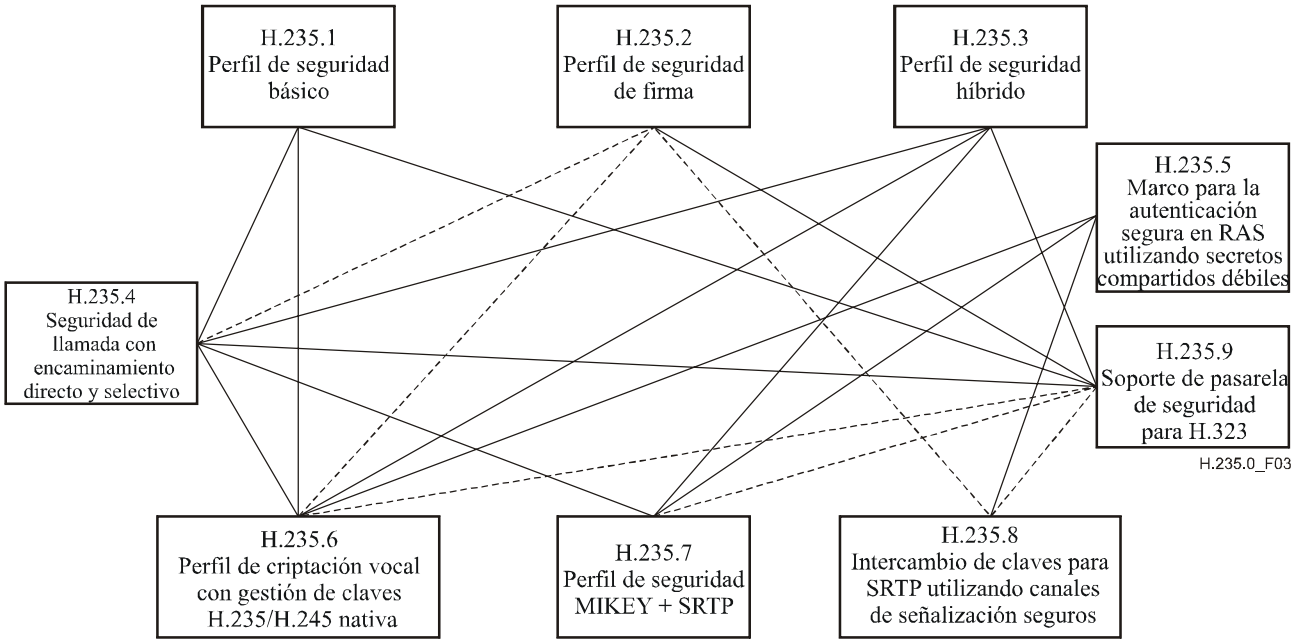


Figura 3/H.235.0 – Ejemplo de combinaciones de perfiles de seguridad

6.10 Paso por NAT/cortafuegos con seguridad

En la Rec. UIT-T H.235.9 se especifican los procedimientos para la detección de presencia de pasarelas de seguridad (tales como las ALG) en el trayecto de señalización RAS H.225.0 entre

entidades H.323 (controlador de acceso, extremo) y para compartir información de seguridad entre el controlador de acceso y la pasarela de seguridad a fin de preservar la integridad y privacidad de la señalización.

Las Recs. UIT-T H.235.1 (Procedimiento IA) y H.235.2 (Procedimiento de autenticación únicamente) describen procedimientos específicos complementarios que permiten autenticar a través de dispositivos NAT/cortafuegos los protocolos RAS y de señalización de llamada H.225.0 para mensajes H.235.

7 Procedimientos de establecimiento de la conexión

Como se indica en la introducción del sistema, el canal de conexión de la llamada (H.225.0 para la serie H.323) y el canal de control de llamada (H.245) funcionarán en el modo seguro o inseguro negociado a partir del primer intercambio. Para el canal de conexión de la llamada, esto se hace previamente (para H.323 un TSAP seguro de TLS (puerto 1300) será utilizado para los mensajes Q.931). Para el canal de control de llamada, el modo de seguridad es determinado por la información transferida en el protocolo de establecimiento de conexión inicial en uso por el terminal de la serie H.

Cuando no hay capacidades de seguridad superpuestas, el terminal llamado puede rechazar la conexión. El error devuelto no debería transferir información sobre cualquier discordancia de seguridad y el terminal llamante tendrá que determinar el problema por otros medios. Cuando el terminal llamante reciba un mensaje sin capacidades de seguridad suficientes, terminará la llamada.

Si los terminales llamante y llamado tienen capacidades de seguridad compatibles, ambos lados supondrán que el canal H.245 funcionará en el modo seguro negociado. La imposibilidad de establecer el canal H.245 en el modo seguro determinado debería considerarse un error de protocolo y terminarse la conexión.

En la Rec. UIT-T H.235.6 se indican otros procedimientos de establecer una conexión con seguridad, en particular la gestión de claves; véanse las cláusulas 7 y 8/H.235.6.

8 Señalización y procedimientos de autenticación

La autenticación se basa en general, bien en la utilización de un secreto compartido (usted está autenticado correctamente si conoce el secreto), bien en métodos de certificación que aplican claves públicas (usted prueba su identidad mediante el procesamiento de la clave privada correcta). Un secreto compartido y el empleo subsiguiente de la criptografía simétrica requiere que se produzca un contacto previo entre las entidades comunicantes. Un contacto cara a cara o contacto seguro previo puede ser sustituido por la generación o el intercambio de la clave secreta compartida en los métodos basados en la criptografía de claves públicas, por ejemplo, el intercambio de claves Diffie-Hellman. Las partes comunicantes en la generación y el intercambio de claves han de ser autenticadas mediante, por ejemplo, mensajes firmados digitalmente; en caso contrario, las partes de la comunicación no pueden estar seguras de con quien comparten el secreto.

Esta Recomendación presenta los métodos de autenticación basados en el abono, es decir, debe producirse un contacto previo para la compartición de un secreto, y se utilizarán métodos de autenticación que apliquen la criptografía de claves públicas para la autenticación, o para la generación del secreto compartido.

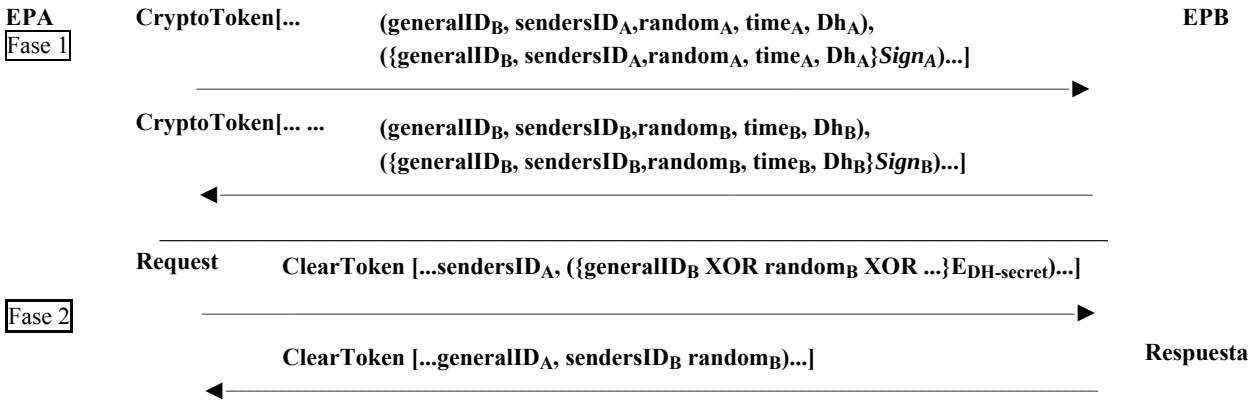
8.1 Intercambio Diffie-Hellman con autenticación facultativa

El propósito no es proporcionar autenticación absoluta a nivel de usuario. Este método proporciona la señalización para generar un secreto compartido entre dos entidades que pueden manipular material para comunicaciones privadas.

Al final de este intercambio ambas entidades poseerán una clave secreta compartida junto con un algoritmo elegido con el cual utilizar esta clave. Esta clave secreta compartida se puede utilizar en cualquier intercambio de petición/respuesta subsiguiente. Cabe señalar que, en casos muy raros, el intercambio Diffie-Hellman puede generar claves *débiles* conocidas para determinados algoritmos. Cuando es así, cada entidad debe desconectar y reconectar para establecer un nuevo conjunto de claves.

La primera fase de la figura 4 muestra los datos intercambiados durante la negociación Diffie-Hellman. La segunda fase prevé que los mensajes de petición específicos de la aplicación o del protocolo sean autenticados por el respondedor. Obsérvese que se puede devolver un nuevo valor aleatorio con cada respuesta.

NOTA – Si el intercambio de mensajes se realiza por un canal inseguro, deben utilizarse las firmas digitales (u otro método de autenticación del origen de los mensajes) para autenticar las partes que compartirán el secreto. Se puede proporcionar también un elemento de firma facultativo, que se ilustra a continuación en ***cursivas***.



[... ...]	Indica una secuencia de testigos.
()	Indica un testigo determinado, que puede contener múltiples elementos.
{}E$_{DH\text{-}secret}$	Indica que los valores contenidos han sido criptados utilizando el secreto Diffie-Hellman.

EPB sabe qué clave secreta compartida ha de utilizar para descifrar el identificador **generalID$_B$** asociándolo con el **generalID$_A$** que debe ser transferido también en el mensaje como **sendersID$_A$**. Obsérvese que el valor criptado en la fase 2 es transferido en el campo **generalID** de un **clearToken** para simplificar la codificación.

Figura 4/H.235.0 – Diffie-Hellman con autenticación facultativa

8.2 Autenticación basada en un acuerdo

Aunque estos procedimientos (y los algoritmos de la ISO de los cuales se derivan) son bidireccionales, pueden ser utilizados solamente en un sentido si la autenticación se necesita solamente en ese sentido. Se describen los procedimientos de dos pasos y de tres pasos. La autenticación mutua (recíproca) de dos pasos sólo puede ejecutarse en un sentido cuando no es preciso autenticar los mensajes procedentes del sentido inverso. Estos intercambios suponen que cada extremo posee algún identificador bien conocido (como un identificador textual) que lo identifica inequívocamente. Para el procedimiento de dos pasos, se establece la hipótesis de que hay una referencia de tiempo mutuamente aceptable (de la cual deriva indicación de tiempo). La diferencia de hora que es aceptable es un asunto de la implementación local. El procedimiento de tres pasos utiliza un número de preguntas imprevisible generado aleatoriamente (que puede ser incrementado por un contador secuencial 'aleatorio') como una pregunta procedente del autenticador. Este número aleatorio se utiliza para la protección contra los ataques de reproducción. A diferencia de los procedimientos de dos pasos, los procedimientos de tres pasos no autentican el primer mensaje inicial que contiene la pregunta del iniciador.

Hay tres variantes diferentes que se pueden aplicar dependiendo de las necesidades:

1) contraseña con criptación simétrica;

2) contraseña con generación numérica;

3) certificado con firma.

En todos los casos, el testigo contendrá la información descrita en las cláusulas siguientes según la variación elegida. Obsérvese que en todos los casos el **generalID** (**ID general**) puede ser conocido a través de la configuración o del directorio, en vez de en el intercambio de protocolos dentro de banda. Para simplificar el procesamiento en el receptor, el emisor debe incluir su identidad dentro de **sendersID** y fijar el **generalID** a la identificación del destinatario.

NOTA 1 – En todos los casos en los que son generadas indicaciones de tiempo y pasadas como parte de un intercambio de seguridad, los implementadores deben adoptar las precauciones que siguen. La granularidad de la indicación de tiempo debe ser suficientemente fina para que quede garantizado su incremento con cada mensaje. Si este incremento no está garantizado, pueden producirse ataques de reproducción (por ejemplo, si las indicaciones de tiempo sólo se incrementan de minuto en minuto, un punto extremo "C" puede engañar a un punto extremo "A" dentro del periodo de un minuto desde que el punto extremo "A" haya enviado un mensaje al punto extremo "B").

NOTA 2 – Si es de multidifusión, entonces el mensaje no está seguro.

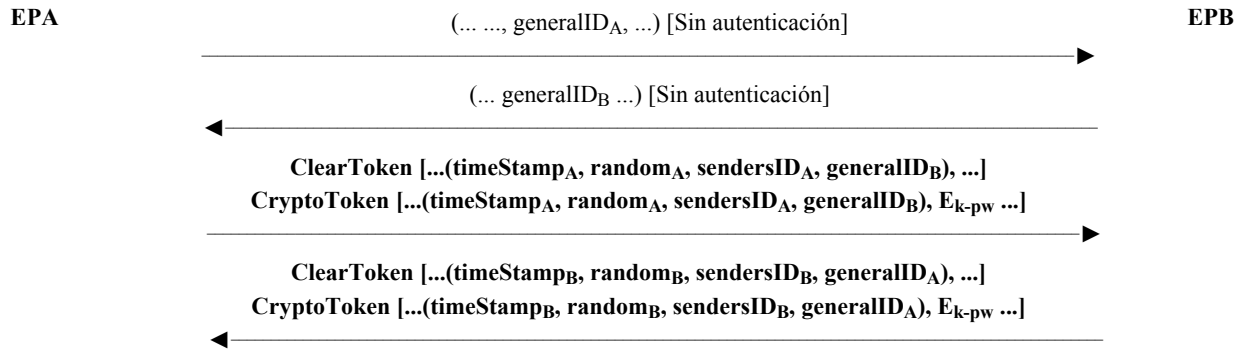
8.2.1 Contraseña con criptación simétrica

En las figuras 5 y 6 se muestra el formato de testigo y el intercambio de mensajes requeridos para realizar este tipo de autenticación en dos pasos o tres pasos, respectivamente. Este protocolo se basa en 5.2.1 (two-pass) y 5.2.2 (three-pass) de ISO/CEI 9798-2, y se supone que se intercambian en el acuerdo un identificador y la contraseña asociada. La clave de criptación tiene una longitud de N octetos (según lo indicado por el AlgorithmID), y se forma como sigue:

– Si la longitud de la contraseña = N, clave = contraseña.

– Si la longitud de la contraseña < N, la clave es rellenada con ceros.

– Si la longitud de la contraseña > N, los primeros N octetos son asignados a la clave, después el N + M-*ésimo* octeto de la contraseña se pone a XOR al Mmod(N)-*ésimo* octeto (para todos los octetos después de N), (es decir, todos los octetos de contraseña "suplementarios" son doblados repetidamente en la clave por XOR).



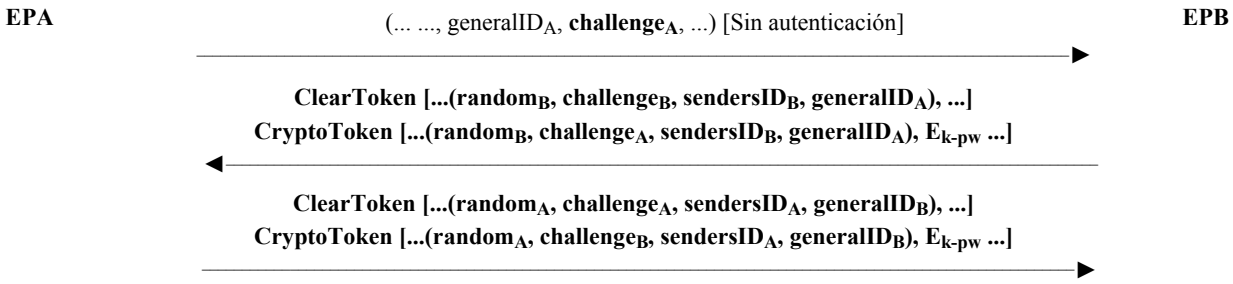
NOTA 1 – La devolución de testigo del EPB es facultativa; si se omite, sólo se logra una autenticación unidireccional.

NOTA 2 – **E$_{k-pw}$** indica valores que han sido criptados utilizando la clave "k" derivada de la contraseña "pw".

NOTA 3 – **random** es un contador monotónicamente creciente que realiza múltiples mensajes con la misma indicación de tiempo única.

NOTA 4 – En el tercer mensaje el EPA proporciona un **ClearToken** separado, que se identifica por el mismo OID que el OID del **CryptoToken**; y viceversa, sucede de manera similar para el cuarto mensaje.

Figura 5/H.235.0 – Contraseña con criptación simétrica; dos pasos



NOTA 1 – **challengeA** y la devolución del **CryptoToken** criptado de B a A no son necesarias si se desea una autenticación unidireccional.

NOTA 2 – **E$_{k-pw}$** indica valores que han sido criptados utilizando la clave "k" derivada de la contraseña "pw".

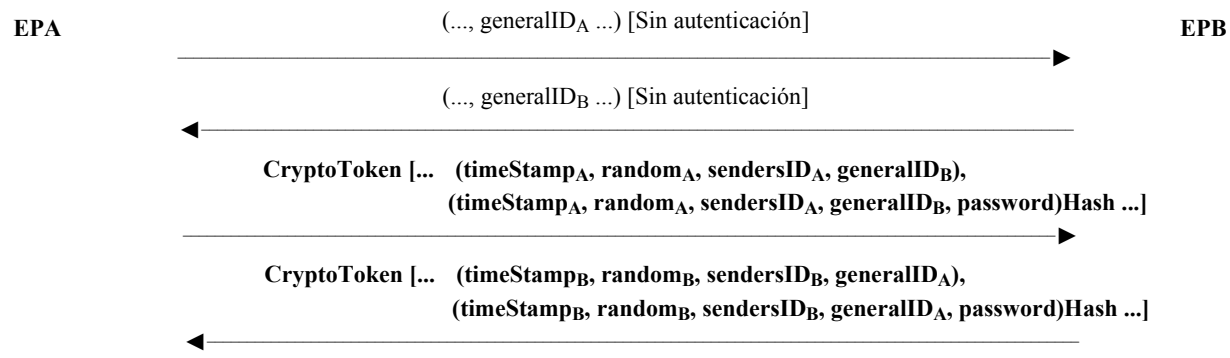
NOTA 3 – En el tercer mensaje el EPA proporciona una nueva **challenge$_A$** en texto claro en un **ClearToken** independiente, que es identificada por el mismo OID que el OID del **CryptoToken**. EPA también devuelve la **challenge$_B$** criptada como respuesta; y viceversa, sucede de manera similar para el segundo mensaje.

NOTA 4 – Para múltiples mensajes pendientes **random** (es decir, un contador monotónicamente creciente) deberá formular una pregunta única.

Figura 6/H.235.0 – Contraseña con criptación simétrica; tres pasos

8.2.2 Contraseña con generación numérica

En las figuras 7 y 8 se muestra el formato de testigo y el intercambio de mensajes requeridos para realizar este tipo de autenticación para dos pasos o tres pasos, respectivamente. Este protocolo se basa en 5.2.1 y 5.2.2 de ISO/CEI 9798-4, y se supone que se intercambian en el acuerdo un identificador y la contraseña asociada. La Rec. UIT-T H.235.1 proporciona una descripción detallada del procedimiento de generación numérica de dos pasos.

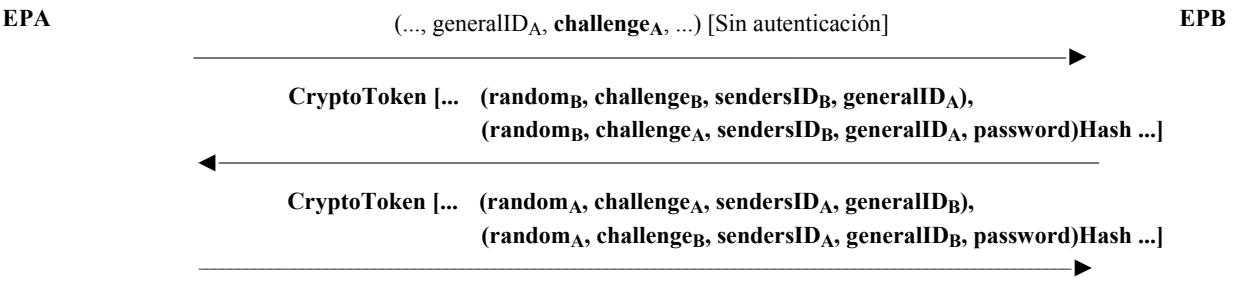


NOTA 1 – La devolución de testigo del EPB es facultativa; si se omite, sólo se logra una autenticación unidireccional.

NOTA 2 – **Hash** indica una función generadora que opera sobre los valores contenidos.

NOTA 3 – **random** es un contador monotónicamente creciente que realiza múltiples mensajes con la misma indicación de tiempo única.

Figura 7/H.235.0 – Contraseña con generación numérica; dos pasos



NOTA 1 – La devolución de testigo del EPB es facultativa; si se omite, sólo se logra una autenticación unidireccional.

NOTA 2 – **Hash** indica una función generadora que opera sobre los valores contenidos.

NOTA 3 – En el tercer mensaje el EPA proporciona una nueva **challenge$_A$** en texto claro dentro del **ClearToken** insertado en **cryptoHashedToken**. EPA también devuelve la **challenge$_B$** troceada como respuesta; y viceversa, sucede de manera similar para el segundo mensaje.

NOTA 4 – Para múltiples mensajes pendientes **random** (es decir, un contador monotónicamente creciente) deberá formular una pregunta única.

Figura 8/H.235.0 – Contraseña con generación numérica; tres pasos

NOTA 1 – La estructura **cryptoHashedToken** se utiliza para transferir los parámetros utilizados en este intercambio. En esta estructura están incluidas las versiones explícitas de los parámetros necesarios para calcular el número generador. Los implementadores deberán incluir la indicación de tiempo en el **hashedVals** y *no* deberán incluir la contraseña. (Por ejemplo, la contraseña y el '**generalID**' deben ser conocidos por el destinatario previamente; los primeros pueden omitirse.)

NOTA 2 – La función generadora deberá aplicarse a la estructura **EncodedGeneralToken** que incluye al menos los campos ID, indicación de tiempo y contraseña. El valor de la contraseña NO deberá ser transferido en el **ClearToken**.

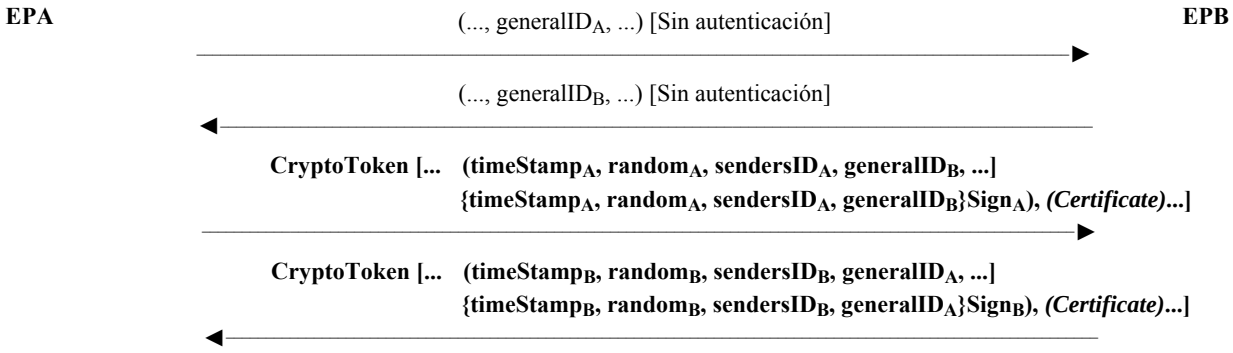
NOTA 3 – Las implementaciones deben garantizar que las contraseñas introducidas por el usuario transportan suficiente entropía. Las contraseñas que son demasiado cortas o que son vulnerables a los ataques de diccionario deben ser rechazadas. En determinados casos puede ser ventajosa la aplicación de frases de paso introducidas por el usuario a través de una función generadora criptográfico y la utilización de los bits resultantes.

8.2.3 Certificado con firma

En las figuras 9 y 10 se muestra el formato de testigo y los mensajes intercambiados requeridos para realizar este tipo de autenticación. Este protocolo se basa en 5.2.1 de ISO/CEI 9798-3, y se supone que se asignan/intercambian en el acuerdo un identificador y el certificado asociado. En la Rec. UIT-T H.235.2 se proporciona una descripción detallada del procedimiento de firma de dos pasos.

NOTA 1 – Se puede proporcionar también un elemento de certificado facultativo, que se ilustra a continuación en ***cursivas***.

NOTA 2 – Si el mensaje es de multidifusión, el identificador del destino (**generalID$_B$** para mensajes originados en A y viceversa) no debe ser incluido en el **ClearToken**.



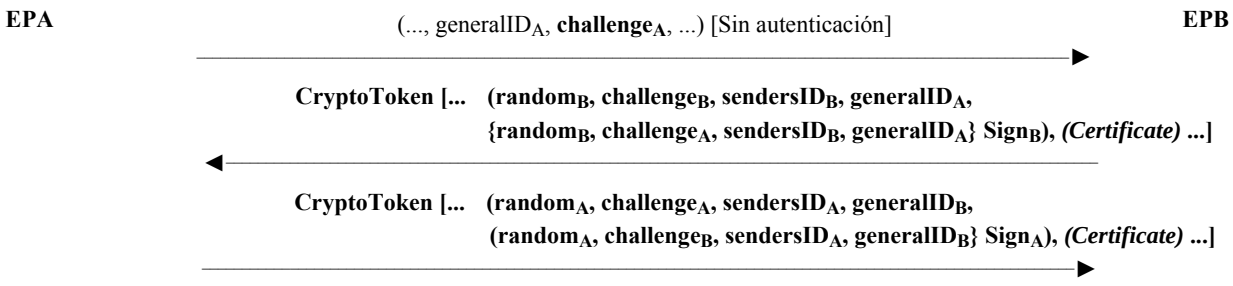
NOTA 1 – La devolución de testigo del EPB es facultativa; si se omite, sólo se logra una autenticación unidireccional.

NOTA 2 – Un certificado de tipo "pago" puede ser incluido facultativamente por el originador EPA.

NOTA 3 – **Sign** indica una función de firma (del certificado asociado) realizada en los valores contenidos.

NOTA 4 – **random** es un contador monotónicamente creciente que realiza múltiples mensajes con la misma indicación de tiempo única.

Figura 9/H.235.0 – Certificado con firma; dos pasos



NOTA 1 – La devolución de testigo del EPB es facultativa; si se omite, sólo se logra una autenticación unidireccional.

NOTA 2 – Un certificado de tipo "pago" puede ser incluido facultativamente por el originador EPA.

NOTA 3 – **Sign** indica una función de firma (del certificado asociado) realizada en los valores contenidos.

NOTA 4 – En el tercer mensaje el EPA proporciona una nueva **challenge$_A$** en texto claro con el **GeneralToken** codificado insertado. El EPA también devuelve la **challenge$_B$** firmada como respuesta; y viceversa, sucede de manera similar para el segundo mensaje.

NOTA 5 – Para múltiples mensajes pendientes **random** (es decir, un contador monotónicamente creciente) deberá formular una pregunta única.

Figura 10/H.235.0 – Certificado con firma; tres pasos

8.2.4 Utilización de contraseñas y secreto compartido

Esta Recomendación utiliza algunas técnicas de criptografía simétrica a efectos de autenticación, integridad y confidencialidad. Este texto usa los términos contraseña y secreto compartido cuando se refiere a técnicas simétricas. Se entiende por secreto compartido el término genérico que identifica una cadena de bits cualquiera. El secreto compartido puede ser asignado o configurado durante el proceso de suscripción de abono del usuario, o puede formar parte de un sistema de cálculo dentro de banda, por ejemplo, un secreto compartido derivado de Diffie-Hellman.

Una contraseña puede verse como una cadena de caracteres alfanuméricos que puede ser memorizada por los usuarios. Es obvio que el uso de las contraseñas debe hacerse con cuidado: las contraseñas sólo son suficientemente seguras cuando se escogen al azar dentro de una muestra suficientemente amplia, cuando portan suficiente entropía de manera tal que son impredecibles y cuando se cambian periódicamente. Las reglas para escoger y actualizar las contraseñas están fuera del alcance de esta Recomendación.

Una buena práctica, para aprovechar las ventajas de las contraseñas y los secretos compartidos, es la de transformar la cadena contraseña del usuario en una cadena de bits como el secreto compartido, usando una función generadora unidireccional criptográficamente fuerte.

Como ejemplo recomendado, cuando se usa el perfil de seguridad de la H.235.1, si se aplica el troceado SHA1 a la cadena contraseña, 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.

Esto es,

secreto compartido := SHA1 (contraseña)

8.3 Señalización RAS/procedimientos de autenticación

Estos procedimientos no garantizan explícitamente ninguna forma de privacidad de mensajes entre controladores de acceso y puntos extremos. Se pueden utilizar dos tipos de autenticación. El primer tipo es la criptación simétrica que no requiere contacto previo entre el punto extremo y el controlador de acceso. El segundo tipo es el acuerdo que tendrá dos formas: contraseña o certificado. Todas estas formas se derivan de los procedimientos indicados en las cláusulas 8, 8.2.1, 8.2.2 y 8.2.3. En esta cláusula, las etiquetas genéricas (EPA y EPB) utilizadas en las cláusulas mencionadas representarán respectivamente al punto extremo y al controlador de acceso.

8.3.1 Autenticación de punto extremo-controlador de acceso (no basada en acuerdo)

Este mecanismo puede proporcionar al controlador de acceso una asociación criptográfica que permite asegurar que un punto extremo determinado registrado previamente es el mismo que emite los subsiguientes mensajes RAS. Cabe señalar que esto no puede proporcionar ninguna autenticación del controlador de acceso al punto extremo, a menos que se incluya el elemento de firma facultativo. El establecimiento de la relación de identidad se produce cuando el terminal emite **GRQ** como se indica en 7.2.1/H.323. El intercambio Diffie-Hellman se producirá junto con los mensajes **GRQ** y **GCF** como se indica en la primera fase de la cláusula 8. Esta clave secreta compartida se utilizará en todo **RRQ/URQ** subsiguiente del terminal al controlador de acceso. Si un controlador de acceso funciona en este modo y recibe **GRQ** sin un testigo que contiene *DHset* o un valor de algoritmo aceptable, devolverá un código de motivo **securityDenial** (**denegación seguridad**) u otro código de error de seguridad adecuado, conforme a 11.1 en el **DRJ**.

La clave secreta compartida Diffie-Hellman creada durante el intercambio **GRQ/GCF** se puede utilizar para autenticación en los siguientes mensajes **xRQ**. Se aplicarán los siguientes procedimientos para completar este modo de autenticación.

Terminal (**xRQ**)

1) El terminal proporcionará toda la información en el mensaje como se describe en las cláusulas pertinentes de la Rec. UIT-T H.225.0.

2) El terminal criptará **GatekeeperIdentifier** (**identificador de controlador de acceso**) (devuelto en el **GCF**) utilizando la clave secreta compartida negociada. Ésta será transferida en un **clearToken** (**testigo claro**) (véase 8.1) como el **generalID**.

Los 16 bits del **random** (**aleatorio**) y después la **requestSeqNum** (**petición número secuencia**) se pondrán a XOR con cada 16 bits del **GatekeeperIdentifier**. Si **GatekeeperIdentifier** no termina en una frontera 16 par, los últimos 8 bits del **GatekeeperIdentifier** se pondrán a XOR con el octeto menos significativo del valor aleatorio y después **requestSeqNum**. El **GatekeeperIdentifier** será criptado utilizando el algoritmo seleccionado en **GCF** (algorithmOID) y utilizando todo el secreto compartido.

El ejemplo a continuación ilustra este procedimiento:

RND16: valor de 16 bits del valor aleatorio

SQN16: valor de 16 bits de requestSeqNum

BMPX: el carácter BMP X-ésimo GatekeeperIdentifier

BMP1' = (BMP1) XOR (RND16) XOR (SQN16)

BMP2' = (BMP2) XOR (RND16) XOR (SQN16)

BMP3' = (BMP3) XOR (RND16) XOR (SQN16)

BMP4' = (BMP4) XOR (RND16) XOR (SQN16)

BMP5' = (BMP5) XOR (RND16) XOR (SQN16)

:

:

BMPn' = (BMPn) XOR (RND16) XOR (SQN16)

Para asociar criptográficamente este mensaje y los siguientes con el registrador original (el punto extremo que emitió **RRQ**), se utilizará el valor **random** más reciente (este valor puede ser uno más nuevo que el valor devuelto en **RCF**, de un ulterior mensaje **xCF**).

Controlador de acceso (**xCF/xRJ**)

1) El controlador de acceso criptará su **GatekeeperIdentifier** (según el procedimiento anterior) con la clave secreta compartida asociada con el punto extremo alias y comparará esto con el valor en **xRQ**.

2) El controlador de acceso devolverá **xRJ** si los dos valores criptados no concuerdan.

3) Si el **GatekeeperIdentifier** concuerda, el controlador de acceso aplicará cualquier lógica local y responderá con **xCF** o **xRJ**.

4) Si **xCF** es enviado por el controlador de acceso, debe contener un **EndpointIdentifier** (**identificador de punto extremo**) asignado y un nuevo valor aleatorio en el campo **random** de un **clearToken**.

Véase la segunda fase de la figura 4 para una representación gráfica de este intercambio. El controlador de acceso sabe la clave secreta compartida que ha de utilizar para descifrar el identificador de controlador de acceso mediante el nombre alias en el mensaje.

8.3.2 Autenticación de punto extremo-controlador de acceso (basada en acuerdo)

Todos los mensajes RAS que no sean **GRQ/GCF** deben contener los testigos de autenticación requeridos por el modo de funcionamiento específico. Hay tres variaciones diferentes que se pueden aplicar según las necesidades y el entorno:

1) contraseña con criptación simétrica;

2) contraseña con generación numérica;

3) certificado con firmas.

En todos los casos el testigo contendrá la información descrita en las siguientes cláusulas de acuerdo con la variación elegida. Si un controlador de acceso funciona en un modo seguro y recibe un mensaje RAS sin un valor de testigo aceptable, devolverá un código de motivo **securityDenial** en el mensaje de rechazo u otro código de error de seguridad adecuado, conforme a 11.1. En todos los casos, el testigo devuelto del controlador de acceso es facultativo; si se omite, sólo se logra la autenticación unidireccional.

8.3.2.1 Contraseña con criptación simétrica

La fase de descubrimiento del controlador de acceso (**GRQ**, **GCF** y **GRJ**) puede ser insegura tal como se muestra en la figura 11 o segura usando para ello los **cryptoTokens**.

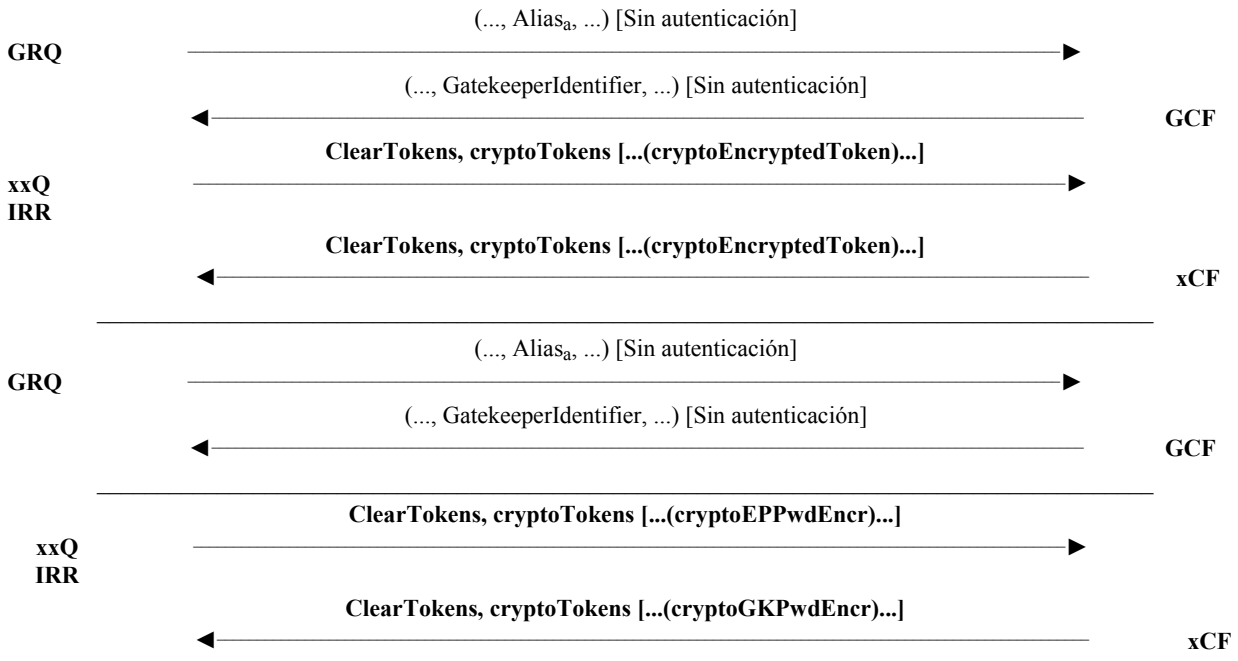


Figura 11/H.235.0 – Contraseña con criptación simétrica

8.3.2.2 Contraseña con generación numérica

La fase de descubrimiento del controlador de acceso (**GRQ**, **GCF** y **GRJ**) puede ser insegura tal como se muestra en la figura 12 o segura de acuerdo con la Rec. UIT-T H.235.1 usando para ello los **cryptoTokens**.

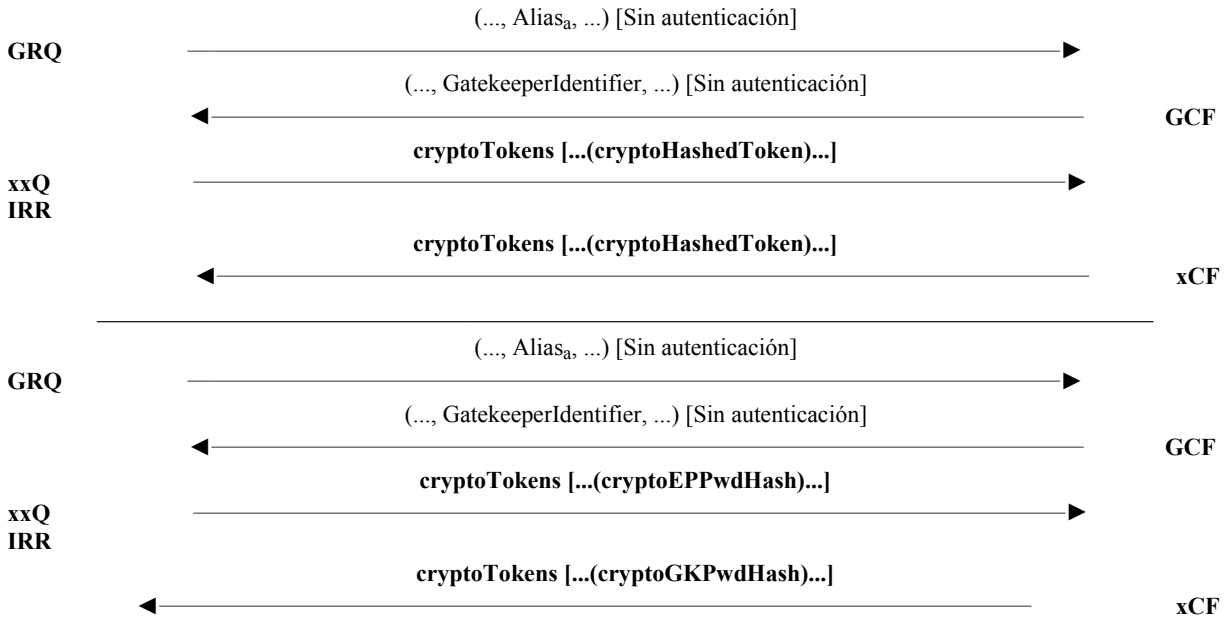


Figura 12/H.235.0 – Contraseña con generación numérica

8.3.2.3 Certificado con firmas

La fase de descubrimiento del controlador de acceso (**GRQ**, **GCF** y **GRJ**) puede ser insegura como se muestra en la figura 13 o segura de acuerdo con la Rec. UIT-T H.235.2 usando para ello los **cryptoTokens**.

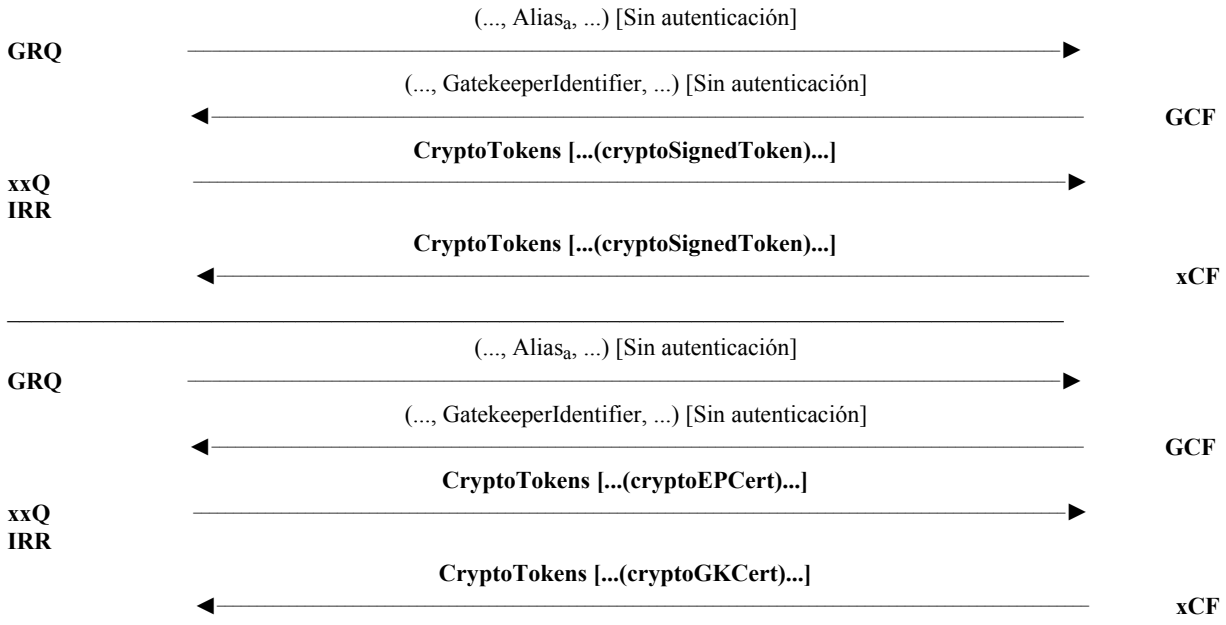


Figura 13/H.235.0 – Certificado con firmas

8.4 Gestión de clave en el canal RAS

En algunos casos, conviene distribuir las claves de sesión (RAS) desde un controlador de acceso hacia uno o varios puntos extremos bajo su control, o desde un punto extremo hacia otro. En el mecanismo propuesto se supone que el controlador de acceso y el punto extremo comparten una

clave secreta fuerte o conocen cada uno la clave pública del otro. Esto ocurre, por ejemplo, cuando un controlador de acceso de encaminamiento emite una clave de sesión a un punto extremo en un mensaje RAS, por ejemplo **RCF** o **ACF**, para que se utilice en la criptación de un canal de señalización encaminado por controlador de acceso. Otro ejemplo ocurre cuando el controlador de acceso emite una clave de sesión para ser utilizada en la criptación que viene después de las comunicaciones RAS (por ejemplo **RRQ** o **ARQ**).

Este mecanismo es similar al que se utiliza para la distribución de claves de sesión de medios. Es posible utilizarlo en algunos casos para evitar la tara de la negociación de clave.

Para el transporte de clave, el campo **h235Key** facultativo del **ClearToken** debería utilizarse en H.235v3. La flexibilidad del elemento **H235Key** permitirá el transporte de material clave de criptación utilizando:

- un canal seguro (la opción **secureChannel**) suponiendo que el RAS o un canal de señalización de llamada ha sido seguro por otros medios (por ejemplo IPsec/SSL);
- un secreto de criptación compartido en un canal despejado (la opción **sharedSecret**) o de la misma manera (aunque preferiblemente) la opción **secureSharedSecret**;
- una criptación y un certificado de clave pública en un canal despejado (la opción **certProtectedKey**).

La utilización de la clave de sesión RAS intercambiada y su aplicación a RAS, mensajes de señalización de llamada y/o canal transporte queda en estudio.

9 Autenticación asimétrica e intercambio de claves utilizando sistemas criptográficos de curva elíptica

Esta Recomendación proporciona técnicas de curva elíptica perfeccionadas con aplicaciones a la firma, la gestión de claves y la criptación. Una de las ventajas principales con respecto a las técnicas asimétricas "clásicas" como el algoritmo RSA son:

- Las claves criptográficas más cortas ofrecen una seguridad comparable al algoritmo RSA: Los criptosistemas de curva elíptica tienen longitudes típicas de claves de 160 bits; es decir, ofrecen una seguridad equivalente a una clave RSA de 1024 bits. Las claves más cortas consumen menos memoria de almacenamiento y hacen los sistemas criptográficos de curva elíptica especialmente atractivos para su implementación en las tarjetas inteligentes, y en cualquier otro dispositivo con necesidades de memoria pequeñas. En el contexto de H.323, los tipos de puntos extremos de audio simples de seguridad (SASET, *secured audio simple endpoint types*) basados en el anexo J/H.323 debido a su bajo precio resultan muy adecuados para el despliegue de las técnicas de curva elíptica.
- La velocidad mejorada de procesamiento que se alcanza en las implementaciones tanto de soporte físico como de soporte lógicos. Las claves más cortas mejoran la velocidad de procesamiento. Como resultado, las respuestas interactivas (del usuario) son más rápidas.

En *ATM Forum Security Specificación Version 1.1*, sección 8.7 puede verse la información básica, la explicación y los procedimientos de procesamiento de la criptografía de curva elíptica. Se recomienda codificar los puntos elípticos en su notación no comprimida afín sin utilizar el método de compresión/descompresión de punto. En ISO/CEI 15946-1 e ISO/CEI 15946-2 se dispone de más información sobre este tema.

9.1 Gestión de claves

Los esquemas del convenio de claves Diffie-Hellman basados en la curva elíptica son similares al caso mod-p clásico definido también en esta Recomendación. Se presentan dos situaciones:

- curvas elípticas sobre un campo primo: **eckasdhp** contiene los parámetros Diffie-Hellman y de curva elíptica;

- curvas elípticas de característica 2: **eckasdh2** contiene los parámetros Diffie-Hellman y de curva elíptica.

La estructura ECKASDH soporta cualquiera de los dos casos. En ISO/CEI 15946-1 se da una lista de algunos ejemplos de curvas elípticas. Se puede utilizar también cualquier otra curva elíptica adecuada.

Como se dispone de una estructura secuenciada del **ClearToken**, las señalizaciones **dhkey** y **eckasdhkey** no se deberían producir a la vez; sólo una de ellas deberá estar presente cuando se aplica el intercambio de claves Diffie-Hellman.

Observación – No se deben confundir los parámetros secretos elegidos aleatoriamente, ***a*** por la parte A o ***b*** por la parte B, con los coeficientes Weierstrass comunes ***a***, ***b***.

9.2 Firma digital

El campo **ECGDSASignature** transporta los valores **r** y **s** de la firma digital basada en la curva elíptica calculada. En la sección 8.7.3 de *ATM Security Specification Version 1.1* y en el capítulo 5 de ISO 15946-2 se proporciona más información acerca del algoritmo de firmas EC-GDSA.

La firma digital basada en la curva elíptica **ECGDSA** deberá ser codificada en ASN.1 e introducida a continuación en el campo **signature** del macro **SIGNED** de esta Recomendación. Para la firma digital el emisor deberá incluir un identificador de objeto en el **algorithmOID** mediante el cual el recipiente sea capaz de determinar la utilización de una firma digital de curva elíptica.

10 Función seudoaleatoria (PRF, *pseudo-random function*)

En esta cláusula se define una función seudoaleatoria para calcular claves dinámicas a partir de material de clave estática y un valor aleatorio.

NOTA – Esta PRF es idéntica a la PRF MIKEY (véase la sección 4.1.2 de la RFC 3830).

El método de cálculo de clave tiene los siguientes parámetros de entrada:

- *inkey*: la clave de entrada para la función de cálculo.
- *inkey_len*: la longitud en bits de la clave de entrada.
- *label*: una etiqueta específica, que depende del tipo de clave que se debe calcular y del valor aleatorio **challenge**.
- *outkey_len*: longitud deseada en bits de la clave de salida.

La función seudoaleatoria tiene el siguiente resultado:

- *outkey*: la clave de salida de longitud deseada.

Esta función seudoaleatoria utilizará la PRF definida en la sección 4.1.2 de la RFC 3830.

11 Recuperación tras error de seguridad

Esta Recomendación no especifica ni recomienda métodos por los cuales los puntos extremos puedan supervisar su privacidad absoluta. Sin embargo, sí recomienda acciones que se han de ejecutar cuando se detecta la pérdida de privacidad.

Si cualquiera de los dos puntos extremos detecta una brecha en la seguridad del canal de conexión de la llamada (por ejemplo, H.225.0 para H.323), debe cerrar inmediatamente la conexión aplicando los procedimientos de protocolo apropiados al punto extremo en cuestión (para 8.5/H.323 con la excepción del paso B-5).

Si cualquiera de los dos puntos extremos detecta una brecha en la seguridad del canal H.245 o del canal lógico (**h235Control**) de datos seguro, debe cerrar inmediatamente la conexión aplicando los procedimientos de protocolo apropiados al punto extremo en cuestión (para 8.5/H.323 con la excepción del paso B-5).

Si cualquier punto extremo detecta una pérdida de privacidad en uno de los canales lógicos, debe solicitar inmediatamente una nueva clave (**encryptionUpdateRequest**) y/o cerrar el canal lógico. A discreción de la MC(U) una pérdida de privacidad en el canal lógico puede provocar el cierre de todos los otros canales lógicos y/o la creación de nuevas claves a discreción de la MC(U). La MC(U) enviará **encryptionUpdateRequest**, **encryptionUpdate** a cualquier y a todos lo puntos extremos afectados.

A discreción de la MC(U), un error de seguridad habido en un canal puede provocar el cierre de las conexiones en todos los puntos extremo de la conferencia, terminándola así.

11.1 Señalización de error

Un controlador de acceso capaz de ofrecer seguridad, u otra entidad H.225.0 con seguridad mejorada, proporcionará indicaciones de error. Un error de seguridad indica que la entidad no pudo procesar correctamente el mensaje recibido. Siempre que sea posible, se proporcionará un código de error detallado.

- **securityWrongSyncTime** indicará que el remitente encontró un problema de seguridad relativo a indicaciones de tiempo inadecuadas. Esto podría deberse a un problema con el servidor de tiempo, una pérdida de sincronización o un retraso excesivo de red.
- **securityReplay** indicará que se ha encontrado un ataque de reproducción. Esto ocurre cuando se presenta más de una vez el mismo número de secuencia para una indicación de tiempo determinada.
- **securityWrongGeneralID** indicará una discordancia del identificador general en el mensaje. Esto podría deberse a un direccionamiento errado.
- **securityWrongSendersID** indicará una discordancia del identificador del remitente en el mensaje. Podría deberse a una entrada errónea del usuario.
- **securityIntegrityFailed** indicará que fracasó el test de integridad/firma. En el caso de H.235.1, podría deberse a una contraseña errónea o mal escrita durante la petición inicial o a haberse encontrado un ataque activo. Para H.235.2 y H.235.3, indicará que falló la prueba de firma digital en el mensaje. Podría deberse a la aplicación de una clave privada/pública errónea o a que se ha encontrado un ataque activo.
- **securityWrongOID** indicará cualquier discordancia en los OID de testigo (testigo despejado o criptado) o en los OID de algoritmo de criptación. Esto indica que se han implementado diversos algoritmos/perfiles de seguridad.
- **securityDHmismatch** indicará cualquier discordancia en los parámetros Diffie-Hellman intercambiados. Esto podría indicar que se han implementado diversos conjuntos de parámetros DH e incluso diversos algoritmos de criptación de voz.
- **securityCertificateExpired** indicará que ha expirado un certificado.
- **securityCertificateDateInvalid** indicará que aún no es válido un certificado.
- **securityCertificateRevoked** indicará que se encontró un certificado revocado.
- **securityCertificateNotReadable** indicará que no se pudo decodificar un certificado mediante ANS.1 o que está en otra forma inadecuada.
- **securityCertificateSignatureInvalid** indicará que la firma en el certificado es incorrecta.
- **securityCertificateMissing** indicará que no se encontró certificado donde se esperaba uno o que no pudo ser localizado de otra manera.

- **securityCertificateIncomplete** indicará que no estaban presentes algunas extensiones de certificados esperadas.
- **securityUnsupportedCertificateAlgOID** indicará que no se entendieron o no se soportan algunos algoritmos de criptación tales como generación numérica (hash) o las firmas digitales, utilizados en certificados. El remitente puede proporcionar, como parte de la respuesta, una lista de los certificados aceptables en testigos separados, para que el destinatario pueda elegir fácilmente uno adecuado.
- **securityUnknownCA** indicará que no se pudo encontrar el certificado CA/root o que no fue posible hacerlo corresponder con un CA de confianza.

Cualquier otro fallo de una operación de seguridad H.235 implicará el retorno de un **securityDenial** para RAS H.225.0 (o **securityDenied** en el caso de la señalización de llamada H.225.0).

NOTA 1 – En los perfiles de seguridad de H.235.1, H.235.2 y H.235.3 pueden aparecer securityWrongSyncTime, securityReplay, securityWrongGeneralID, securityWrongSendersID, SecurityIntegrityFailed, securityDHmismatch y securityWrongOID

NOTA 2 – En los perfiles de seguridad de H.235.2 y H.235.3 pueden aparecer securityCertificateExpired, securityCertificateDateInvalid, securityCertificateRevoked, securityCertificateNotReadable, securityCertificateSignatureInvalid, securityCertificateMissing, securityCertificateIncomplete, securityUnsupportedCertificateAlgOID y securityUnknownCA.

Anexo A

ASN.1 del protocolo H.235

```
H235-SECURITY-MESSAGES DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

-- EXPORTS All

ChallengeString         ::= OCTET STRING (SIZE(8..128))
TimeStamp               ::= INTEGER(1..4294967295)     -- seconds since 00:00
                                                       -- 1/1/1970 UTC
RandomVal               ::= INTEGER -- 32-bit Integer
Password                ::= BMPString (SIZE (1..128))
Identifier              ::= BMPString (SIZE (1..128))
KeyMaterial             ::= BIT STRING(SIZE(1..2048))

NonStandardParameter ::= SEQUENCE
{
     nonStandardIdentifier   OBJECT IDENTIFIER,
     data                    OCTET STRING
}

-- if local octet representations of these bit strings are used they shall
-- utilize standard Network Octet ordering (e.g., Big Endian)
DHset ::= SEQUENCE
{
     halfkey        BIT STRING (SIZE(0..2048)), -- = g^x mod n
     modSize        BIT STRING (SIZE(0..2048)), --  n
     generator      BIT STRING (SIZE(0..2048)), -- g
     ...
}
```

```
ECpoint ::= SEQUENCE -- uncompressed (x, y) affine coordinate representation of
                     -- an elliptic curve point
{
     x         BIT STRING (SIZE(0..511)) OPTIONAL,
     y         BIT STRING (SIZE(0..511)) OPTIONAL,
     ...
}

ECKASDH::= CHOICE -- parameters for elliptic curve key agreement scheme Diffie-
Hellman
{
     eckasdhp SEQUENCE -- parameters for elliptic curves of prime field
     {
          public-key    ECpoint, -- This field contains representation of
               -- the ECKAS-DHp public key value. This field contains the
               -- initiator's ECKAS-DHp public key value (aP) when this
               -- information element is sent from originator to receiver. This
               -- field contains the responder's ECKAS-DHp public key value (bP)
               -- when this information element is sent back from receiver to
               -- originator.
          modulus       BIT STRING (SIZE(0..511)), -- This field contains
               -- representation of the ECKAS-DHp public modulus value (p).
          base          ECpoint, -- This field contains representation of the
               -- ECKAS-DHp public base (P).
          weierstrassA  BIT STRING (SIZE(0..511)), -- This field contains
               -- representation of the ECKAS-DHp Weierstrass coefficient (a).
          weierstrassB  BIT STRING (SIZE(0..511)) -- This field contains
               -- representation of the ECKAS-DHp Weierstrass coefficient (b).
     },

     eckasdh2 SEQUENCE -- parameters for elliptic curves of characteristic 2
     {
          public-key    ECpoint, -- This field contains representation of
               -- the ECKAS-DH2 public key value.
               -- This field contains the initiator's ECKAS-DH2 public key value
               -- (aP) when this information element is sent from originator to
               -- receiver. This field contains the responder's ECKAS-DH2 public
               -- key value (bP) when this information element is sent back from
               -- receiver to originator.
          fieldSize     BIT STRING (SIZE(0..511)), -- This field contains
               -- representation of the ECKAS-DH2 field size value (m).
          base          ECpoint, -- This field contains representation of the
               -- ECKAS-DH2 public base (P).
          weierstrassA  BIT STRING (SIZE(0..511)), -- This field contains
               -- representation of the ECKAS-DH2 Weierstrass coefficient (a).
          weierstrassB  BIT STRING (SIZE(0..511)) -- This field contains
               -- representation of the ECKAS-DH2 Weierstrass coefficient (b).
     },
     ...
}

ECGDSASignature::= SEQUENCE -- parameters for elliptic curve digital signature
               -- algorithm
{
     r         BIT STRING (SIZE(0..511)), -- This field contains the
               -- representation of the r component of the ECGDSA digital
               -- signature.
     s         BIT STRING (SIZE(0..511)) -- This field contains the
               -- representation of the s component of the ECGDSA digital
               -- signature.
}
```

```
TypedCertificate ::= SEQUENCE
{
     type           OBJECT IDENTIFIER,
     certificate    OCTET STRING,
     ...
}

AuthenticationBES ::= CHOICE

{
     default        NULL, -- encrypted ClearToken
     radius         NULL, -- RADIUS-challenge/response
     ...

}

AuthenticationMechanism  ::= CHOICE
{
     dhExch         NULL, -- Diffie-Hellman
     pwdSymEnc      NULL, -- password with symmetric encryption
     pwdHash        NULL, -- password with hashing
     certSign       NULL, -- Certificate with signature
     ipsec          NULL, -- IPSEC based connection
     tls            NULL,
     nonStandard    NonStandardParameter, -- something else.
     ...,
     authenticationBES  AuthenticationBES, -- user authentication for BES
     keyExch   OBJECT IDENTIFIER -- key exchange profile
}

ClearToken          ::= SEQUENCE  -- a "token" may contain multiple value types.
{
     tokenOID       OBJECT IDENTIFIER,
     timeStamp      TimeStamp OPTIONAL,
     password       Password OPTIONAL,
     dhkey          DHset OPTIONAL,
     challenge      ChallengeString OPTIONAL,
     random         RandomVal OPTIONAL,
     certificate    TypedCertificate OPTIONAL,
     generalID      Identifier OPTIONAL,
     nonStandard    NonStandardParameter OPTIONAL,
     ...,
     eckasdhkey     ECKASDH OPTIONAL,  -- elliptic curve Key Agreement
                                       -- Scheme-Diffie Hellman Analogue
                                       -- (ECKAS-DH)
     sendersID      Identifier OPTIONAL,
     h235Key        H235Key OPTIONAL, -- central distributed key in V3
     profileInfo    SEQUENCE OF ProfileElement OPTIONAL  -- profile-specific
}

--   An object identifier should be placed in the tokenOID field when a
--   ClearToken is included directly in a message (as opposed to being
--   encrypted). In all other cases, an application should use the object
--   identifier { 0 0 } to indicate that the tokenOID value is not present.
--   Start all the cryptographic parameterized types here...
--

ProfileElement      ::= SEQUENCE
{
     elementID      INTEGER (0..255), -- element identifier, as defined by
                                      -- profile
     paramS         Params OPTIONAL,  -- any element-specific parameters
     element        Element OPTIONAL, -- value in required form
     …
}
```

```
Element ::= CHOICE
{
     octets              OCTET STRING,
     integer             INTEGER,
     bits                BIT STRING,
     name                BMPString,
     flag                BOOLEAN,
     …
}


SIGNED { ToBeSigned } ::= SEQUENCE {
     toBeSigned          ToBeSigned,
     algorithmOID        OBJECT IDENTIFIER,
     paramS              Params,   -- any "runtime" parameters
     signature           BIT STRING -- could be an RSA or an ASN.1 coded
ECGDSA Signature
} ( CONSTRAINED BY { -- Verify or Sign Certificate -- } )


ENCRYPTED { ToBeEncrypted } ::= SEQUENCE {
     algorithmOID        OBJECT IDENTIFIER,
     paramS              Params,   -- any "runtime" parameters
     encryptedData       OCTET STRING
} ( CONSTRAINED BY { -- Encrypt or Decrypt -- ToBeEncrypted } )

HASHED { ToBeHashed } ::= SEQUENCE {
     algorithmOID        OBJECT IDENTIFIER,
     paramS              Params,   -- any "runtime" parameters
     hash                BIT STRING
} ( CONSTRAINED BY { -- Hash -- ToBeHashed } )

IV8 ::= OCTET STRING (SIZE(8)) -- initial value for 64-bit block ciphers
IV16 ::= OCTET STRING (SIZE(16)) -- initial value for 128-bit block ciphers

-- signing algorithm used must select one of these types of parameters
-- needed by receiving end of signature.

Params ::= SEQUENCE {
     ranInt         INTEGER OPTIONAL, -- some integer value
     iv8            IV8 OPTIONAL, -- 8-octet initialization vector
     ...,
     iv16           IV16 OPTIONAL,-- 16-octet initialization vector
     iv             OCTET STRING OPTIONAL, -- arbitrary length initialization
     vector
     clearSalt      OCTET STRING OPTIONAL -- unencrypted salting key for
     encryption
}

EncodedGeneralToken ::= TYPE-IDENTIFIER.&Type (ClearToken -- general usage token
-- )
PwdCertToken ::= ClearToken (WITH COMPONENTS {..., timeStamp PRESENT, generalID
PRESENT})
EncodedPwdCertToken ::= TYPE-IDENTIFIER.&Type (PwdCertToken)

CryptoToken::= CHOICE
{

     cryptoEncryptedToken SEQUENCE -- General purpose/application specific token
     {
          tokenOID       OBJECT IDENTIFIER,
          token          ENCRYPTED { EncodedGeneralToken }
     },
```

```
    cryptoSignedToken  SEQUENCE -- General purpose/application specific token
    {
        tokenOID       OBJECT IDENTIFIER,
        token          SIGNED { EncodedGeneralToken }
    },
    cryptoHashedToken SEQUENCE -- General purpose/application specific token
    {
        tokenOID           OBJECT IDENTIFIER,
        hashedVals         ClearToken,
        token HASHED { EncodedGeneralToken }
    },
    cryptoPwdEncr ENCRYPTED { EncodedPwdCertToken },
    ...
}

-- These allow the passing of session keys within the H.245 OLC structure.
-- They are encoded as standalone ASN.1 and based as an OCTET STRING within
-- H.245
H235Key  ::=CHOICE  -- This is used with the H.245 or ClearToken "h235Key"
field
{
    secureChannel           KeyMaterial,
    sharedSecret            ENCRYPTED {EncodedKeySyncMaterial},
    certProtectedKey        SIGNED {EncodedKeySignedMaterial },
    ...,
    secureSharedSecret      V3KeySyncMaterial -- for H.235 V3 endpoints
}

KeySignedMaterial ::= SEQUENCE {
    generalId     Identifier, -- slave's alias
    mrandom       RandomVal, -- master's random value
    srandom       RandomVal OPTIONAL, -- slave's random value
    timeStamp     TimeStamp OPTIONAL, -- master's timestamp for unsolicited EU
    encrptval     ENCRYPTED { EncodedKeySyncMaterial }
}
EncodedKeySignedMaterial ::= TYPE-IDENTIFIER.&Type (KeySignedMaterial)

H235CertificateSignature    ::= SEQUENCE
{
    certificate             TypedCertificate,
    responseRandom          RandomVal,
    requesterRandom         RandomVal OPTIONAL,
    signature               SIGNED { EncodedReturnSig },
    ...
}

ReturnSig ::= SEQUENCE {
    generalId               Identifier, -- slave's alias
    responseRandom          RandomVal,
    requestRandom           RandomVal OPTIONAL,
    certificate             TypedCertificate OPTIONAL -- requested certificate
}

EncodedReturnSig ::= TYPE-IDENTIFIER.&Type (ReturnSig)
KeySyncMaterial    ::= SEQUENCE
{
    generalID     Identifier,
    keyMaterial   KeyMaterial,
    ...
}
EncodedKeySyncMaterial  ::=TYPE-IDENTIFIER.&Type (KeySyncMaterial)
```

```
V3KeySyncMaterial  ::= SEQUENCE
{
     generalID               Identifier OPTIONAL, -- peer terminal ID
     algorithmOID            OBJECT IDENTIFIER OPTIONAL, -- encryption algorithm
     paramS                  Params, -- IV
     encryptedSessionKey     OCTET STRING OPTIONAL, -- encrypted session key
     encryptedSaltingKey     OCTET STRING OPTIONAL, -- encrypted media salting
                                                    -- key
     clearSaltingKey         OCTET STRING OPTIONAL, -- unencrypted media salting
                                                    -- key
     paramSsalt              Params OPTIONAL, -- IV (and clear salt) for salting
                                                    -- key encryption
     keyDerivationOID        OBJECT IDENTIFIER OPTIONAL, -- key derivation
                                                    -- method
     ...,
     genericKeyMaterial      OCTET STRING OPTIONAL -- ASN.1-encoded key material
                         -- form is dependent on associated media encryption tag

}


END  -- End of H235-SECURITY-MESSAGES DEFINITIONS
```

Anexo B

Aspectos específicos de H.324

Queda en estudio.

Apéndice I

Precisiones sobre implementaciones H.323

I.1 Ejemplos de implementaciones

En las siguientes subcláusulas se describen ejemplos de posibles implementaciones con el protocolo H.235. No se pretende restringir las muchas otras posibilidades disponibles dentro de esta Recomendación, sino más bien dar ejemplos más concretos de utilización dentro de la Rec. UIT-T H.323.

I.1.1 Testigos

Esta cláusula describe un ejemplo de utilización de testigos de seguridad para oscurecer u ocultar la información de direccionamiento de destino. El caso de ejemplo es un punto extremo que desea hacer una llamada a otro punto extremo utilizando su alias conocido. Más concretamente, esto comprende un punto extremo H.323, un controlador de acceso, una pasarela POTS y un teléfono como se ilustra en la figura I.1.

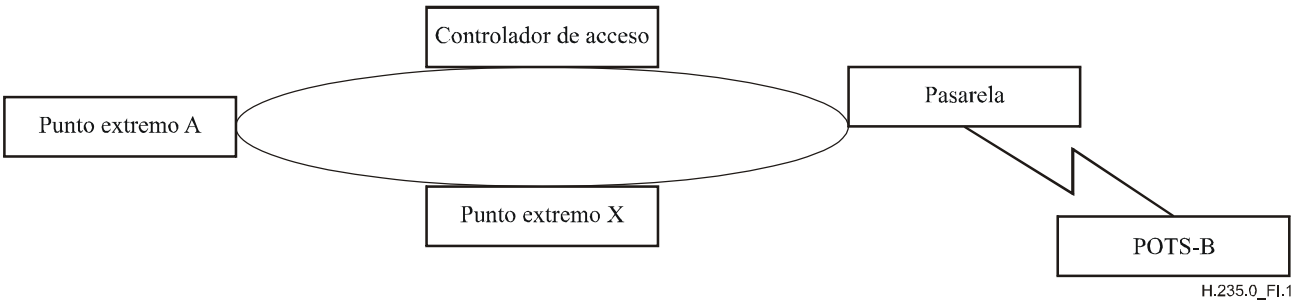


Figura I.1/H.235.0 – Testigos

Actualmente, el protocolo H.323 puede funcionar de manera similar a una red telefónica con el ID del llamante. Este escenario ilustra una situación en la cual el *llamante* no desea exponer su dirección física, a la vez que permite que se complete la llamada. Esto puede ser importante en pasarelas POTS-H.323, cuando el número telefónico deseado puede tener que permanecer privado.

Se supone que EPA está tratando de llamar a POTS-B y que POTS-B no desea exponer su número telefónico E.164 a EPA. (La manera en que se establece esta política está fuera del alcance de este ejemplo.)

- EPA enviará **ARQ** a su controlador de acceso para resolver la dirección del teléfono POTS representada por su alias/pasarela. El controlador de acceso reconocerá esto como un alias "privado" sabiendo que para completar la conexión debe devolver la dirección de pasarela de POTS (de manera similar a la devolución de la dirección H.320 si un punto extremo H.320 es llamado por un punto extremo H.323).
- En el **ACF** devuelto, el controlador de acceso devuelve la dirección de pasarela de POTS según lo previsto. La información de direccionamiento requerida para marcar el teléfono del extremo (es decir el número telefónico) es devuelta en un testigo criptado incluido en **ACF**. Este testigo criptado contiene el número telefónico E.164 real del teléfono que no puede ser descifrado ni comprendido por el llamante (es decir, EPA).
- El punto extremo emite el mensaje ESTABLECIMIENTO al dispositivo de pasarela (cuya dirección de señalización de llamada fue devuelta en **ACF**) incluidos los testigos opacos que recibió con **ACF**.

- La pasarela, al recibir el mensaje ESTABLECIMIENTO, emite su **ARQ** a su controlador de acceso incluidos cualesquiera testigos que fueron recibidos en el mensaje ESTABLECIMIENTO.
- El controlador de acceso puede descifrar el testigo o testigos y devolver el número telefónico en **ACF**.

A continuación se muestra la ASN.1 parcial de la estructura de un testigo de ejemplo, describiendo el contenido de campo. Se supone que se utiliza **testigo general codificado en cifra (cryptoEncodedGeneralToken)** para contener el número telefónico criptado.

Una implementación pudiera elegir un **OID de testigo (tokenOID)** que indica que este testigo contiene el número telefónico E.164. El método particular que se utiliza para criptar este número telefónico (por ejemplo, DES de 56 bits) se incluiría en el **OID de algoritmo (algorithmOID)** de la definición de "CRIPTAR".

```
CryptoToken::= CHOICE
{
     cryptoEncodedGeneralToken SEQUENCE    -- General purpose/application
                                           --  specific token
     {
          tokenOID  OBJECT IDENTIFIER,
          ENCRYPTED { EncodedGeneralToken }
     },
.
.
. [abbreviated text]
.

}
```

El **testigo cifrado (CryptoToken)** se transferiría en los mensajes ESTABLECIMIENTO (del EPA a la pasarela) y **ARQ** (de la pasarela al controlador de acceso) como se indica anteriormente. Una vez que el controlador de acceso descriptó el testigo (el número telefónico) transferirá la versión clara en el **testigo claro (ClearToken)**.

I.1.2 Utilización de testigos en los sistemas H.323

Ha habido alguna confusión en la utilización de **CryptoH323Tokens** individuales pasados en mensajes RAS. Existen dos categorías principales de **CryptoH323Tokens**: los utilizados para los procedimientos H.235 y los utilizados en un modo específico de la aplicación. El uso de estos testigos debe adecuarse a las siguientes reglas:

- Todos los definidos de H.235 (por ejemplo, **cryptoEPPwdHash**, **cryptoGKPwdHash**, **cryptoEPPwdEncr**, **cryptoGKPwdEncr**, **cryptoGKCert** y **cryptoFastStart**), se deberán utilizar con los procedimientos y algoritmos descritos en esta Recomendación.
- Si se trata de testigos de uso exclusivo o específicos de la aplicación, se deberá utilizar el **nestedcryptoToken** para sus intercambios.
- Cada **nestedcryptoToken** utilizado debe tener una **tokenOID** que lo identifique inequívocamente.

I.1.3 Utilización del valor aleatorio H.235 en sistemas H.323

El valor aleatorio que se pasa en la secuencia **xRQ**/**xCF** entre puntos extremos y controladores de acceso puede ser actualizado por el controlador de acceso. Como se describe en 8.3.1, este valor aleatorio puede ser renovado en cualquier mensaje **xCF** para ser utilizado por un mensaje **xRQ** subsiguientes procedente del punto extremo. Como pueden perderse mensajes RAS (incluidos **xCF**/**xRJ**), el valor aleatorio actualizado también puede perderse. La recuperación desde esta situación puede consistir en la reinicialización del contexto de seguridad, pero se deja a la implementación local.

Las implementaciones que requieren la utilización de múltiples peticiones RAS pendientes estarán limitadas por la actualización de los valores aleatorios utilizados en toda autenticación. Si la actualización de este valor se produce con cada respuesta a una petición, no están permitidas las peticiones en paralelo. Una solución posible a esta situación es disponer de una "ventana" lógica durante la cual un valor aleatorio permanece constante. Este tema es incumbencia de la implementación local.

I.1.4 Contraseña

En este ejemplo, se supone que el usuario está abonado al controlador de acceso (es decir, el usuario estará en su zona) y tiene un ID de abono y una contraseña asociada. El usuario se registrará con el controlador de acceso utilizando el ID de abono (transferido en un alias – H323ID) y criptando una cadena de preguntas presentada por el controlador de acceso. Esto supone que el controlador de acceso conoce también la contraseña asociada con el ID de abono. El controlador de acceso autenticará al usuario verificando que la cadena de preguntas está criptada correctamente.

El procedimiento de registro de ejemplo con autenticación de controlador de acceso es el siguiente:

1) Si el punto extremo utiliza **GRQ** para descubrir un controlador de acceso, uno de los alias del mensaje sería el ID del acuerdo (como un **H323ID**). La **capacidad de autenticación (authenticationcapability)** contendría un **Mecanismo de autenticación (AuthenticationMechanism)** de **criptación simétrica de contraseña (pwdSymEnc)** y los **OID de algoritmo (algorithmOIDs)** se fijarían para indicar el conjunto completo de algoritmos de criptación soportados por el punto extremo. (Por ejemplo, uno de estos sería DES de 56 bits en modo EBC.)

2) El controlador de acceso respondería con **GCF** (suponiendo que reconoce el alias) que transporta un elemento **testigos (tokens)** que contiene un **testigo claro (ClearToken)**. Este **Testigo claro** contendría una **pregunta** y un elemento de **indicación de tiempo**. La **pregunta** contendría 16 octetos. (Para impedir ataques de reproducción, el **Testigo claro** contendría una **indicación de tiempo**.) El **modo de autenticación** se pondría a **criptación simétrica de contraseña** y el **OID de algoritmo** se fijaría para indicar el algoritmo de criptación requerido por el controlador de acceso (por ejemplo, DES de 56 bits en modo EBC).

   Si el controlador de acceso no soporta algunos de los **algorithmOIDs** indicados en el **GRQ**, respondería con un mensaje **GRJ** que contiene un **Motivo de rechazo de controlador de acceso (GatekeeperRejectReason)** de **recurso no disponible (resourceUnavailable)**.

3) La aplicación de punto extremo trataría de registrarse con (uno de) los controladores de acceso que respondieron con un **GCF** enviando un **RRQ** que contiene una **contraseña de EP cifrada (cryptoEPPwdEncr)** en los **testigos cifrados**. La **contraseña de EP criptada** tendría el **OID del algoritmo** de criptación acordado en el intercambio **GRQ/GCF**, y la pregunta criptada.

   La clave de criptación se construye a partir de la contraseña del usuario utilizando el procedimiento descrito en 8.2.1. La "cadena" de octetos resultante se utiliza como la clave DES para criptar la **pregunta**.

4) Cuando el controlador de acceso recibe la pregunta criptada en el **RRQ**, la comparará con una pregunta criptada generada idénticamente para autenticar al usuario que registra. Si las dos cadenas criptadas no concuerdan, el controlador de acceso responderá con un **RRJ** con el **Motivo de rechazo de registro (RegistrationRejectReason)** puesto a **denegación de seguridad** u otro código de error de seguridad adecuado, conforme a 11.1. Si concuerdan, el guardián de puerta envía un **RCF** al punto extremo.

5) Si el controlador de acceso recibe un **RRQ** que no contiene un elemento **Testigos criptados** aceptable, debe responder con un **RRJ** con un **Motivo de rechazo de**

controlador de acceso de descubrimiento requerido (discoveryRequired). El punto extremo, al recibir este **RRJ** puede efectuar un descubrimiento que le permitirá al controlador de acceso/punto extremo intercambiar una nueva pregunta.

NOTA – El mensaje **GRQ** puede enviarse al controlador de acceso por unidifusión.

I.1.5 IPsec

En general IPsec ([RFC 2401], RFC 2406 [ESP]) y RFC 2409 [IKE] se pueden utilizar para proporcionar autenticación y, facultativamente, confidencialidad (es decir, criptación) en la capa IP transparente a cualquier protocolo (aplicación) que funcione por encima de ella. El protocolo de aplicación no tiene que ser actualizado para permitir esto; sólo la política de seguridad en cada extremo.

Por ejemplo, para utilizar al máximo IPsec para una llamada simple punto a punto, se puede aplicar lo que sigue:

1) El punto extremo llamante y su controlador de acceso fijarían la política para requerir la utilización de IPsec (autenticación y, facultativamente confidencialidad) en el protocolo RAS. De este modo, antes de que el primer mensaje RAS sea enviado desde el punto extremo al controlador de acceso, el protocolo ISAKMP (RFC 2407)/Oakley (RFC 2412) en el punto extremo negociará los servicios de seguridad que se han de utilizar en paquetes a y desde el puerto bien conocido del canal RAS. Una vez completada la negociación, el canal RAS funcionará exactamente como si no fuese seguro. Al utilizar este canal de seguridad, el controlador de acceso informará al punto extremo la dirección y el número de puerto del canal de señalización de la llamada en el punto extremo llamado.

2) Después de obtener la dirección y el número de puerto del canal de señalización de llamada, el punto extremo llamante actualizaría dinámicamente su política de seguridad para requerir la seguridad IPsec deseada en esa dirección y par de protocolo/puerto. En ese momento, cuando el punto extremo llamante intenta ponerse en contacto con esta dirección/puerto, los paquetes se pondrían en cola mientras se realiza una negociación ISAKMP (RFC 2407)/Oakley (RFC 2412) entre los puntos extremos. Al completar esta negociación, existirá una asociación de seguridad (SA, *security association*) IPsec para la dirección/puerto y se puede pasar a la señalización Q.931.

3) En el intercambio de los mensajes ESTABLECIMIENTO y CONEXIÓN Q.931, los puntos extremos pueden negociar la utilización de IPsec para el canal H.245. Esto permitiría a los puntos extremos actualizar de nuevo dinámicamente sus bases de datos de política IPsec para forzar el uso de IPsec en esa conexión.

4) Al igual que en el caso del canal de señalización de llamada, se producirá una negociación ISAKMP (RFC 2407)/Oakley (RFC 2412) transparente antes de que se transmitan paquetes H.245. La autenticación realizada por esta negociación ISAKMP (RFC 2407)/Oakley (RFC 2412) será el intento inicial de la autenticación de usuario a usuario, y establecerá entre los dos usuarios un canal (probablemente) seguro por el cual negociar las características del canal de audio. Si después de Q y A de persona a persona, uno de los dos usuarios no está satisfecho con la autenticación, se pueden elegir diferentes certificados y repetir el intercambio ISAKMP (RFC 2407)/Oakley (RFC 2412).

5) Después de cada autenticación ISAKMP(RFC 2407)/Oakley H.245 (RFC 2412), se intercambia nuevo material de claves para el canal de audio RTP. Este material de claves es distribuido por el terminal director por el canal H.245 seguro. Como el protocolo H.245 está definido para que el director distribuya el material de clave de los medios por el canal H.245 (para la comunicación multipunto), no se recomienda utilizar IPsec para el canal RTP.

Un canal H.245 criptado es un posible problema para servidores intermedios o cortafuegos NAT, porque los números de puerto asignados dinámicamente son transportados en el protocolo H.245.

Estos cortafuegos tendrían que descifrar, modificar y cifrar de nuevo el protocolo para funcionar correctamente. Por este motivo, se introdujo el canal lógico de "seguridad" en la Rec. UIT-T H.245. Si este canal se utiliza, el canal H.245 puede permanecer inseguro; la autenticación y la generación de claves se haría con el canal lógico de "seguridad". La señalización de canal lógico permitiría que este canal estuviese protegido con IPsec, y la clave secreta utilizada en el canal lógico de "seguridad" se emplearía para proteger el campo **sincronización criptada** distribuido por el terminal director por el canal H.245.

I.1.6 Soporte de servicios fuera del terminal

Los servidores fuera del terminal son una función suplementaria importante en un entorno multimedia que globalmente está basado en H.323. Por ejemplo, los BES proporcionan servicios para la autenticación del usuario y la autorización del servicio, así como la facturación, tarificación, contabilidad y otros servicios. En un modelo simple el controlador de acceso puede proporcionar tales servicios. En una arquitectura fraccionada el controlador de acceso no siempre puede proveer tales servicios; bien porque no tiene acceso a las bases de datos BES o bien porque estas pueden ser parte de un dominio administrativo diferente. Del mismo modo, el terminal o usuario no conoce normalmente sus BES.

En la figura I.2 se muestra un escenario con un terminal multimedia (por ejemplo, un SASET), un controlador de acceso y un BES enlazado. No cae en el ámbito de la Rec. UIT-T H.323 el modo en los BES comunican exactamente con el GK. Se pueden aplicar varios métodos y protocolos: RADIUS (véase RFC 2865) se considera uno de los más importantes, y es desplegado ampliamente por los proveedores del servicio.

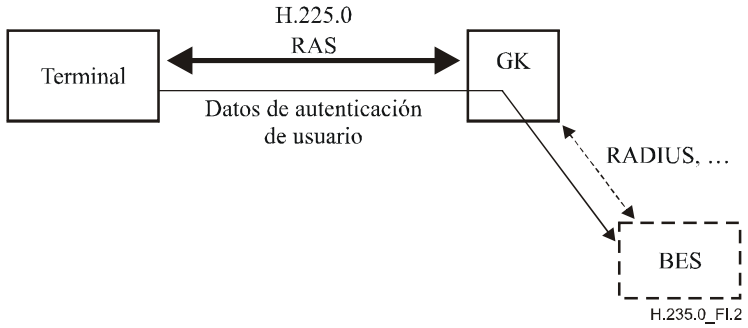


Figura I.2/H.235.0 – Escenario con servidor fuera del terminal

Un GK que ofrece el soporte BES debería soportar al menos los dos modos siguientes:

1) **modo por defecto**: en este modo el terminal no conoce el BES y necesita una relación de confianza con el GK. El terminal envía al GK los datos de autenticación de usuario en forma criptada (**cryptoEncryptedToken**), y el GK descripta estos datos, extrae la información de autenticación de usuario y la envía hacia el BES. La criptación basada en contraseñas del **ClearToken** se realiza aplicando un secreto distinto del compartido entre el terminal y el GK al **CryptoToken**. La clave de criptación puede obtenerse a partir de la contraseña con la cual el terminal se registra de modo seguro en el GK.

   CryptoToken tiene un campo **cryptoEncryptedToken** que contiene un **tokenOID** puesto a "M" para indicar el modo por defecto de BES y el testigo:

   - **algorithmOID**, que indica el algoritmo de criptación: "Y" (DES56-CBC), "Z" (3DES-ocbc); véase la cláusula 11/H.235.6;
   - **paramS**, no utilizado;
   - **encryptedData**, fijado a la representación de octetos del **ClearToken** criptado.

El **ClearToken** contiene como **password** los datos de autenticación de usuario. La información **ClearToken** protegida puede ser contraseña/PIN, identificación de usuario, número de tarjeta de llamadas de previo pago y número de tarjeta de crédito. El campo **timeStamp** se fija al tiempo real del terminal; **random** contiene un número secuencial monotónicamente creciente, **sendersID** se fija al valor del ID de terminal y **generalID** al valor del identificador de GK. El valor inicial (IV) del algoritmo de criptación deberá mantenerse constante; este valor puede formar parte del secreto del abono del terminal.

NOTA – El **ClearToken** no se transmite.

2) **modo RADIUS**: en este modo el BES y el usuario terminal comparten un secreto común y el GK no debería ser servidor intermedio para la autenticación RADIUS de BES. El GK simplemente reenvía una consulta RADIUS recibida del BES dentro de *Access-Challenge* hacia el terminal y envía la respuesta del usuario como una respuesta RADIUS dentro de *Access-Request* en la dirección inversa. El terminal y el GK negocian la capacidad consulta/respuesta **radius** en **AuthenticationBES** dentro del **AuthenticationMechanism** durante el descubrimiento del controlador de acceso.

   Tras la recepción de un mensaje *Access-Challenge* RADIUS que transporta una consulta, el GK coloca la consulta de 16 octetos en el campo **challenge** del **ClearToken** cuando se pregunta al terminal con un **GCF** o cualquier otro mensaje RAS. El **tokenOID** 'K' en el **ClearToken** indica una consulta RADIUS.

   El terminal puede entonces presentar la consulta al usuario y esperar la respuesta. El terminal deberá contestar con un mensaje RAS en el cual se ha introducido la respuesta en el campo **challenge** del **ClearToken**. El **tokenOID** 'L' en el **ClearToken** indica una respuesta RADIUS.

En el cuadro I.1 se da una lista de los OIDs considerados.

Cuadro I.1/H.235.0 – Identificadores de objeto utilizados en los procedimientos de I.1.6

Referencia del identificador de objeto	Valor del identificador de objeto	Descripción
"K"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 31}	indica una consulta RADIUS en el ClearToken
"L"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 32}	indica una respuesta RADIUS (cursada en el campo consulta) en el ClearToken
"M"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 33}	indica el modo por defecto BES con una contraseña protegida en el ClearToken

Apéndice II

Precisiones sobre implementaciones del protocolo H.324

Queda en estudio.

Apéndice III

Otras precisiones sobre implementaciones de la serie H

Queda en estudio.

Apéndice IV

Tabla de correspondencia de las cláusulas de la H.235v3 y su enmienda 1 y corrigendum 1, con las Recomendaciones de la subserie H.235v4

El presente apéndice es informativo y muestra el lugar donde figuran las cláusulas de la H.235v3, y su enmienda 1 y corrigendum 1, en las Recomendaciones de la subserie H.235v4.

Cuadro IV.1/H.235.0 – Tabla de correspondencia de cláusulas

Cláusula de H.235v3, enm.1, corr.1	Título	Recomendación de la subserie H.235v4.x	Cláusula
Cuerpo principal	–	–	–
1	Alcance	H.235.0	1
2	Referencias	H.235.0	2
		H.235.1	2
		H.235.2	2
		H.235.3	2
3	Términos y definiciones	H.235.0	3
		H.235.2	3
		H.235.6	3
4	Símbolos y abreviaturas	H.235.0	4
		H.235.3	4
		H.235.6	4
5	Convenios	H.235.0	5
		H.235.2	5
		H.235.6	5

Cuadro IV.1/H.235.0 – Tabla de correspondencia de cláusulas

Cláusula de H.235v3, enm.1, corr.1	Título	Recomendación de la subserie H.235v4.x	Cláusula
6	Presentación del sistema	H.235.0	6
6.1	Resumen	H.235.0	6.1
6.2	Autenticación	H.235.0	6.2
6.2.1	Certificados	H.235.0	6.2.1
6.3	Seguridad de establecimiento de la comunicación	H.235.0	6.3
6.4	Seguridad de control de la llamada (H.245)	H.235.0	6.4
6.5	Privacidad de trenes de medios	H.235.0	6.5
6.6	Elementos de confianza	H.235.0	6.6
6.6.1	Depósito de claves	H.235.0	6.6.1
6.7	No repudio	H.235.0	6.7
6.8	Seguridad en entorno de movilidad	H.235.0	6.8
6.9	Perfiles de seguridad	H.235.0	6.9
7	Procedimientos de establecimiento de la conexión	H.235.0	7
7.1	Introducción	H.235.0	–
8	Señalización y procedimientos H.245	H.235.6	7
8.1	Funcionamiento seguro del canal H.245	H.235.6	7.1
8.2	Funcionamiento inseguro del canal H.245	H.235.6	7.2
8.3	Intercambio de capacidades	H.235.6	7.3
8.4	Cometido de terminal director	H.235.6	7.4
8.5	Señalización de canal lógico	H.235.6	7.5
8.6	Seguridad de conexión rápida	H.235.6	7.6
8.6.1	Seguridad de arranque rápido unidireccional	H.235.6	7.6.1
8.6.1.1	Utilización de algoritmos de criptación múltiple en la conexión rápida	H.235.6	7.6.1.1
8.6.2	Seguridad de canales bidireccionales durante el arranque rápido	H.235.6	7.6.2
8.7	DTMF H.245 criptadas	H.235.6	7.7
8.7.1	Cadena básica criptada	H.235.6	7.7.1
8.7.2	Cadena iA5 criptada	H.235.6	7.7.2
8.7.3	Cadena general criptada	H.235.6	7.7.3
8.7.4	Lista de identificadores de objeto	H.235.6	7.7.4
8.8	Operación Diffie-Hellman	H.235.6	7.8

Cuadro IV.1/H.235.0 – Tabla de correspondencia de cláusulas

Cláusula de H.235v3, enm.1, corr.1	Título	Recomendación de la subserie H.235v4.x	Cláusula
9	Procedimientos multipunto	H.235.6	8.8
9.1	Autenticación	H.235.6	8.8.1
9.2	Privacidad	H.235.6	8.8.2
10	Señalización y procedimientos de autenticación	H.235.0	8
10.1	Introducción	H.235.0	---
10.2	Intercambio Diffie-Hellman con autenticación facultativa	H.235.0	8.1
10.3	Autenticación basada en acuerdo	H.235.0	8.2
10.3.1	Introducción	H.235.0	–
10.3.2	Contraseña con criptación simétrica	H.235.0	8.2.1
10.3.3	Contraseña con generación numérica	H.235.0	8.2.2
10.3.4	Certificado con firma	H.235.0	8.2.3
10.3.5	Utilización de contraseñas y secreto compartido	H.235.0	8.2.4
11	Procedimiento de criptación de tren de medios	H.235.6	9
11.1	Claves de sesión de medios	H.235.6	9.1
11.2	Antiinundación de medios	H.235.6	9.2
11.2.1	Lista de identificadores de objeto	H.235.6	9.2.1
12	Recuperación tras error de seguridad	H.235.0	11
13	Autenticación asimétrica e intercambio de claves utilizando sistemas criptográficos de curva elíptica	H.235.0	9
13.1	Gestión de claves	H.235.0	9.1
13.2	Firma digital	H.235.0	9.2
Apéndice I	Detalles de las implementaciones H.323	H.235.0	Apéndice I
I.1	Métodos de relleno de texto cifrado	H.235.6	I.1
I.2	Nuevas claves	H.235.6	8.7.2
I.3	Elementos de confianza H.323	H.235.6	8.7.3
I.4	Ejemplos de implementaciones	H.235.0	I.1
I.4.1	Testigos	H.235.0	I.1.1
I.4.2	Utilización de testigos en los sistemas H.323	H.235.0	I.1.2
I.4.3	Utilización del valor aleatorio H.235 en sistemas H.323	H.235.0	I.1.3
I.4.4	Contraseña	H.235.0	I.1.4

Cuadro IV.1/H.235.0 – Tabla de correspondencia de cláusulas

Cláusula de H.235v3, enm.1, corr.1	Título	Recomendación de la subserie H.235v4.x	Cláusula
I.4.5	IPsec	H.235.0	I.1.5
I.4.6	Soporte de servicios fuera del terminal	H.235.0	I.1.6
Apéndice II	Precisiones sobre implementaciones del protocolo H.324	H.235.0	Apéndice II
Apéndice III	Otras precisiones sobre implementaciones de la serie H	H.235.0	Apéndice III
Apéndice IV	Bibliografía	H.235.0	2.2
Anexo A	**ASN.1 del protocolo H.235**	**H.235.0**	**Anexo A**
Anexo B	**Aspectos específicos de H.323**	**H.235.6**	**–**
B.1	Antecedentes	H.235.0	6
B.2	Señalización y procedimientos	H.235.6	8
B.2.1	Compatibilidad con la revisión 1	H.235.6	8.1
B.2.2	Señalización de error	H.235.0	11.1
B.2.3	Indicación de característica de la versión 3	H.235.6	8.2
B.2.4	Transporte de clave	H.235.6	8.3
B.2.4.1	Transporte de clave mejorado en la versión 3 de H.235	H.235.6	8.3.1
B.2.5	Modo OFB mejorado	H.235.6	8.4
B.2.6	Actualización y sincronización de clave	H.235.6	8.6
B.2.6.1	Actualización de clave sin acuse	H.235.6	8.6.1
B.2.6.2	Actualización de clave mejorada	H.235.6	8.6.2
B.2.6.3	Actualización y sincronización de clave basada en el tipo de cabida útil	H.235.6	8.6.3
B.3	Aspectos relativos a RTP/RTCP	H.235.6	9.3
B.3.1	Vectores de inicialización	H.235.6	9.3.1
B.3.1.1	Vector de inicialización CBC	H.235.6	9.3.1.1
B.3.1.2	Vector de inicialización EOFB	H.235.6	9.3.1.2
B.3.2	Relleno	H.235.6	9.3.2
B.3.3	Protección RTCP	H.235.6	9.3.3
B.3.4	Tren de cabida útil seguro	H.235.6	9.3.4
B.3.5	Interfuncionamiento con J.170	H.235.6	9.3.5
B.4	Señalización RAS/procedimientos de autenticación	H.235.0	8.3
B.4.1	Introducción	H.235.0	–
B.4.2	Autenticación de punto extremo – controlador de acceso (no basada en acuerdo)	H.235.0	8.3.1

Cuadro IV.1/H.235.0 – Tabla de correspondencia de cláusulas

Cláusula de H.235v3, enm.1, corr.1	Título	Recomendación de la subserie H.235v4.x	Cláusula
B.4.3	Autenticación de punto extremo – controlador de acceso (basada en acuerdo)	H.235.0	8.3.2
B.4.3.1	Contraseña con criptación simétrica	H.235.0	8.3.2.1
B.4.3.2	Contraseña con generación numérica	H.235.0	8.3.2.2
B.4.3.3	Certificado con firmas	H.235.0	8.3.3.3
B.5	Interacciones no relacionadas con terminales	H.235.6	8.7
B.5.1	Pasarela	H.235.6	8.7.1
B.6	Gestión de clave en el canal RAS	H.235.0	8.4
B.7	Función seudoaleatoria (PRF)	H.235.0	10
Anexo C	**Aspectos específicos del protocolo H.324**	**H.235.0**	**Anexo B**
Anexo D	**Perfil de seguridad básico**	**H.235.1**	
D.1	Introducción	H.235.1	
D.2	Convenios	H.235.1	5
D.3	Alcance	H.235.1	1
D.4	Abreviaturas	H.235.1	4
D.5	Referencias normativas	H.235.1	2.1
D.6	Perfil de seguridad básico	H.235.1	
D.6.1	Visión general	H.235.1	6.1
D.6.1.1	Perfil de seguridad básico	H.235.1	6.2
D.6.1.2	Perfil de seguridad de criptación vocal	H.235.6	6.1
D.6.2	Autenticación e integridad	H.235.1	3.1
D.6.3	Requisitos H.323	H.235.1	6.3
D.6.3.1	Visión general	H.235.1	6.4
D.6.3.2	Detalles de la autenticación de mensajes señalización basada en claves simétricas (procedimiento I)	H.235.1	7
D.6.3.3	Cálculo del número generador basado en contraseñas	H.235.1	7.1
D.6.3.3.1	HMAC-SHA1-96	H.235.1	7.2
D.6.3.3.2	Autenticación e integridad	H.235.1	7.3
D.6.3.3.3	Sólo autenticación (procedimiento IA)	H.235.1	8
D.6.3.4	Ilustración de la utilización del procedimiento I	H.235.1	9
D.6.3.4.1	Autenticación e integridad de los mensajes RAS	H.235.1	9.1

Cuadro IV.1/H.235.0 – Tabla de correspondencia de cláusulas

Cláusula de H.235v3, enm.1, corr.1	Título	Recomendación de la subserie H.235v4.x	Cláusula
D.6.3.4.2	Autenticación e integridad de los mensajes H.225.0	H.235.1	9.2
D.6.3.4.3	Autenticación e integridad de los mensajes H.245	H.235.1	9.3
D.6.4	Escenario con encaminamiento directo	H.235.1	9.4
D.6.5	Soporte de los servicios fuera del terminal	H.235.1	10
D.6.6	Compatibilidad con H.235 versión 1	H.235.1	11
D.6.7	Comportamiento multidifusión	H.235.1	12
D.7	Perfil de seguridad de criptación vocal	H.235.6	6.1
D.7.1	Gestión de claves	H.235.6	8.5
D.7.2	Actualización de claves y sincronización	H.235.6	8.6
D.7.3	DES triple en modo CBC exterior	H.235.6	9.4
D.7.4	Algoritmo DES que funciona en modo EOFB	H.235.6	9.5
D.7.5	DES triple en el modo EOFB exterior	H.235.6	9.6
D.8	Interceptación legal	H.235.6	10
D.9	Lista de mensajes de señalización seguros	H.235.1	13
D.9.1	RAS H.225.0	H.235.1	13.1
D.9.2	Señalización de llamada H.225.0	H.235.1	13.2
D.9.3	Control de llamada H.245	H.235.1	13.3
D.10	Utilización de sendersID y de generalID	H.235.1	14
D.11	Lista de identificadores de objeto	H.235.1 H.235.6	15 11
D.12	Bibliografía	H.235.1 H.235.6	2.2 2.2
Anexo E	**Perfil de seguridad de firmas**	**H.235.2**	
E.1	Visión general	H.235.2	6
E.2	Convenios acerca de las especificaciones	H.235.2	5
E.3	Requisitos H.323	H.235.2	6.1
E.4	Servicios de seguridad	H.235.2	5
E.5	Detalles de las firmas digitales con parejas de claves privada/clave pública (procedimiento II)	H.235.2	7

Cuadro IV.1/H.235.0 – Tabla de correspondencia de cláusulas

Cláusula de H.235v3, enm.1, corr.1	Título	Recomendación de la subserie H.235v4.x	Cláusula
E.6	Procedimientos para la conferencia multipunto	H.235.2	8
E.7	Autenticación de extremo a extremo (procedimiento III)	H.235.2	9
E.8	Autenticación solamente	H.235.2	10
E.9	Autenticación e integridad	H.235.2	11
E.10	Cálculo de la firma digital	H.235.2	12
E.11	Verificación de la firma digital	H.235.2	13
E.12	Tratamiento de los certificados	H.235.2	14
E.13	Ilustración del empleo del procedimiento II	H.235.2	15
E.13.1	Autenticación, integridad y no repudio de mensajes RAS	H.235.2	15.1
E.13.2	Autenticación solamente de mensajes RAS	H.235.2	15.2
E.13.3	Autenticación, integridad y no repudio de mensaje H.225.0	H.235.2	15.3
E.13.4	Autenticación e integridad de los mensajes H.245	H.235.2	15.4
E.14	Compatibilidad con la versión 1 de H.235	H.235.2	16
E.15	Comportamiento multidifusión	H.235.2	17
E.16	Lista de mensajes de señalización seguros	H.235.2	18
E.16.1	RAS H.225	H.235.2	18.1
E.16.2	Señalización de llamada H.225.0	H.235.2	18.2
E.17	Utilización de sendersID y generalID	H.235.2	19
E.18	Lista de identificadores de objeto	H.235.2	20
Apéndice IV (Anexo E)	Bibliografía	H.235.2	2.2
Anexo F	**Perfil de seguridad híbrido**	**H.235.3**	
F.1	Visión general	H.235.3	6
F.2	Referencias normativas	H.235.3	2.1
F.3	Acrónimos	H.235.3	4
F.4	Convenios de especificación	H.235.3	5
F.5	Requisitos relativos a H.323	H.235.3	6.1
F.6	Autenticación e integridad	H.235.3	6.2
F.7	Procedimiento IV	H.235.3	7

Cuadro IV.1/H.235.0 – Tabla de correspondencia de cláusulas

Cláusula de H.235v3, enm.1, corr.1	Título	Recomendación de la subserie H.235v4.x	Cláusula
F.8	Asociación de seguridad para llamadas concurrentes	H.235.3	8
F.9	Actualización de clave	H.235.3	9
F.10	Ejemplos ilustrativos	H.235.3	11
F.11	Comportamiento multidifusión	H.235.3	12
F.12	Lista de mensajes de señalización securizados	H.235.3	13
F.12.1	RAS H.225.0	H.235.3	13.1
F.12.2	Señalización de llamada H.225.0 (dominio administrativo simple)	H.235.3	13.2
F.12.3	Señalización de llamada H.225.0 (dominio administrativo múltiple)	H.235.3	13.3
F.13	Lista de identificadores de objeto	H.235.3	14
Apéndice IV	Bibliografía	H.235.3	2.2
Anexo G	**Utilización del protocolo de transporte en tiempo real seguro (SRTP, *secure real-time transport protocol*) junto con el protocolo de gestión de clave MIKEY en H.235**	**H.235.7**	
G.1	Alcance	H.235.7	1
G.2	Referencias	H.235.7	2
G.2.1	Referencias normativas	H.235.7	2.1
G.2.2	Referencias informativas	H.235.7	2.2
G.3	Términos y definiciones	H.235.7	3
G.4	Símbolos y siglas	H.235.7	4
G.5	Convenios de especificación	H.235.7	5
G.6	Introducción	H.235.7	6
G.7	Panorama general e hipótesis	H.235.7	7
G.7.1	Funcionamiento de MIKEY en el "nivel de sesión"	H.235.7	7.1
G.7.2	Funcionamiento de MIKEY en el "nivel de medios"	H.235.7	7.2
G.7.3	Negociación de capacidad MIKEY	H.235.7	7.3
G.8	Perfil de seguridad utilizando técnicas de seguridad simétricas	H.235.7	8
G.8.1	Terminación de una llamada H.323	H.235.7	8.1
G.8.2	Creación de nuevas claves TGK y actualización del CSB	H.235.7	8.2
G.8.3	Soporte de tunelización H.245	H.235.7	8.3
G.8.4	Algoritmos SRTP	H.235.7	8.4

Cuadro IV.1/H.235.0 – Tabla de correspondencia de cláusulas

Cláusula de H.235v3, enm.1, corr.1	Título	Recomendación de la subserie H.235v4.x	Cláusula
G.8.5	Lista de identificadores de objetos	H.235.7	8.5
G.9	Perfil de seguridad que utiliza técnicas de seguridad asimétricas	H.235.7	9
G.9.1	Terminación de una llamada H.323	H.235.7	9.1
G.9.2	Creación de nuevas claves TGK y actualización del CSB	H.235.7	9.2
G.9.3	Soporte de tunelización H.245	H.235.7	9.3
G.9.4	Algoritmos SRTP	H.235.7	9.4
G.9.5	Lista de identificadores de objeto	H.235.7	9.5
G.I	Opción MIKEY-DHHMAC	H.235.7	Apéndice I
G.I.1	Terminación de una llamada H.323	H.235.7	I.1
G.I.2	Creación de nuevas claves TGK y actualización del CSB	H.235.7	I.2
G.II	Utilización del anexo I de H.235 para establecer un secreto precompartido	H.235.7	Apéndice II
G.II.1	Terminación de una llamada H.323	H.235.7	II.1
G.II.2	Creación de nuevas claves TGK y actualización del CSB	H.235.7	II.2
Anexo H	**Gestión de clave RAS**	**H.235.5**	
H.1	Introducción	H.235.5	–
H.2	Alcance	H.235.5	1
H.3	Referencias	H.235.5	2
H.3.1	Referencias normativas	H.235.5	2.1
H.3.2	Referencias informativas	H.235.5	2.2
H.4	Definiciones	H.235.5	3
H.5	Abreviaturas	H.235.5	4
H.6	Marco básico	H.235.5	6
H.6.1	Capacidades de negociación mejoradas en H.235v3	H.235.5	6.1
H.6.2	Utilización entre punto extremo y controlador de acceso	H.235.5	6.2
H.6.3	Utilización de perfiles entre controladores de acceso	H.235.5	6.3
H.6.4	Criptación y autenticación de canales de señalización	H.235.5	6.4
H.7	Perfil de seguridad específico (SP1)	H.235.5	7
H.8	Extensiones al marco (informativo)	H.235.5	9
H.8.1	Utilización de la clave maestra para securizar el canal de señalización de llamada mediante TLS	H.235.5	9.1

Cuadro IV.1/H.235.0 – Tabla de correspondencia de cláusulas

Cláusula de H.235v3, enm.1, corr.1	Título	Recomendación de la subserie H.235v4.x	Cláusula
H.8.1.1	Registro de punto extremo	H.235.5	9.1.1
H.8.2	Utilización de certificados para autenticar al controlador de acceso	H.235.5	9.2
H.8.3	Utilización de otros mecanismos de seguridad de la señalización	H.235.5	9.3
H.9	Amenazas (informativo)	H.235.5	10
H.9.1	Ataque pasivo	H.235.5	10.1
H.9.2	Ataques por denegación de servicio	H.235.5	10.2
H.9.3	Ataques de hombre-en-el-medio	H.235.5	10.3
H.9.4	Ataques por intentos de adivinar	H.235.5	10.4
H.9.5	Media clave del controlador de acceso no criptada	H.235.5	10.5
Anexo I	**Soporte de llamadas con encaminamiento directo**	**H.235.4**	
I.1	Alcance	H.235.4	1
I.2	Introducción	H.235.4	6
I.3	Convenios de especificación	H.235.4	5
I.4	Términos y definiciones	H.235.4	3
I.5	Símbolos y abreviaturas	H.235.4	4
I.6	Referencias normativas	H.235.4	2
I.7	Generalidades	H.235.4	7
I.8	Limitaciones	H.235.4	8
I.9	Procedimiento DRC	H.235.4	9
I.10	Procedimiento de cálculo de clave basado en PRF	H.235.4	12
I.11	Procedimiento de cálculo de clave basado en FIPS-140	H.235.4	13
I.12	Lista de identificadores de objeto	H.235.4	14
Apéndice I (Anexo I)	Bibliografía	H.235.4	2.2

Apéndice V

Tabla de correspondencia de las figuras de la H.235v3 y su enmienda 1 y corrigendum 1, con las Recomendaciones de la subserie H.235v4

El presente apéndice es informativo y muestra el lugar de las figuras de la H.235v3, y su enmienda 1 y corrigendum 1, en las Recomendaciones de la subserie H.235v4.

Cuadro V.1/H.235.0 – Tabla de correspondencia de figuras

Figura de H.235v3, enm.1, corr.1	Título	Recomendación de la subserie H.235v4.x	Figura
Figura 1	Diffie-Hellman con autenticación facultativa	H.235.0	4
Figura 2a	Contraseña con criptación simétrica; dos pasos	H.235.0	5
Figura 2b	Contraseña con criptación simétrica; tres pasos	H.235.0	6
Figura 3a	Contraseña con generación numérica; dos pasos	H.235.0	7
Figura 3b	Contraseña con generación numérica; tres pasos	H.230.0	8
Figura 4a	Certificado con firma; dos pasos	H.235.0	9
Figura 4b	Certificado con firma; tres pasos	H.235.0	10
Figura 5	Criptación de trenes de medios	H.235.6	7
Figura 6	Descriptación de trenes de medios	H.235.6	8
Figura 7	Formato de paquete RTP para la antiinundación de medios	H.235.6	9
Figura I.1	Apropiación de texto cifrado en modo ECB	H.235.6	I.1
Figura I.2	Apropiación de texto cifrado en modo CBC	H.235.6	I.2
Figura I.2a	Relleno de ceros en modo CBC	H.235.6	I.3
Figura I.3	Relleno de ceros en modo CFB	H.235.6	I.4
Figura I.4	Relleno de ceros en modo OFB	H.235.6	I.5
Figura I.4.1	Modo EOFB con relleno de ceros	H.235.6	I.6
Figura I.5	Relleno prescrito por RTP	H.235.6	I.7
Figura I.6	Testigos	H.235.0	I.1
Figura I.7	Escenario con servidor fuera del terminal	H.235.0	I.2
Figura B.1	Visión general	H.235.0	2
Figura B.1.1	Distribución o actualización de clave de sesión sin acuse del terminal director a(los) subordinado(s)	H.235.6	4
Figura B.1.2	Actualización de clave de sesión en el canal lógico del subordinado	H.235.6	5

Cuadro V.1/H.235.0 – Tabla de correspondencia de figuras

Figura de H.235v3, enm.1, corr.1	Título	Recomendación de la subserie H.235v4.x	Figura
Figura B.1.3	Actualización de clave de sesión en el canal lógico de terminal director	H.235.6	6
Figura B.2	Contraseña con criptación simétrica	H.235.0	11
Figura B.3	Contraseña con generación numérica	H.235.0	12
Figura B.4	Certificado con firmas	H.235.0	13
Figura D.1	Ilustración de la utilización del procedimiento I en un escenario GK-GK con ambos EP en zonas de encaminamiento por controlador de acceso	H.235.1	1
Figura D.2	Ilustración de la utilización del procedimiento I en un escenario mixto con EP1 en una zona de encaminamiento por controlador de acceso y EP2 en una zona de encaminamiento directo	H.235.1	2
Figura D.3	Ilustración de la utilización del procedimiento I en un escenario con ambos EP en zonas que utilizan un modelo de GK con encaminamiento directo	H.235.1	3
Figura D.4	Criptación DES triple en modo CBC exterior	H.235.6	10
Figura D.5	Criptación DES triple en modo EOFB exterior	H.235.6	11
Figura E.1	Utilización simultánea de la seguridad salto por salto y la autenticación de extremo a extremo	H.235.2	1
Figura E.2	Ilustración de la utilización de claves públicas en un modelo encaminado por GK-GK	H.235.2	2
Figura F.1	Asociación de seguridad para llamadas concurrentes	H.235.3	1
Figura F.2	Diagrama de flujo en un dominio administrativo simple	H.235.3	2
Figura F.3	Diagrama de flujo en un dominio administrativo múltiple	H.235.3	3
Figura G.1	Escenario	H.235.7	1
Figura G.2	Hipótesis de seguridad con MIKEY y SRTP	H.235.7	2
Figura G.3	Caso salto por salto sólo con secretos compartidos	H.235.7	3

Cuadro V.1/H.235.0 – Tabla de correspondencia de figuras

Figura de H.235v3, enm.1, corr.1	Título	Recomendación de la subserie H.235v4.x	Figura
Figura G.4	Ejemplo del punto extremo B llamando al punto extremo A (llamada encaminada por GK) con procesamiento precompartido MIKEY	H.235.7	4
Figura G.5	Procesamiento precompartido MIKEY mediante EP B	H.235.7	5
Figura G.6	Procesamiento precompartido MIKEY mediante EP A	H.235.7	6
Figura G.7	Ejemplo del punto extremo B terminando una llamada	H.235.7	7
Figura G.8	Ejemplo del punto extremo B actualizando una clave	H.237.7	8
Figura G.9	Escenario de extremo a extremo utilizando PKI (múltiples GK)	H.235.7	9
Figura G.10	Ejemplo del EP B llamando al EP A (llamada encaminada por múltiples GK) con protocolo MIKEY-PK-SIGN	H.235.7	10
Figura G.11	Procesamiento del protocolo MIKEY-PK-SIGN por el EP B	H.235.7	11
Figura G.12	Procesamiento del protocolo MIKEY-PK-SIGN por el EP A	H.235.7	12
Figura G.13	Ejemplo de terminación de llamada por el punto extremo B	H.235.7	13
Figura G.14	Ejemplo de iniciación de la creación de nuevas claves TGK y actualización de claves por el EP B (iniciador)	H.235.7	14
Figura G.I-1	Ejemplo del punto extremo B llamando al punto extremo A (llamada encaminada por GK) con el protocolo MIKEY-DHHMAC	H.235.7	I.1
Figura G.I-2	Ejemplo de terminación de una llamada por el punto extremo B	H.235.7	I.2
Figura G.I-3	Ejemplo del punto extremo B actualizando una clave	H.235.7	I.3
Figura G.II-1	Ejemplo del punto extremo B llamando al punto extremo A (sin encaminamiento por GK) con secreto precompartido MIKEY y DRC conforme a H.235.4	H.235.7	II.1
Figura H.1	Flujo de información para perfil de seguridad y TLS	H.235.5	1
Figura I.1	Caso de una llamada con encaminamiento directo	H.235.4	1
Figura I.2	Flujo básico de comunicación	H.235.4	2

Apéndice VI

Tabla de correspondencia de los cuadros de la H.235v3 y su enmienda 1 y corrigendum 1, con las Recomendaciones de la subserie H.235v4

El presente apéndice es informativo y muestra el lugar donde figuran los cuadros de la H.235v3, y su enmienda 1 y corrigendum 1, en las Recomendaciones de la subserie H.235v4.

Cuadro VI.1/H.235.0 – Tabla de correspondencia de cuadros

Cuadro de H.235v3, enm.1, corr.1	Título	Recomendación de la subserie H.235v4.x	Cuadro
Cuadro 1	Identificador de objeto para la criptación NULL	H.235.6	2
Cuadro 2	Identificadores de objeto para la criptación de DTMF H.245	H.235.6	3
Cuadro 3	Identificadores de objeto utilizados para la antiinundación	H.235.6	5
Cuadro I.1	Identificadores de objeto utilizados en I.4.6	H.235.0	I.1
Cuadro D.1	Resumen de los perfiles de seguridad del anexo D	----	---
Cuadro D.2	Perfil de seguridad básico	H.235.1	1
Cuadro D.3	Perfil de criptación vocal	H.235.6	1
Cuadro D.4	Grupos Diffie-Hellman	H.235.6	4
Cuadro D.5	Utilización de SendersID y GeneralID	H.235.1	2
Cuadro D.6	Identificadores de objeto utilizados en el anexo D	H.235.1 H.235.6	3 6
Cuadro E.1	Perfil de seguridad de firmas	H.235.2	1
Cuadro E.2	Utilización de SendersID y GeneralID	H.235.2	2
Cuadro E.3	Identificadores de objeto utilizados por el anexo E	H.235.2	3
Cuadro F.1	Visión general del perfil de seguridad híbrida	H.235.3	1
Cuadro F.2	Identificadores de objeto utilizados en el anexo F	H.235.3	2
Cuadro G.1	Protocolos de gestión de claves MIKEY	H.235.7	1
Cuadro H.1	Elementos de los perfiles	H.235.5	1
Cuadro I.0	Cálculo de las claves adicionales y de criptación a partir de un secreto compartido	H.235.4	1
Cuadro I.1	Identificadores de objeto utilizados por H.235.4	H.235.4	2

SERIES DE RECOMENDACIONES DEL UIT-T

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

Impreso en Suiza
Ginebra, 2006