UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T H.235

(02/98)

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

SERIE H: SISTEMAS AUDIOVISUALES Y MULTIMEDIOS

Infraestructura de los servicios audiovisuales – Aspectos de los sistemas

---

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

Recomendación UIT-T H.235

(Anteriormente Recomendación del CCITT)

RECOMENDACIONES DE LA SERIE H DEL UIT-T

SISTEMAS AUDIOVISUALES Y MULTIMEDIOS

Características de los canales de transmisión para usos distintos de los telefónicos	H.10–H.19
Utilización de circuitos de tipo telefónico para telegrafía armónica	H.20–H.29
Utilización de circuitos o cables telefónicos para transmisiones telegráficas de diversos tipos o transmisiones simultáneas	H.30–H.39
Utilización de circuitos de tipo telefónico para telegrafía facsímil	H.40–H.49
Características de las señales de datos	H.50–H.99
CARACTERÍSTICAS DE LOS SISTEMAS VIDEOTELEFÓNICOS	H.100–H.199
INFRAESTRUCTURA DE LOS SERVICIOS AUDIOVISUALES	
Generalidades	H.200–H.219
Multiplexación y sincronización en transmisión	H.220–H.229
Aspectos de los sistemas	**H.230–H.239**
Procedimientos de comunicación	H.240–H.259
Codificación de imágenes vídeo en movimiento	H.260–H.279
Aspectos relacionados con los sistemas	H.280–H.299
Sistemas y equipos terminales para los servicios audiovisuales	H.300–H.399

Para más información, véase la Lista de Recomendaciones del UIT-T.

RECOMENDACIÓN UIT-T H.235

SEGURIDAD Y CRIPTADO PARA TERMINALES MULTIMEDIOS DE LA SERIE H (BASADOS EN LAS RECOMENDACIONES H.323 Y H.245)

Resumen

La presente 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* (cifrado de datos). El esquema propuesto es aplicable a conferencias punto a punto y multipunto para cualesquiera terminales que utilicen la Recomendación H.245 como su protocolo de control.

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 segura en tiempo real por redes inseguras plantea generalmente dos problemas importantes: *autenticación* y *privacidad*.

La presente Recomendación describe la infraestructura de seguridad y técnicas de privacidad específicas que han de emplear los terminales multimedios 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. La presente Recomendación proporciona el protocolo y algoritmos necesarios entre las entidades H.323.

La presente Recomendación utiliza las facilidades generales admitidas en la Recomendación 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.

La presente 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. La presente Recomendación admite 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). La presente Recomendación admite 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 admitan el mayor número posible de algoritmos para lograr el interfuncionamiento. Esto es paralelo al concepto de que el soporte del protocolo H.245 no garantiza el interfuncionamiento entre códecs de dos entidades.

Orígenes

La Recomendación UIT-T H.235 ha sido preparada por la Comisión de Estudio 16 (1997-2000) del UIT-T y fue aprobada por el procedimiento de la Resolución N.° 1 de la CMNT el 6 de febrero de 1998.

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 Conferencia Mundial de Normalización de las Telecomunicaciones (CMNT), 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 N.° 1 de la CMNT.

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

NOTA

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

PROPIEDAD INTELECTUAL

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

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

ÍNDICE

Recomendación H.235

SEGURIDAD Y CRIPTADO PARA TERMINALES MULTIMEDIOS DE LA SERIE H (BASADOS EN LAS RECOMENDACIONES H.323 Y H.245)

(Ginebra, 1998)

1 Alcance

La finalidad primaria de la presente Recomendación es proporcionar la autenticación, privacidad e integridad dentro del marco de los protocolos vigentes de la serie H. El texto actual de esta Recomendación (1998) proporciona detalles sobre la implementación con la Recomendación H.323. Se prevé que este marco funcione junto con otros protocolos de la serie H que utilizan el protocolo H.245 como su protocolo de control.

Entre los objetivos adicionales de esta Recomendación cabe citar:

1) La arquitectura de seguridad se debe desarrollar como un marco extensible y flexible para aplicar un sistema de seguridad para los terminales de la serie H. 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) La presente Recomendación no excluye la integración de otras funciones de seguridad en entidades H.3xx que puedan protegerlas contra ataques de la red.

4) La presente 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 asegurados 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 la presente Recomendación.

6) Se prevé el funcionamiento en un entorno mixto (entidades seguras e inseguras).

7) La presente 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 debe ser parte de la presente Recomendación.)

La arquitectura de seguridad, descrita en la presente Recomendación, no supone que los participantes están familiarizados entre sí. 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 escucha furtiva en la red o algún otro método de desviar los trenes de medios.

La Recomendación H.323 (1996) proporciona los medios para conducir una conferencia de audio, vídeo y datos entre dos o más partes, pero no proporciona el mecanismo para que cada participante

pueda autenticar la identidad de los otros participantes, ni proporciona los medios para que las comunicaciones sean privadas (es decir, criptado de los trenes).

Las Recomendaciones H.323, H.324 y H.310 utilizan los procedimientos de señalización de canal lógico de la Recomendación 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 los receptores que pueden decodificar 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.

2 Referencias normativas

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes.

– Recomendación UIT-T H.225.0 (1998), *Protocolos de señalización de llamadas y paquetización de trenes de medios para sistemas de comunicaciones multimedios basadas en paquetes.*

– Recomendación UIT-T H.245 (1998), *Protocolo de control para comunicaciones multimedios*.

– Recomendación UIT-T H.323 (1998), *Sistemas de comunicaciones multimedios basados en paquetes.*

– Recomendación UIT-T Q.931 (1993), *Especificación de la capa 3 de la interfaz usuario-red de la red digital de servicios integrados para el control de llamada básica.*

– Recomendación UIT-T X.509 (1997) | ISO/CEI 9594-8:1997, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio - Marco de autenticación.*

– Recomendación X.800 del CCITT (1991), *Arquitectura de seguridad para 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, *Tecnolología 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 9798-2:1994, *Information technology – Security techniques – Entity authentication – Part 2: Mechanisms using symmetric encipherment algorithms.*

– ISO/CEI 9798-3:1993, *Information technology – Security techniques – Entity authentication mechanisms – Part 3: Entity authentication using public a key algorithm.*

– ISO/CEI 9798-4:1995, *Information technology – Security techniques – Entity authentication – Part 4: Mechanisms using a cryptographic check function.*

– ATKINSON (R.): Security Architecture for the Internet Protocol, RFC 1825, *Internet Engineering Task Force, 1995*.

– KRAWCZYK (H.), BELLARE (M.), CANETTI (R.): HMAC: Keyed-Hashing for Message Authentication, RFC 2104, *Internet Engineering Task Force, 1997*.

3 Definiciones

A los efectos de la presente Recomendación se aplican las definiciones que figuran en la cláusula 3 de las Recomendaciones H.323, H.225.0 y H.245 juntos con las de esta cláusula. Algunos de los siguientes términos se utilizan como se define en la Rec. X.800 del CCITT | ISO 7428-2 y las Recomendaciones X.803, X.810 y X.811.

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 (X.800).

3.2 autenticación: Provisión de seguridad de la identidad alegada de una entidad (X.811).

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

3.4 ataque: Actividades realizadas para anular 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 anulan 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 lo servicios de integridad y autenticación de origen de datos para los datos (X.810). En la presente 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, clave: Algoritmo criptográfico, una transformación 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.

3.9 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, archivo y aplicación de claves de acuerdo con una política de seguridad (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 la cifra.

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 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 (X.810).

3.18 amenaza: Violación potencial de la seguridad (X.800).

4 Símbolos y abreviaturas

En esta Recomendación se utilizan las siguientes siglas.

DSS Norma sobre firmas digitales (*digital signature standard*)

IPSEC Seguridad de protocolo Internet (*Internet protocol security*)

QOS Calidad de servicio (*quality of service*)

RSA Rivest, Shamir y Adleman (algoritmo de clave pública)

SDU Unidad de servicio de datos (*service data unit*)

TLS Seguridad de nivel de transporte (*transport level security*)

5 Convenios

En la presente Recomendación se utilizan los siguientes convenios:

– El tiempo futuro indica un requisito obligatorio.

– El condicional "debería" indica una acción aconsejada pero facultativa.

– La palabra "puede" indica una acción facultativa, en vez de una recomendación de que se haga algo.

Las referencias a cláusulas, subcláusulas, anexos y apéndices se relacionan con puntos de la presente Recomendación, a menos que se indique explícitamente otra Recomendación. Por ejemplo, "1.4" hace referencia a la subcláusula 1.4 de la presente Recomendación; 6.4/H.245 hace referencia a la subcláusula 6.4 de la Recomendación H.245.

La presente 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 se representan en el tipo de letra negritas [**fluctuación de retardo de fase máxima** (**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 cuya letra inicial aparece en mayúsculas [**Llamada en curso** (**Call Proceeding**)].

6 Presentación del sistema

6.1 Resumen

1) El canal de señalización de llamada se puede asegurar utilizando TLS [**TLS**] o IPSEC [**13/IPSEC**] en un puerto conocido seguro (H.225.0).

2) Los usuarios pueden ser autenticados durante la conexión de llamada inicial, en el proceso de asegurar el canal H.245 y/o intercambiando 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 **Apertura canal lógico** (**OpenLogicalChannel)** o **Acuse apertura canal lógico (OpenLogicalChannelAck)**.

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

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.

La presente 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 la presente 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, la presente Recomendación proporciona la señalización para completar distintos casos de pregunta/respuesta. 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.

Como una tercera opción, la autenticación puede ser completada dentro del contexto de un protocolo de seguridad distinto, tal como TLS [**TLS**] o IPSEC [**13/IPSEC**].

La autenticación bidireccional y unidireccional puede ser admitida por entidades pares. Esta autenticación se puede producir en algunos o en todos los canales de comunicación.

Todos los mecanismos de autenticación específicos descritos en la presente 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 la presente 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 llamada

Hay por lo menos dos razones para motivar la seguridad del canal de establecimiento de llamada (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 constricciones de una política de autorización específica del servicio están fuera del alcance de la presente Recomendación.

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

El canal de control de llamada (H.245) debe estar asegurado también de alguna manera 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 encriptados 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 por el cual el canal H.245 es seguro 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

La presente 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 **Apertura canal lógico** H.245 están protegidas.

El canal seguro H.245 puede funcionar con diferentes características 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 **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 la **Apertura canal lógico**. 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 criptada o cualesquiera canales lógicos del tipo **datos criptados** (**encryptedData)** serán considerados un elemento de confianza de la conexión; esto incluye las unidades de control multipunto y las cabeceras. 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". La presente 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, la presente Recomendación contiene disposiciones para que las entidades que utilizan el protocolo H.235 admitan una técnica de recuperación de claves dentro de los elementos de señalización.

Se debe admitir 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 tercero de confianza (TTP, *trusted third party*). Esta facilidad seguirá siendo objeto de estudio.

6.7 No repudio

Queda en estudio.

7 Procedimientos de establecimiento de la conexión

7.1 Introducción

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 debe transferir información sobre cualquier discordancia de seguridad y el terminal llamante tendrá que determinar el problema por otros medios. Cuando el terminal llamante recibe un mensaje de ACUSE DE CONEXIÓN 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 debe considerarse un error de protocolo y la conexión será terminada.

8 Señalización y procedimientos H.245

En general, los aspectos de privacidad de los canales de medio son controlados de la misma manera que cualquier otro parámetro de codificación; cada terminal indica sus capacidades, la fuente de los datos selecciona un formato que ha de utilizar y el receptor acepta o rechaza el modo. Todos los aspectos del mecanismo independientes del transporte, tales como selección de algoritmo, se indican en elementos de canal lógico genéricos. Los elementos específicos de transporte, tales como la sincronización de algoritmos de clave/criptación son transferidos en estructuras específicas de transporte.

8.1 Funcionamiento seguro del canal H.245

Suponiendo que los procedimientos de conexión mencionados en la cláusula anterior indiquen un modo de funcionamiento seguro, se llevará a cabo la toma de contacto y la autenticación negociadas para el canal lógico H.245 antes de que se intercambie cualquier mensaje H.245. Si se ha negociado,

cualquier intercambio de certificados se producirá utilizando este mecanismo apropiado para los terminales de la serie H. Después de completar la seguridad del canal H.245, los terminales utilizarán el protocolo H.245 de la misma manera que si funcionasen en un modo inseguro.

8.2 Funcionamiento inseguro del canal H.245

Como otra posibilidad, el canal H.245 puede funcionar de una manera insegura y las dos entidades abren un canal lógico seguro con el cual efectuar la autenticación y/o la derivación de secreto compartido. Por ejemplo, se puede utilizar TLS o IPSEC abriendo un canal lógico con el **tipo de datos** que contiene un valor para **datos de criptación (encryptionData)**. Este canal se utilizaría para derivar un secreto compartido que protege cualesquiera clave de sesión de medios o para transportar la **sincronización de criptación (encryptionSync)**.

8.3 Intercambio de capacidades

De acuerdo con los procedimientos de 8.3/H.245 (Procedimientos de intercambio de capacidades) y las Recomendaciones apropiadas relativas a sistemas de la serie H, los puntos extremos intercambian capacidades utilizando mensajes H.245. Estos conjuntos de capacidades pueden contener definiciones que indiquen parámetros de seguridad y criptación. Por ejemplo, un punto extremo pudiera proporcionar capacidades para enviar y recibir vídeo H.261. Puede señalizar también la posibilidad de enviar y recibir vídeo H.261 criptado.

Cada algoritmo de criptación que se utilice junto con un códec de medios determinado, supone una nueva definición de capacidad. Como con cualquier otra capacidad, los puntos extremos pueden suministrar códecs codificados independientes y dependientes en su intercambio. Esto permitirá a los puntos extremos ampliar sus capacidades de seguridad basadas en la tara y recursos disponibles.

Una vez completado el intercambio de capacidades, los puntos extremos pueden abrir canales lógicos seguros para los medios, de la misma manera que lo harían en un modo inseguro.

8.4 Cometido de terminal director

La determinación de terminal director-subordinado de H.245 se utiliza para establecer la entidad directora a los efectos del funcionamiento de canales bidireccionales y la resolución de otros conflictos. Este cometido de director se utiliza también en los métodos de seguridad. Aunque los modos de seguridad de un tren de medios son fijados por la fuente (en deferencia a las capacidades del receptor), el director es el punto extremo que genera la clave de criptación. Esta generación de la clave de criptación se hace con independencia de si el director es el receptor o la fuente de los medios criptados. Para efectuar el funcionamiento de canales multidistribución con claves compartidas, el controlador multipunto (también el director) debe generar las claves.

8.5 Señalización de canal lógico

Los puntos extremos abren canales lógicos de medios seguros de la misma manera que abren canales lógicos de medios inseguros. Cada canal puede funcionar de una manera completamente independiente con respecto a los otros canales, en particular cuando esto incumbe a la seguridad. El modo particular será definido en el campo **tipo datos (dataType)** de **apertura canal lógico**. La clave de criptación inicial se transferirá en **Apertura de canal lógico** o **Acuse apertura canal lógico** dependiendo de la relación director/subordinado del originador de **Apertura canal lógico**.

El **Acuse apertura canal lógico** actuará como una confirmación del modo de criptación. Si **apertura canal lógico** no es aceptable al recibiente, se devolverá **tipo datos no admitido** (**dataTypeNotSupported)** o **tipo datos no disponible** (**dataTypeNotAvailabl**e) (condición transitoria) en el campo de causa de **Rechazo apertura canal lógico (OpenLogicalCbannelReject)**.

Durante el intercambio de protocolos que establece el canal lógico, la clave de criptación será transferida del terminal director al subordinado (con independencia de quién inició **Apertura canal lógico**). Para los canales de medios abiertos por un punto extremo (que no sea el director), el director devolverá la clave de criptación inicial y el punto de sincronización inicial en **Acuse apertura canal lógico** (en el campo **sincronización de criptación**). Para los canales de medios abiertos por el director, **Apertura canal lógico** incluirá la clave de criptación inicial y el punto de sincronización en el campo **sincronización de criptación**.

9 Procedimientos multipunto

9.1 Autenticación

La autenticación se producirá entre un punto extremo y la MC(U) de la misma manera que se haría en una conferencia punto a punto. La MC(U) fijará la política relativa al nivel y rigor de autenticación. Como se indica en 6.6, se confía en la MC(U); los puntos extremos existentes en una conferencia pueden estar limitados por el nivel de autenticación empleado por la MC(U). Las nuevas instrucciones **petición conferencia/respuesta conferencia** permiten que los puntos extremos obtengan de la MC(U) los certificados de otros participantes en la conferencia. Como se indica en los procedimientos H.245, los puntos extremos en una conferencia multipunto pueden solicitar cualquier otro certificado de punto extremo por medio del MC, pero no pueden realizar la autenticación criptográfica directa dentro del canal H.245.

9.2 Privacidad

La MC(U) ganará todos los intercambios director/subordinado y como tal suministrará las claves de criptación a los participantes en una conferencia multipunto. La privacidad para cada fuente dentro de una sesión común (suponiendo multidistribución) se puede lograr con claves individuales o comunes. Estos dos modos pueden ser elegidos arbitrariamente por la MC(U) y no serán controlables desde ningún punto extremo particular, salvo en modos permitidos por la política de la MC(U). En otras palabras, se puede utilizar una clave común a través de múltiples canales lógicos abiertos por diferentes fuentes.

10 Señalización y procedimientos de autenticación

10.1 Introducción

Se puede utilizar dos tipos de autenticación. El primer tipo se basa en criptación simétrica que no requiere un contacto previo entre las entidades comunicantes. El segundo tipo se basa en la capacidad de tener algún secreto compartido previo (denominado "abono"). Se proporcionan dos formas de autenticación basada en abono: contraseña y certificado.

10.2 Intercambio Diffie-Hellman con autenticación facultativa

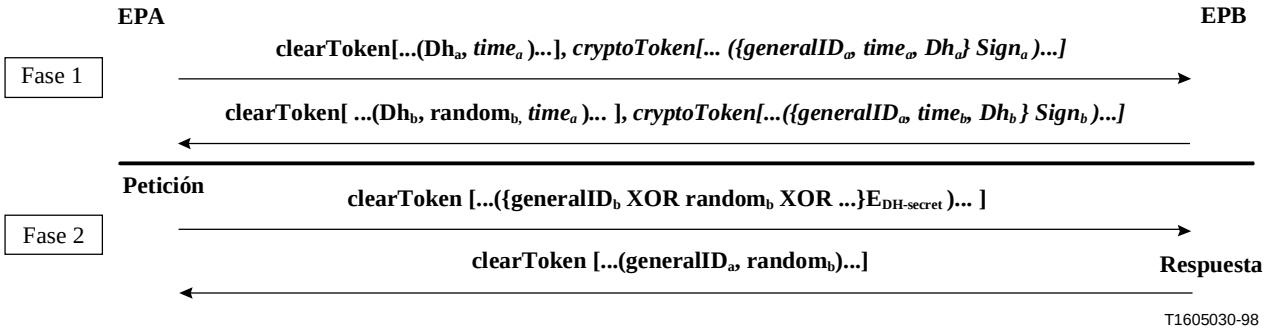
El propósito no es proporcionar autenticación absoluta a nivel de usuario. Este método proporciona la señalización para generar un secreto compartido entre dos entidades que pueden manipular material para comunicaciones privadas.

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 1 siguiente 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 – 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 contiene múltiples elementos

{}$\mathbf{E_{DH\text{-}Secret}}$ indica que los valores contenidos han sido criptados utilizando el secreto Diffie-Hellman

El punto extremo B (EPB) sabe qué clave secreta compartida ha de utilizar para descifrar el identificador **ID_b general** asociándolo con el **ID_a general** que debe ser transferido también en el mensaje. Obsérvese que el valor criptado en la fase 2 es transferido en el campo **ID general** de un **testigo claro** para simplificar la codificación.

Figura 1/H.235

10.3 Autenticación basada en abono

10.3.1 Introducción

Aunque los procedimientos esbozados aquí (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. Estos intercambios suponen que cada extremo posee algún identificador bien conocido (como un identificador textual) que lo identifica inequívocamente. Otra hipótesis es que hay una referencia de tiempo mutuamente aceptable (de la cual derivar sellos de hora). La diferencia de hora que es aceptable es un asunto de la implementación local.

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

1) Contraseña con criptación simétrica.

2) Contraseña con troceado.

3) Certificado con firma.

En todos los casos, el testigo contendrá la información descrita en las subcláusulas siguientes según la variación elegida. Obsérvese que en todos los casos el **ID general** puede ser conocido a través de la configuración o del directorio, en vez de en el intercambio de protocolos dentro de banda.

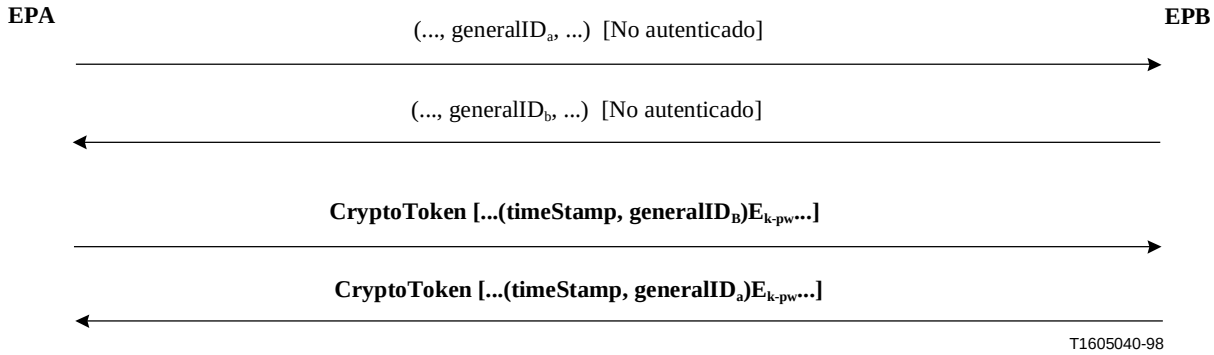
10.3.2 Contraseña con criptación simétrica

En la figura 2 se muestra el formato de testigo y el intercambio de mensajes requeridos para realizar este tipo de autenticación. Este protocolo se basa en 5.2.1 de ISO/CEI 9798-2, y se supone que un identificador y la contraseña asociada son intercambiados durante el abono. La clave de criptación tiene una longitud de N octetos (según lo indicado por el ID de algoritmo), y se forma como sigue:

– Si la longitud de la contraseña = N, claves = 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).



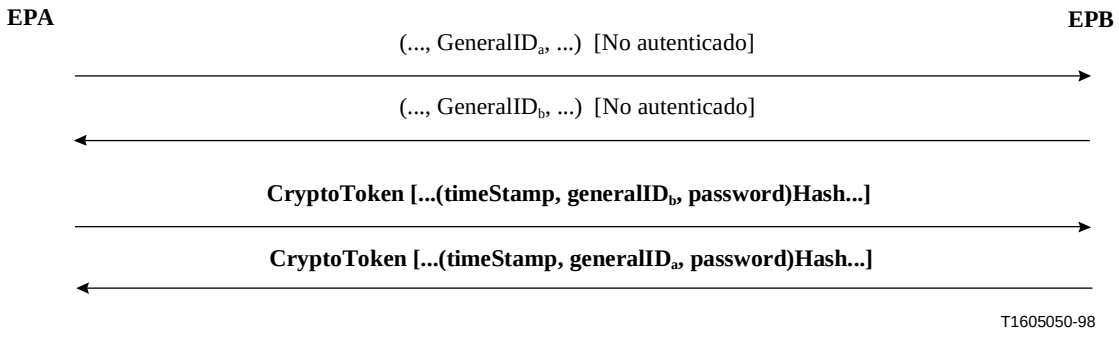
NOTA 1 – La devolución de testigo del EPB es facultativa; si se omite, sólo se logra la autenticación unidireccional.

NOTA 2 – **E_{k-pw}** indica valores que han sido cifrados utilizando la clave "k" derivada de la contraseña "pw".

Figura 2/H.235

10.3.3 Contraseña con troceado

En la figura 3 se muestra el formato de testigo y el intercambio de mensajes requeridos para realizar este tipo de autenticación. Este protocolo se basa en 5.2.1 de ISO/CEI 9798-4, y se supone que un identificador y la contraseña asociada son intercambiados durante el abono.



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

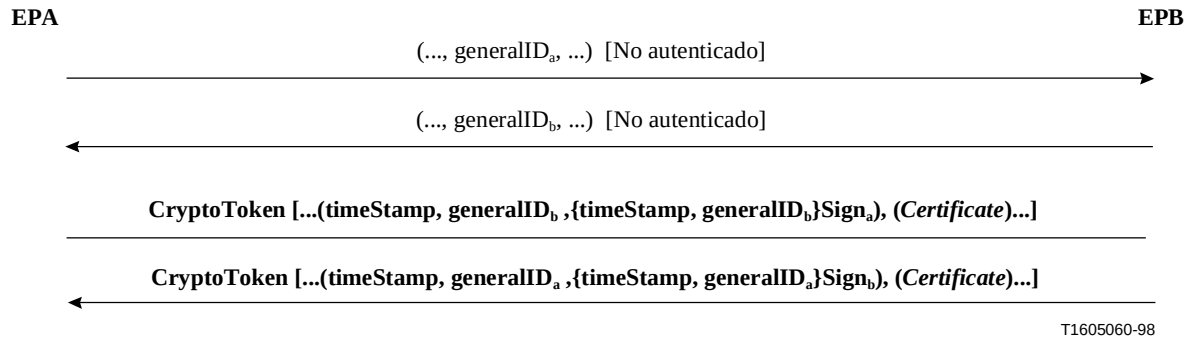
NOTA 2 – **Troceado (Hash)** indica una función de troceado que funciona en los valores contenidos.

Figura 3/H.235

10.3.4 Certificado con firma

En la figura 4 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 un identificador y el certificado asociado son asignados/intercambiados durante el abono.

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



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

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

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

Figura 4/H.235

11 Procedimientos de criptación de tren de medios

Los trenes de medios se codificarán utilizando el algoritmo y la clave presentados en el canal H.245. Las figuras 5 y 6 muestran el flujo general. Obsérvese que se adjunta la unidad de datos de servicio (SDU) de transporte después que la SDU ha sido criptada. Los segmentos opacos indican privacidad. A medida que el transmisor recibe nuevas claves y éstas son utilizadas en la criptación, el encabezamiento SDU indicará de alguna manera al receptor que ahora se está utilizando la nueva clave. Por ejemplo, en el protocolo H.323 el encabezamiento RTP (SDU) cambiará su tipo de cabida útil para indicar la conmutación a la nueva clave.

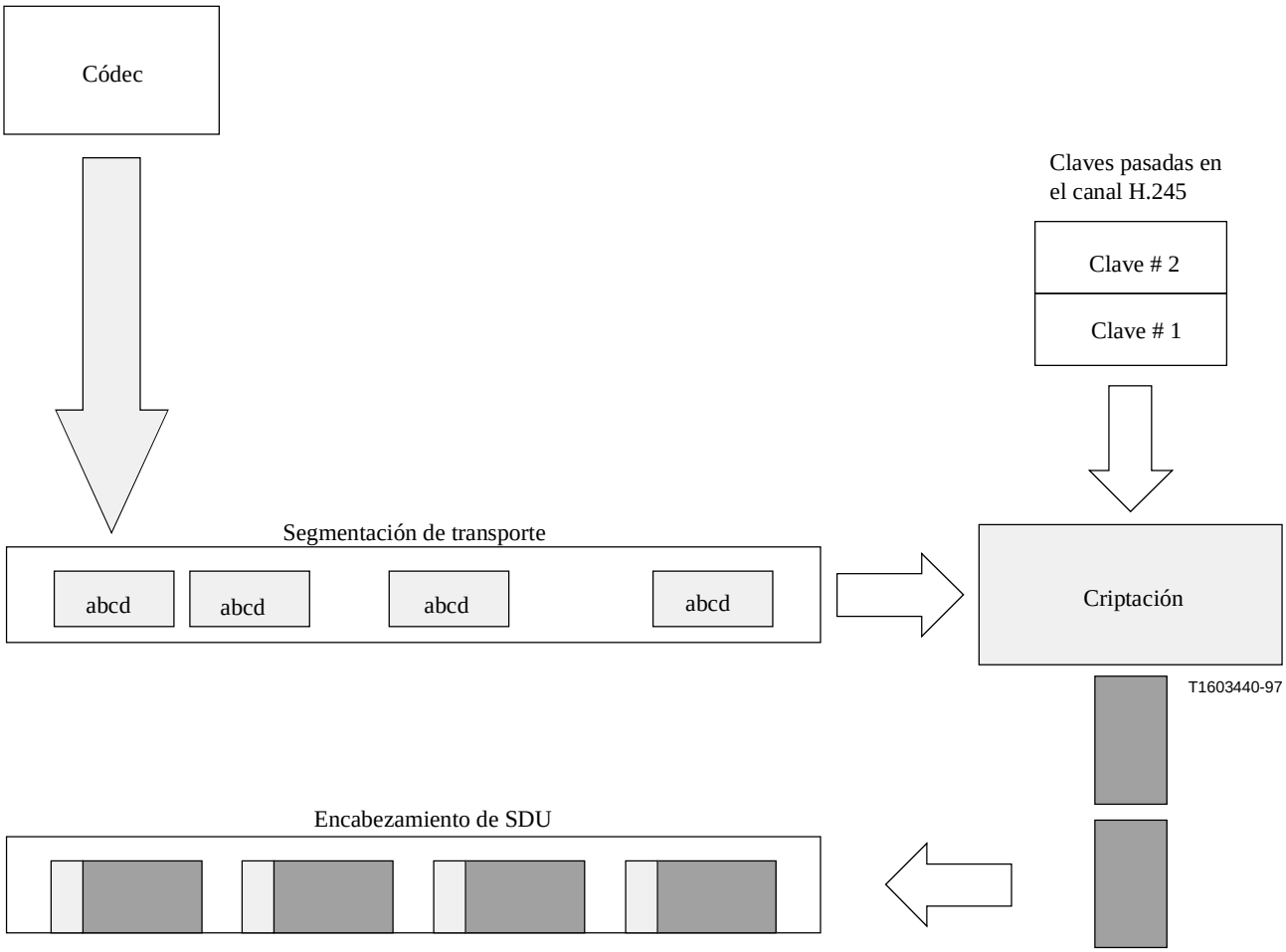


Figura 5/H.235 – Criptación de medios

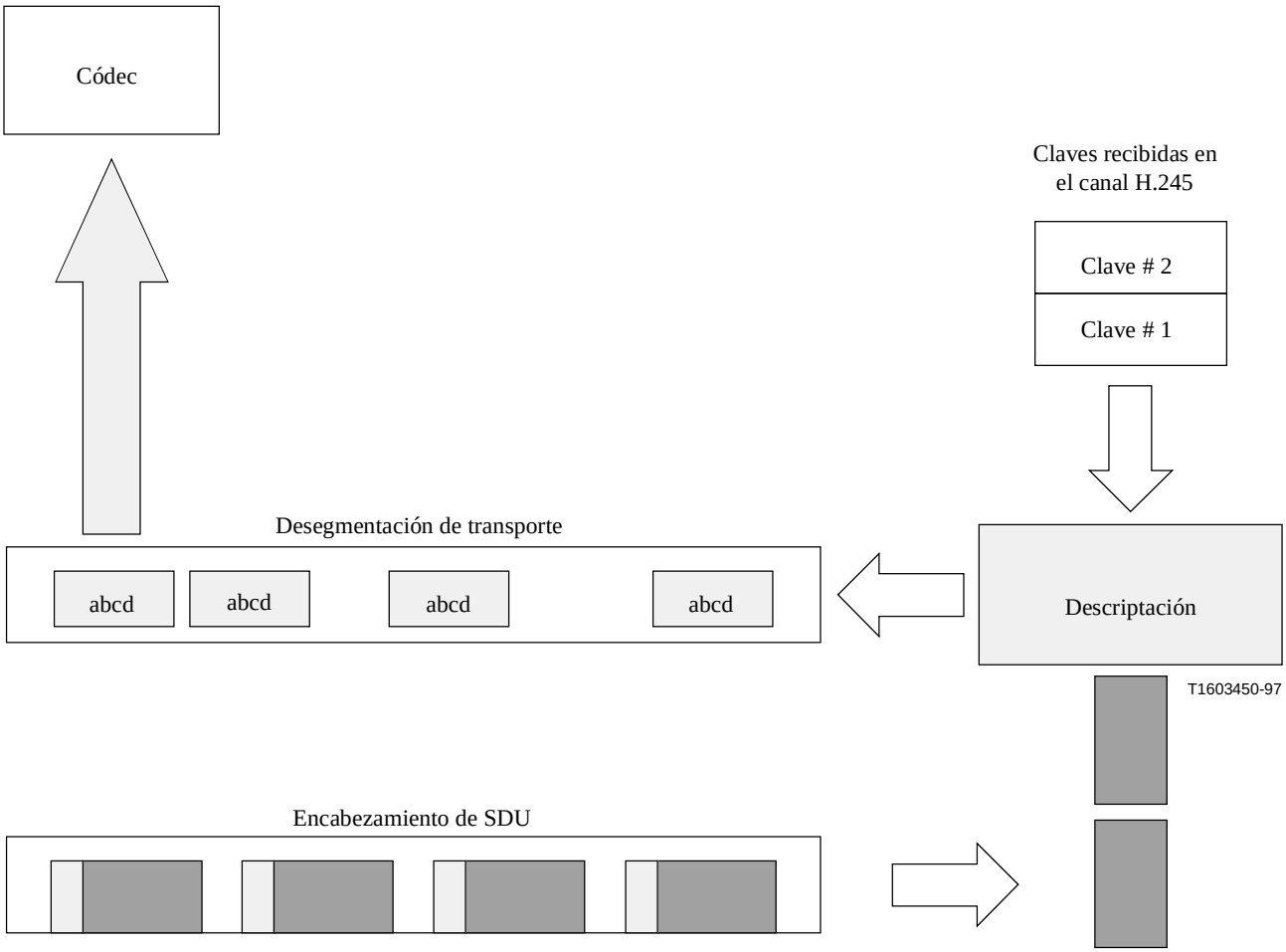


Figura 6/H.235 – Descriptación de medios

11.1 Claves de sesión de medios

Clave h.235 (h235Key) se incluye en la **actualización de criptación**. **Clave h235** está codificada en ASN.1 dentro del contexto del árbol ASN.1 del protocolo H.235 y se transfiere como una cadena de octetos opaca con respecto al protocolo H.245. Se puede proteger la clave utilizando uno de los tres mecanismos posibles a medida que son transferidos entre dos puntos extremos.

- Si el canal H.245 es seguro, no se aplica protección adicional al material de claves. La clave se transfiere en "claro" con respecto a este campo; se utiliza la opción ASN.1 de **canal seguro (secureChannel)**.
- Si se ha establecido una clave y un algoritmo secretos fuera del canal H.245 (es decir, fuera del protocolo H.323 o en un canal lógico **control h235 (h235Control**), el secreto compartido se utiliza para criptar el material de clave, y se incluye la clave cifrada resultante. En este caso, se utiliza la opción ASN.1 de **secreto compartido (sharedSecret).**
- Se pueden utilizar certificados cuando el canal H.245 no es seguro, pero se pueden utilizar también además para el canal H.245 seguro. Cuando se emplean certificados, el material de claves es cifrado utilizando la clave pública del certificado y el constructivo ASN.1 **clave protegida de certificado (certProtectedKey).**

En cualquier punto en una conferencia, un receptor (o un transmisor) puede solicitar una nueva clave (**petición actualización criptación**). Una razón para hacer esto pudiera ser si se sospecha que se ha perdido la sincronización de uno de los canales lógicos. El terminal director que recibe esta petición

generará nuevas claves en respuesta a esta instrucción y puede decidir también asíncronamente distribuir nuevas claves y, si lo hace así, utilizará el mensaje **actualización criptación**.

Después de recibir una **petición actualización criptación**, el terminal director enviará **actualización criptación**. Si se trata de una conferencia multipunto, el MC (también el director) distribuirá la nueva clave a todos los receptores antes de dar esta clave al transmisor. El transmisor de los datos por el canal lógico utilizará la nueva clave tan pronto sea posible después de recibir el mensaje.

Un transmisor (que se supone no es el director) puede solicitar también una nueva clave. Si el transmisor forma parte de una conferencia multipunto, el procedimiento será el siguiente:

- El transmisor enviará **petición actualización criptación** al MC (director).
- El MC debe generar una nueva clave y enviar un mensajes **actualización criptación** a todos los participantes en la conferencia, salvo al transmisor.
- Después de distribuir las nuevas claves a todos los participantes, el MC enviará **actualización criptación** al transmisor que utilizará entonces la nueva clave.

12 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 [8.5/H.323 con la excepción del paso 5)].

Si cualquiera de los dos puntos extremos detecta una brecha en la seguridad del canal H.245 o del canal lógico (**control h235**) de datos seguro, debe cerrar inmediatamente la conexión aplicando los procedimientos de protocolo apropiados al punto extremo en cuestión [8.5/H.323 con la excepción del paso 5)].

Si cualquier punto extremo detecta una pérdida de privacidad en uno de los canales lógicos, debe solicitar inmediatamente una nueva clave (**petición actualización criptación**) 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 **petición actualización criptación, actualización criptación** a cualquier y a todos lo puntos extremos afectados.

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

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
```

```
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
        ...
}

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

AuthenticationMechanism ::=CHOICE
{
        dhExch                  NULL, -- Diffe-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.
        ...
}

ClearToken          ::= SEQUENCE  -- a "token" may contain multiple value types.
{
        timeStamp               TimeStamp OPTIONAL,
        password                Password OPTIONAL,
        dhkey                   DHset OPTIONAL,
        challenge               ChallengeString OPTIONAL,
        random                  RandomVal OPTIONAL,
        certificate             TypedCertificate OPTIONAL,
        generalID               Identifier OPTIONAL,
        nonStandard             NonStandardParameter OPTIONAL,
        ...
}

--
-- Start all the cryptographic parameterized types here...
--


SIGNED { ToBeSigned } ::= SEQUENCE {
  toBeSigned        ToBeSigned,
  algorithmOID      OBJECT IDENTIFIER,
  paramS            Params,       -- any "runtime" parameters
```

```
  signature          BIT STRING
} ( 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))

-- 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
        ...
}

EncodedGeneralToken ::= TYPE-IDENTIFIER.&Type (ClearToken -- general usage token
PwdCertToken ::= ClearToken (WITH COMPONENTS {..., timeStampPRESENT, generalIDPRESENT})
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 "h235Key" field
{
        secureChannel       KeyMaterial,
        sharedSecret        ENCRYPTED {EncodedKeySyncMaterial},
        certProtectedKey            SIGNED { EncodedKeySignedMaterial },
```

```
        ...
}

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-INDENTIFIER.&Type (KeySyncMaterial)



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

ANEXO B

Aspectos específicos del protocolo H.323

B.1 Antecedentes

En la figura B.1 se muestra un diagrama con una visión general del alcance de protocolo H.235 en el marco de la Recomendación H.323.

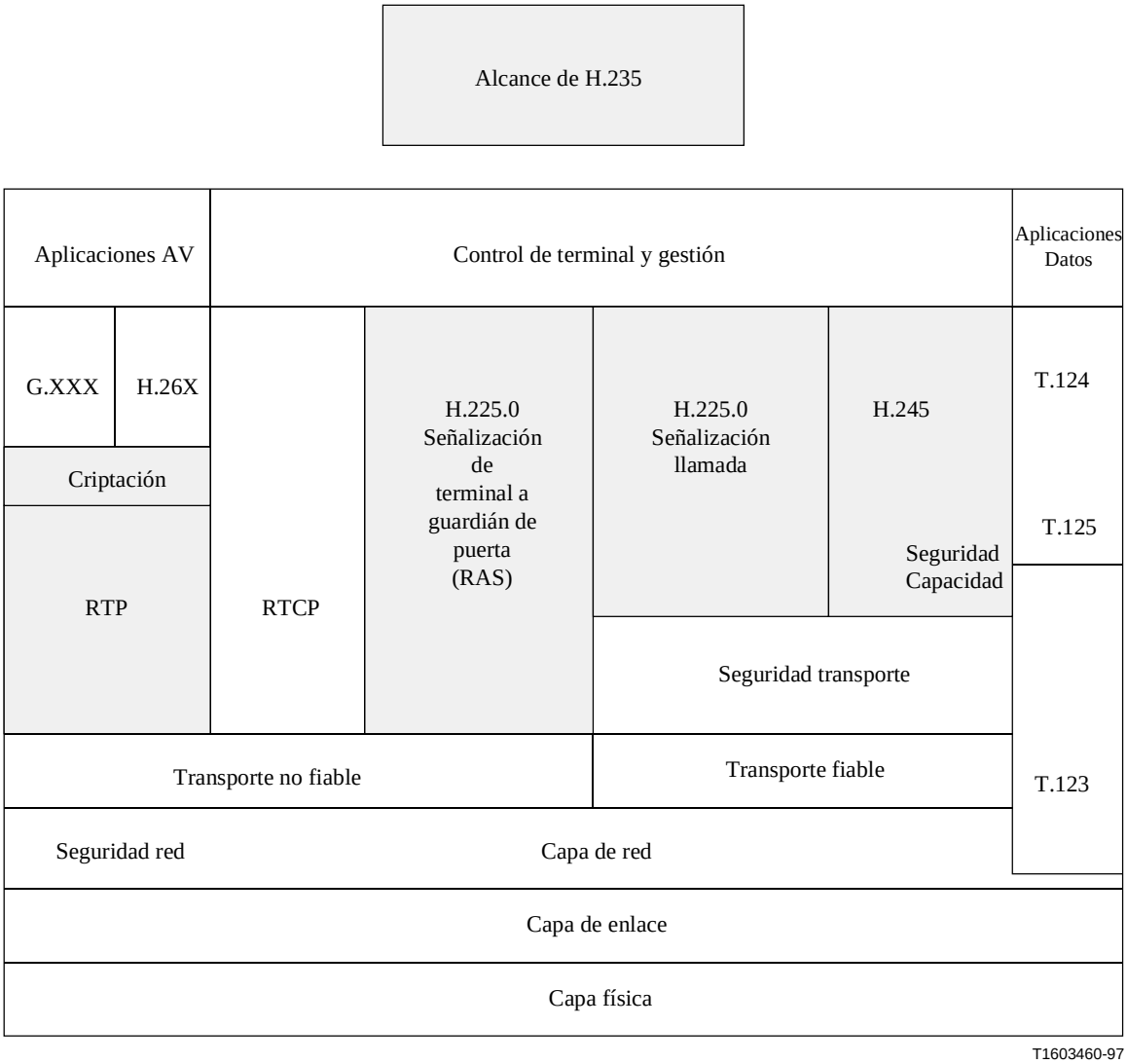


Figura B.1/H.235

Para el protocolo H.323, la señalización del uso de TLS, IPSEC o un mecanismo patentado en el canal de control H.245 se producirá en el canal H.225.0 seguro o inseguro durante el intercambio inicial de mensajes Q.931.

B.2 Señalización y procedimientos

Se aplicarán los procedimientos indicados en la cláusula 8/H.323 (Procedimientos de señalización de la llamada). Los puntos extremos H.323 tendrán la capacidad de codificar y reconocer la presencia (o ausencia) de requisitos de seguridad (para el canal H.245) señalizado en los mensajes H.225.0.

Cuando el propio canal H.225.0 ha de ser asegurado, se seguirán los mismos procedimientos indicados en la cláusula 8/H.323. La diferencia de funcionamiento es que las comunicaciones sólo se producirán después de conectar con el identificador de TSAP y utilizar los modos de seguridad predeterminados (por ejemplo, TLS). Debido a que los mensajes H.225.0 son intercambiados primero cuando se establecen comunicaciones H.323, no puede haber negociaciones de seguridad "dentro de banda" para el canal H.225.0. En otras palabras, ambas partes deben conocer previamente que están utilizando un modo de seguridad particular. Para H.323 en IP, se utiliza un puerto bien conocido alternativo (1300) para comunicaciones TLS.

Una finalidad de los intercambios H.225.0 en lo que concierne a su relación con la seguridad H.323, es proporcionar un mecanismo para establecer el canal H.245 seguro. Facultativamente puede haber autenticación durante el intercambio de mensajes H.225.0. Esta autenticación puede estar basada en certificado o en contraseña, utilizando criptación y/troceado (por ejemplo, firma). Los aspectos específicos de estos modos de funcionamiento se describen en 10.2 a 10.3.4.

Un punto extremo H.323 que recibe un mensaje ESTABLECIMIENTO con la **Capacidad seguridad h245** (**h245SecurityCapability**) fijada responderá con el correspondiente **Modo seguridad h245** (**h245SecurityMode**) aceptable en el mensaje CONEXIÓN. En el caso en que no haya capacidades superpuestas, el terminal llamado puede rechazar la conexión enviando **Liberación completa** con el código de motivo fijado a ***Seguridad denegada***. No se prevé que este error transporte ninguna información sobre cualquier discordancia de seguridad y el terminal llamante tendrá que determinar el problema por algún otro medio. Cuando el terminal llamante recibe un mensaje CONEXIÓN sin un modo de seguridad suficiente o aceptable, puede terminar la llamada con **Liberación completa** con el motivo ***Seguridad denegada***. Cuando el terminal llamante recibe un mensaje CONEXIÓN sin ninguna capacidad de seguridad, puede terminar la llamada con **Liberación completa** con ***motivo no definido***.

Si el terminal llamante recibe un modo **Seguridad h245** aceptable, abrirá y utilizará el canal H.245 en el modo seguro indicado. El hecho de no poder establecer el canal H.245 en el modo seguro determinado se debe considerar como un error de protocolo y la conexión es terminada.

B.2.1 Compatibilidad con la revisión 1

Un punto extremo capaz de seguridad no devolverá ningún campo, indicaciones o estado relacionados con la seguridad al punto extremo que no es capaz de ofrecer seguridad. Si la parte llamada recibe un mensaje ESTABLECIMIENTO que no contiene capacidades y/o testigo de autenticación **Seguridad H245**, puede devolver **Liberación completa** para rechazar la conexión, pero en este caso utilizará el código ***Motivo no definido***. De manera correspondiente, si una parte llamante recibe un mensaje CONEXIÓN sin **Modo seguridad H245** y/o testigo de autenticación habiendo enviado un mensaje ESTABLECIMIENTO con **Seguridad H245** y/o testigo de autenticación, puede también terminar la conexión emitiendo un mensaje **Liberación completa** con un código ***Motivo no definido***.

B.3 Aspectos relativos a RTP/RTCP

La utilización de criptación en el tren RTP seguirá la metodología general recomendada en el documento referenciado en [**RTP**]. La criptación de los medios se producirá de manera independiente, paquete por paquete[1]. El encabezamiento RTP (incluido el encabezamiento de cabida útil) no será encriptado. La sincronización de nuevas claves y textos encriptados se basa en el tipo de cabida útil dinámica.

La clave de criptación inicial es presentada por el terminal director junto con el número de cabida útil dinámica (mediante **Sincronización de criptación** en H.245). El receptor o receptores del tren de medios comenzará el uso inicial de la clave al recibir el número de esta cabida útil en el encabezamiento RTP. El punto extremo director puede distribuir nuevas claves en cualquier momento. La sincronización de la clave más nueva con el tren de medios será indicada por el cambio del tipo de cabida útil a un nuevo valor dinámico. Obsérvese que los valores específicos no tienen importancia, mientras cambien para cada nueva clave que se distribuye.

---

[1] Cabe señalar que si el tamaño de paquete RTP es mayor que el tamaño MTU, la pérdida parcial (de fragmento) hará que todo el paquete RTP sea indescifrable.

Se supone que esta criptación se aplica sólo a la cabida útil en cada paquete RTP, los encabezamientos RTP permanecen en claro. Se supone que todos los paquetes RTP deben ser un múltiplo de octetos completos. El modo de encapsular los paquetes RTP en la capa de transporte o de red no es pertinente a la presente Recomendación. Todos los modos deben tener en cuenta los paquetes perdidos (o fuera de secuencia), además del relleno de paquetes a un múltiplo de octetos apropiado.

El descifrado del tren debe ser independiente con respecto a los paquetes que se puedan perder, cada paquete es descifrable por sí mismo. Dos requisitos del modo algoritmo de bloque funcionarán como sigue:

a) Vectores de inicialización

La mayor parte de los modos de bloque conllevan algún "encadenamiento"; cada ciclo de criptación depende en cierta manera de la salida del ciclo anterior. Por consiguiente, al comienzo de un paquete, se debe proporcionar algún valor de bloque inicial [generalmente denominado un vector de inicialización (IV, *initialization vector*)] para comenzar el proceso de criptación. Con independencia del número de octetos de tren que son procesados en cada ciclo de inscripción, la longitud de IV es siempre igual a la longitud de un bloque. Todos los modos, salvo el modo libro de código electrónico (ECB, *electronic code book*) requieren un IV. En todos los casos, el IV se construirá a partir de los primeros octetos de B (donde B es el tamaño de bloque): (Seq# + sello de hora). Este esquema se debe repetir hasta que se hayan generado octetos suficientes. Cabe señalar que el IV generado de esta manera puede producir un esquema de clave que se considera "débil" para un algoritmo determinado.

b) Relleno

Los modos ECB y CBC procesan siempre el tren de entrada un bloque cada vez y mientras CFB y OFB pueden procesar la entrada en cualquier número de octetos, N (≤ B), se recomienda que N = B.

Se dispone de dos métodos para tratar paquetes cuya cabida útil no es un múltiplo de bloques:

1) Apropiación de texto cifrado para ECB y CBC; relleno de ceros para CFB y OFB.

2) Relleno de la manera prescrita por [**RTP**] (sección 5.1).

La sección 5.1 [**RTP**] describe un método de relleno en el cual la cabida útil es rellenada hasta un múltiplo de bloque, el último octeto es fijado con el número de octetos de relleno (incluido el último), y el bit P fijado en el encabezamiento RTP. El valor de relleno debe ser determinado por el convenio normal del algoritmo de cifrado.

Todas las implementaciones H.235 admitirán ambos esquemas. El esquema en uso puede ser deducido como sigue: si el bit P está fijado en el encabezamiento RTP, el paquete tiene relleno. Si el paquete no es un múltiplo de B y el bit P no está fijado, se aplica el apropiación de texto cifrado, en los demás casos el paquete es un múltiplo de B, y no se aplica relleno.

La integridad y protección contra reproducción del tren RTP queda en estudio.

La aplicación de técnicas criptográficas a los elementos RTCP requiere también estudio.

B.4 Señalización RAS/procedimientos de autenticación

B.4.1 Introducción

Este anexo no proporciona explícitamente ninguna forma de privacidad de mensajes entre guardianes de puerta 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 guardián de puerta.

El segundo tipo es el abono que tendrá dos formas, contraseña o certificado. Todas estas formas se derivan de los procedimientos indicados en 10.2, 10.3.2, 10.3.3 y 10.3.4. En este anexo, las etiquetas genéricas (EPA y EPB) utilizadas en las subcláusulas mencionadas representarán respectivamente al punto extremo y al guardián de puerta.

B.4.2 Autenticación de punto extremo-guardián de puerta (no basada en abono)

Este mecanismo puede proporcionar al guardián de puerta un enlace criptográfico 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 guardián de puerta 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 10.2. Esta clave secreta compartida será utilizada en cualquier **RRQ/URQ** subsiguiente del terminal al guardián de puerta. Si un guardián de puerta funciona en este modo y recibe **GRQ** sin un testigo que contiene *DHset* o un valor de algoritmo aceptable, devolverá un código de motivo **denegación seguridad** 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 subcláusulas pertinentes de la Recomendación H.225.0.

2) El terminal encriptará **Identificador de guardián de puerta** (devuelto en el **GCF**) utilizando la clave secreta compartida negociada. Ésta será transferida en un **testigo de cifrado** como el **ID general**.

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

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

Guardián de puerta (**xCF/xRJ**):

1) El guardián de puerta cifrará su **Identificador de guardián de puerta** (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 guardián de puerta devolverá **xRJ** si los dos valores criptados no concuerdan.

3) Si el **Identificador de guardián de puerta** concuerda, el guardián de puerta aplicará cualquier lógica local y responderá con **xCF** o **xRJ**.

4) Si **xCF** es enviado por el guardián de puerta, debe contener un **Identificador de punto extremo** asignado y un nuevo valor aleatorio en el campo **aleatorio** de un **testigo claro**.

Véase la segunda fase de la figura 1 de 10.2 para una representación gráfica de este intercambio. El guardián de puerta sabe la clave secreta compartida que ha de utilizar para descifrar el identificador de guardián de puerta mediante el nombre alias en el mensaje.

B.4.3 Autenticación de punto extremo-guardián de puerta (basada en abono)

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 troceado.

3) Certificado con firmas.

En todos los casos el testigo contendrá la información descrita en las siguientes subcláusulas de acuerdo con la variación elegida. Si un guardián de puerta funciona en un modo seguro y recibe un mensaje RAS sin un valor de testigo aceptable, devolverá un código de motivo **rechazo seguridad** en el mensaje de rechazo. En todos los casos, el testigo devuelto de guardián de puerta es facultativo; si se omite, sólo se logra la autenticación unidireccional.

B.4.3.1 Contraseña con criptación simétrica

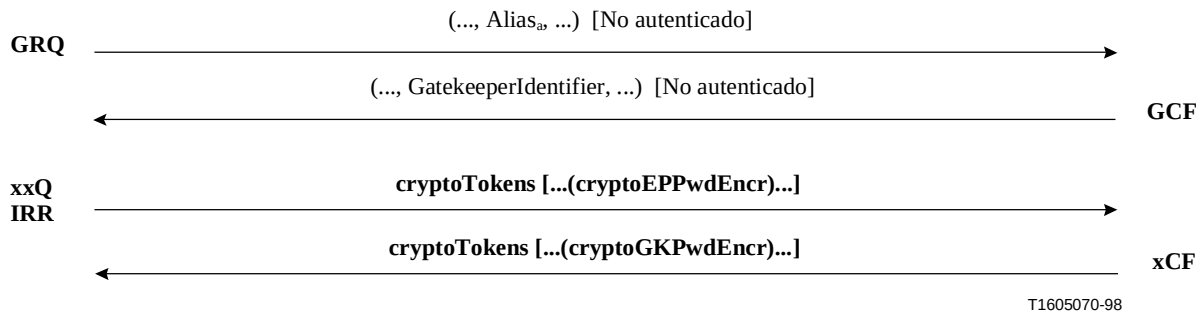


Figura B.2/H.235

B.4.3.2 Contraseña con troceado

Se supone que un alias y la contraseña asociada son intercambiados fuera de banda para este intercambio de mensajes.

Figura B.3/H.235

B.4.3.3 Certificado con firmas

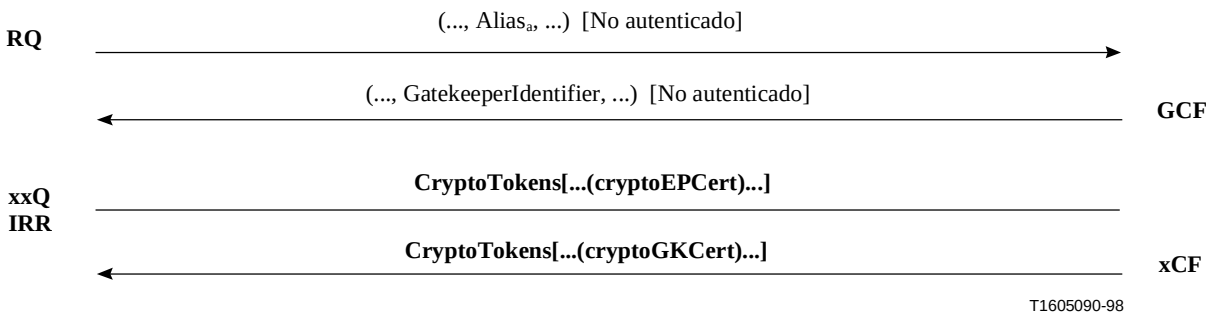


Figura B.4/H.235

B.5 Interacciones no relacionadas con terminales

B.5.1 Cabecera

Como se indica en 6.6, se debe considerar que una cabecera H.323 es un elemento de confianza. Esto incluye cabeceras de protocolo (H.323-H.320, etc.) y cabeceras de seguridad (apoderados/cortafuegos). La privacidad de los medios puede ser asegurada entre el punto de extremo y el dispositivo de cabecera comunicantes, pero lo que se produce en el extremo distante de la cabecera se debe considerar inseguro por defecto.

ANEXO C

Aspectos específicos del protocolo H.324

Queda en estudio.

APÉNDICE I

Detalles de las implementaciones H.323

I.1 Métodos de relleno de texto cifrado

En **[Schneier]**, páginas 191 y 196, hay una descripción de apropiación de texto cifrado (Ciphertext Stealing). Las figuras I.1 a I.5 ilustran la técnica.

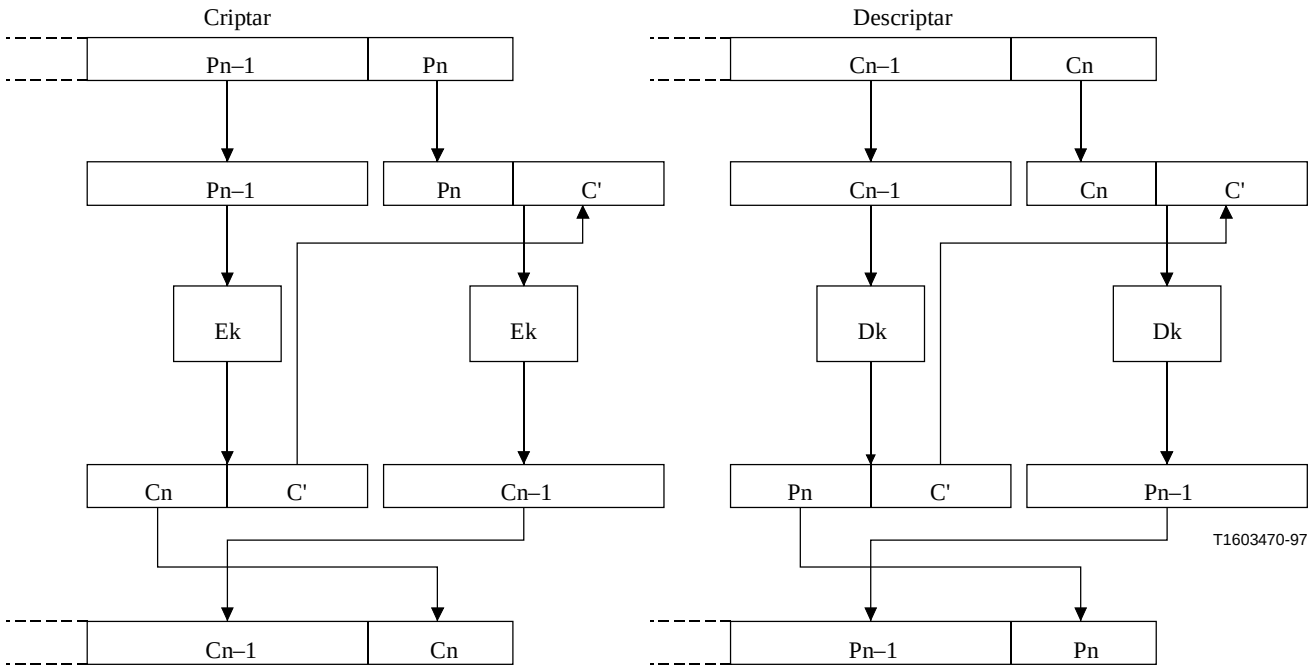


Figura I.1/H.235 – Apropiación de texto cifrado en modo ECB

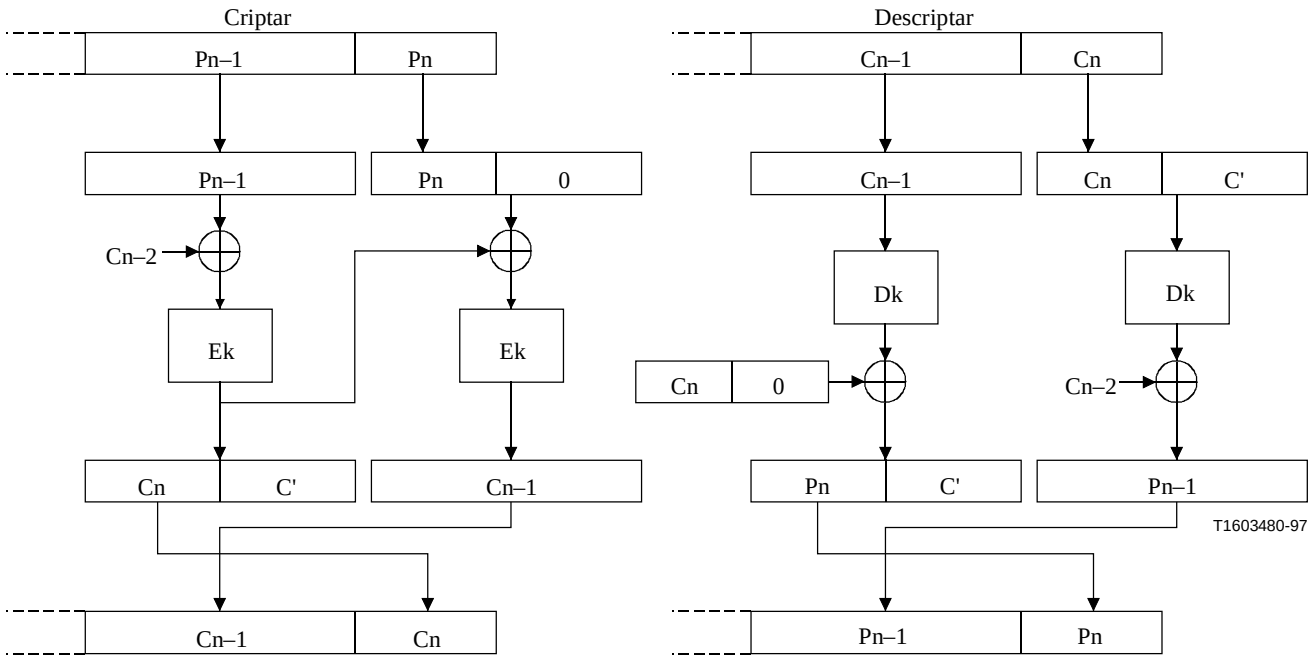


Figura I.2/H.235 – Apropiación de texto cifrado en modo CBC

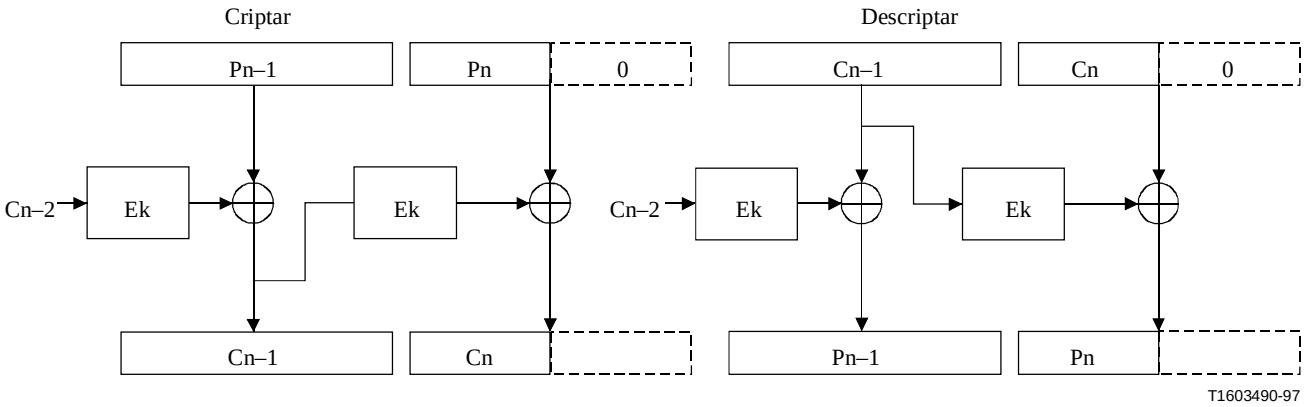
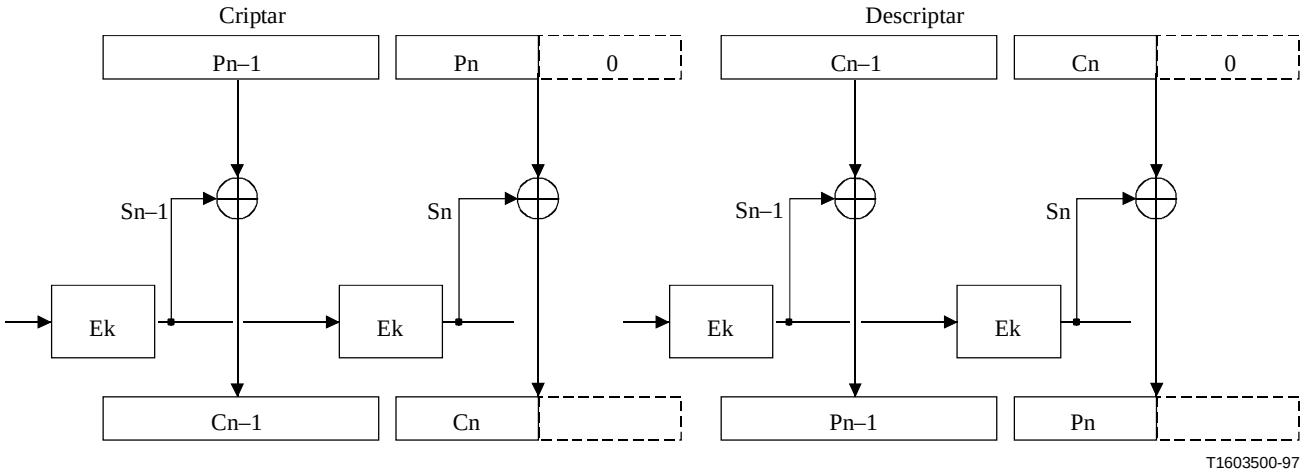


Figura I.3/H.235 – Relleno de ceros en modo CFB



NOTA - Si es el resultado de criptación repetitivo (es decir, permutas) del IV.

Figura I.4/H.235 – Relleno de ceros en modo OFB

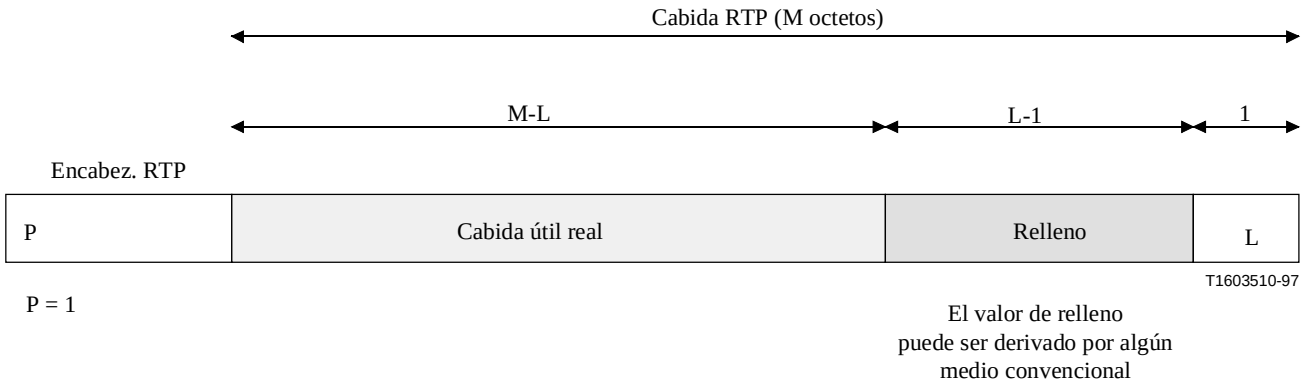


Figura I.5/H.235 – Relleno prescrito por RTP

I.2 Nuevas claves

Los procedimientos indicados en 8.5/H.323 son completados por un MC para sacar a un participante de la conferencia. El terminal director puede generar nuevas claves de criptación para los canales lógicos (y no distribuirlas a la parte eliminada); esto se puede utilizar para evitar que la parte eliminada supervise los trenes de medios.

I.3 Elementos de confianza H.323

En general, las MC(U), las cabeceras y los guardianes de puerta (si se aplica el modelo con encaminamiento por guardián de puerta) son fiables con respecto a la privacidad del canal de control. Si el canal de establecimiento de la conexión (H.225.0) es seguro *y* es encaminado a través del guardián de puerta, se debe considerar también de confianza. Si algunos de estos componentes H.323 deben funcionar en los trenes de medios (es decir, mezcla, transcodificación), por definición, serán considerados también de confianza para la privacidad de los medios.

Se puede confiar también en los apoderados/cortafuegos (aunque no son elementos específicos de H.323), porque terminan conexiones, y pueden tener que manipular los mensajes y los trenes de medios.

I.4 Ejemplos de implementaciones

A continuación se describen ejemplos de implementaciones que pudieran ser desarrolladas dentro del 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 del protocolo H.323.

I.4.1 Testigos

Esta subcláusula 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 guardián de puerta, una cabecera POTS y un teléfono como se ilustra a continuación.

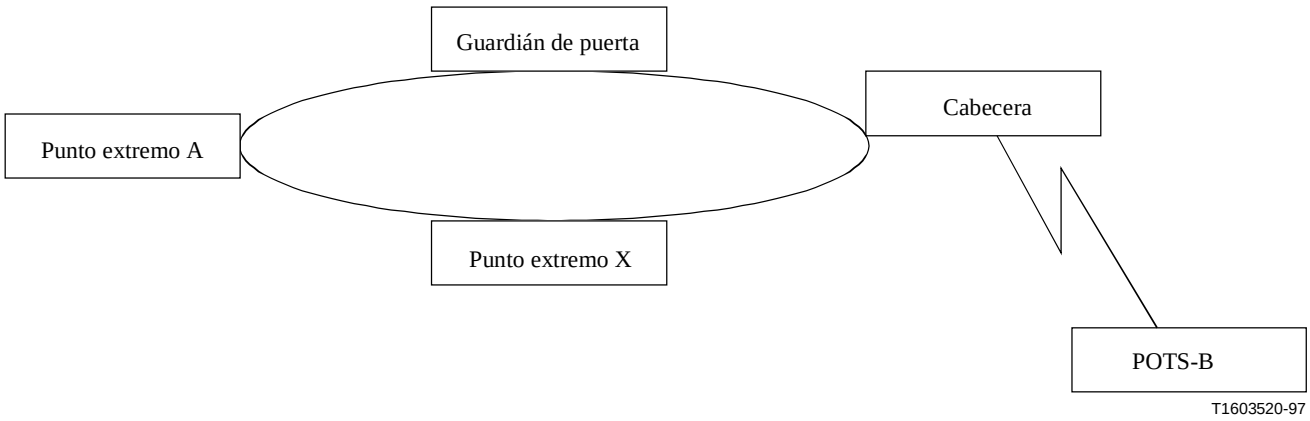


Figura I.6/H.235

Actualmente, el protocolo H.323 puede funcionar de manera similar a una red telefónica con el ID del llamante. Este caso ilustra una situación en la cual la *parte llamada* no desea exponer su

dirección física, a la vez que permite que se complete la llamada. Esto puede ser importante en cabeceras 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 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 guardián de puerta para resolver la dirección del teléfono POTS representada por su alias/cabecera. El guardián de puerta reconocerá esto como un alias "privado" sabiendo que para completar la conexión debe devolver la dirección de cabecera 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 guardián de puerta devuelve la dirección de cabecera 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 cabecera (cuya dirección de señalización de llamada fue devuelta en ACF) incluidos los testigos opacos que recibió con ACF.
- La cabecera, al recibir el mensaje ESTABLECIMIENTO, emite su ARQ a su guardián de puerta incluidos cualesquiera testigos que fueron recibidos en el mensaje ESTABLECIMIENTO.
- El guardián de puerta 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 cifrar 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 cabecera) y **ARQ** (de la cabecera al guardián de puerta) como se indica anteriormente. Una vez que el guardián de puerta descriptó el testigo (el número telefónico) transferirá la versión clara en el **testigo claro (clearToken)**.

I.4.2 Contraseña

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

El procedimiento de registro de ejemplo con autenticación de guardián de puerta es el siguiente:

1) Si el punto extremo utiliza **GRQ** para descubrir un guardián de puerta, uno de los alias del mensaje sería el ID de suscripción (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 admitidos por el punto extremo. (Por ejemplo, uno de estos sería DES de 56 bits en modo EBC.)

2) El guardián de puerta 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 **sello de hora**. La **pregunta** contendría 16 octetos. (Para impedir ataques de reproducción, el **Testigo claro** contendría un **sello de hora**.) 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 guardián de puerta (por ejemplo, DES de 56 bits en modo EBC).

   Si el guardián de puerta no admite algunos de los **algorithmOIDs** indicado en el **GRQ**, respondería con un mensaje **GRJ** que contiene un **Motivo de rechazo de guardián de puerta (GatekeeperRejectReason)** de **recurso no disponible (resourceUnavailable).**

3) La aplicación de punto extremo trataría de registrarse con (uno de) los guardianes de puerta 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 10.3. La "cadena" de octetos resultante se utiliza como la clave DES para criptar la **pregunta**.

4) Cuando el guardián de puerta recibe la pregunta cifrada 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 guardián de puerta responderá con un **RRJ** con el **Motivo de rechazo de registro** (**RegistrationRejectReason)** puesto a **denegación de seguridad**. Si concuerdan, el guardián de puerta envía un **RCF** al punto extremo.

5) Si el guardián de puerta recibe un **RRQ** que no contiene un elemento **Testigos cifrados** aceptable, debe responder con un **RRJ** con un **Motivo de rechazo de guardián de puerta** de **descubrimiento requerido (discoveryRequired)**. El punto extremo, al recibir este **RRJ** puede efectuar un descubrimiento que le permitirá al guardián de puerta/punto extremo intercambiar una nueva pregunta. Obsérvese que el mensaje **GRQ** puede ser unidifundido al guardián de puerta.

I.4.3 IPSEC

En general IPSEC **[13/IPSEC]** se puede 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 guardián de puerta 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 guardián de puerta, el protocolo ISAKMP/Oakley 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 guardián de puerta 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/Oakley 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/Oakley transparente antes de que se transmitan paquetes H.245. La autenticación realizada por esta negociación ISAKMP/Oakley 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/Oakley.

5) Después de cada autenticación ISAKMP/Oakley H.245, 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 apoderados 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 Recomendación H.245. Si este canal se utiliza, el canal H.245 puede permanecer no seguro; 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.

APÉNDICE II

Detalles de implementaciones del protocolo H.324

Queda en estudio.

APÉNDICE III

Otros detalles de implementaciones de la serie H

Queda en estudio.

APÉNDICE IV

Bibliografía

[Daemon]

– DAEMON (J.): Cipher and Hash function design, Ph.D. Thesis, Katholieke Universiteit Leuven, marzo de 1995.

[IPSEC]

– ORMAN (H.K.): The Oakley Key Determination Protocol, draft-ietf-ipsec-oakley-02.txt, *Internet Engineering Task Force*, 1997.

– MAUGHAN (D.), SCHERTLER (M.), SCHNEIDER (M.) TURNER (J.): Internet Security Association and Key Management Protocol (ISAKMP), draft-ietf-ipsec-isakmp-08.text, *Internet Engineering Task Force*, 1997.

– KENT (S.), ATKINSON (R.): IP Authentication Header, draft-ietf-ipsec-auth-header-01.txt, *Internet Engineering Task Force*, 1997.

– HARKINS (D.), CARREL (D.): The resolution of ISAKMP with Oakley, draft-ietf-ipsec-isakmp-oakley-04.txt, *Internet Engineering Task Force*, 1997.

[RTP]

– SCHULZRINNE (H.), CASNER (S.), FREDERICK (R.), JACOBSON (V.): RTP: A Transport Protocol for Real-Time Applications, RFC 1889, *Internet Engineering Task Force*, 1996.

[Schneier]

– SCHNEIER (B.): Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition, John Wiley & Sones, Inc., 1995.

[TLS]

– DIEKS (T.), ALLEN (C.): The TLS Protocol Version 1.0, draft-ietf-tls-protocol-03.txt, *Internet Engineering Task Force*, 1997.

SERIES DE RECOMENDACIONES DEL UIT-T

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