Unión Internacional de Telecomunicaciones

UIT-T H.235.8

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

(09/2005)

SERIE H: SISTEMAS AUDIOVISUALES Y MULTIMEDIOS

Infraestructura de los servicios audiovisuales – Aspectos de los sistemas

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.235.8

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.235.8

Marco de seguridad H.323: Intercambio de claves para el protocolo de transporte en tiempo real seguro utilizando canales de señalización seguros

Resumen

La finalidad de esta Recomendación es describir los procedimientos de seguridad durante el intercambio de claves para el protocolo de transporte en tiempo real seguro (SRTP) utilizando canales de señalización seguros por las redes H.323/H.235.

Esta Recomendación requiere la conformidad con las Recs. UIT-T H.323 y H.225.0 versiones 4 o posteriores.

Orígenes

La Recomendación UIT-T H.235.8 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.

PREFACIO

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

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

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

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

NOTA

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

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

PROPIEDAD INTELECTUAL

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

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

ÍNDICE

Recomendación UIT-T H.235.8

Marco de seguridad H.323: Intercambio de claves para el protocolo de transporte en tiempo real seguro utilizando canales de señalización seguros

1 Alcance

La finalidad de esta Recomendación es proporcionar recomendaciones relativas a los procedimientos de seguridad necesarios para soportar el protocolo de transporte en tiempo real seguro (SRTP, *secure real time transport protocol*) del IETF entre puntos extremos H.323, en los casos en que la información criptográfica del canal de medios se transporta por un canal de señalización seguro, por ejemplo, IPsec (RFC 2401), TLS (RFC 2246) u otros mecanismos H.235. Estos procedimientos de seguridad se ofrecen como una alternativa a otros procedimientos de seguridad H.235 que soportan el protocolo SRTP.

En esta Recomendación se describen los procedimientos utilizados para soportar el protocolo de transporte en tiempo real seguro (SRTP) del IETF en la Rec. UIT-T H.323. El protocolo SRTP ofrece servicios de seguridad para los medios basados en el protocolo de transporte en tiempo real (RTP) y se combina con otros protocolos que proporcionan servicios de gestión de claves y la negociación de los parámetros criptográficos. Estos procedimientos no deberían utilizarse cuando el canal de señalización seguro termina en un sistema intermedio, en cuyo caso la información criptográfica SRTP debería ser transportada por un mecanismo seguro extremo a extremo.

Estos procedimientos soportan la señalización, la negociación y el transporte de claves criptográficas SRTP, identificadores del algoritmo de autenticación y criptación, y otros parámetros de sesión entre puntos extremos H.323.

Un aspecto esencial de esos procedimientos es que tanto el subordinado como el director H.245 podrán generar y distribuir claves criptográficas.

Para el intercambio de capacidades de seguridad SRTP pueden utilizarse los mecanismos de intercambio existentes, y con entradas h235SecurityCapability en el cuadro capabilityTable del mensaje TerminalCapabilitySet H.245. El campo genericH235SecurityCapability, que forma parte del campo encryptionAuthenticationAndIntegrity en la entrada h235SecurityCapability, contiene el campo SrtpCryptoCapability que especificará los conjuntos criptográficos (*crypto-suites*) SRTP.

Se especifica un parámetro cripto SRTP para señalar y negociar parámetros criptográficos SRTP. En esta Recomendación, la definición del parámetro criptográfico se limita a trenes de medios unidifusión entre dos partes, cuando cada fuente dispone de una clave criptográfica única; el soporte de trenes de medios multidifusión o trenes unidifusión multipunto queda en estudio.

El parámetro cripto SRTP permite establecer los parámetros criptográficos SRTP en un solo mensaje o en un único intercambio de mensajes de ida y vuelta. En el caso de un intercambio de este tipo, los parámetros criptográficos podrán ser negociados. Por ejemplo, en la conexión rápida, el punto extremo H.323 oferente envía un conjunto de parámetros criptográficos SRTP que se ofrecen al punto extremo H.323 que responde, y cada vez lo encapsula en un mensaje OpenLogicalChannel H.245 independiente. El punto extremo H.323 que responde puede aceptar uno de los parámetros ofrecidos y emitir una respuesta que incluye el subconjunto de parámetros seleccionados encapsulado en un mensaje OpenLogicalChannel H.245.

En el caso de un solo intercambio de mensajes no hay negociación. El punto extremo H.323 oferente envía los parámetros criptográficos SRTP al punto extremo H.323 que responde, el cual acepta los parámetros ofrecidos o rechaza la llamada.

Pueden añadirse procedimientos criptográficos de claves públicas para garantizar la confidencialidad extremo a extremo y autenticar la información de claves de sesión SRTP

intercambiada entre puntos extremos H.323. La información de claves SRTP puede criptarse y firmarse cuando el protocolo de seguridad de encapsulación (por ejemplo, IPsec, TLS) termina en un dispositivo intermedio, lo que impide garantizar la seguridad extremo a extremo.

2 Referencias

2.1 Referencias normativas

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

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

– Recomendación UIT-T H.235.0 (2005), *Marco de seguridad H.323: Marco de seguridad para sistemas multimedia de la serie H. (H.323 y otras basadas en H.245)*.

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

– Recomendación UIT-T H.460.11 (2004), *Establecimiento diferido de la comunicación en los sistemas H.323*.

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

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

– IETF RFC 2733 (1999), *An RTP Payload Format for Generic Forward Error Correction*.

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

– IETF RFC 3550 (2003), *RTP: A Transport Protocol for Real-Time Applications*.

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

– IETF RFC 3852 (2004), *Cryptographic Message Syntax (CMS)*.

2.2 Referencias informativas

– IETF Draft, F. Andreasen, M. Baugher, D. Wing: *Session Description Protocol Security Descriptions for Media Streams,* <draft-ietf-mmusic-sdescriptions-11.txt>.

3 Abreviaturas, siglas o acrónimos

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

AES Norma de criptación avanzada (*advanced encryption algorithm*)

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

CA Autoridad de certificación (*certificate authority*)

CEK Clave de criptación de contenido (*content encryption key*)

CMS Sintaxis de mensaje criptográfico (*cryptographic message syntax*)

EP Punto extremo (*endpoint*)

FEC Corrección de errores en recepción (*forward error correction*)

FFS En estudio (*for further study*)

F8 Algoritmo de criptación UMTS (*UMTS encryption algorithm*)

GK Controlador de acceso (*gatekeeper*)

GW Pasarela (*gateway*)

HMAC Código de autenticación de mensaje de troceo con aplicación de clave (*keyed-hash message authentication code*)

IETF Grupo de tareas especiales de ingeniería en Internet (*Internet engineering task force*)

KDR Tasa de obtención de claves (*key derivation rate*)

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

MKI Identificador de clave maestra (*master key identifier*)

OID Identificador de objeto (*object identifier*)

OLC Apertura de canal lógico (*open logical channel*)

PKI Infraestructura de claves públicas (*public key infrastructure*)

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

ROC Contador con retorno a cero (*roll-over counter*)

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*)

SHA1 Algoritmo de generación numérica seguro N.º 1 (*secure hash algorithm 1*)

SRTCP Protocolo de control de transporte en tiempo real seguro (*secure real-time transport control protocol*)

SRTP Protocolo de transporte en tiempo real seguro (*secure real-time transport protocol*)

SSRC Fuente de sincronización (*synchronization source*)

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

WSH Indicio de tamaño de ventana (*window size hint*)

4 Descripción de parámetros

Para el intercambio de la capacidad criptográfica y la información de claves de SRTP se utilizan dos parámetros:

– **SrtpCryptoInfo** dentro de **StrpCryptoCapability** contendrá el conjunto criptográfico y los parámetros de sesión. El parámetro **SrtpCryptoInfo** será transportado en el parámetro **genericH235SecurityCapability** de H.245 para señalar y negociar los parámetros criptográficos SRTP.

– **SrtpKeyParameters** dentro de **SrtpKeys** contendrá la información de claves SRTP. El contenedor **SrtpKeys** en el parámetro **h235Key** de H.245 transportará uno o varios **SrtpKeyParameters** con las claves SRTP.

En esta Recomendación, la utilización de los parámetros criptográficos SRTP se limita a trenes de medios unidifusión entre dos partes, cuando cada fuente dispone de una clave criptográfica única; el soporte de trenes de medios multidifusión o trenes unidifusión multipunto queda en estudio.

4.1 Transporte de parámetros SRTP

Una conexión de medios SRTP dúplex consiste en dos canales unidireccionales, uno en cada sentido; cada oferta criptográfica se transporta en un mensaje **OpenLogicalChannel** H.245 separado.

4.1.1 Transporte de la información SrtpKeys

La información de claves criptográficas SRTP **SrtpKeys** será transportada en el campo **genericKeyMaterial** del parámetro **secureSharedSecret** (**V3KeySyncMaterial**) incluido en el contenedor **h235Key**, en el parámetro **encryptionSync** de los mensajes **OpenLogicalChannel** de H.245.

El contenido de clave criptográfica SRTP en el contenedor **genericKeyMaterial** será identificado mediante el valor del identificador de objeto H.235.8 (véase el cuadro 1) en el campo **standard** de **capabilityIdentifier**, dentro del campo **genericH235SecurityCapability** de **encryptionAuthenticationAndIntegrity** en **h235Media** del **dataType** en la instrucción de apertura OLC.

Se podrá utilizar la misma oferta criptográfica en propuestas alternativas de **OpenLogicalChannel** para el mismo canal, con el mismo valor de **sessionID** en **H2250LogicalChannelParameters**. Como sólo se aceptará una de estas sesiones alternativas, está garantizada la unicidad de la clave.

4.1.2 Transporte del parámetro SrtpCryptoCapability

El parámetro **SrtpCryptoCapability** será transportado en el campo **genericH235SecurityCapability** de **encryptionAuthenticationAndIntegrity** en **h235Media** del parámetro **dataType** de los mensajes **OpenLogicalChannel**.

El mensaje **TerminalCapabilitySet** H.245 puede incluir una o varias entradas **h235SecurityCapability** en el **capabilityTable**. A fin de poder indicar el soporte de esos procedimientos, el punto extremo H.323 deberá especificar los siguientes valores para **genericH235SecurityCapability** dentro de **encryptionAuthenticationAndIntegrity** en una entrada **h235SecurityCapability**:

- **capabilityIdentifier** contendrá el OID H.235.8 (véase el cuadro 1) en el campo **standard**;
- **maxbitRate**, **collapsing**, **nonCollapsing** y **transport** no serán utilizados;
- **nonCollapsingRaw** contendrá el parámetro **SrtpCryptoCapability**.

Cuadro 1/H.235.8 – Identificador de objeto H.235.8

Valor de OID
{ itu-t (0) recommendation (0) h (8) 235 version (0) 4 90 }

4.2 Descripción del parámetro SrtpCryptoCapability

Este parámetro puede contener uno o varios parámetros **SrtpCryptoCapability** que podrán utilizarse para especificar las capacidades de la sesión SRTP. Los elementos **BOOLEANOS FACULTATIVOS** se interpretarán así:

1) si es FALSO, el sistema no soporta la capacidad;

2) si es VERDADERO, la capacidad se necesita y el sistema la soporta;

3) si no se incluye, el sistema soporta la capacidad, pero no es necesaria.

Cuando se utiliza **SrtpCryptoCapability** en un intercambio de capacidades, existe la posibilidad de indicar todas las opciones aceptables dentro de una capacidad genérica única. En este caso, la

omisión de un elemento **BOOLEANO FACULTATIVO** significará que el sistema soporta la capacidad, pero no es necesaria.

Cuando se utiliza en una expresión **dataType** de la instrucción OLC, sólo puede utilizarse una opción y deberán observarse las siguientes reglas:

- **FecOrder** puede contener sólo uno de los valores facultativos.
- En **SrtpSessionParameters**, los valores **BOOLEANOS FACULTATIVOS** deben ser VERDADERO o FALSO.
- **SrtpCryptoCapability** debe contener sólo un elemento **SrtpCryptoInfo** único.

El parámetro **SrtpCryptoInfo** consiste en un campo **cryptoSuite** obligatorio y campos facultativos **sessionParams** y **allowMKI** que se describen a continuación.

Cuadro 2/H.235.8 – Identificadores de objetos de conjunto criptográfico H.235.8

Conjunto criptográfico	Valor de OID
AES_CM_128_HMAC_SHA1_80	{ itu-t (0) recommendation (0) h (8) 235 version (0) 4 91 }
AES_CM_128_HMAC_SHA1_32	{ itu-t (0) recommendation (0) h (8) 235 version (0) 4 92 }
F8_128_HMAC_SHA1_80	{ itu-t (0) recommendation (0) h (8) 235 version (0) 4 93 }

4.2.1 cryptoSuite

El identificador de objeto (véase el cuadro 2) en el campo **cryptoSuite** especifica los algoritmos de criptación y de autenticación que van a ser utilizados en la sesión SRTP. La especificación de SRTP tiene muchos parámetros que se agrupan en tres opciones, denominadas "conjuntos criptográficos", a los que pueden añadirse otros conjuntos criptográficos. Los tres que se definen son AES_CM_128_HMAC_SHA1_80, AES_CM_128_HMAC_SHA1_32, y F8_128_HMAC_SHA1_80. Los parámetros SRTP agrupados en cada uno de estos conjuntos se muestran en las filas del cuadro 3.

Cuadro 3/H.235.8 – Valores por defecto de los conjuntos criptográficos

Parámetro SRTP	AES_CM_128_ HMAC_SHA1_80	AES_CM_128_ HMAC_SHA1_32	F8_128_ HMAC_SHA1_80
Longitud de la clave maestra	128 bits	128 bits	128 bits
Valor complementario	112 bits	112 bits	112 bits
Vida útil	2^31 paquetes	2^31 paquetes	2^31 paquetes
Cifrado	Contador AES	Contador AES	F8
Clave de criptación	128 bits	128 bits	128 bits
MAC	HMAC-SHA1	HMAC-SHA1	HMAC-SHA1
Longitud del rótulo de autenticación	80 bits	32 bits	80 bits
Longitud de la clave de autenticación SRTP	160 bits	160 bits	160 bits
Longitud de la clave de autenticación SRTCP	160 bits	160 bits	160 bits

El campo **cryptoSuite** es un parámetro negociado.

4.2.2 sessionParams (parámetros de la sesión)

Los parámetros de la sesión pueden ser negociados o declarativos; la definición de un parámetro de sesión específico indicará si se trata de un parámetro negociado o declarativo. Los parámetros negociados pueden aplicarse a los datos que se envían en ambos sentidos, mientras que los declarativos se aplican únicamente a los medios enviados por la entidad que generó la descripción de la sesión. Por consiguiente, un parámetro declarativo en una oferta se aplica a los medios enviados por el oferente, mientras que un parámetro declarativo en una respuesta se aplica a los medios enviados por el respondedor.

El campo facultativo **sessionParams** contiene parámetros de sesión SRTP.

4.2.2.1 kdr (tasa de obtención de claves)

KDR especifica la tasa de obtención de claves que se describe en la sección 4.3.1 de (RFC 3711). El valor debe ser un entero de la serie {1, 2, ..., 24}, que denota una potencia de 2 entre 2^1 y 2^24, inclusive. La tasa de obtención de claves SRTP controla con qué frecuencia se obtiene la clave de una nueva sesión de una clave maestra SRTP (RFC 3711). Cuando no se especifique la tasa de obtención de claves (se omite el parámetro KDR), se realiza una deducción de clave inicial única (RFC 3711). KDR representa un parámetro declarativo.

4.2.2.2 unencryptedSrtp (SRTP no criptado)

Se trata de un campo booleano facultativo que, si está presente, indica que las cabidas útiles del paquete SRTP no han sido criptadas. Éste es un parámetro negociado.

4.2.2.3 unencryptedSrtcp (SRTCP no criptado)

Se trata de un campo booleano facultativo que, si está presente, indica que las cabidas útiles del paquete SRTCP no han sido criptadas. Éste es un parámetro negociado.

4.2.2.4 unauthenticatedSrtp (SRTP no autenticado)

Las cabidas útiles de los paquetes SRTP y SRTCP son autenticadas por defecto. Se trata de un campo booleano facultativo que, si está presente, indica que las cabidas útiles del paquete SRTP no han sido autenticadas. La especificación de SRTP exige la autenticación de mensajes para SRTCP, pero no para SRTP (RFC 3711). Éste es un parámetro negociado.

4.2.2.5 fecOrder (orden de la FEC)

fecOrder indica el orden del tratamiento de la corrección de errores en recepción para los paquetes RTP (RFC 3550, RFC 2733) con relación a la criptación SRTP en el emisor. Si el valor que se asigna a **fecOrder** es **fecBeforeSrtp**, se aplica la corrección de errores en recepción antes de procesar el protocolo SRTP en el emisor de medios SRTP y después de procesarlo en el receptor de medios SRTP; **fecBeforeSrtp** es la opción por defecto. **fecAfterSrtp** indica un procesamiento en el orden inverso. **fecOrder** es un parámetro declarativo.

4.2.2.6 windowSizeHint (indicación de tamaño de ventana)

SRTP define el parámetro SRTP-WINDOW-SIZE (tamaño de ventana SRTP) (RFC 3711, sección 3.3.2) para la protección contra los ataques por reproducción. El valor mínimo es 64 (RFC 3711), no obstante este valor puede resultar demasiado bajo para algunas aplicaciones, por ejemplo, vídeo.

Este parámetro (WSH) ofrece una indicación de que tan grande debería ser esta ventana para que funcione satisfactoriamente (por ejemplo, basándose en el conocimiento del emisor en cuanto al número de paquetes por segundo). Sin embargo, los descriptores de paquetización de medios podrían aportar suficiente información para facilitar que un receptor deduzca el parámetro satisfactoriamente. Por consiguiente, este valor se considera únicamente como una indicación al receptor, que podrá decidir no tener en cuenta el valor proporcionado.

windowSizeHint es un parámetro declarativo.

4.2.2.7 Definición de nuevos parámetros de sesión SRTP

Los nuevos parámetros de sesión SRTP son obligatorios por defecto. El campo **newParameter** se utiliza como un mecanismo de extensión para los nuevos parámetros de sesión. Si un punto extremo H.323 antiguo recibe un parámetro **SrtpCryptoInfo** con un parámetro de sesión desconocido en el campo **newParameter**, ese nuevo parámetro **SrtpCryptoInfo** se considerará no válido.

4.3 Descripción del parámetro SrtpKeys

El campo **SrtpKeys** contiene uno o varios parámetros de claves **SrtpKeyParameter** que habrán de utilizarse para la sesión SRTP. Cada **SrtpKeyParameter** contiene la información de claves (clave maestra y complementaria) y todas las políticas relacionadas con esa clave maestra, incluyendo cuánto tiempo puede utilizarse (vida útil) y si emplea o no un identificador de clave maestra (MKI) para asociar un paquete SRTP entrante con una determinada clave maestra. Las implementaciones conformes obedecen las políticas asociadas con una clave maestra, y no aceptarán paquetes entrantes que no cumplan con esa política (por ejemplo, una vez que ha expirado la vida útil de la clave maestra).

4.3.1 masterKey (clave maestra)

Se trata de la clave maestra criptográfica que hay que utilizar para la sesión SRTP. La longitud de esta clave queda determinada por el conjunto criptográfico al que se aplica la clave. Si la longitud no concuerda con la especificada para el conjunto criptográfico, el parámetro criptográfico en cuestión se considerará no válido. Cada clave maestra será un número aleatorio criptográficamente y será único para el flujo de medios propuesto.

4.3.2 masterSalt (valor complementario maestro)

Se trata de un valor complementario criptográfico maestro que hay que utilizar para la sesión SRTP. La longitud de este valor la determina el conjunto criptográfico al que se aplica la clave. Si la longitud no concuerda con la especificada para la combinación criptográfica, el parámetro criptográfico en cuestión se considerará no válido. Cada valor complementario maestro será un número aleatorio desde el punto de vista criptográfico y será único para el flujo de medios propuesto.

4.3.3 lifetime (vida útil)

Este campo facultativo representa la vida útil de la clave maestra, que se indica como el número máximo de paquetes SRTP o SRTCP que utiliza esa clave maestra (es decir, el número de paquetes SRTP y el número de paquetes SRTCP tienen que ser, cada uno de ellos, menores que la vida útil). El valor de vida útil puede expresarse como un entero positivo distinto de cero o como una potencia de dos. El valor "vida útil" no debe sobrepasar el valor máximo de vida útil del paquete del conjunto criptográfico. Si la vida útil es demasiado larga o no es válida por otro motivo, todo el parámetro criptográfico se considerará no válido. Si el campo vida útil no está presente se utilizará la vida útil por defecto. Esto resulta conveniente cuando la vida útil de la clave criptográfica SRTP es el valor por defecto.

4.3.4 masterKeyId (identificador de clave maestra)

Este campo facultativo permite especificar la política sobre cómo han de identificarse las claves para la sesión SRTP. MKI representa el identificador de la clave maestra SRTP. Si se proporciona el MKI, también debe proporcionarse su longitud, que viene dada por el tamaño del campo MKI en el paquete SRTP, especificado en bytes. Si no se especifica la longitud de MKI o si su valor sobrepasa 128 (bytes), todo el parámetro criptográfico se considerará no válido.

Como se mencionó antes, el parámetro de clave puede contener una o varias claves maestras. Cuando este parámetro contiene más de una clave maestra, todas las claves maestras en ese

parámetro de clave incluirán un valor MKI. Cuando se utiliza el MKI, su longitud debe ser la misma para todas las claves en un parámetro criptográfico determinado.

4.4 Inicialización del contexto criptográfico SRTP

Además de los diversos parámetros SRTP que se definieron anteriormente, hay tres piezas de información que son esenciales para el funcionamiento de las claves SRTP por defecto:

- SSRC: Fuente de sincronización
- ROC: Contador con retorno a cero para una SSRC determinada
- SEQ: Número de secuencia de una SSRC determinada

En una sesión unidifusión, como se define aquí, existen tres limitaciones de esos valores. La primera se aplica a la SSRC y hace que un tren de claves SRTP sea único con respecto a otros participantes. Como se explicó en SRTP, el tren de claves no debe utilizarse nuevamente en dos o más piezas diferentes de texto normal.

Si se reutiliza el tren de claves, el texto cifrado será vulnerable al análisis criptográfico. Una de las vulnerabilidades es que los campos de texto normal conocido en un tren pueden exponer porciones del tren de claves reutilizado y esto puede exponer a su vez más texto normal en otros trenes. El uso compartido de claves es un problema general (RFC 3711) porque todas las transformadas de criptación SRTP actuales utilizan trenes de claves. SRTP permite mitigar ese problema al incluir la SSRC del emisor en el tren de claves. No obstante, SRTP no resuelve completamente este problema ya que el protocolo de transporte en tiempo real sufre de colisiones SSRC, las cuales son poco frecuentes (RFC 3550) aunque bastante posibles. Durante una colisión, dos o más SSRCs que comparten una clave maestra tendrán trenes de claves idénticos para porciones del espacio de número de secuencia RTP que se superponen. La descripción de la seguridad de SRTP impide que el tren de claves se utilice nuevamente obligando al emisor y al receptor de la descripción de seguridad a utilizar claves maestras únicas. Por consiguiente, la primera limitación se satisface.

Ahora bien, hay otro tipo de colisiones SSRC: la SSRC se utiliza para identificar el contexto criptográfico y, por tanto, la criptación, la clave, el ROC, etc., para poder procesar los paquetes entrantes. En caso de colisiones SSRC, la identificación del contexto criptográfico se vuelve ambigua y los paquetes no pueden procesarse correctamente. Además, si va a enviarse un paquete BYE de RTCP para una SSRC que colisiona, probablemente habrá que protegerlo.

La segunda limitación es que el ROC debe estar en cero en el momento en que cada SSRC comienza a enviar paquetes. Por lo tanto, no existe el concepto de "adhesión tardía" en las descripciones de seguridad de SRTP, que están limitadas a la unidifusión y a funcionar por parejas. El ROC y la SEQ forman un "índice de paquete" en la transformada SRTP por defecto y el ROC se fija sistemáticamente a cero al inicio de la sesión, con arreglo a esta Recomendación.

La tercera limitación tiene que ver con el valor inicial de SEQ, que debería elegirse en la gama de 0..2^15 – 1; esto impedirá una ambigüedad cuando se pierden paquetes al comienzo de la sesión. Si la fuente SSRC selecciona aleatoriamente un valor de número de secuencia alto al empezar la sesión, puede colocar el receptor en una situación ambigua: si los paquetes iniciales se pierden durante el tránsito hasta alcanzar el punto de retorno a cero del número de secuencia (superior a 2^16 – 1), es posible que el receptor no reconozca que tiene que incrementar el ROC. Al restringir la SEQ inicial a la gama de 0..2^15 – 1, la determinación del índice de paquete SRTP encontrará el valor correcto del ROC, a menos que se pierdan todos los primeros 2^15 paquetes (lo cual no es imposible, pero sí bastante improbable). Véase la sección 3.3.1 de la especificación de SRTP en lo que concierne a la determinación del índice de paquete (RFC 3771).

4.4.1 Vinculación tardía de varios SSRC a un contexto criptográfico

Por consiguiente, el índice de paquete depende de la SSRC, la SEQ de un paquete entrante y el ROC, el cual representa una variable del contexto criptográfico SRTP. Por lo tanto, la seguridad

del SRTP depende en gran medida de la unicidad de la SSRC. Dadas las limitaciones anteriores, los contextos criptográficos SRTP unidifusión pueden ser establecidos sin la necesidad de negociar valores SSRC en la descripción de la seguridad SRTP. En cambio, en esta Recomendación se recomienda un método denominado "vinculación tardía". Cuando llega un paquete, su SSRC puede ser vinculada al contexto criptográfico al comenzar la sesión (es decir, cuando llega el paquete SRTP) y no en el momento de la señalización de la sesión (es decir, cuando se recibe un mensaje H.245). Cuando llega el paquete que contiene la SSRC, el receptor mantiene todos los elementos de datos necesarios para el contexto criptográfico SRTP (obsérvese que el valor ROC es 0 por definición; si tuvieran que soportarse valores distintos de 0, se requeriría señalización adicional). En otras palabras, el contexto criptográfico para una sesión RTP segura utilizando vinculación tardía se identifica inicialmente mediante el mensaje H.245 como:

<*, address, port>

donde '*' es una SSRC comodín, "address" es la dirección de recepción local del **mediaChannel**, y "port" es el puerto de recepción local de **portNumber**. Cuando se recibe el primer paquete con ssrcX en su campo SSRC, se define un ejemplar del contexto criptográfico

<ssrcX, address, port>

sujeto a las siguientes limitaciones:

- Los paquetes de medios son autenticados: la autenticación debe ser satisfactoria; de lo contrario, no se crea un ejemplar del contexto criptográfico.
- Los paquetes de medios no son autenticados: el ejemplar de contexto criptográfico se crea automáticamente.

Debería observarse que la utilización de la vinculación tardía cuando no hay autenticación de los paquetes de medios SRTP está sometida a diversos ataques contra la seguridad y por consiguiente no es recomendable (por supuesto, puede decirse lo mismo del SRTP no autenticado en general).

Obsérvese asimismo que la utilización de la vinculación tardía sin autenticación producirá la creación de un estado local como resultado de la recepción de un paquete de cualquier SSRC desconocida. Por lo tanto, no se recomienda el SRTP no autenticado ya que propicia los ataques por denegación de servicio. No hay ese inconveniente en la vinculación tardía con autenticación.

4.4.2 Compartición de contextos criptográficos entre sesiones o varias SSRC

Con las limitaciones y los procedimientos descritos anteriormente no es necesario señalar explícitamente la SSRC, el ROC y la SEQ para una sesión RTP unidifusión. Así, no hay parámetros criptográficos SRTP para señalizar SSRC, ROC o SEQ. Por consiguiente, múltiples SSRC de la misma entidad compartirán los parámetros criptográficos SRTP cuando se emplea la vinculación tardía. La situación de múltiples SSRC de la misma entidad se presenta cuando hay múltiples fuentes (micrófonos, cámaras, etc.) o varias cabidas útiles RTP que necesitan multiplexación SSRC dentro de esa misma sesión.

El protocolo H.245 posibilita la definición de múltiples sesiones RTP en la misma descripción de medios, y las sesiones RTP compartirán además los parámetros criptográficos SRTP. Una aplicación que utiliza el parámetro criptográfico SRTP de esta manera comparte una clave maestra entre sesiones RTP o SSRC y sustituirá la clave maestra cuando el número agregado de paquetes entre todas las SSRC se aproxime a 2^31. Las SSRC que comparten una clave maestra deben ser únicas entre ellas.

La vida útil de todas las claves que se obtienen a partir de la clave maestra depende de la vida útil de esta clave maestra. Si la vida útil de la clave maestra es 2^31 paquetes y una clave deducida ha enviado 2^31 – y paquetes, en ese caso cualquier clave obtenida de esa clave maestra puede enviar sólo *y* paquetes. Esto se debe a que la vida útil corresponde a la cantidad de entropía o de aleatoriedad en la clave, y al deducir una clave de una clave maestra no se introduce aleatoriedad (la aleatoriedad o entropía es fija).

4.4.3 Supresión de contextos criptográficos

El mecanismo definido anteriormente aborda la cuestión de la creación de contextos criptográficos. Sin embargo, en la práctica, los participantes en la sesión pueden desear la supresión de contextos criptográficos antes de la terminación de la sesión. Debido a que un contexto criptográfico contiene información que no puede ser recuperada automáticamente (por ejemplo, ROC), es importante que el emisor y el receptor se pongan de acuerdo sobre cuándo puede suprimirse un contexto criptográfico y, quizás más importante, cuando no se puede suprimir.

Cuando el contexto criptográfico se suprime, el ROC se pierde y no puede ser recuperado automáticamente (a menos que sea 0) aun cuando se utilice la vinculación tardía para un tren unidifusión.

Los contextos criptográficos serán suprimidos cuando se recibe un **CloseLogicalChannel**. Además, la supresión del contexto criptográfico seguirá las mismas reglas de la supresión de SSRC a partir del cuadro de miembros (RFC 3711); obsérvese que esto puede suceder como resultado de un paquete BYE SRTCP o de un fin de temporización simple debido a inactividad. Los participantes en una sesión inactiva que no desean que se aplique el fin de temporización a sus contextos criptográficos deben enviar paquetes SRTCP a intervalos regulares.

5 Procedimientos

Los procedimientos SRTP que se describen a continuación deben ser utilizados únicamente para negociar la seguridad de los trenes de medios unidifusión de las dos partes en aquellas situaciones cuando el canal de señalización H.245 esté protegido por un protocolo de seguridad de los datos por encapsulación, por ejemplo, IPsec (RFC 2401), TLS (RFC 2246). El intercambio de parámetros criptográficos SRTP mediante mensajes H.245 permitirá las siguientes funciones:

1) Intercambio y negociación de capacidades de criptación e integridad de medios SRTP.
2) Negociación y establecimiento de la criptación inicial y los algoritmos, claves y parámetros de sesión que habrán de utilizarse para los trenes SRTP en cada sentido.
3) Modificación de la criptación y los algoritmos, claves y parámetros de sesión en cualquier momento durante la sesión SRTP.

5.1 Intercambio de capacidades de seguridad

Las combinaciones criptográficas SRTP, los algoritmos de criptación e integridad que puede soportar un punto extremo H.323 serán identificados mediante **SrtpCryptoCapability**.

El intercambio de capacidades de seguridad será proporcionado por el intercambio de capacidades de terminal existente, utilizando una o varias entradas **h235SecurityCapability** en el **capabilityTable** del mensaje **TerminalCapabilitySet** H.245. El campo **mediaCapability** en la entrada **h235SecurityCapability** del **capabilityTable** se utiliza para asociar la capacidad de seguridad con una entrada de capacidad de medios particular en el **capabilityTable**.

El campo **encryptionAuthenticationAndIntegrity** en la entrada **h235SecurityCapability** contiene el campo **genericH235SecurityCapability** que especificará las combinaciones criptográficas SRTP identificadas por los OID H.235.8. Si el campo **standard** del **capabilityIdentifier** del campo **genericH235SecurityCapability** contiene el OID H.235.8 (véase el cuadro 1), el campo **SrtpCryptoCapability** contendrá uno o varios parámetros **SrtpCryptoInfo** que representan las combinaciones criptográficas que soporta el punto extremo H.323. El campo **cryptoSuite** en el campo **SrtpCryptoInfo** contiene un OID definido en el cuadro 2 que permite identificar una combinación criptográfica particular. Dentro del campo **SrtpCryptoInfo**, el campo **sessionParams** identifica los parámetros de sesión, y el campo **allowMKI** indica si el punto extremo H.323 soporta el MKI.

5.2 Negociación inicial

5.2.1 Oferta criptográfica inicial

Cada oferta criptográfica es transportada en un mensaje **OpenLogicalChannel** independiente, y contendrá una estructura **SrtpCryptoInfo** en **SrtpCryptoCapability**, y una o varias estructuras **SrtpKeyParameters** en **SrtpKeys**.

Para los procedimientos H.245 normales (sin conexión rápida) el punto extremo H.323 incluirá la oferta criptográfica que se describe en las estructuras **SrtpCryptoInfo** y **SrtpKeyParameters,** en un mensaje **OpenLogicalChannel** H.245 enviado hacia adelante (del punto extremo H.323 oferente al punto extremo H.323 respondedor). El punto extremo H.323 debería ofrecer la capacidad de seguridad de mayor preferencia para el director, tal y como se indicó durante el intercambio de capacidades de terminal, siempre y cuando disponga de esa capacidad.

Para los procedimientos de conexión rápida, el punto extremo H.323 oferente debe enviar cada oferta criptográfica descrita en las estructuras **SrtpCryptoInfo** y **SrtpKeyParameters**, en mensajes **OpenLogicalChannel** H.245 independientes enviados hacia adelante (desde el punto extremo H.323 oferente hacia el punto extremo H.323 respondedor).

Los mensajes **OpenLogicalChannel** ofrecidos se transmitirán por orden de preferencia, enumerando en primer lugar el conjunto criptográfico preferente. Los conjuntos criptográficos de mayor preferencia deben ser criptográficamente más fuertes que los siguientes. Por lo general, un conjunto criptográfico con mayor preferencia debería ser criptográficamente más fuerte que otro con menor preferencia.

Cuando se expide una oferta criptográfica, el oferente debe estar preparado para soportar la seguridad de los medios de conformidad con cualquiera de los parámetros criptográficos ofrecidos, lo que puede plantear dos problemas. El primero es que el oferente no sabe qué clave utilizará el respondedor para los medios enviados al oferente. Como pueden llegar medios antes de la respuesta criptográfica, existe la posibilidad de que se produzca un retardo o un recorte. Si el oferente no puede aceptarlo, debería utilizar un mecanismo como el de los procedimientos de establecimiento diferido de la comunicación de H.460.11 a fin de evitar el problema antes mencionado.

Cuando existen varias ofertas puede presentarse otro problema: el oferente no puede deducir cuál de las ofertas fue aceptada por el respondedor hasta que se recibe la respuesta criptográfica, y entretanto pueden llegar medios. Si el oferente no puede aceptarlo, debería enviar una oferta como máximo, o bien debería utilizar un mecanismo tal como los procedimientos de establecimiento diferido de la comunicación de H.460.11 a fin de evitar este problema.

SrtpCryptoInfo puede incluir parámetros de sesión.

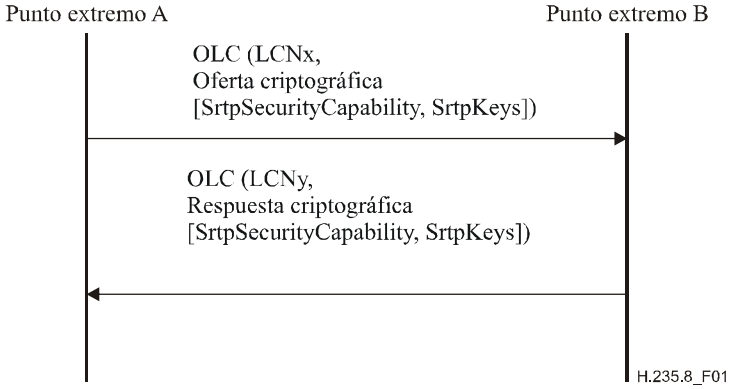

Figura 1/H.235.8 – Intercambio oferta-respuesta de la conexión rápida

5.2.1.1 Respuesta criptográfica inicial

5.2.1.1.1 Observaciones generales

Estos procedimientos se aplican tanto a los procedimientos de conexión rápida como a los de H.245 normales. Una respuesta criptográfica debe contener una estructura **SrtpCryptoInfo** en la **SrtpCryptoCapability** y una o varias estructuras **SrtpKeyParameters** en **SrtpKeys**.

El punto extremo H.323 respondedor aplicará el conjunto criptográfico seleccionado de la oferta criptográfica al canal SRTP unidireccional correspondiente en el sentido inverso y generará la clave o claves que habrán de ser utilizadas para ese canal SRTP en el sentido inverso.

Adicionalmente, el punto extremo H.323 respondedor debe incluir una o varias claves en **SrtpKeys**, que hay que utilizar en el tren SRTP desde el punto extremo H.323 respondedor hacia el punto extremo H.323 oferente. El punto extremo H.323 respondedor también puede incluir cualesquiera parámetros de sesión de la oferta criptográfica que desee negociar.

Sólo podrán ser aceptados los parámetros que sean válidos; éstos no violan ninguna de las reglas generales definidas para las descripciones de seguridad, ni ninguna de las reglas específicas definidas para los métodos de transporte y de asignación de claves en cuestión.

Para la conexión rápida, cuando se selecciona una de las ofertas criptográficas válidas, el respondedor debe seleccionar la de mayor preferencia que soporte, es decir, el primer parámetro soportado válido en la lista, considerando las capacidades del respondedor y las políticas de seguridad. Si ninguna de las ofertas es válida, o no soporta ninguna de las ofertas válidas, se rechazará el tren de medios ofrecido.

Cuando se acepta una oferta criptográfica, la respuesta correspondiente contendrá la clave o claves que habrá de utilizar el respondedor para enviar medios al oferente. Obsérvese que se proporcionará una clave, independientemente de los parámetros de sentido en la oferta o la respuesta.

Además, en la respuesta criptográfica se incluirán los parámetros de sesión que van a ser negociados. En la respuesta criptográfica no se incluyen los parámetros de sesión declarativos proporcionados por el oferente, pero el respondedor puede proporcionar su propio conjunto de parámetros de sesión declarativos.

Cuando el respondedor acepta uno de los parámetros criptográficos ofrecidos, puede empezar a enviar medios al oferente de conformidad con la oferta criptográfica seleccionada. Obsérvese, sin embargo, que es posible que el oferente no pueda procesar correctamente esos paquetes de medios hasta haber recibido la respuesta criptográfica.

5.2.1.1.2 Procedimientos de conexión rápida

Para los procedimientos de conexión rápida, el punto extremo H.323 respondedor que recibe las ofertas criptográficas en uno o varios mensajes **OpenLogicalChannel** H.245 responderá aceptando una de las ofertas criptográficas mediante el envío de un mensaje **OpenLogicalChannel** H.245 que contendrá la respuesta criptográfica mostrada en la figura 1, o rechazando todas las ofertas criptográficas mediante el envío de un mensaje **ReleaseComplete** en el que se indique en **ReleaseCompleteReason**, el motivo **securityDenied**, o bien enviando un elemento **FastConnectRefused** en un mensaje H.225.0. Si el punto extremo H.323 respondedor no soporta esta Recomendación ni ninguna de las propuestas en la oferta criptográfica, rechazará la oferta criptográfica enviando un mensaje **ReleaseComplete** con **ReleaseCompleteReason** fijada a **securityDenied**, o enviando un elemento **FastConnectRefused** en un mensaje H.225.0.

5.2.1.1.3 Procedimientos H.245 normales

Para los procedimientos H.245 normales (sin conexión rápida) se aplica el siguiente procedimiento. Si el punto extremo H.323 aún no ha enviado un **OpenLogicalChannel** que contenga una oferta criptográfica, y recibe un **OpenLogicalChannel** que contiene una oferta criptográfica, enviará un

OpenLogicalChannelAck seguido por un **OpenLogicalChannel** que contenga la respuesta criptográfica como se muestra en la figura 2.

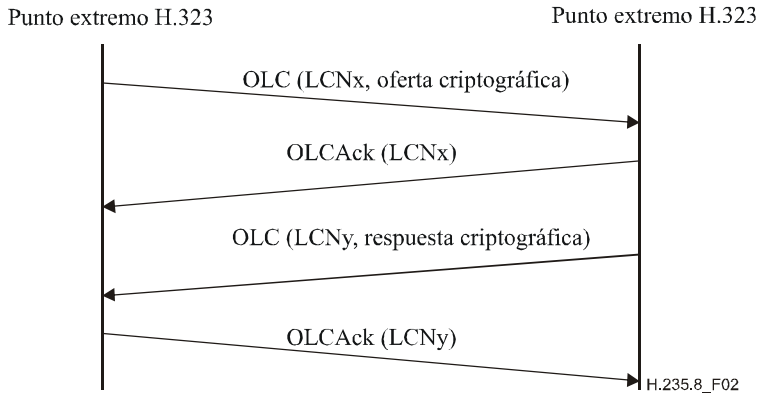

Figura 2/H.235.8 – Intercambio de oferta-respuesta

Si el punto extremo H.323 ya ha enviado un **OpenLogicalChannel** con una oferta criptográfica, y recibe un **OpenLogicalChannel** que contiene una oferta criptográfica, los puntos extremo H.323 director y subordinado seguirán este procedimiento:

1) Un punto extremo H.323 director procesará la oferta criptográfica recibida y si resulta compatible con la oferta criptográfica que ya ha enviado, la aceptará como una respuesta criptográfica enviando un **OpenLogicalChannelAck** como se muestra en la figura 3. Si la oferta criptográfica recibida no es compatible con la oferta criptográfica que ya había enviado, el punto extremo H.323 director la rechazará enviando un **OpenLogicalChannelReject** con el valor **cause** de **securityDenied** como se muestra en la figura 4. Aquí "compatible" significa que los siguientes parámetros en la oferta criptográfica deben concordar con los parámetros correspondientes en la respuesta criptográfica: **cryptoSuite** y los parámetros de sesión negociados.

2) Un punto extremo H.323 subordinado procesará la oferta criptográfica recibida y si es compatible con la oferta criptográfica que ya había enviado, la aceptará como una respuesta criptográfica enviando un **OpenLogicalChannelAck** como se muestra en la figura 3. Si la oferta criptográfica recibida no es compatible con la oferta criptográfica que ya había enviado, pero desea aceptarla, el punto extremo H.323 subordinado podrá hacerlo enviando los siguientes mensajes que se indican en la figura 4:

   a) **OpenLogicalChannelAck** para aceptar la oferta criptográfica inicial del director.

   b) **CloseLogicalChannel** para dar por terminada su propia oferta criptográfica inicial si aún no ha sido recibido el **OpenLogicalChannelReject** del director.

   c) **OpenLogicalChannel** con una respuesta criptográfica que concuerda con la oferta criptográfica del director.

Si el punto extremo H.323 subordinado no soporta la propuesta en la oferta o no desea aceptar la propuesta criptográfica, la rechazará enviando un **OpenLogicalChannelReject** en el que se indique para **cause** el motivo **securityDenied**.

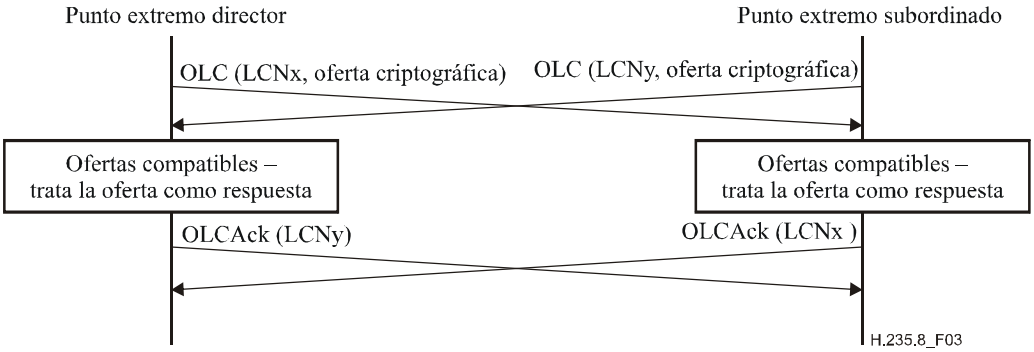

Figura 3/H.235.8 – Intercambio de mensajes oferta-respuesta compatible simultáneo

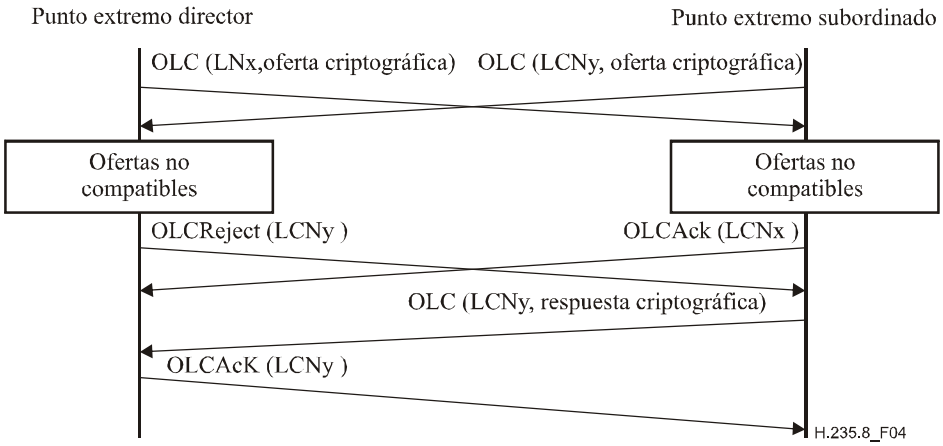

Figura 4/H.235.8 – Intercambio de mensajes oferta-respuesta incompatible simultáneo

5.2.1.2 Procesamiento de la respuesta inicial por el oferente

Cuando el oferente recibe la respuesta criptográfica, verifica si una de las ofertas criptográficas iniciales fue aceptada y reproducida en la respuesta criptográfica. Además, la respuesta criptográfica incluirá una o varias claves que se utilizarán para los medios enviados del respondedor al oferente.

El oferente deberá cerciorarse de que las claves en la respuesta criptográfica no concuerdan con ninguna de las claves en la oferta criptográfica. Si ésta contenía algún parámetro de sesión negociado obligatorio, el oferente deberá cerciorarse de que dichos parámetros están incluidos en la respuesta criptográfica y que concuerdan con los parámetros correspondientes en la oferta criptográfica. Si la respuesta criptográfica contiene algún parámetro de sesión declarativo obligatorio, el oferente podrá soportarlo.

Si no se cumple alguna de estas condiciones, la negociación se considerará fallida.

5.3 Modificación de sesión

Una vez establecido, el tren de medios SRTP podrá ser modificado en cualquier momento utilizando nuevos intercambios de oferta-respuesta para realizar la generación de nuevas claves o modificar el conjunto criptográfico. La nueva oferta criptográfica y la nueva respuesta criptográfica serán transportadas en los parámetros **SrtpCryptoCapability** y **SrtpKeys** de un **OpenLogicalChannel** H.245 para abrir un nuevo canal lógico que sustituirá al existente utilizando los procedimientos **replacementFor**. El punto extremo H.323 oferente incluirá las ofertas criptográficas en uno o varios mensajes **OpenLogicalChannel** H.245.0 dentro de un mensaje H.225.0.

El punto extremo H.323 respondedor que recibe las ofertas criptográficas responderá aceptando una de ellas mediante el envío de un **OpenLogicalChannel** H.245 dentro de un mensaje H.225.0 o rechazando las ofertas con un mensaje **OpenLogicalChannelReject** con **cause** fijado a **securityDenied**. Si la oferta criptográfica se rechaza, se conservan los antiguos parámetros criptográficos.

Cuando se establece una nueva clave maestra habrá una ventana de tiempo durante la cual el punto extremo H.323 debe recibir los medios criptados de conformidad con el intercambio de mensajes de oferta-respuesta nuevo y antiguo. El MKI del paquete SRTP entrante será utilizado para asociar ese paquete con la clave maestra antigua o bien con la clave maestra nueva. Por este motivo, si se prevé que las claves van a cambiar durante una sesión que no modifica las direcciones y los puertos de origen-destino, la utilización del MKI es obligatoria para facilitar que el receptor pueda identificar la información de claves asociada durante el cambio de las claves.

5.4 Sin negociación

En el caso de que no haya negociación del conjunto criptográfico, la clave criptográfica o los parámetros de la sesión, el emisor determinará los parámetros de seguridad para el tren. Debido a que no hay mecanismo de negociación, el emisor sólo incluirá una oferta criptográfica que el receptor aceptará, o que rechazará, enviando un mensaje **ReleaseComplete** con **ReleaseCompleteReason** fijada a **securityDenied**, o un mensaje **OpenLogicalChannelReject** con **cause** fijado a **securityDenied**. El emisor debería seleccionar la descripción de seguridad que considere más segura para sus propósitos.

5.5 Corrección de errores en recepción

Para proteger un tren FEC debe especificarse una clave maestra diferente que se envía a otra dirección IP y/o par de puertos distintos de aquellos a los que se aplica el tren de medios SRTP como se describe en la sección 11.1 de RFC 2733. Este tren FEC será establecido utilizando un mensaje **OpenLogicalChannel** H.245 separado, indicando para **dataType** la especificación **fec**. La clave maestra para el tren FEC será transportada en el campo **genericKeyMaterial** del parámetro **secureSharedSecret** (**V3KeySyncMaterial**) incluido en el contenedor **h235Key** en el parámetro **encryptionSync** del mensaje **OpenLogicalChannel** H.245. La clave maestra será diferente de las demás claves maestras ofrecidas para el tren de medios asociado.

6 Criptografía de clave pública necesaria para asegurar el intercambio de claves para SRTP

Podrán añadirse procedimientos de criptografía de clave pública para proporcionar confidencialidad y autenticación extremo a extremo de la información de las claves de sesión SRTP intercambiada entre puntos extremos H.323, mediante la criptación y posteriormente la firma de la información de las claves SRTP. La criptografía de clave pública puede ser utilizada en aquellos casos en los que el protocolo de seguridad de encapsulación, por ejemplo, IPsec, TLS, termina en un dispositivo intermedio y, por consiguiente, no puede proporcionar seguridad extremo a extremo.

La clave de sesión SRTP que permite criptar los medios SRTP del punto extremo llamante al punto extremo llamado se encripta utilizando la clave pública del punto extremo llamado y se firma con la clave privada del punto extremo llamante. De forma similar, otra clave de sesión SRTP que cripta los medios SRTP del punto extremo llamado al punto extremo llamante será criptada utilizando la clave pública del punto extremo llamante y firmada con la clave privada del punto extremo llamado. El procedimiento que se describe en esta cláusula puede terminar bien en una pasarela o un controlador de acceso, bien en un punto extremo.

La clave de sesión SRTP será transportada utilizando los cuerpos de la sintaxis de mensaje criptográfico (CMS, *cryptographic message syntax*) dentro de mensajes H.245. Dicha sintaxis (RFC 3852) se utiliza para firmar y criptar digitalmente contenido arbitrario del mensaje. La

sintaxis CMS posibilita encapsulaciones múltiples, lo que permite anidar un sobre de encapsulación dentro de otro. En particular, la información de claves de sesión SRTP será transportada dentro de un cuerpo **EnvelopedData** CMS que se firma mediante un cuerpo **SignedData** CMS.

6.1 Identificación del punto extremo

Para identificar un punto extremo, una pasarela o un controlador de acceso en un certificado de clave pública debe utilizarse lo siguiente:

- URL H.323.
- URL normalizado no H.323, por ejemplo, *tel*.
- Identificación de dispositivo/certificado (queda en estudio).

Debe utilizarse un certificado de clave pública para evaluar la asociación de la identidad del punto extremo con su clave pública. El URL H.323 o el URL normalizado no H.323 será almacenado en el campo **subjectAltName** del certificado.

Los puntos extremos pueden mantener un almacén de claves local que contiene los certificados de clave pública de otros puntos extremos con los que desea establecer comunicaciones seguras extremo a extremo. Un punto extremo que envía contenido firmado para proporcionar autenticación extremo a extremo debe incluir un certificado de clave pública que tenga la clave pública necesaria para verificar la firma. Por consiguiente, un punto extremo receptor:

a) verifica que el certificado del emisor esté firmado por una autoridad de certificación (CA) reconocida,

b) o, confía en una confirmación de seguridad en virtud del certificado expedido por una tercera parte. La confirmación debe estar firmada por información de claves que pueda ser verificable mundialmente.

NOTA – Esto puede tener ventajas en aquellos casos en los que no se disponga de una PKI de usuario mundial y se estén utilizando certificados autofirmados o certificados de dispositivo.

6.2 Procedimientos de intercambio de claves SRTP

Si los puntos extremos llamante y llamado desean garantizar la confidencialidad y autenticación extremo a extremo de su información de claves de la sesión SRTP en el caso en que para el establecimiento de la comunicación resulte necesario atravesar uno o varios dispositivos de señalización intermedios, los puntos extremos deberían utilizar la criptografía de claves públicas y el intercambio de certificados de claves públicas X.509 (RFC 3280).

Los procedimientos de oferta-respuesta descritos en cláusulas anteriores de este documento no se modifican excepto por lo que se establece más adelante.

6.2.1 Intercambio de capacidades

Para negociar la utilización de certificados de clave pública para el intercambio de claves SRTP el punto extremo H.323 fijará la **genericH235SecurityCapability** dentro de **encryptionAuthenticationAndIntegrity** en una entrada **h235SecurityCapability** en el **capabilityTable** de un mensaje **TerminalCapabilitySet** H.245 de la siguiente manera:

- el **capabilityIdentifier** debe contener el identificador de objeto CMS H.235.8 (véase el cuadro 4) en el campo **standard**;
- **maxbitRate**, **collapsing**, **nonCollapsing** y **transport** no serán utilizados;
- **nonCollapsingRaw** contendrá el parámetro **SrtpCryptoCapability**.

6.2.2 Intercambio de claves

Si la clave de la sesión SRTP debe criptarse utilizando claves públicas, la clave de la sesión SRTP criptada se transporta dentro de cuerpos de la sintaxis de mensaje criptográfico (CMS) en

mensajes H.245. El cuerpo **EnvelopedData** de CMS y el cuerpo **SignedData** de CMS serán transportados en lugar de las **SrtpKeys** en el campo **genericKeyMaterial** del parámetro **secureSharedSecret** (**V3KeySyncMaterial**) incluido en el contenedor **h235Key** en el parámetro **encryptionSync** de los mensajes **OpenLogicalChannel** H.245. El cuerpo **EnvelopedData** de CMS se colocará en el campo **genericKeyMaterial** seguido inmediatamente por el cuerpo **SignedData** de CMS.

La estructura **SrtpKeys** será criptada utilizando la clave de criptación de contenido (CEK, *content encryption key*) de CMS y se transportará en la estructura **EncryptedContentInfo** de un cuerpo **EnvelopedData** de CMS.

La presencia de un cuerpo CMS que contenga información de clave de sesión SRTP en el contenedor **genericKeyMaterial** será identificada utilizando el valor del identificador de objeto CMS H.235.8 (véase el cuadro 4) en el campo **standard** de **capabilityIdentifier** dentro del campo **genericH235SecurityCapability** de **encryptionAuthenticationAndIntegrity** en **h235Media** del **dataType** en el mensaje de apertura (OLC).

Cuadro 4/H.235.8 – Identificador de objeto CMS H.235.8

Valor de OID
{ itu-t (0) recommendation (0) h (8) 235 version (0) 4 94 }

6.3 Utilización del cuerpo CMS

El punto extremo que genera la información de clave de sesión SRTP **SrtpKeys** (emisor), la criptará utilizando la clave de criptación de contenido (CEK) de CMS, que a su vez es criptada por la clave pública del punto extremo receptor, y colocará dicha información en un cuerpo **EnvelopedData** de CMS. A continuación, el punto extremo emisor firmará digitalmente el cuerpo **EnvelopedData** con su clave privada y creará un cuerpo **SignedData** de CMS que se denomina "firma separada". El punto extremo emisor incluirá el certificado con su clave pública en el cuerpo **SignedData** de CMS, y enviará el cuerpo **EnvelopedData** con el cuerpo **SignedData** "firma separada" al punto extremo receptor. La creación de los cuerpos **EnvelopedData** y **SignedData** por el punto extremo emisor se describe con mayor detalle en las siguientes cláusulas.

El cuerpo **EnvelopedData** y el cuerpo **SignedData** "firma separada" se muestran en la figura 5.

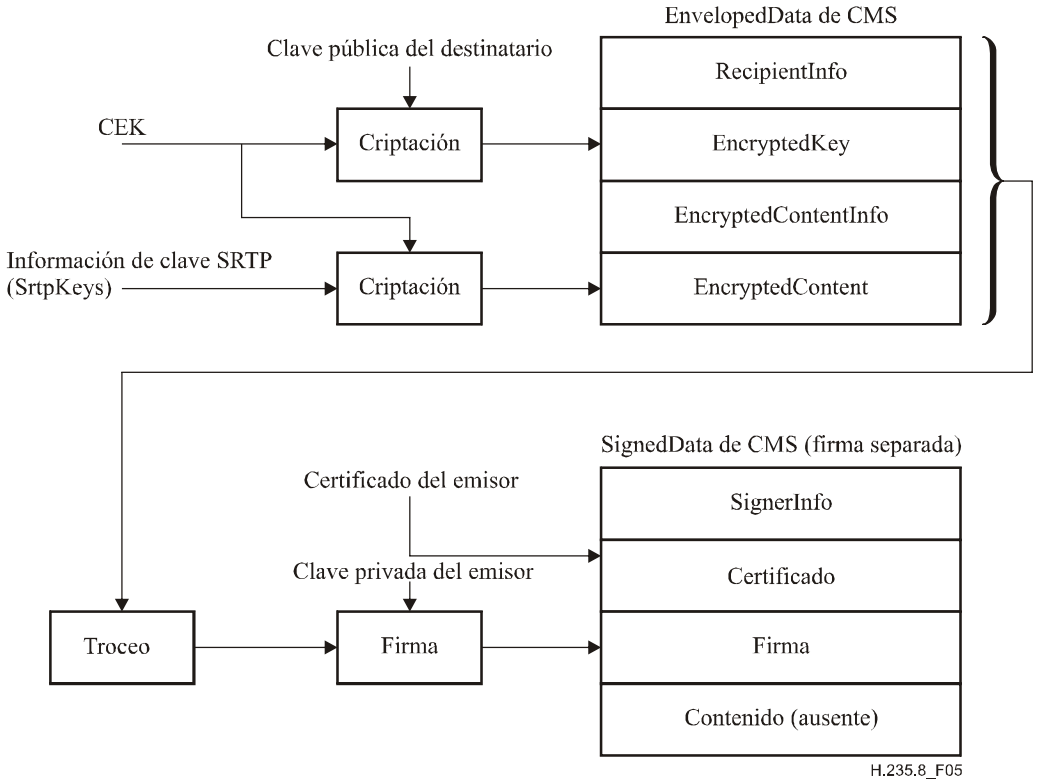

Figura 5/H.235.8 – Cuerpos EnvelopedData y SignedData de CMS

6.3.1 Procedimientos del punto extremo emisor

El punto extremo emisor realizará los siguientes procedimientos para generar, criptar y firmar la información de la clave de sesión SRTP.

6.3.1.1 Cuerpo EnvelopedData (datos en sobre)

El punto extremo emisor creará el cuerpo **EnvelopedData** de la siguiente manera:

1) Genera la información de clave de sesión SRTP **SrtpKeys** para el conjunto criptográfico.
2) Genera una clave de criptación de contenido (CEK) aleatoria.
3) Cripta la CEK utilizando la clave pública del punto extremo receptor. Se supone que el punto extremo emisor ya tiene la clave pública y el certificado del punto extremo receptor. Coloca el identificador del algoritmo utilizado para la criptación de la CEK en el campo **keyEncryptionAlgorithm** de la estructura **RecipientInfo.ktri**.
4) Coloca la CEK criptada en el campo **encryptedKey** de la estructura **RecipientInfo** de un cuerpo **EnvelopedData**. El campo **rid** de la estructura **RecipientInfo.ktri** se utiliza para identificar el certificado y la clave pública del punto extremo receptor que fue utilizado para criptar la CEK.
5) Cripta la información de la clave SRTP **SrtpKeys** utilizando la CEK y coloca el identificador del algoritmo empleado para criptar en el campo **contentEncryptionAlgorithm** de la estructura **EncryptedContentInfo**.
6) Coloca la información de la clave SRTP criptada en el campo **encryptedContent** de la estructura **EncryptedContentInfo**.

6.3.1.2 Cuerpo SignedData (datos firmados)

El punto extremo emisor creará el cuerpo **SignedData** "firma separada" de la siguiente manera:

1) Calcula un resumen de mensaje o valor de troceo para el **EnvelopedData**. El identificador del algoritmo del resumen de mensaje se coloca en el campo **digestAlgorithm** de la estructura **SignerInfo**.

2) Firma el resumen de mensaje mediante la clave privada del punto extremo emisor y coloca el valor de la firma en el campo **signature** de la estructura **SignerInfo**. El identificador del algoritmo de firma se coloca en el campo **signatureAlgorithm** de la estructura **SignerInfo**.

3) Coloca el certificado que contiene la clave pública del punto extremo emisor en la estructura **certificates** de la estructura **SignerData**. El campo **sid** de la estructura **SignerInfo** se fijará de tal manera que permita identificar el certificado utilizando el nombre distinguido del emisor y el número de serie del certificado, o el valor de extensión subjectKeyIdentifier X.509.

4) El campo **eContentType** de la estructura **encapContentInfo** en el cuerpo **SignedData** contendrá el identificador de objeto id-envelopedData. El campo **eContent** de la estructura **encapContentInfo** en el cuerpo **SignedData** no estará presente ya que se trata de una firma separada y el contenido firmado real es el cuerpo **EnvelopedData**.

6.3.2 Procedimientos del punto extremo receptor

El punto extremo receptor llevará a cabo los siguientes procedimientos a fin de verificar y criptar la información de clave de sesión SRTP.

Si el punto extremo receptor detecta cualquier fallo de validación en los procedimientos que se describen más adelante, la llamada será rechazada enviando **ReleaseComplete** con **ReleaseCompleteReason** fijado a **securityDenied**, o enviando un elemento **FastConnectRefused** en un mensaje H.225.0.

6.3.2.1 Cuerpo SignedData (datos firmados)

El punto extremo receptor verificará la recepción del cuerpo **SignedData** "firma separada" de la siguiente manera:

1) Obtiene el certificado del punto extremo emisor de la estructura **certificates** de la estructura **SignerData**.

2) Valida el certificado del punto extremo emisor. Los detalles correspondientes a la validación del trayecto del certificado quedan fuera del alcance de esta Recomendación. Si el receptor no puede autenticar el punto extremo emisor, podrá rechazar la llamada.

3) El punto extremo receptor podrá, por consiguiente, añadir el certificado validado en su almacén de claves.

4) Verifica el valor de la firma en el campo **signature** de la estructura **SignerInfo** utilizando la clave pública del punto extremo emisor a partir del certificado validado. Utiliza el algoritmo de firma especificado en el campo **signatureAlgorithm** de la estructura **SignerInfo**. El resultado de la descriptación será el resumen de mensaje del cuerpo **EnvelopedData** calculado por el punto extremo emisor.

5) Calcula el resumen de mensaje para el cuerpo **EnvelopedData** recibido utilizando el identificador del algoritmo de resumen de mensaje especificado en el campo **digestAlgorithm** de la estructura **SignerInfo**.

6) Compara el valor del resumen de mensaje descriptado con el valor del resumen de mensaje calculado. Si ambos concuerdan, podrá procesarse el cuerpo **EnvelopedData**. Si los resúmenes no concuerdan, el punto extremo receptor rechazará la llamada.

6.3.2.2 Cuerpo EnvelopedData

El punto extremo receptor extraerá la información de clave de sesión SRTP del cuerpo **EnvelopedData** de la siguiente manera:

1) Utiliza el campo **rid** de la estructura **RecipientInfo** para identificar el certificado y la clave privada correspondiente al punto extremo receptor en el almacén de claves de este último. Si el punto extremo receptor recibe un cuerpo **EnvelopedData** que está criptado con una clave pública que le es desconocida, rechazará la llamada.
2) Extrae la CEK criptada del campo **encryptedKey** de una estructura **RecipientInfo.ktri** de un cuerpo **EnvelopedData**.
3) Descripta la CEK utilizando la clave privada del punto extremo receptor y el algoritmo especificado en el campo **keyEncryptionAlgorithm** de la estructura **RecipientInfo.ktri**.
4) Extrae la información de clave de sesión SRTP criptada de la información de clave de sesión SRTP criptada en el campo **encryptedContent** de la estructura **EncryptedContentInfo**.
5) Descripta la información de clave de sesión SRTP por medio de la CEK y el algoritmo especificado en el campo **contentEncryptionAlgorithm** de la estructura **EncryptedContentInfo**.

7 Sintaxis de las descripciones de seguridad SRTP H.235

La sintaxis ASN.1 se define a continuación:

```
H235-SRTP DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

IMPORTS
     GenericData
FROM H323-MESSAGES;


 SrtpCryptoCapability ::= SEQUENCE OF SrtpCryptoInfo -- used in H.245
 genericH235SecurityCapability


 SrtpCryptoInfo ::= SEQUENCE
 {
    cryptoSuite                     OBJECT IDENTIFIER OPTIONAL ,
    sessionParams                   SrtpSessionParameters OPTIONAL,
    allowMKI                        BOOLEAN OPTIONAL,
    ...
 }

 SrtpKeys ::= SEQUENCE OF SrtpKeyParameters  -- used in H.235 V3KeySyncMaterial

 SrtpKeyParameters ::= SEQUENCE
 {
    masterKey                       OCTET STRING,
    masterSalt                      OCTET STRING,
    lifetime                        CHOICE
    {
        powerOfTwo                  INTEGER,
        specific                    INTEGER,
        …
    } OPTIONAL,
    mki                             SEQUENCE
    {
        length                      INTEGER(1..128),
        value                       OCTET STRING,

      ...
    } OPTIONAL,
```

```
    ...
}


SrtpSessionParameters ::= SEQUENCE
{
    kdr                             INTEGER(0..24) OPTIONAL, -- power of 2
    unencryptedSrtp                 BOOLEAN OPTIONAL,
    unencryptedSrtcp                BOOLEAN OPTIONAL,
    unauthenticatedSrtp             BOOLEAN OPTIONAL,
    fecOrder                        FecOrder OPTIONAL,
    windowSizeHint                  INTEGER(64..65535) OPTIONAL,
    newParameter                    SEQUENCE OF GenericData  OPTIONAL,
    ...
}

FecOrder ::= SEQUENCE
{
    fecBeforeSrtp                   NULL OPTIONAL,
    fecAfterSrtp                    NULL OPTIONAL,
    ...
}

END
```

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