Unión Internacional de Telecomunicaciones

UIT-T H.235.6

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: Perfil de criptación vocal con gestión de claves H.235/H.245 nativa

Recomendación UIT-T H.235.6

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.235.6

Marco de seguridad H.323: Perfil de criptación vocal con gestión de claves H.235/H.245 nativa

Resumen

En la presente Recomendación se describen los procedimientos de seguridad para el perfil de criptación vocal (anterior anexo D/H.235), en particular la gestión de claves H.235/H.245 nativa.

En las versiones anteriores de la subserie H.235, este perfil figuraba en el cuerpo principal de la Recomendación H.235 y en su anexo D. En los apéndices IV, V, VI a la H.235.0 se indica la correspondencia entre las cláusulas, las figuras y los cuadros de las versiones 3 y 4.

Orígenes

La Recomendación UIT-T H.235.6 fue aprobada el 13 de septiembre de 2005 por la Comisión de Estudio 16 (2005-2008) del UIT-T por el procedimiento de la Recomendación UIT-T A.8.

Palabras clave

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

PREFACIO

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

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

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

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

NOTA

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

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

PROPIEDAD INTELECTUAL

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

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

ÍNDICE

		Página
1	Alcance	1
2	Referencias	1
	2.1 Referencias normativas	1
	2.2 Referencias informativas	2
3	Términos y definiciones	3
4	Abreviaturas, siglas o acrónimos	3
5	Convenios	5
6	Presentación del sistema	5
	6.1 Perfil de seguridad de criptación vocal	5
7	Señalización y procedimientos H.245	7
	7.1 Funcionamiento seguro del canal H.245	7
	7.2 Funcionamiento inseguro del canal H.245	7
	7.3 Intercambio de capacidades	7
	7.4 Cometido de terminal director	8
	7.5 Señalización de canal lógico	8
	7.6 Seguridad de conexión rápida	8
	7.7 DTMF H.245 criptadas	11
	7.8 Operación Diffie-Hellman	12
8	Señalización y procedimientos	17
	8.1 Compatibilidad con la revisión 1	18
	8.2 Indicación de característica de la versión 3	18
	8.3 Transporte de clave	19
	8.4 Modo OFB mejorado	20
	8.5 Gestión de claves	21
	8.6 Actualización de claves y sincronización	23
	8.7 Interacciones no relacionadas con terminales	28
	8.8 Procedimientos multipunto	28
9	Procedimiento de criptación de tren de medios	29
	9.1 Claves de sesión de medios	30
	9.2 Antiinundación de medios	31
	9.3 Aspectos relativos a RTP/RTCP	33
	9.4 DES triple en modo CBC exterior	35
	9.5 Algoritmo DES que funciona en modo EOFB	36
	9.6 DES triple en el modo EOFB exterior	36
10	Interceptación lícita	37
11	Lista de identificadores de objeto	37

Página

Apéndice I – Detalles de las implementaciones H.323 39
I.1 Métodos de relleno de texto cifrado 39
I.2 Nuevas claves 41

Recomendación UIT-T H.235.6

Marco de seguridad H.323: Perfil de criptación vocal con gestión de claves H.235/H.245 nativa

1 Alcance

En esta Recomendación se especifica un perfil de seguridad para la criptación vocal con gestión de claves H.235/H.245 nativa. Se especifican los procedimientos de criptación vocal y también para la correspondiente gestión de clave H.245 nativa.

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 llamadas y paquetización de trenes de medios para sistemas de comunicaciones multimedios por paquetes*.
- Recomendación UIT-T H.235, versión 1 (1998), *Seguridad y criptado para terminales multimedios de la serie H (basados en las Recomendaciones H.323 y H.245)*.
- Recomendación UIT-T H.235, versión 2 (2000), *Seguridad y criptado para terminales multimedios de la serie H (basados en las Recomendaciones H.323 y H.245)*.
- Recomendación UIT-T H.235, versión 3 (2003), *Seguridad y criptado para terminales multimedios de la serie H (basados en las Recomendaciones H.323 y H.245)* más corrigendum 1 (2005).
- Recomendación UIT-T H.235.0 (2005), *Marco de seguridad H.323*: *Marco de seguridad para sistemas multimedia de la serie H (H.323 y otros basados en H.245)*.
- Recomendación UIT-T H.235.1 (2005), *Marco de seguridad H.323: Perfil de seguridad básico*.
- Recomendación UIT-T H.235.2 (2005), *Marco de seguridad H.323: Perfil de seguridad de firma*.
- Recomendación UIT-T H.235.3 (2005), *Marco de seguridad H.323: Perfil de seguridad híbrido*.
- Recomendación UIT-T H.245 (2005), *Protocolo de control para comunicación multimedia*.
- Recomendación UIT-T H.323 (2003), *Sistemas de comunicación multimedios basados en paquetes*.
- Recomendación UIT-T H.323, anexo F (1999), *Tipos de punto extremo simples*.

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

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

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

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

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

– IETF RFC 2198 (1997), *RTP Payload for Redundant Audio Data*.

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

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

– IETF RFC 2833 (2000), *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*.

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

– US National Institute of Standards, "Advanced Encryption Algorithm (AES)", *Federal Information Processing Standard, (FIPS)* Publication 197, noviembre de 2001, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

– ISO/CEI 9797-1:1999, *Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher*.

– ISO/CEI 9797-2:2002, *Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function*.

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

– ISO/CEI 10116:2006, *Information technology – Security techniques – Modes of operation for an n-bit block cipher*.

2.2 Referencias informativas

[DES FIPS-46-2] US National Institute of Standards, Data Encryption Standard, *Federal Information Processing Standard*, (FIPS) Publication 46-2, diciembre de 1993, http://www.itl.nist.gov/fipspubs/fip46-2.htm.

[DES FIPS-74] US National Institute of Standards, Guidelines for Implementing and Using the Data Encryption Standard, *Federal Information Processing Standard*, (FIPS) Publication 74, abril de 1981, http://www.itl.nist.gov/div897/pubs/fip74.htm.

[DES FIPS-81] US National Institute of Standards, DES Modes of Operation, *Federal Information Processing Standard*, (FIPS) Publication 81, diciembre de 1980, http://www.itl.nist.gov/fipspubs/fip81.htm.

[FIPS PUB 180-1] NIST, FIPS PUB 180-1: *Secure Hash Standard*, abril de 1995 http://csrc.nist.gov/fips/fip180-1.ps.

[LI] ETSI TR 101 772 V1.1.2, Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Service Independent requirements definition; Lawful interception – top level requirements.

[OIW] Stable Implementation – Agreements for Open Systems Interconnection Protocols: Part 12 – OS Security; redactado por el Grupo de Trabajo de implementadores de sistemas abiertos (OIW) en diciembre de 1994; http://nemo.ncsl.nist.gov/oiw/agreements/stable/OSI/12s_9412.txt.

[RFC2268] IETF RFC 2268 (1998), *A Description of the RC2(r) Encryption Algorithm*.

[RFC2405] IETF RFC 2405 (1998), *The ESP DES-CBC Cipher Algorithm With Explicit IV*.

[RFC2412] IETF RFC 2412 (1998), *The OAKLEY Key Determination Protocol*.

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

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

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

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

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

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

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

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

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

3 Términos y definiciones

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

El terminal director genera la **clave de sesión** para la criptación de trenes de medios sólo para una determinada sesión del RTP (sobre un OLC) y cuando más para la duración de una llamada. La clave de sesión generada se cripta con una clave que se calcula a partir del **secreto compartido** de Diffie-Hellman calculado por ambos puntos extremos. En este caso, el secreto compartido DH sirve de clave maestra para la protección de las claves de la sesión.

4 Abreviaturas, siglas o acrónimos

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

3DES DES triple (*triple DES*)

AES Algoritmo de criptación avanzado (*advanced encryption algorithm*)

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

CBC Concatenación de bloques cifrados (*cipher block chaining*)

CFB Retroalimentación cifrada (*cipher feedback*)

DES	Norma de criptación de datos (*data encryption standard*)
DH	Diffie-Hellman
DTMF	Multifrecuencia bitono (*dual tone multi-frequency*)
ECB	Libro de código electrónico (*electronic code book*)
EOFB	Modo OFB mejorado (*enhanced OFB mode*)
EP	Punto extremo (*endpoint*)
FEC	Corrección de errores en recepción (*forward error correction*)
GK	Controlador de acceso (*gatekeeper*)
HMAC	Código de autenticación de mensaje troceado (*hashed message authentication code*)
IPsec	Seguridad del protocolo Internet (*Internet protocol security*)
IV	Vector de inicialización (*initialization vector)*
KS	Clave adicional de seguridad en modo EOFB (*salting key in EOFB mode*)
MAC	Código de autenticación de mensaje (*message authentication code*)
MC	Controlador multipunto (*multipoint controller*)
MCU	Unidad de control multipunto (*multipoint control unit*)
MPS	Tren de cabida útil múltiple (*multiple payload stream*)
OFB	Modo realimentación de salida (*output feedback mode*)
OID	Identificador de objeto (*object identifier*)
OLC	Apertura de canal lógico (*open logical channel*)
RAS	Registro, admisiones y estado (*registration, admission and status*)
RC	Cifrado Rivest (*Rivest cipher*)
ROC	Contador continuo (*roll-over counter*)
RSA	Rivest, Shamir y Adleman
RTCP	Protocolo de control en tiempo real (*real-time control protocol*)
RTP	Protocolo en tiempo real (*real-time protocol*)
SDU	Unidad de datos de servicio (*service data unit*)
SEQ	Número secuencial (*sequence number*)
SHA	Algoritmo troceado asegurado (*secure hash algorithm*)
TCP	Protocolo de control de transmisión (*transmission control protocol*)
TLS	Seguridad de la capa de transporte (*transport layer security*)
TSAP	Punto de acceso al servicio de transporte (*transport service access point*)
UDP	Protocolo de datagrama de usuario (*user datagram protocol*)
UIT	Unión Internacional de Telecomunicaciones
XOR	O exclusivo (*exclusive OR*)

5 Convenios

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

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

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

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

Cuando se utiliza la criptación de medios junto con el relleno de cabida útil, a veces se dice que: "el valor del relleno debería establecerse utilizando el convenio normal del algoritmo de cifrado"; véanse por ejemplo 7.6.1, 8.3 y la figura I.7. Con esto se pretende decir que algunos algoritmos de cifrado (por ejemplo, DES) permiten saber más acerca de cómo el remitente puede escoger el valor del (los) byte(s) de relleno: puede ser, por ejemplo, valores de relleno aleatorios, valores estáticos u otros patrones generados. Aunque el método escogido no afecta la compatibilidad, la calidad de seguridad puede muy bien depender de él. Esto se considera como un aspecto de implementación y no se trata más en esta Recomendación.

6 Presentación del sistema

6.1 Perfil de seguridad de criptación vocal

El perfil de seguridad de criptación vocal no es un perfil independiente como el perfil de seguridad básico. Es más bien una opción del perfil de seguridad básico y se puede utilizar junto con él. Este perfil también depende de ciertos servicios de seguridad como parte de los procedimientos de señalización de llamada y de establecimiento de la conexión; por ejemplo, el convenio de claves Diffie-Hellman y otras funciones de gestión de claves.

Las entidades H.323 pueden implementar esta Recomendación para conseguir la confidencialidad de la conversación. Se ofrecen a tal fin cuatro algoritmos de criptación: los esquemas propuestos consisten en la criptación que utiliza AES, la norma compatible con RC2, la DES o la DES triple basada en el modelo comercial y el requisito de exportabilidad. Además del modo de criptación CBC, las entidades H.323 pueden implementar el modo de criptación de cifrado de trenes EOFB. Algunos entornos que ya ofrecen cierto grado de confidencialidad no necesitarán posiblemente la criptación vocal. En este caso, tampoco se necesitan el convenio de claves Diffie-Hellman ni otros procedimientos de gestión de claves.

Para el caso de la confidencialidad de la voz facultativa, se propone un esquema de criptación que utilice AES de 128 bits compatible con RC2, DES o DES triple basado en el modelo comercial y en el requisito de exportabilidad. Algunos entornos que ya están ofreciendo cierto grado de confidencialidad posiblemente no necesiten la criptación vocal. En este caso, tampoco serán necesarios el convenio de claves Diffie-Hellman ni otros procedimientos de gestión de claves.

En esta Recomendación se describe también la lista de posibles algoritmos de criptación vocal que ofrecen la Rec. UIT-T H.235 versión 2 anexo D o la Rec. UIT-T H.235 versión 3 anexo D.

NOTA 1 – En la especificación de estos otros algoritmos de criptación se tienen en cuenta las observaciones relativas al análisis criptográfico y la seguridad de los algoritmos de criptación, así como la modificación de políticas de exportación criptográfica. En particular, se incluyen en la especificación de esta Recomendación los requisitos de interfuncionamiento con los sistemas que son conformes a las versiones 2 ó 3 de H.235.

Las entidades H.323 que implementen esta Recomendación con la versión 4 de la H.235 o una versión posterior utilizarán preferentemente el algoritmo de criptación vocal AES de 128 bits en sus capacidades de seguridad disponibles a fin lograr la mayor eficacia y seguridad. Estas entidades H.323 podrán asimismo ofrecer como opción un algoritmo de criptación vocal DES triple de

168 bits con miras a alcanzar una mayor compatibilidad con los sistemas H.323 que emplean las funciones de criptación vocal del anexo D/H.235, versiones 2 y 3. Dado que los algoritmos de criptación DES de 56 bits y los compatibles con RC2 (exportables) de 56 bits ya no se consideran lo suficientemente seguros, las entidades H.323 no deberían ofrecer estos algoritmos de criptación débiles, salvo que haya razones específicas para ello, por ejemplo para mantener la compatibilidad con los sistemas de criptación vocal del anexo D/H.235, versiones 2 y 3.

Las entidades H.323 que implementen esta Recomendación con la versión 4 de la Rec. UIT-T H.235 aceptarán preferentemente el algoritmo AES de 128 bits siempre que se lo permita su política de seguridad. Asimismo, estas entidades H.323 deberían aceptar el algoritmo DES triple de 168 bits si el AES de 128 bits no se ofrece o su política de seguridad no permite aceptarlo. Por razones de seguridad, estas entidades no deberían aceptar el DES de 56 bits ni los compatibles con RC2 de 56 bits, a no ser que su política de seguridad permita explícitamente utilizar estos algoritmos poco seguros, o que sea necesario por razones de exportabilidad, y no se ofrezcan alternativas más seguras como el AES de 128 bits o el DES triple de 168 bits.

Los métodos de control de acceso no se describen explícitamente y se pueden implementar localmente para la información recibida transportada en los campos de señalización H.235 (ClearToken, CryptoToken).

La presente Recomendación no describe los procedimientos para la asignación de claves secretas/contraseñas por acuerdo y su gestión y administración. Tales procedimientos pueden darse fuera del alcance de esta Recomendación.

Las entidades de comunicación involucradas son capaces de determinar implícitamente la utilización, bien del perfil de seguridad básico o bien del perfil de seguridad de firmas mediante la evaluación de los identificadores de objeto de seguridad señalados de los mensajes (**tokenOID**, y **algorithmOID**; véase también la cláusula 11).

En el cuadro 1 se resumen las características de seguridad del perfil de criptación vocal. El perfil de seguridad de criptación vocal se especifica en las cláusulas 7, 8 y 9.

Cuadro 1/H.235.6 – Perfil de criptación vocal

<table>
<tr><th>Servicios de seguridad</th><th colspan="4">Funciones de llamada</th></tr>
<tr><th></th><th>RAS</th><th>H.225.0</th><th>H.245</th><th>RTP</th></tr>
<tr><td>Autenticación e integridad</td><td></td><td></td><td></td><td></td></tr>
<tr><td>No repudio</td><td></td><td></td><td></td><td></td></tr>
<tr><td>Confidencialidad</td><td></td><td></td><td></td><td>DES de 56 bits | Compatible con RC2 de 56 bits | DES triple de 168 bits | AES de 128 bits
Modo CBC o modo EOFB</td></tr>
<tr><td>Control de acceso</td><td></td><td></td><td></td><td></td></tr>
<tr><td>Gestión de claves</td><td></td><td>Intercambio de claves Diffie-Hellman autenticadas</td><td>Gestión de claves de sesión H.235 integrada (distribución de claves, actualización de claves)</td><td></td></tr>
</table>

El procedimiento general establece un secreto compartido (intercambio Diffie-Hellman) entre las dos partes comunicantes al iniciarse una conexión. Este secreto compartido se utiliza entonces para proteger (un conjunto de) claves de medios que son utilizadas para criptar las sesiones de medios (RTP).

El perfil de seguridad de criptación vocal es una mejora facultativa del perfil de seguridad básico y del perfil de seguridad de firmas; su empleo puede negociarse como parte de la negociación de capacidades de seguridad del terminal. En los contextos en que la confidencialidad de la conversación está asegurada por otros medios, no es necesario implementar la criptación de medios y los procedimientos de gestión de claves correspondientes (convenio de claves Diffie-Hellman, actualización de claves y sincronización).

Los algoritmos de criptación elegidos son AES, compatibles con RC2, DES y DES triple.

NOTA 2 – Como una implementación del algoritmo DES triple se puede también utilizar para el algoritmo DES, el resultado es una implementación compacta.

Con independencia del algoritmo de criptación de medios específico que se haya elegido, deberán seguirse de manera explícita las opciones a continuación.

- Generación, si es necesario, del vector inicialización (IV, *initialization vector*) como se especifica en 9.3.1.
- Relleno, si es necesario, de acuerdo con la descripción de 9.3.2.

La cabida útil audio será criptada mediante el algoritmo de criptación negociado ("X", "Y", "Z3" o "Z") de conformidad con los procedimientos descritos en la cláusula 9 y en 9.3, y con los métodos de relleno de texto cifrado de I.1. Se puede criptar la cabida útil de audio utilizando el algoritmo de criptación negociado ("X1", "Y1", "Z1" o "Z2") con un modo de cifrado de trenes (EOFB).

7 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.

7.1 Funcionamiento seguro del canal H.245

Suponiendo que los procedimientos de conexión indiquen un modo de funcionamiento seguro, se llevará a cabo la toma de contacto y la autenticación negociadas para el canal de control H.245 antes de que se intercambie cualquier otro 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.

7.2 Funcionamiento inseguro del canal H.245

Como otra posibilidad, el canal H.245 puede funcionar de una manera insegura, en cuyo caso las dos entidades abren un canal lógico seguro con el cual efectuar la autenticación y/o la obtención del secreto compartido. Por ejemplo, se puede utilizar TLS (RFC 2246, RFC 3546) o IPsec (RFC 2401) abriendo un canal lógico con el **dataType** (**tipo de datos**) que contiene un valor para **h235Control**. Este canal se utilizaría para obtener un secreto compartido que proteja cualesquiera clave de sesión de medios o para transportar la **EncryptionSync** (**sincronización de criptación**).

7.3 Intercambio de capacidades

De acuerdo con los procedimientos de 5.2/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 puede proporcionar capacidades para enviar y recibir vídeo H.261. También puede indicar 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, según 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.

7.4 Cometido de terminal director

La determinación de terminal director-subordinado 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 (considerando 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.

7.5 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 **dataType** de **OpenLogicalChannel**. La clave de criptación inicial se transferirá en **OpenLogicalChannel** o **OpenLogicalChannelAck** dependiendo de la relación director/subordinado del originador de **OpenLogicalChannel**.

El **OpenLogicalChannelAck** actuará como una confirmación del modo de criptación. Si el receptor no puede aceptar **OpenLogicalChannel**, se devolverá **dataTypeNotSupported** (**tipo datos no soportado**) o **dataTypeNotAvailable** (**tipo datos no disponible**) (condición transitoria) en el campo de causa de **OpenLogicalChannelReject** (**rechazo apertura canal lógico**).

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 **OpenLogicalChannel**). 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 **OpenLogicalChannelAck** (en el campo **encryptionSync**). Para los canales de medios abiertos por el director, **OpenLogicalChannel** incluirá la clave de criptación inicial y el punto de sincronización en el campo **encryptionSync**.

7.6 Seguridad de conexión rápida

Es posible que los puntos extremos utilicen el procedimiento de conexión rápida (véanse 8.1.7 y 8.1.7.1/H.323) utilizando el elemento de arranque rápido para intercambiar con seguridad material de claves (clave maestra y claves de criptación de sesión). Los procedimientos presentados en 7.6.1. describen el arranque rápido "básico" en que no se utilizan los diversos algoritmos de criptación ofrecidos, mientras que en 7.6.1.1 se describe el caso particular de un arranque rápido con diversos algoritmos de criptación ofrecidos, lo que facilita una codificación más compacta de mensaje.

7.6.1 Seguridad de arranque rápido unidireccional

Este procedimiento describe cómo establecer un canal lógico de seguridad unidireccional (semidúplex) desde el emisor hasta el receptor de la llamada.

Procedimientos del llamante (emisor)

El llamante (fuente del SETUP**)** presenta tanto su testigo DH como las estructuras FastStart soportadas. El testigo DH se transportará dentro de un ClearToken incorporado como parte de un CryptoToken, o como un ClearToken separado, véase también 7.8. Durante la secuencia SETUP-a-CONNECT, se efectuará un intercambio Diffie-Hellman (DH), de manera que se establezca en ambos puntos extremos un secreto compartido. El campo **ClearToken** de los campos **CryptoToken** incluirá una **dhkey**, utilizada para pasar los parámetros conforme a esta Recomendación. **halfkey** contiene la clave pública aleatoria de una parte, **modsize** el número primo DH y **generator** el grupo DH. En el cuadro 4 se indican los parámetros DH que se han de utilizar. Para mayor información véase RFC 2412, apéndice E2.

NOTA 1 – Puesto que los mensajes H.225.0 son autenticados (como se describió en el procedimiento I), el intercambio DH es autenticado.

En cualquier sentido, con un mensaje de señalización de llamada H.225.0 que transporte media clave Diffie-Hellman, si se dispone de información de identificación, el llamante o el llamado cuando estén registrados incluirán también un **ClearToken** extremo a extremo separado, en el que **sendersID** será el identificador de punto extremo del remitente y **tokenOID** será "E". Toda entidad de señalización H.323 intermedia reenviará este testigo extremo a extremo sin modificación.

Las estructuras FastStart incluyen los canales lógicos abiertos ofrecidos con las capacidades de seguridad propuestas. Se debería ofrecer tanto el canal H235Cap como nonH235Cap. Durante el intercambio de capacidades H.245, los puntos extremos presentan entradas **H235SecurityCapability** para los códecs que soportan. Cada códec se asocia con una capacidad de seguridad H.235 independiente. Conforme al cuadro 6 estas capacidades deberían indicar el soporte de AES-CBC de 128 bits (OID – "Z3") y CBC RC2 compatible de 56 bits (OID – "X") y DES-CBC de 56 bits (OID – "Y"), y podrían indicar el soporte de DES triple-CBC de 168 bits (OID – "Z"), o de DES triple EOFB de 168 bits (OID – "Z1"), RC2 compatible con EOFB (OID – "X1"), DES-EOFB (OID – "Y1") o de AES-EOFB (OID – "Z2").

La instrucción **OpenLogicalChannel** transporta tanto **forwardLogicalChannelParameters** como **reverseLogicalChannelParameters** y en **dataType** se especifica **h235Media** con **encryptionAuthenticationAndIntegrity**, no indicando más de un algoritmo de criptación (**MediaEncryptionAlgorithm**) en **encryptionCapability**.

A efectos de la relación de seguridad, el destinatario será en principio el terminal director, véase también 7.4.

El llamante debería poner **mediaWaitForConnect** a verdadero, con el fin de afirmar que se dispone de material de clave de sesión y que se pueden descriptar los medios criptados recibidos. Siempre que se desee un establecimiento de canal "temprano", por ejemplo cuando el llamado transmita simultáneamente medios criptados o no criptados con respuestas a mensajes y material de clave de criptación, el llamante debería estar preparado para no poder descriptar los contenidos a menos que disponga de material de clave.

NOTA 2 – En este caso, si el llamado envía medios criptados al llamante (algo que en teoría puede hacer, puesto que tiene su dirección RTP/RTCP), éste no podrá descifrarlo sin la ayuda del secreto compartido proporcionado en el mensaje de Conexión (Aviso o Llamada en curso).

Procedimientos del llamado

Durante el FastStart, el llamado presenta su testigo DH (véase también 7.8) y las estructuras FastStart aceptadas. Cuando se utiliza el procedimiento Diffie-Hellman, se recomienda que el llamado retorne su testigo DH como parte del mensaje respuesta tan pronto como pueda. Es decir, en el mensaje respuesta que viene inmediatamente después del SETUP. De esta manera, el llamante podrá calcular la clave maestra a partir del secreto compartido DH y estará preparado para recibir la clave de sesión y los medios criptados.

NOTA 3 – De no haber algoritmo de criptación disponible en ambos lados, se puede dejar el tren de medios sin criptar o se puede abandonar la conexión dependiendo de la política de seguridad.

Cada entidad tomará los bits menos significativos adecuados a partir del secreto Diffie-Hellman compartido común para la clave de criptación principal (clave maestra), es decir una cantidad de bits menos significativos del secreto Diffie-Hellman correspondiente a: 56 para OID "X", OID "X1", OID "Y1" u OID "Y", 168 para OID "Z", OID "Z1" u OID "Z2", y 128 para OID "Z3" u OID "Z2". Véase también el cuadro 6.

Se emiten respuestas **OpenLogicalChannel(Ack)** con la clave de sesión creada (maestro) incluida en el campo **encryptionSync**. Este campo incluye la clave de sesión para el canal lógico dirigido desde el llamante hacia el llamado. El transporte de clave se hará conforme al procedimiento descrito en 8.3, ya sea utilizando **KeySyncMaterial** o **V3KeySyncMaterial** (véase 8.3.1). La clave de sesión se criptará utilizando el secreto compartido DH, como se describe a continuación.

NOTA 4 – No existe ningún método preestablecido para generar las claves de sesión utilizadas en la criptación de medios. La generación de estos valores depende de la implementación que, a su vez, se ve afectada por los recursos locales, las políticas, y el algoritmo de criptación que se vaya a utilizar. Conviene tener cuidado de no generar claves débiles.

Utilizando el procedimiento de 8.3, se transportará la clave de sesión criptada en el **H.235Key/sharedSecret** dentro del campo **encryptionSync**. La clave de sesión se transportará en el campo **keyMaterial** del **KeySyncMaterial**, y cuando no sea un múltiplo del tamaño del bloque se aplicará un relleno para completarla antes de la criptación. El valor del relleno se debería estimar mediante el convenio normal del algoritmo de cifrado. El **KeySyncMaterial** (de relleno) se codificará conforme a:

– 56 bits del secreto compartido, empezando por los menos significativos del secreto Diffie-Hellman para OID "X", OID "X1" , OID "Y1" u OID "Y".

– Todos los bits del secreto compartido para OID "Z2", OID "Z" u OID "Z1", comenzando con los bits menos significativos del secreto DH.

Por otra parte, y siempre que se pueda, se debería utilizar el transporte de clave mejorado conforme a 8.3.1, debido al resultado del procedimiento indicativo de la versión 3 (véase 8.2).

Cuando se deba establecer un canal de medios seguro dúplex utilizando un arranque rápido, de entre dos canales unidireccionales, el llamado abrirá un segundo canal lógico hacia el llamante. Este canal se señalará en un elemento fastStart separado. Utilizando el secreto compartido DH disponible como clave maestra, el recipiente incluirá otra clave de sesión para este canal lógico en el **encryptionSync**.

7.6.1.1 Utilización de algoritmos de criptación múltiple en la conexión rápida

La negociación de la criptación de medios como parte de los procedimientos de conexión rápida provoca un incremento ineficaz de la cantidad de elementos **OpenLogicalChannel** en el elemento **fastConnect** de un mensaje SETUP porque se necesita un **OLC** independiente para cada combinación de códecs (**dataType**) y algoritmo de criptación (incluido "none").

Se especifica el algoritmo de criptación que se ha de aplicar a un tren de medios incluyendo el **datatype** apropiado **dataType.h235Media.encryptionAuthenticationAndIntegrity.encryptionCapability** en el **OLC**. En H.235v2 se recomienda incluir solamente un único **MediaEncryptionAlgorithm** en la **encryptionCapability**, aunque este último elemento se defina como una secuencia de los elementos anteriores. Así pues, se puede incluir una secuencia ordenada por preferencias de capacidades de criptación en cada **OLC** ofrecido. El receptor de **OLC** escogerá entonces un algoritmo único de entre aquellos que se ofrecen, y retornará el **OLC** con únicamente el algoritmo escogido (junto con las direcciones de transporte e información clave de criptación apropiadas).

Para garantizar una eficacia máxima, el identificador de objeto "NULL-ENCR" (véase el cuadro 2) representa el algoritmo de criptación "null", o lo que es lo mismo indica que no tiene lugar ninguna operación de criptación. De esta manera, se necesita solamente un **OLC** por códec ofrecido y para cada sentido.

Cuadro 2/H.235.6 – Identificador de objeto para la criptación NULL

Referencia de identificador de objeto	Valor de identificador de objeto	Descripción
"NULL-ENCR"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 26}	Indica el "algoritmo de criptación NULL"

Procedimientos para el llamante (véase 8.1.7.1/H.323)

Si se especifica en un elemento **dataType** ofrecido la criptación a través de la selección de **h235Media**, es posible que el elemento **encryptionAuthenticationAndIntegrity** allí presente incluya un elemento **encryptionCapability** que contenga diversos algoritmos de criptación (incluido el algoritmo NULL). Esta construcción estará destinada a ofrecer la posibilidad de escoger entre los diversos algoritmos especificados para la criptación de las capacidades de medios correspondientes.

Procedimientos para el llamado (véase 8.1.7.1/H.323)

Si se ofrecen diversos algoritmos de criptación para un canal, el punto extremo llamado deberá seleccionar uno y modificar el **OpenLogicalChannel** a fin de suprimir los otros.

7.6.2 Seguridad de canales bidireccionales durante el arranque rápido

La seguridad de los canales de datos T.120 bidireccionales queda en estudio.

7.7 DTMF H.245 criptadas

Los puntos extremos pueden enviar señales DTMF (RFC 2833) criptadas para lograr confidencialidad. Usando la clave de criptación de sesión, estos puntos pueden criptar las señales DTMF (RFC 2833) en **UserInputIndication** de la siguiente manera:

- Cadena básica criptada: **encryptedAlphanumeric**.
- Cadena iA5 criptada: **encryptedSignalType** en **signal**.
- Cadena general criptada: **encryptedAlphanumeric** en **extendedAlphanumeric**.

NOTA 1 – No se criptan los parámetros adicionales para el RTP en la cadena iA5, con indicaciones de tiempo y números de canal lógico o la actualización de señal con la duración de tono, al no considerarlos adecuados para transportar información confidencial.

La capacidad negociada **secureDTMF** está relacionada con una cadena iA5 criptada.

La gestión de clave que se explica en la cláusula 6.1, debería aplicarse para obtener una clave de criptación de sesión. Dicha clave se utilizará para criptar las señales DTMF H.245 (RFC 2833).

NOTA 2 – Esto no significa necesariamente que se deba aplicar la clave de sesión también para la criptación de cabida útil RTP.

No obstante, cuando se use también la DTMF (FC 2833) a través del RTP (se ha validado el indicador **rtpPayloadIndication**), se recomienda enfáticamente que se asegure la cabida útil RTP mediante el perfil de criptación de voz de 6.1.

En el cuadro 3 se presentan los algoritmos de criptación disponibles (DES, 3DES o AES) que deberían utilizar el modo EOFB (incluyendo el modo OFB como un caso especial; véase 8.4). Para evitar un posible relleno de caracteres DTMF (RFC 2833), se recomienda no utilizar para la

criptación de señales DTMF (RFC 2833) los modos CBC, CFB u otros modos de encadenamiento de bloques que puedan requerir el relleno.

7.7.1 Cadena básica criptada

Si se ha seleccionado **encryptedBasicString** en **UserInputCapability**, el **encryptedAlphanumeric** indicará qué algoritmo de criptación se aplica en el **algorithmOID**, y **paramS** tiene el valor inicial para la operación de criptación. Se colocará la cadena alfanumérica criptada en **encrypted**.

7.7.2 Cadena iA5 criptada

Si se selecciona **encryptedIA5String** en **UserInputCapability**, en el campo **encryptedSignalType** se incluirá el **ClearSignalType** criptado, donde **sig** transporta el carácter **signalType** de texto claro. **signalType** tendrá un valor ficticio "!" que será descartado por el recipiente.

algorithmOID indicará cuál algoritmo de criptación se aplica y **paramS** tiene el valor inicial para la operación de criptación.

7.7.3 Cadena general criptada

Si se escoge una **encryptedGeneralString** en **UserInputCapability**, el **encryptedAlphanumeric** en el **extendedAlphanumeric** indicará el algoritmo de criptación aplicado dentro del **algorithmOID**, mientras que **alphanumeric** mantendrá una cadena vacía y **paramS** el valor inicial para la operación de criptación.

7.7.4 Lista de identificadores de objeto

Cuadro 3/H.235.6 – Identificadores de objeto para la criptación de DTMF H.245

Referencia de identificador de objeto	Valor(es) de identificador de objeto	Descripción
"DES-EOFB-DTMF"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 12}	Criptación de DTMF H.245 con DES-56 en modo EOFB
"3DES-EOFB-DTMF"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 13}	Criptación de DTMF H.245 con 3DES-168 en modo EOFB
"AES-EOFB-DTMF"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 14}	Criptación de DTMF H.245 con AES-128 en modo EOFB

7.8 Operación Diffie-Hellman

En esta Recomendación se soporta el protocolo Diffie-Hellman para el acuerdo de clave de extremo a extremo. Dependiendo de la situación, la clave Diffie-Hellman negociada puede funcionar como clave maestra (véase 6.1) o como clave dinámica de sesión (Recs. UIT-T H.235.3 y H.530).

El sistema Diffie-Hellman se caracteriza por los parámetros de sistema g y p, donde p es un número primo grande y g indica el generador del grupo multiplicativo módulo p o de un subgrupo fuerte módulo p. g^x mod p indica la media clave Diffie-Hellman (pública) del llamante, mientras que g^y mod p la del llamado. En RFC 2412 se presenta más información acerca de ello y se aconseja cómo escoger parámetros Diffie-Hellman seguros.

La Rec. UIT-T H.235.0 transporta un ejemplar de Diffie-Hellman (g, p, g^x) codificado con un **ClearToken**, donde **dhkey** mantiene la **halfkey** g^x mod p (o g^y mod p, cuando sea el caso) para alguna x (o y) aleatoria secreta, el p primo en **modsize** y el **generator** g. Un caso especial ocurre con la **dhkey** vacía, o lo que es lo mismo el triplete (0, 0, 0), que no representa un ejemplar DH, pero que se utilizará para señalizar que no está utilizando el perfil de criptación de voz.

Los parámetros de sistema DH *p* y *g* se suelen fijar para un conjunto de aplicaciones con valores bien definidos, aunque es posible también que los sistemas extremos escojan su propio conjunto de parámetros. Conviene que la entidad llamada sepa que los parámetros DH no estándar pueden proporcionar menos seguridad de lo que podría parecer a primera vista; es decir, el llamante pudo haber escogido un número no primo, o es posible que *g* genere simplemente un pequeño subgrupo. Aunque en la práctica es imposible efectuar una prueba exhaustiva de los parámetros, depende de la política de seguridad del recipiente si se aceptan o rechazan dichas ofertas.

Para los parámetros de sistema DH fijo, es posible obtener mensajes codificados más compactos utilizando abreviaturas que incluyendo valores literales. Un **ClearToken** que transporte un ejemplar DH con parámetros DH fijos y normalizados, puede hacer referencia a este ejemplar mediante un DH OID en el campo **tokenOID**, a menos que **tokenOID** se utilice para otros efectos (por ejemplo para un **CryptoToken** particular, en la cláusula 7/H.235.1). Asimismo, el remitente puede incluir los valores literales DH, aunque no está obligado hacerlo.

Cuando se deban indicar varios ejemplares DH, cada uno mediante un DH-OID, se omitirán los parámetros DH en un **CryptoToken** particular (se trata en H.235.1), sin **dhkey** y cada ejemplar DH se transportará entonces en un **ClearTokens** independiente, donde el **tokenOID** incluirá el DH-OID, y es posible que no haya **dhkey**; no se utilizará ningún otro campo en el **ClearToken**.

NOTA 1 – Esto no excluye la posibilidad de transportar un ejemplar DH en un **CryptoToken** particular u otros **ClearTokens** disponibles incluyendo literalmente los valores de los parámetros DH.

Cuando se deba indicar un ejemplar DH no estándar, se utilizará el DH-OID "DHdummy" y se proporcionarán explícitamente los parámetros de grupo DH no estándar en el **ClearToken**.

El llamante puede presentar uno o varios **ClearTokens** que transporta cada uno un ejemplar diferente Diffie-Hellman. Conviene que el llamante suministre el mayor número posible de ejemplares DH permitido por su política de seguridad. De esta manera, el receptor puede escoger el ejemplar adecuado para la respuesta, incrementando así la probabilidad de encontrar un buen conjunto común de parámetros.

El receptor escogerá y aceptará un único ejemplar DH (si se decide hacerlo) a partir del conjunto desordenado suministrado por el llamante en el mensaje SETUP. Cuando el receptor pueda escoger un ejemplar DH conforme a sus propias necesidades de seguridad, no necesitará modificar un ejemplar DH propuesto o retornar uno que no haya sido enviado por el llamante. La solidez de los algoritmos de criptación de que disponen ambos puntos extremos durante la llamada debería corresponder a la solidez del ejemplar DH escogido entre los proporcionados que retorna el recipiente; véase el cuadro 4. El recipiente indicará el ejemplar DH escogido en el mensaje de respuesta.

Cuando el llamado rechace cualquiera de las propuestas por razones de seguridad o debido a falta de capacidades de procesamiento, no incluirá **dhkey** en el mensaje de respuesta.

La entidad llamada incluirá su testigo DH en la respuesta SETUP-a-CONNECT. Podrá también incluirlo en el mensaje de respuesta inmediatamente después del SETUP o después, pero en el peor de los casos en el mensaje CONNECT.

NOTA 2 – Es necesario tener en cuenta diversos aspectos al considerar cuándo el llamado puede incluir el (los) testigo(s) DH durante la respuesta SETUP-a-CONNECT: el tiempo de respuesta, la carga de procesamiento en el recipiente, la capacidad de establecimiento de los canales de medios temprano, y otros más. Todos estos aspectos dependen de la implementación.

Es posible, sin embargo, que ciertos GK de encaminamiento no entreguen la respuesta SETUP-a-CONNECT al llamante. Es decir, se pueden perder uno o varios mensajes de respuestas señalización de llamada H.225.0, incluido un posible testigo DH, que por tanto no llegarían al llamante. En ese caso, éste no podría calcular la clave maestra y la(s) clave(s) de sesión de medios DH. Para evitar que esto ocurra, el llamado debería incluir siempre el mismo testigo DH en cada mensaje de respuesta SETUP-a-CONNECT.

Cuando el DH-OID indique un ejemplar DH diferente del que se está transportando en **modsize** y **generator**, los valores literales transportados en estos dos parámetros tendrán prioridad sobre el DH-OID en el testigo. Para la respuesta, el llamado debería reemplazar el DH-OID que provoca conflicto por el DH-OID estático, es decir "DH1024", que corresponde al **modsize** y **generator** o "DHdummy" cuando no exista un DH-OID correspondiente.

7.8.1 Petición de renegociación de parámetros DH a mitad de la llamada

El controlador de acceso H.323 puede solicitar la renegociación de parámetros DH a mitad de la llamada utilizando para ello los procedimientos definidos en esta cláusula. Estos procedimientos de renegociación pueden ser necesarios para que el punto extremo conectado al controlador de acceso y un punto extremo que desea conectarse se pongan de acuerdo sobre la clave DH (véase la figura 1). El procedimiento de renegociación de los parámetros Diffie-Hellman es necesario para ofrecer varios servicios complementarios. Todos los procedimientos definidos en esta cláusula deberán emplearse únicamente cuando el punto extremo H.323 se encuentra en el estado "lado transmisor en pausa" definido en la cláusula 8.4.6 de la H.323.

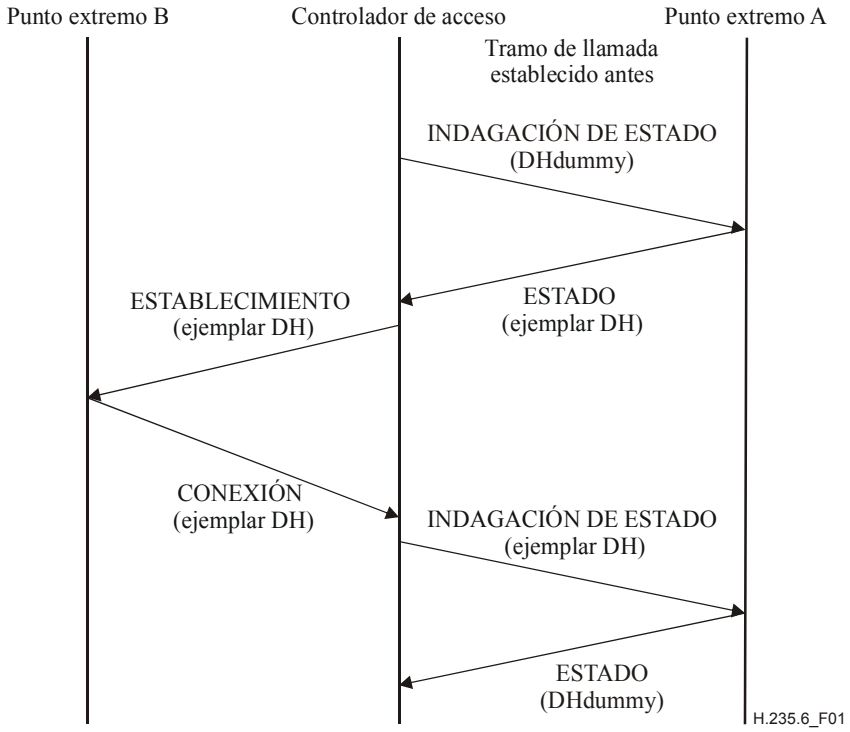


Figura 1/H.235.6 – Utilización del procedimiento de petición de parámetros DH a mitad de la llamada para servicios complementarios

Para solicitar los parámetros DH a mitad de la llamada, la entidad H.323 enviará un mensaje INDAGACIÓN DE ESTADO (STATUS INQUIRY) que incorpore el campo **ClearToken** y especifique DH-OID "DHdummy" en el campo **tokenOID**, y omitirá el resto de los campos.

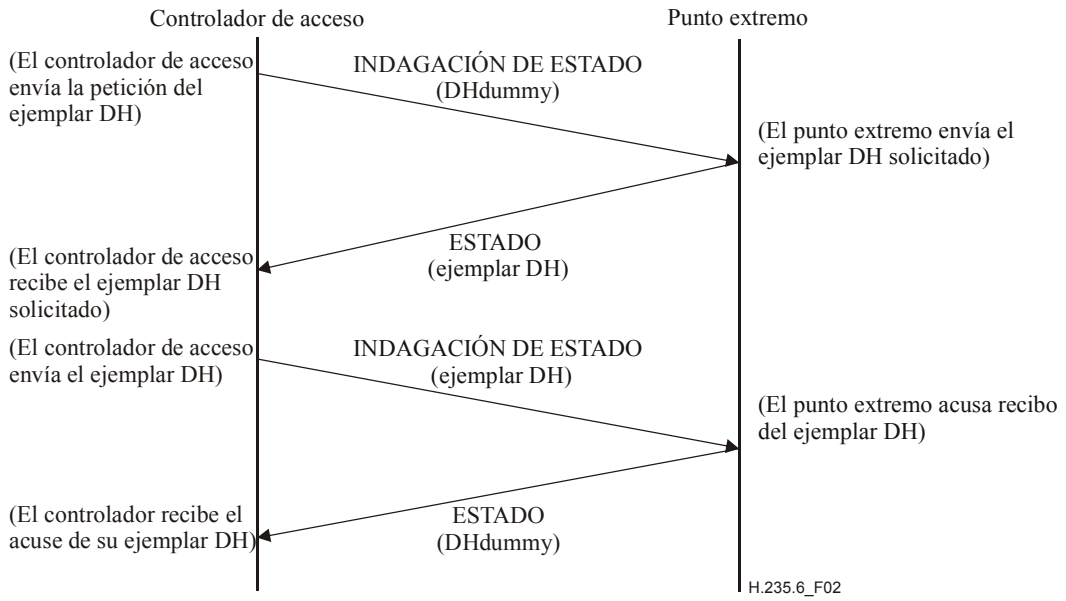


Figura 2/H.235.6 – Petición de parámetros DH a mitad de la llamada

Si una entidad H.323 recibe el mensaje INDAGACIÓN DE ESTADO que incorpora el campo **ClearToken** y el DH-OID "DHdummy" en el campo **tokenOID**, el punto extremo H.323 responderá con el mensaje ESTADO (STATUS) el cual incluirá el conjunto de ejemplares DH, véase la figura 2. Los ejemplares DH se especificarán en este mensaje ESTADO de conformidad con las reglas definidas en 7.8 para el mensaje ESTABLECIMIENTO (SETUP).

NOTA 1 – La entidad H.323 que no soporte este procedimiento tendrá que responder al mensaje INDAGACIÓN DE ESTADO con el mensaje ESTADO sin ejemplares DH.

Para transportar el ejemplar DH aceptado a mitad de la llamada, la entidad H.323 enviará el mensaje INDAGACIÓN DE ESTADO que contenga el ejemplar DH aceptado, véase la figura 2. Los ejemplares DH se especificarán en ese mensaje INDAGACIÓN DE ESTADO con arreglo a las reglas definidas en 7.8 para la respuesta al mensaje ESTABLECIMIENTO.

Si un punto extremo H.323 recibe un mensaje INDAGACIÓN DE ESTADO que contiene el ejemplar DH en el campo **ClearToken**, el punto extremo H.323 contestará con el mensaje ESTADO el cual incorporará el campo **ClearToken** y especificará el DH-OID "DHdummy" en el campo **tokenOID**, y omitirá el resto de los campos.

NOTA 2 – La entidad H.323 que no soporte este procedimiento tendrá que responder al mensaje INDAGACIÓN DE ESTADO con el mensaje ESTADO sin ejemplares DH.

El punto extremo H.323 que reciba el mensaje INDAGACIÓN DE ESTADO con el ejemplar DH recalculará el secreto compartido DH a partir de ese ejemplar DH y el último conjunto de ejemplares DH que haya enviado ese punto extremo H.323 en esa determinada llamada.

Si un controlador de acceso H.323 recibe un mensaje INDAGACIÓN DE ESTADO que incorpora el campo **ClearToken** y el DH-OID "DHdummy" en el campo **tokenOID**, este controlador reenviará el mensaje al segundo tramo de la llamada en el contexto en que se recibió el mensaje, salvo en los casos que se indican a continuación.

Si un controlador de acceso H.323 recibe el mensaje ESTADO como respuesta al mensaje INDAGACIÓN DE ESTADO reenviado, ese controlador de acceso devolverá el mensaje ESTADO al tramo de llamada por el que recibió el mensaje INDAGACIÓN DE ESTADO.

Si un controlador de acceso H.323 está esperando la respuesta al mensaje, que el mismo ha enviado, INDAGACIÓN DE ESTADO que incorpora el campo **ClearToken** y el DH-OID "DHdummy" en el campo **tokenOID**, y recibe un mensaje INDAGACIÓN DE ESTADO que incorpora el campo

ClearToken, que tiene el DH-OID "DHdummy" en el campo **tokenOID** y la bandera CRV puesta a 1, el controlador de acceso responderá con el mensaje ESTADO que incorpora el campo **ClearToken** y el DH-OID "DHdummy" en el campo **tokenOID** (véase la figura 3).

Si un controlador de acceso H.323 recibe el mensaje INDAGACIÓN DE ESTADO que incorpora el ejemplar DH en el campo **ClearToken** o el DH-OID "DHdummy" en el campo **tokenOID**, cuando aún no se ha establecido el segundo tramo de la llamada, el controlador de acceso esperará a que se establezca el segundo tramo de la llamada, enviará un conjunto de capacidades vacío por ese tramo de llamada y luego reenviará por él el mensaje INDAGACIÓN DE ESTADO recibido (véase la figura 3).

El controlador de acceso H.323 no iniciará los procedimientos definidos en esta cláusula después de haber enviado el mensaje ESTADO con un ejemplar DH ni antes de recibir el mensaje INDAGACIÓN DE ESTADO con un ejemplar DH.

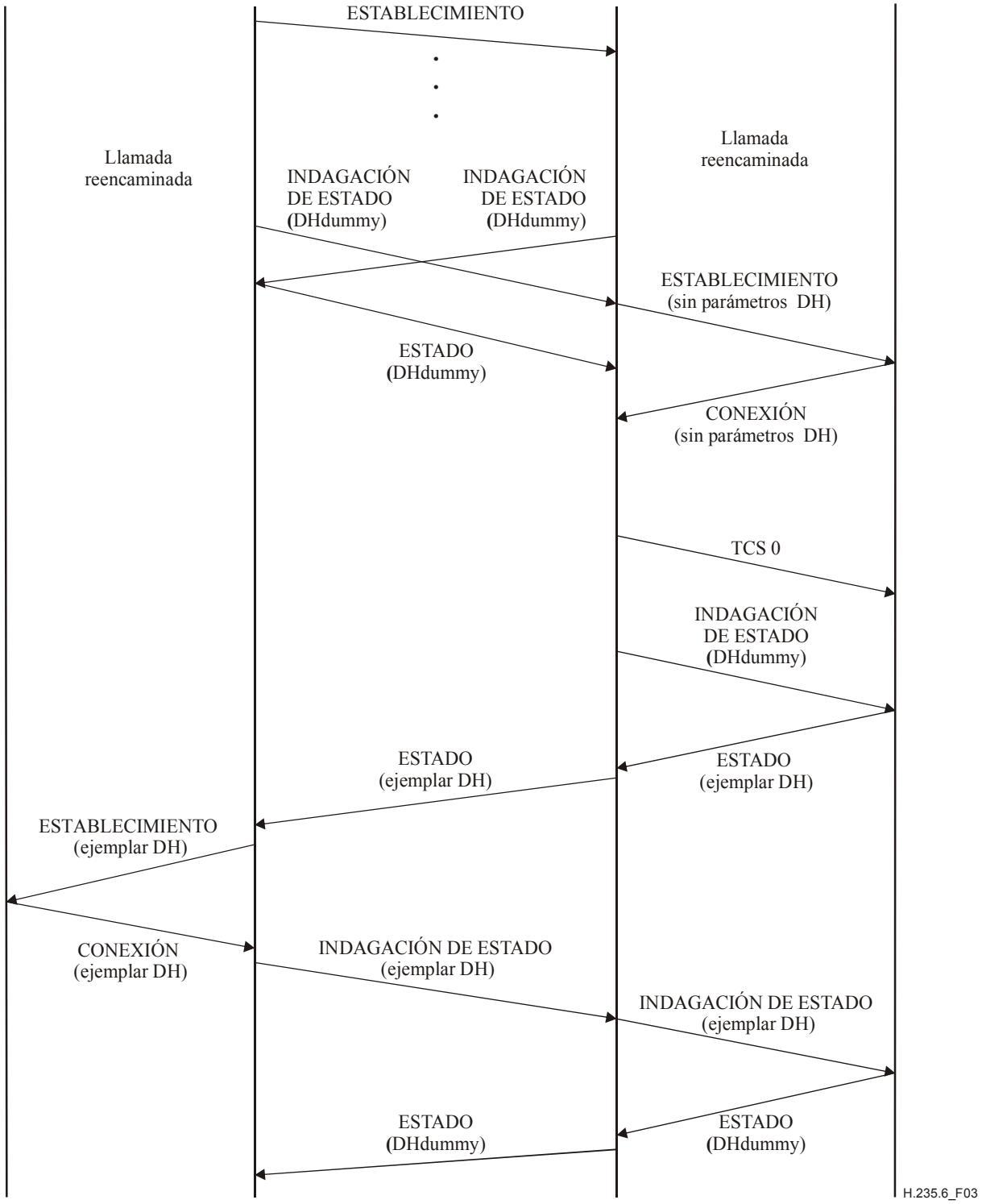


Figura 3/H.235.6 – Utilización del procedimiento de solicitud de parámetros DH a mitad de la llamada para el reencaminamiento simultáneo por los dos controladores de acceso

8 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), que se indica en mensajes H.225.0.

Cuando el propio canal H.225.0 ha de ser seguro, 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 seguro y utilizando los modos de seguridad predeterminados (por ejemplo, TLS (RFC 2246, RFC 3546)). 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 H.225.0. En otras palabras, ambas partes deben conocer *a priori* que están utilizando un modo de seguridad particular. Para H.323 en IP, se utiliza un puerto bien conocido alternativo (1300) para comunicaciones seguras TLS (RFC 2246, RFC 3546).

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/o generación numérica (por ejemplo, firma). Los aspectos específicos de estos modos de funcionamiento se describen en las cláusulas 8.1 a 8.2.3/H.235.0.

Un punto extremo H.323 que recibe un mensaje ESTABLECIMIENTO en que se ha validado la opción **h245SecurityCapability** (**Capacidad seguridad h245**) responderá con el correspondiente **h245SecurityMode** (**Modo de seguridad h245**) aceptable en el mensaje CONEXIÓN. En el caso en que no haya coincidencia de capacidades, el terminal llamado puede rechazar la conexión enviando **Release Complete (Liberación completa)** con el código de motivo fijado a ***SecurityDenied*** (***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 **Release Complete** con el motivo ***SecurityDenied***. Cuando el terminal llamante recibe un mensaje CONEXIÓN sin ninguna capacidad de seguridad, puede terminar la llamada con **Release Complete** con ***undefinedReason*** (***motivo no definido***).

Si el terminal llamante recibe un modo **h245Security** (**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 debería considerar como un error de protocolo y debería terminarse la conexión.

8.1 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 **H245Security**, puede devolver **Release Complete** para rechazar la conexión, pero en este caso utilizará el código ***UndefinedReason***. De manera correspondiente, si una parte llamante recibe un mensaje CONEXIÓN sin **H245SecurityMode** y/o testigo de autenticación, habiendo enviado un mensaje ESTABLECIMIENTO con **H245Security** y/o testigo de autenticación, también puede terminar la conexión emitiendo un mensaje **Release Complete** con un código ***UndefinedReason***.

8.2 Indicación de característica de la versión 3

Los puntos extremos conformes a la versión 3 y versiones superiores de H.235 proporcionan procedimientos mejorados de seguridad en el trayecto de medios que no soportan las versiones 1 y 2, a saber:

- el transporte de clave mejorado (**V3KeySyncMaterial**, véase 8.3.1),
- la actualización de clave mejorada, véase 8.6.2.

Puesto que suele ocurrir que los puntos extremos no sepan que soportan mutuamente la versión 3 de H.235, se añade durante el establecimiento de la comunicación una indicación explícita de la versión utilizada.

Los puntos extremos conformes a la versión 3 y versiones superiores de H.235 deberían utilizar siempre el procedimiento descrito en esta cláusula para determinar las capacidades de la versión 3 (transporte de clave mejorado, sincronización de criptación mejorada). Dependiendo del resultado del proceso de señalización lógico, los puntos extremos pueden utilizar los procedimientos (véase 8.3) para la compatibilidad con los puntos extremos de las versiones 1 ó 2 de dicha Recomendación.

Con el fin de indicar si se utilizan los procedimientos mejorados de la versión 3 de H.235, los puntos extremos llamante y llamado incluirán un **ClearToken** adicional que indique la capacidad versión 3 durante la señalización de llamada (SETUP, CONNECT, etc.). La ausencia de dicho **ClearToken** indicaría que se soporta solamente la versión 1 o la versión 2. En este caso, el punto extremo utilizará el procedimiento de 8.3. De lo contrario, puede utilizar los procedimientos mejorados que se describen en 8.3.1, o el procedimiento 8.3 de la versión 1 o de la versión 2.

En el **ClearToken** habrá que indicar "V3" como **tokenOID** con el siguiente valor.

"V3"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 24}	Indicación de capacidad de versión 3 en ClearToken durante la señalización de llamada

Todos los demás campos en dicho **ClearToken** permanecerán inutilizados, a menos que se usen para transportar parámetros DH.

8.3 Transporte de clave

El terminal director generará material de clave de sesión y lo distribuirá al(los) par(es). Existen dos procedimientos para el transporte de clave:

- Un procedimiento destinado en principio a los puntos extremos de las versiones 1 ó 2 de H.235; descrito en esta cláusula.
- Un procedimiento mejorado para los puntos extremos conformes a la versión 3 y versiones superiores de H.235, descrito en 8.3.1.

Los puntos extremos de la versión 1 o versión 2 de H.235 aplican el siguiente procedimiento para el transporte de clave de sesión:

KeySyncMaterial incluye el identificador de punto extremo del terminal director en **generalID** y transporta el material clave de sesión en **keyMaterial**. Debería incluirse el valor **generalID** para proporcionar un nivel mínimo de autenticación de la fuente de la clave de sesión (véase también 8.6). El receptor debería verificar si el **generalID** recibido es correcto.

NOTA – En esta Recomendación se supone que cada punto extremo se ha registrado con un controlador de acceso y ha obtenido un identificador de punto extremo que se puede transportar en **generalID**. En esta Recomendación no se soporta la opción sin controladores de acceso; que queda en estudio.

KeySyncMaterial será criptado utilizando la clave maestra negociada. El **KeySyncMaterial** se rellenará siempre hasta un múltiplo de bloques antes de criptarlo, donde el último octeto se fijará al número de octetos de relleno (incluido el último). El valor del relleno debería determinarse utilizando la convención normal del algoritmo de cifrado. Se almacenará el resultado de la criptación en **sharedSecret** de **H235Key**.

8.3.1 Transporte de clave mejorado en la versión 3 de H.235

Se ha observado que la definición de sintaxis ASN.1 de **KeySyncMaterial** y la manera como se aplica la operación ENCRYPTED{} a los datos de las versiones 1 y 2 de H.235 dejan bastante texto claro conocido: en primer lugar el **generalID** del terminal director, aunque también algunos bits de

codificación conocidos para la estructura. Incluso cuando se ha criptado el **generalID**, es posible deducirlo de otras partes no criptadas del mensaje de señalización (por ejemplo **senderID**). Se cree que la presencia de dicho texto claro conocido debilita significativamente el esquema de seguridad, puesto que un atacante podría violar con más facilitad la clave de sesión, especialmente si se trata de un cifrado en bloques de menor tamaño, por ejemplo DES-56 o compatible con RC2.

Además, la versión 3 de H.235 será capaz de transportar otro material de clave:

- Transporte seguro de clave adicional al (los) par(es). Dicha clave se introduce para el modo OFB mejorado; véase 8.4.

La versión 3 de H.235 amplía **H235Key** con un **secureSharedSecret** que contiene **V3KeySyncMaterial**, con los siguientes parámetros:

generalID incluye el identificador de punto extremo del remitente de origen, si lo hay, o de lo contrario no se usa.

algorithmOID indica el algoritmo de criptación aplicado y el modo de funcionamiento.

paramS incluye el valor de inicialización que se aplica para la criptación de la(s) clave(s) transportada(s).

NOTA 1 – El IV en **paramS** no debería confundirse con el IV de paquete RTP que no está siendo señalado. Como opción, **ClearSalt** mantiene una clave adicional sin codificar para la criptación de clave de sesión (por ejemplo, para EOFB).

encryptedSessionKey incluye el texto cifrado de la clave de sesión criptada para los datos originales.

encryptedSaltingKey incluye el texto cifrado de la clave adicional criptada para los datos originales (en su caso). La clave adicional es necesaria para el modo OFB mejorado.

clearSaltingKey puede incluir la clave adicional sin criptar para los datos originales. En las implementaciones habrá que asegurarse de que no se utilicen simultáneamente **encryptedSaltingKey** y **clearSaltingKey**.

paramSsalt mantiene el valor inicial para la criptación de la clave adicional. Como opción, **ClearSalt** mantiene una clave adicional sin criptar para la criptación de clave adicional (por ejemplo, para EOFB).

NOTA 2 – **generalID**, **algorithmOID** y **paramS** se transmiten siempre en texto claro, mientras que **encryptedSessionKey** y **encryptedSaltingKey** mantienen el texto cifrado del material clave criptado.

El terminal director genera la(s) clave(s) conforme a las capacidades de terminal negociadas y la(s) envía al (los) punto(s) extremo(s) par(es) utilizando **V3KeySyncMaterial**. Los controladores de acceso intermedios, si los hay, reenviarán el **V3KeySyncMaterial** sin modificación.

Los puntos extremos de la versión 3 o versiones superiores de H.235 deberían utilizar siempre **secureSharedSecret** en **H235Key**, pero también pueden, según el resultado del procedimiento de señalización lógico de 8.2 y utilizando la indicación **ClearToken** de versión 3, utilizar **sharedSecret** para la compatibilidad con los puntos extremos de las versiones 1 ó 2.

8.4 Modo OFB mejorado

El modo OFB (ISO/CEI 10116) define un modo de funcionamiento que utiliza un cifrado de trenes con algoritmos de criptación de bloque. Este modo proporciona:

- calidad de funcionamiento mejorada gracias a un retraso reducido del procesamiento de criptación,
- un manejo más fácil y menos complejo de los bloques incompletos,
- buena resistencia contra los errores de bits.

El modo OFB mejorado es una ligera modificación del modo OFB que se llamará de aquí en adelante modo de "retroalimentación de salida mejorado" (EOFB). Además de las características del OFB, tiene las siguientes:

1) utiliza una clave adicional KS (*salting key*) además de la clave de criptación KE (*encryption key*); y

2) introduce un índice de paquete implícito.

La utilización de una clave adicional KS secreta, a la que se aplica una operación XOR con el resultado de la retroalimentación, produce más seguridad contra el análisis del texto claro conocido. Éste es un beneficio de seguridad importante que no puede ser proporcionado por otros modos de funcionamiento estándar (tales como CBC, OFB, etc.). El uso del modo EOFB conllevaría entonces a un incremento de seguridad contra los textos claros de alta redundancia y contra el análisis de los textos claros conocidos.

El método EOFB se define como $C_i = P_i \oplus S_i$, con $S_i = E_{KE}(KS \oplus S_{i-1})$ para $i = 1 \ldots n$ y $S_0 = IV$, donde C_i es el i-ésimo bloque de texto cifrado, P_i el i-ésimo bloque de texto claro, S_i el i-ésimo bloque de tren de clave, KE la clave de criptación y $\oplus$ el XOR basado en bit. En la figura I.6 se ilustra el EOFB.

Es posible también que el EOFB funcione en el modo OFB normal, de tal manera que sea compatible con éste. Siempre que se desee dicha compatibilidad, se fijará la clave adicional KS bien a todo cero o bien se dejará vacío **encryptedSaltingKey** en **V3KeySyncMaterial**. No obstante, es altamente recomendable utilizar una clave adicional para aquellos casos en que se cripten cabidas útiles RTP cuyo cifrado de bloque tenga un tamaño de bloque menor, como por ejemplo DES-56 o compatible con RC2.

Después de procesar un máximo de 2^{48} paquetes habrá que reemplazar la clave de criptación de sesión KE y la clave adicional KS, o de lo contrario podría ocurrir una reutilización de trenes de clave lo que pondría en riesgo la seguridad.

En la cláusula 11 se definen los identificadores de objeto para EOFB DES-56, EOFB compatible RC2, EOFB 3-DES y EOFB AES.

8.5 Gestión de claves

Los puntos extremos que se ajusten a esta Recomendación deberían utilizar el procedimiento de conexión rápida conforme a 7.6.1. Si no se aplica el arranque rápido, se utilizará entonces la tunelización H.245 para asegurar los mensajes de control de llamada H.245, conforme a esta Recomendación. El procedimiento de arranque rápido permite el establecimiento de uno o dos canales lógicos unidireccionales. El procedimiento de arranque rápido tiene en cuenta la negociación de las capacidades de seguridad, para la distribución de un secreto común compartido (secreto DH compartido) que funciona como clave maestra, y para la distribución segura de una clave de criptación.

En el cuadro 4 se proporcionan los OID atribuidos a los diversos algoritmos de criptación, y se muestra su relación con los OID atribuidos al grupo Diffie-Hellman. Se identifican tres grupos DH mediante un OID:

- "DHdummy": Se debería aplicar un ejemplar de este grupo DH siempre que se aspire a tener una seguridad exportable (512 bits), o se utilice cualquier grupo DH no estándar.

  NOTA 1 – No se define un grupo particular DH; el OID se refiere a cualquier grupo DH no estándar.

- Se utilizará un ejemplar de un grupo DH de 512 bits para generar una clave maestra para la distribución de clave(s) de sesión para los algoritmos de criptación compatible RC2 ("X") o DES de 56 bits ("Y").

- "DH1024": Este grupo DH se ha de aplicar siempre que se pretenda conseguir una alta seguridad (1024 bits). El OID se refiere a un grupo DH normalizado y fijo. Este grupo DH se utilizará para generar una clave maestra para la distribución de clave(s) de sesión para los algoritmos de criptación DES triple ("Z").
- "DH1536": Este grupo DH se ofrece como opción para los puntos extremos de la versión 3 que posean requisitos muy exigentes de seguridad, superiores a los del grupo DH de 1024 bits. El OID se refiere a un grupo DH fijo. Este grupo se utilizará para generar una clave maestra para la distribución de clave(s) de sesión para los algoritmos de criptación DES triple ("Z", "Z1") o AES-128 ("Z2", "Z3").

Se recomienda aplicar los grupos DH de 1024 bits, o en su lugar los de 1536 definidos, a menos que por otros requisitos de seguridad se prefiera utilizar otros parámetros Diffie-Hellman. Además, se recomienda utilizar los OID definidos que identifican los grupos DH, como se explica en 7.8. No obstante, las implementaciones deberían estar preparadas para obtener literalmente los parámetros de grupo DH sin necesidad de una indicación explícita de OID. En este caso, deberían afirmar que el grupo DH correcto está siendo transportado conforme al cuadro 4.

Los puntos extremos pueden utilizar parámetros de grupo DH no estándar. La utilización del OID "DHdummy" indica la presencia de dichos grupos DH no estándar. Es potestad del destinatario de la llamada aceptar o no dichos grupos DH.

NOTA 2 – La selección de uno de dichos grupos DH no implica que no sea necesario negociar el algoritmo real de criptación de medios. Esto se debe lograr mediante el procedimiento de negociación de capacidades de terminal H.245.

NOTA 3 – Durante el establecimiento de la conexión (SETUP-a-CONNECT) no se utilizarán los OID de algoritmo de criptación para indicar un ejemplar Diffie-Hellman.

Cuadro 4/H.235.6 – Grupos Diffie-Hellman

OID del algoritmo de criptación	DH-OID	Descripción del grupo D-H
"X", "X1" (compatible con RC2), "Y", "Y1" (DES)	"DHdummy"	Mod-P, cualquier primo de 512 bits adecuado
"Z", "Z1" (DES triple), "Z2", "Z3" (AES)	"DH1024"	Mod-P, primo de 1024 bits Primo = $2^{1024} - 2^{960} - 1 + 2^{64} \times \{ [2^{894}\ \text{pi}] + 129093 \}$ = (179769313486231590770839156793787453197860296048756011706444423684197180216158519368947833795864925541502180565485980503646440548199239100050792877003355816639229553136239076508735759914822574862575007425302077447712589550957937778424442426617334727629299387668709205606050270810842907692932019128194467627007)$_{10}$ Generador (nota) = 2

Cuadro 4/H.235.6 – Grupos Diffie-Hellman

OID del algoritmo de criptación	DH-OID	Descripción del grupo D-H
"Z", "Z1" (DES triple), "Z2", "Z3" (AES)	"DH1536"	Mod-P, primo de 1536 bits Primo = $2^{1536} – 2^{1472} – 1 + 2^{64} \times \{ [2^{1406}$ pi] + 741804 } = (2410312426921032588552076022197566074856950548502459942654116941958108831682612228890093858261341614673227141477904012196503648957050582631942730706805009223062734745341073406696246014589361659774041027169249453200378729434170325843778659198143763193776859869524088940195577346119843545301547043747207749969763750084308926339295559968882457872412993810129130294592999479263652640592846472097303849472116814344647144384885209401274598442888593365268963209196339 $)_{10}$ Generador (nota) = 2
NOTA – El generador se utiliza para generar el testigo DH.		

8.6 Actualización de claves y sincronización

Para cifrados de bloque de 64 bits, la tasa de renovación de claves *deberá* ser tal que no se cripten más de 2^{32} bloques con la misma clave. Las implementaciones *deberían* renovar las claves antes de que se hayan criptado 2^{30} bloques utilizando la misma clave (véase 9.1). Cuando se trate de cifrados de bloque de 128 bits, la tasa de renovación de claves *deberá* ser tal que no se cifren más de 2^{64} bloques con la misma clave. Las implementaciones *deberían* renovar las claves antes de que se hayan criptado 2^{62} bloques utilizando la misma clave (véase 9.1). Las dos entidades involucradas tienen libertad para intercambiar la clave de sesión de medios con la frecuencia que consideren necesaria de acuerdo con su política de seguridad. Por ejemplo, el terminal director puede distribuir una nueva clave de sesión utilizando la **encryptionUpdate** o **encryptionUpdateCommand** del mensaje **miscellaneousCommand**. Por otra parte, el terminal subordinado puede solicitar una nueva clave de sesión al terminal director utilizando la **encryptionUpdateRequest** del mensaje **miscellaneousCommand**.

El mensaje **MiscellaneousCommand** contiene los campos **encryptionUpdate** y **encryptionUpdateCommand**, en los que se determina **encryptionSynch** con los siguientes parámetros:

- **synchFlag**: el nuevo número de cabida útil RTP dinámica que indica la conmutación de clave;
- **h235key**: que cursa la nueva clave de sesión criptada. Es un parámetro **H235Key** codificado en ASN.1 H.235 pasado como una cadena de octetos.

El campo **sharedSecret** dentro de la estructura **H235Key** utiliza los siguientes campos:

- **algorithmOID**: puesto a "X", "X1" para el compatible con RC2 de 56 bits, puesto a "Y", "Y1" para el DES de 56 bits o puesto a "Z", "Z1" para el DES triple de 168 bits o puesto a "Z3" para AES de 128 bits.

  NOTA 1 – El algoritmo de criptación de clave de sesión es el algoritmo de criptación de medios negociado.

- **paramS**: puesto al valor inicial. Para cifrados de tren de bloques de 64 bits, **iv8** contiene un esquema de bits de bloques de 64 bits aleatorios que genera el iniciador. Para cifrados de tren de bloques de 128 bits, **iv16** contiene un esquema de bits de bloques de 128 bits aleatorios que genera el iniciador. Este campo no se usará en el modo CBC y se fijará a NULO (NULL), lo que indica que se ha de poner a 0 la CBC-IV para la criptación de clave de sesión; se utilizará solamente para el transporte del IV en el modo EOFB.
- **encryptedData**: puesto al resultado del **KeySyncMaterial** criptado.

Como parte del **KeySyncMaterial**:

- **generalID**: identificador de la fuente que distribuye la clave.

  NOTA 2 – En esta Recomendación se supone que cada punto extremo se ha registrado con un controlador de acceso y ha obtenido un identificador de punto extremo que puede ser transportado en **generalID**. En esta Recomendación no se soportan los casos en que no haya controladores de acceso; esto queda en estudio.
- **keyMaterial**: puesto a la nueva clave de sesión. Para DES y compatible con RC2 ésta es un clave de 56 bits, para DES triple es una clave de 168 bits y para AES es una clave de 128 bits. El terminal director deberá generar una nueva clave de sesión que cumpla al menos los siguientes criterios de seguridad: no es una clave DES débil o semidébil y utilizará una fuente aleatoria suficientemente segura.

El mensaje **MiscellaneousCommand** contiene la **encryptionUpdateRequest** que a su vez contiene el **keyProtectionMethod** en el que la bandera de **sharedSecret** es puesta a VERDADERO.

NOTA 3 – Como la actualización y sincronización de claves depende de mensajes H.245 que no son transportados durante la conexión rápida, es necesario utilizar la tunelización H.245 para las entidades H.323 aseguradas.

Las claves de sesión de medios tienen una vida útil limitada. En algún momento, toda clave expira. Se debería entonces utilizar una clave nueva para proteger la sesión de seguridad en curso. En los entornos de conferencia, se debería definir y distribuir una nueva clave de sesión de grupo cuando los miembros del grupo se unan o se retiren de la conferencia, evitando así que puedan acceder datos pasados o futuros, respectivamente.

- La actualización y sincronización de clave basada en el tipo de cabida útil define un nuevo tipo de cabida útil dinámica para la nueva clave de sesión; véanse 8.6.1, 8.6.2 y 8.6.3.

A efectos de la actualización de clave, en esta Recomendación se ofrece un procedimiento de toma de contacto sin acuse, que se aplica también para los puntos extremos de las versiones 1 y 2 de H.235 y también uno robusto y con acuse para la versión 3 y versiones superiores.

8.6.1 Actualización de clave sin acuse

En la figura 4 se muestra el procedimiento de toma de contacto sin acuse para la distribución o actualización de claves de sesión. Si el terminal subordinado desea una clave de sesión actualizada, puede pedir una nueva clave de sesión al terminal director enviándole una **encryptionUpdateRequest** a éste. El terminal director enviará una nueva clave de sesión (con una **encryptionUpdateRequest** anterior o sin ella del subordinado) al subordinado dentro de un mensaje **EncryptionUpdate**.

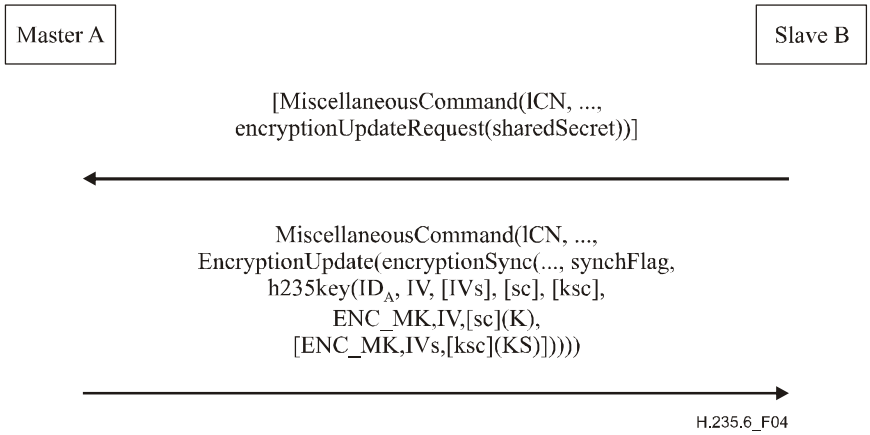


Figura 4/H.235.6 – Distribución o actualización de clave de sesión sin acuse del terminal director a(los) subordinado(s)

donde:

lCN	es el número de canal lógico
synchFlag	es el nuevo número de cabida útil RTP dinámica
ID_A	es el **generalID** del origen
IV	es el valor o vector inicial para la criptación de la clave de sesión
IVs	es el valor o vector inicial para la criptación de la clave adicional
ENC_MK,IV,sc(K)	indica la criptación del texto claro *K* utilizando la clave *M*, el vector inicial *IV* [y una clave adicional *sc*, solamente para EOFB]
KS	es la clave adicional para los medios (solamente para el modo EOFB)
K	es la clave de sesión de texto claro
sc	es la clave adicional sin criptar, cuando se ha venido utilizando el modo EOFB para la criptación de la clave sesión
ksc	es la clave adicional sin criptar cuando se ha venido utilizando el modo EOFB para la criptación de la clave adicional
s2M/m2S	es la bandera **direction** (solamente para la versión 3 de H.235) (s2m = subordinado a director, m2s = director a subordinado)
[]	representa algo facultativo

En los métodos de actualización de clave descritos en las cláusulas siguientes se puede desplegar el modo de criptación EOFB para proteger el material de clave transmitido. Para ello, de la misma manera que para la protección de la cabida útil de medios, se debe utilizar una clave adicional (sc o ksc).

8.6.2 Actualización de clave mejorada

Los puntos extremos conformes a la versión 3 de H.235 y a versiones superiores ejecutarán un procedimiento de actualización de clave con acuse explícito o implícito. De esta manera, se proporcionan métodos fiables de actualización de clave, que se basan en el método de actualización de claves sin acuse suministrado por las versiones anteriores a la 3. La capacidad de dicho procedimiento se negociará utilizando la indicación de característica de la versión 3, según 8.2.

En la figura 5 se muestran los procedimientos de actualización de clave para un canal lógico que pertenece al subordinado. Cuando éste inicie la actualización de clave y solicite una nueva clave de sesión al terminal director, el subordinado enviará una **MiscellaneousCommand** al director, donde **logicalChannelNumber** mantendrá el número de canal lógico (definido por el subordinado), **sharedSecret** se fijará a verdadero, la bandera **direction** se fijará a **slaveToMaster** y se solicitará el nuevo número de cabida útil dinámica en **synchFlag** dentro de **EncryptionUpdateRequest**. De lo contrario, si el director inicia la actualización de clave, no se enviará este mensaje **EncryptionUpdateRequest**.

El director emitirá, bien como respuesta a una petición del subordinado o bien por su propia iniciativa, una **EncryptionUpdateCommand** en la que **logicalChannelNumber** mantendrá el número de canal lógico, **direction** se fijará a **slaveToMaster** en **MiscellaneousCommand**, y **synchFlag** dentro de **encryptionSync** refleja el nuevo número de cabida útil dinámica.

h235key transportará la nueva clave de sesión, y mantendrá la identidad del director en **generalID** y el vector inicial aplicado *IV* en **paramS**. La clave de sesión de medios criptada se transportará en **encryptedSessionKey**, para el que la función de criptación aplicará la clave de sesión maestra y el valor inicial en **paramS** a la clave de sesión *K*. Para EOFB, se transporta una clave adicional sin criptar en **ClearSalt** dentro de **paramS** (*sc*). **encryptedSaltingKey** transportará la clave adicional de medios criptada, con la función de criptación aplicando la clave de sesión maestra y el valor inicial **paramSsaltIV** a la clave adicional de medios *KS*. Para EOFB, se transporta una clave adicional no criptada (*ksc*) en **ClearSalt** dentro de **paramSsalt**. **clearSaltingKey** puede mantener una clave adicional de medios sin criptar, en cuyo caso **encryptedSaltingKey** permanecerá vacía y viceversa. La transmisión de una clave adicional sin criptar se logrará solamente si no afecta la seguridad, de lo contrario se recomienda criptar la clave adicional de medios.

El terminal director estará preparado para recibir medios criptados con la nueva clave de sesión tras presentar el **EncryptionUpdateCommand**, pero debería seguir utilizando la clave antigua hasta la recepción del **EncryptionUpdateAck**. El director puede aplicar la nueva sesión a partir de la recepción del **encryptionUpdateAck**, mientras que el subordinado puede hacerlo a partir de la recepción del **EncryptionUpdateCommand**.

NOTA 1 – El director puede escoger cualquier valor de tipo de cabida útil dinámico para el subordinado, puesto que el tipo de cabida útil depende solamente del puerto de canal de medios.

NOTA 2 – No es necesario que el subordinado acuse explícitamente recepción de la nueva clave. El director puede deducir que aquél ya la recibió cuando le lleguen medios criptados mediante el nuevo tipo de cabida útil.

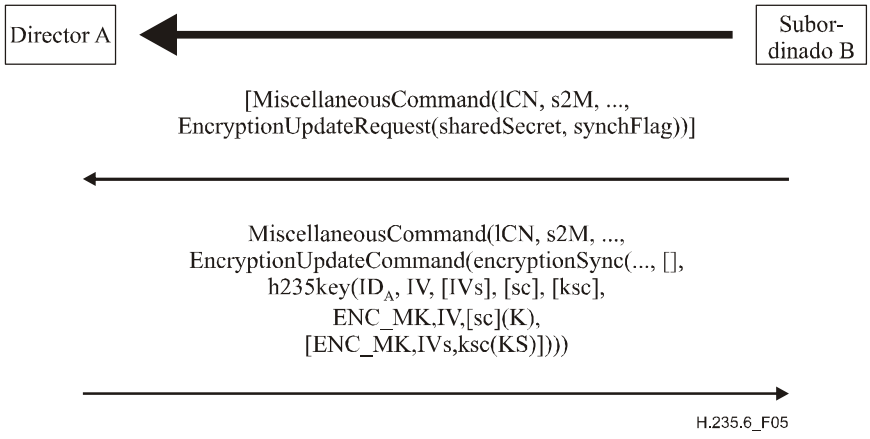


Figura 5/H.235.6 – Actualización de clave de sesión en el canal lógico del subordinado

En la figura 6 se muestran los procedimientos de actualización de clave para un canal lógico propiedad del director. Si el subordinado inicia la actualización de clave y solicita una nueva clave de sesión al director, aquél enviará una **MiscellaneousCommand** a éste, donde **logicalChannelNumber** indicará el número de canal lógico (definido por el director), **sharedSecret** se fijará a verdadero, y la bandera **direction** se fijará a **masterToSlave**. De lo contrario, si el director inicia la actualización de clave, no se enviará este mensaje **EncryptionUpdateRequest**.

El director emitirá, como respuesta una petición del subordinado o por su propia iniciativa, una **EncryptionUpdateCommand** donde **logicalChannelNumber** indicará el número de canal lógico, **direction** se fijará a **masterToSlave**, **encryptionSync** proveerá la **synchFlag** con el nuevo número de cabida útil dinámica. **h235key** transportará la nueva clave de sesión y mantendrá la identidad del director en **generalID** y el vector inicial applied *IV* en **paramS**. La clave de sesión de medios criptada será transportada en **encryptedSessionKey**, donde la función de criptación aplicará la clave maestra y el valor inicial en **paramS** a la clave de sesión *K*. Para EOFB, se transporta una clave adicional sin criptar en **ClearSalt** dentro **paramS** (*sc*). Para EOFB, **encryptedSaltingKey** transportará la clave adicional de medios criptada, donde la función de criptación aplicará la clave de sesión maestra y el valor inicial **paramSsaltIV** a la clave adicional *KS*. Para EOFB, se transporta una clave adicional sin criptar (*ksc*) en **ClearSalt** dentro de **paramSsalt**. **clearSaltingKey** puede mantener una clave adicional de medios sin criptar, en cuyo caso **encryptedSaltingKey** permanecerá vacía y viceversa. Se transmitirá una clave adicional sin criptar solamente si no se afecta la seguridad, de lo contrario se recomienda criptar la clave adicional de medios.

El subordinado acusará recibo de recepción de la nueva clave de sesión respondiendo con una **MiscellaneousCommand**, donde el **logicalChannelNumber** indicará el número de canal lógico y **encryptionUpdateAck** indicará el nuevo número de cabida útil dinámica en la **synchFlag**.

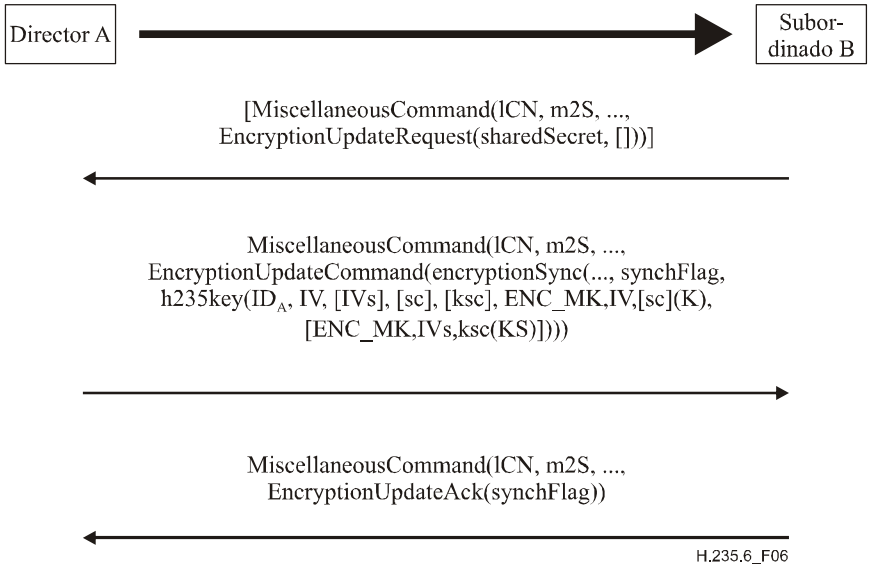


Figura 6/H.235.6 – Actualización de clave de sesión en el canal lógico de terminal director

8.6.3 Actualización de clave y sincronización basada en el tipo de cabida útil

El terminal director presenta la clave de criptación inicial junto con el número de cabida útil dinámica en **synchFlag** (a través de **EncryptionSync** en la Rec. UIT-T H.245). El(los) receptor(es) del tren de medios empezará(n) a utilizar la clave tras recibir este número de cabida útil en el encabezamiento RTP.

Si el canal lógico negociado transporta sólo un tipo de cabida útil, el valor de la **synchFlag** puede reemplazar el tipo de cabida útil negociado en el encabezamiento RTP. Por otra parte, si el canal lógico negociado puede transportar más de un tipo de cabida útil (incluso si lo hace solamente en paquetes RTP separados), los paquetes RTP tendrán el formato descrito en RFC 2198, el valor **synchFlag** será el tipo de cabida útil encapsulamiento, y el tipo o tipos de cabida útil real estarán en el bloque o bloques adicionales de encabezamiento, como se especifica en RFC 2198.

El punto extremo director puede distribuir en cualquier momento una o varias nuevas claves. La sincronización de la clave más reciente con el tren de medios se indicará cambiando el tipo de cabida útil a un nuevo valor dinámico.

NOTA – Los valores concretos pueden ser cualesquiera, siempre que cambien para cada nueva clave que se distribuya.

8.7 Interacciones no relacionadas con terminales

8.7.1 Pasarela

Como se indica en 6.6/H.235.0, se debe considerar que una pasarela H.323 es un elemento de confianza. Esto incluye pasarelas de protocolo (H.323-H.320, etc.) y pasarelas de seguridad (servidores intermedios/cortafuegos). La privacidad de los medios puede ser asegurada entre el punto de extremo y el dispositivo de pasarela comunicante, pero lo que se produce en el extremo distante de la pasarela se debe considerar inseguro por defecto.

8.7.2 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.

8.7.3 Elementos de confianza H.323

En general, las MC(U), las pasarelas y los controladores de acceso (si se aplica el modelo con encaminamiento por controlador de acceso) 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 controlador de acceso, 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 servidores intermedios/cortafuegos (aunque no son elementos específicos H.323), porque terminan conexiones, y pueden tener que manipular los mensajes y los trenes de medios.

8.8 Procedimientos multipunto

8.8.1 Autenticación

La autenticación se producirá entre un punto extremo y la MC(U) (unidad de control multipunto) 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/H.235.0, 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 **ConferenceRequest/ConferenceResponse** (**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 (control multipunto), pero no pueden realizar la autenticación criptográfica directa dentro del canal H.245.

8.8.2 Privacidad

La MC(U) ha de abrir 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.

9 Procedimiento 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 7 y 8 muestran el flujo general. Obsérvese que el encabezamiento de transporte se adjunta a 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 la Rec. UIT-T H.323, el encabezamiento RTP (SDU) cambiará su tipo de cabida útil para indicar la conmutación a la nueva clave.

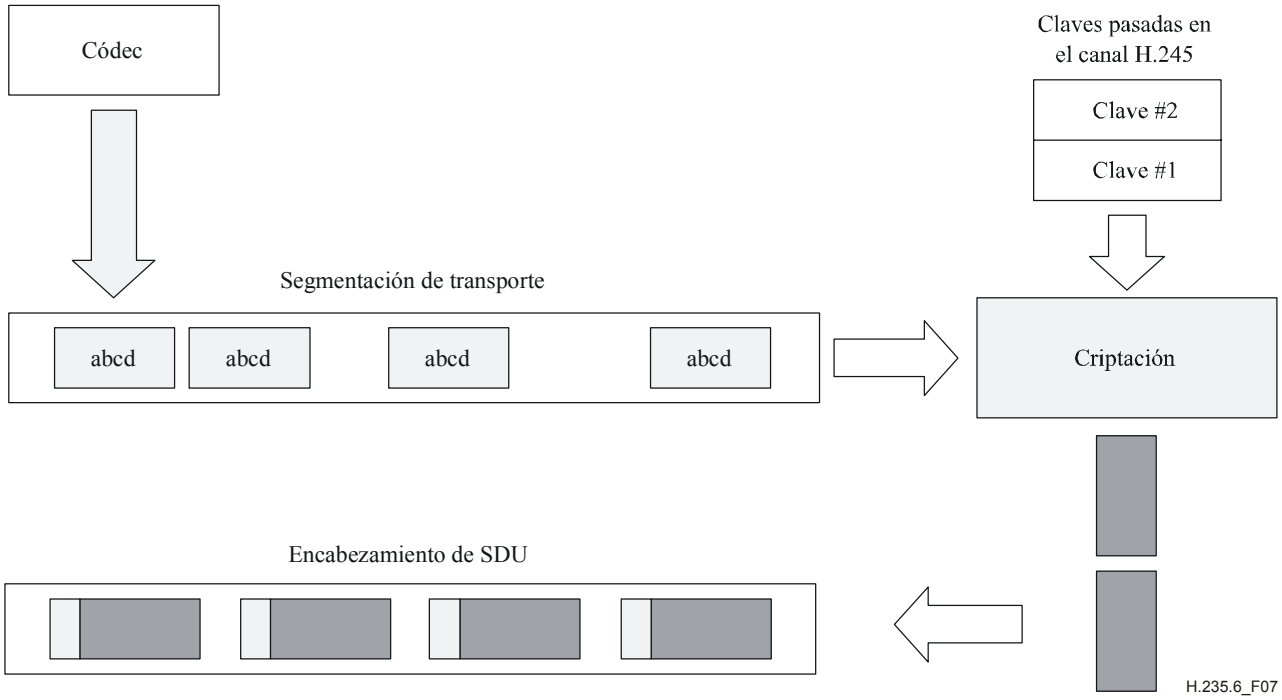


Figura 7/H.235.6 – Criptación de trenes de medios

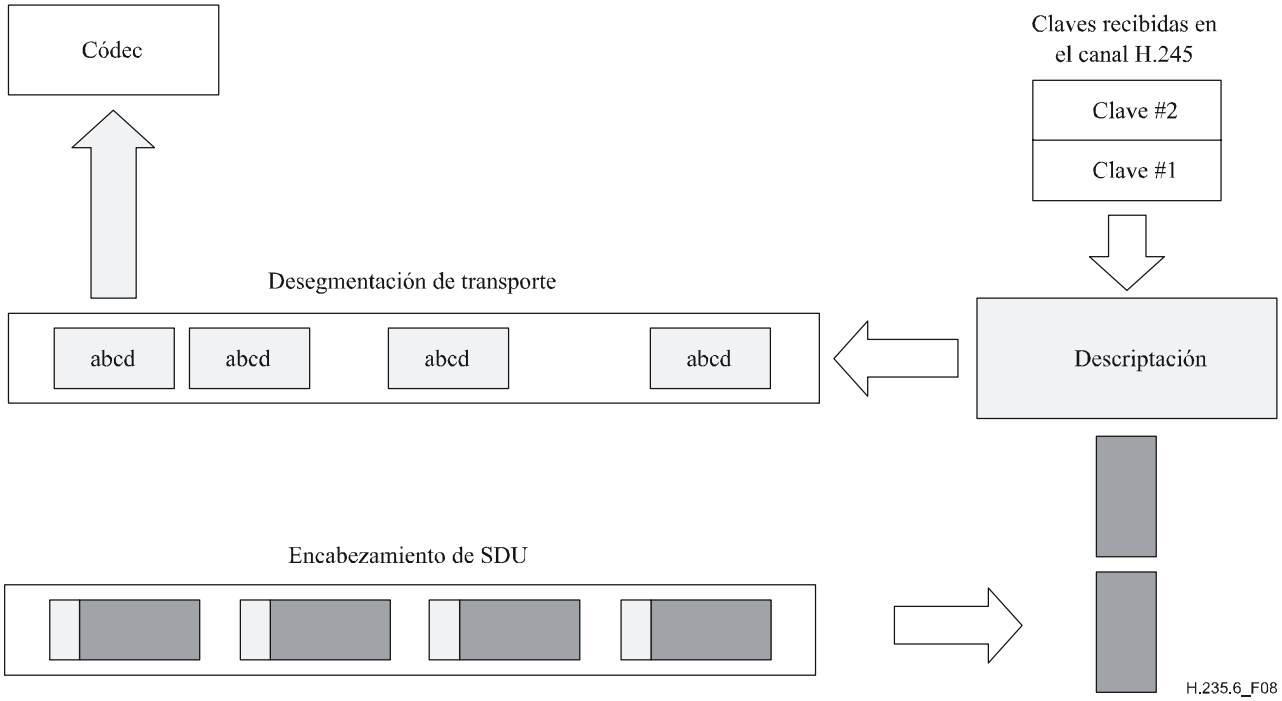


Figura 8/H.235.6 – Desencriptación de trenes de medios

9.1 Claves de sesión de medios

h235Key (**clave h235**) se incluye en **encryptionUpdate** (**actualización de criptación**). **h235Key** 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 **secureChannel** (**canal seguro**).
- 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 **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 **sharedSecret** (**secreto compartido**).
- 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 **certProtectedKey** (**clave protegida de certificado**).

En cualquier punto en una conferencia, un receptor (o un transmisor) puede solicitar una nueva clave (**encryptionUpdateRequest**). 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 **encryptionUpdate**.

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

9.2 Antiinundación de medios

El receptor de un tren de medios RTP puede desear contrarrestar los ataques de tipo inundación y de denegación del servicio en los puertos RTP/UDP descubiertos. Cuando tienen implementada la capacidad antiinundación, los receptores pueden determinar rápidamente si un paquete RTP obtenido procede de una fuente no autorizada y en tal caso descartarlo.

Al activarla se indica el empleo del mecanismo antiinundación:

- bien para datos de medios de texto claro sin criptación de medios (véase el caso 1 más abajo); o
- bien en combinación con datos de medios criptados cuando **EncryptionCapability** caracteriza un algoritmo de criptación (véase el caso 2 más abajo).

Ambas opciones proporcionan una **autenticación de paquetes RTP** simplificada en campos seleccionados mediante un código de autenticación de mensajes (MAC, *message authentication code*) calculado. El MAC puede ser calculado utilizando los identificadores de objeto definidos en 9.2.1. Los algoritmos criptográficos están constituidos por:

- un algoritmo de criptación (por ejemplo, DES en modo MAC; véase ISO/CEI 9797-1 y 9797-2). DES en MAC se indica mediante el OID "N", mientras que DES triple en MAC se indica mediante el OID "O"; o
- utilizando una función unidireccional criptográfica (por ejemplo, SHA1). Se utilizará el OID "M".

El algoritmo MAC se indica en el identificador de objeto de **antiSpamAlgorithm**. El OID del algoritmo indica también implícitamente el tamaño del MAC; por ejemplo, 1 bloque = 64 bits para DES MAC. Para ahorrar anchura de banda, el MAC puede ser truncado si bien sacrificando alguna seguridad; por ejemplo, pasando a un MAC de 32 bits; esto requiere utilizar entonces un identificador de objeto diferente. El método antiinundación es independiente de cualquier criptación de cabida útil adicional (véanse los casos 1 y 2 más adelante).

La antiinundación utiliza el siguiente formato de paquete RTP (véase la figura 9), en el que la secuencia de relleno RTP se interpreta como sigue (véase la cláusula 5 de RFC 3550).

- El bit P del encabezamiento RTP se fijará a 1.
- Se añadirán bytes de relleno al final de la cabida útil con el significado siguiente:

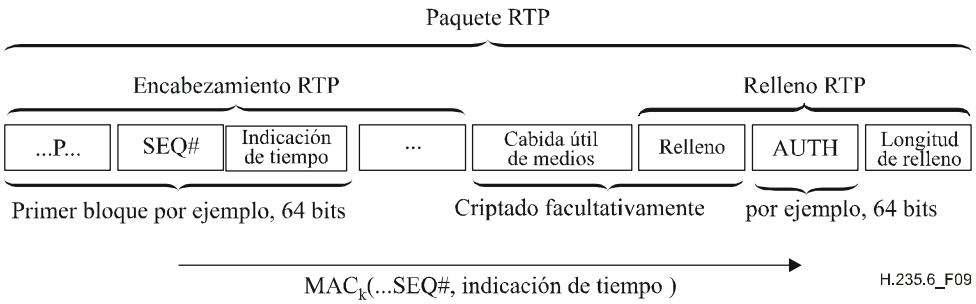


Figura 9/H.235.6 – Formato de paquete RTP para la antiinundación de medios

NOTA 1 – Si no se utiliza la antiinundación, tampoco se utilizan los campos AUTH y longitud de relleno y se aplica el formato de paquete RTP normal.

1) *Caso de antiinundación solamente*

Este caso se aplica cuando los datos de medios no están criptados y los campos de relleno se han dejado vacíos. El último octeto del relleno RTP contiene una cuenta del número de octetos que deberán ser ignorados al final del paquete RTP. Los otros bytes de relleno transportan el MAC. El MAC deberá ser calculado sobre el primer bloque criptográfico del encabezamiento RTP que incluye la indicación de tiempo variable y el número secuencial utilizando el algoritmo MAC negociado de **antiSpamAlgorithm** y aplicando el secreto simétrico. Puede utilizarse un secreto compartido estático o configurado manualmente, o un secreto *k* compartido negociado dinámicamente de conformidad con los procedimientos de la Rec. UIT-T H.235.0. Para tamaños de bloque superiores (más de 64 bits), deberán tomarse algunos bits adicionales suficientes del encabezamiento RTP o incluso la primera cabida útil de medios.

Como clave para el cálculo de MAC se recomienda utilizar la clave obtenida a partir de la distribución de claves de sesión de medios H.235; aún cuando la clave de sesión aplicada no se utiliza para la criptación de cabida útil. Para la gestión de claves se puede utilizar una conexión rápida segura con establecimiento de claves (véase anexo J/H.323) o la asignación manual de claves. El emisor calcula el MAC como se ha descrito anteriormente e incluye el resultado en el campo MAC del campo AUTH del relleno RTP. El emisor y el receptor conocen el tamaño del campo AUTH y la longitud del MAC mediante el **antiSpamAlgorithm**.

La verificación del MAC en el lado receptor debería realizarse cuanto antes, si fuera posible ya dentro de la pila RTP o a más tardar antes de la descriptación o descompresión de la cabida útil. El receptor recalcula en primer lugar el MAC del mismo modo que lo hizo el emisor y compara el MAC calculado con el MAC entregado en el relleno RTP. Si existe discordancia entre los MAC, ello significa que el encabezamiento RTP ha sido modificado en tránsito ha sido enviado por una entidad no autorizada que no es propietaria de la clave. Por ello, el paquete RTP autenticado equivocadamente deberá ser descartado y el evento puede ser registrado; esto probablemente indica una tentativa de ataque de denegación del servicio. En caso contrario, se puede seguir procesando el paquete RTP autenticado, el relleno RTP es eliminado y la cabida útil es suministrada a través del códec.

NOTA 2 – El cálculo/verificación del MAC ligero con criptación DES implica sólo una operación de criptación única; alternativamente, el MAC SHA1 se calcula sobre una parte pequeña de los paquetes de longitud fija, de modo que las operaciones criptográficas consumen recursos de procesamiento realmente mínimos.

2) *Caso del método antiinundación y criptación de la cabida útil*

Este caso se aplica cuando se efectúa una criptación de los datos de medios y se invoca el método antiinundación. Cuando la cabida útil no representa un número entero de bloques, se han de añadir algunos bytes de relleno adicionales a la cabida útil delante del MAC. La criptación de la cabida útil de medios ha de hacerse conforme a esta cláusula 9.

EncryptionCapability define el algoritmo de criptación de cabida útil mientras que **antiSpamAlgorithm** define el método antiinundación. Por motivos de seguridad, la criptación de medios y el MAC deberán utilizar diferentes claves de sesión. La clave *k* de MAC se calcula suministrando la clave de criptación *K* a través de la función generadora unidireccional SHA1;

k = SHA1(*K*); deberán tomarse suficientes bits del número generador resultante en el orden de bytes de red. Cuando el **antiSpamAlgorithm** indica un algoritmo de criptación, los bits recopilados deberán formar una clave de criptación correcta; por ejemplo, fijando los bits de paridad de DES.

Después de que el receptor haya verificado con éxito la autenticidad del paquete RTP, se desencripta la cabida útil y se descarta el relleno RTP. El procedimiento general es conforme al caso 1 anterior.

9.2.1 Lista de identificadores de objeto

En el cuadro 5 se listan todas las referencias de los OID.

Cuadro 5/H.235.6 – Identificadores de objeto utilizados para la antiinundación

Referencia del identificador de objeto	Valor del identificador de objeto	Descripción
"M"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 8}	Antiinundación que utiliza HMAC-SHA1-96
"N"	{iso(1) identified-organization(3) oiw(14), secsig(3) algorithm(2) desMAC(10)}	Antiinundación que utiliza MAC DES (56 bits) (véase ISO/CEI 9797-1 y 9797-2) con MAC de 64 bits.
"O"	{iso(1) identified-organization(3) oiw(14) secsig(3) algorithm(2) desEDE(17)}	Antiinundación que utiliza DES triple en MAC (168 bits) (véase ISO/CEI 9797-1 y 9797-2)

9.3 Aspectos relativos a RTP/RTCP

La utilización de criptación en el tren RTP seguirá la metodología general recomendada en el documento al que se hace referencia en [RTP]. La criptación de los medios se producirá de manera independiente, paquete por paquete.

NOTA – Cabe señalar que si el tamaño del paquete RTP es superior al tamaño de MTU, la pérdida parcial (de fragmento) hará que el paquete RTP completo sea indescifrable.

El encabezamiento RTP no será criptado. Para los códecs de audio/vídeo, se criptará toda la cabida útil de códec de audio/vídeo, incluido(s) todos los encabezamientos de cabida útil de audio/vídeo. La sincronización de nuevas claves y textos criptados se basa en el tipo de cabida útil dinámica (véase 8.6.3).

Se supone que esta criptación se aplica sólo a la cabida útil en cada paquete RTP, no se cifran los encabezamientos RTP. 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 hacerse sin tener en cuenta el estado, porque se pueden perder paquetes; cada paquete debería descifrarse independientemente. Dos requisitos del modo algoritmo de bloque funcionarán como sigue:

9.3.1 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 criptación, 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.

9.3.1.1 Vector de inicialización CBC

Se requiere un IV cuando se utilice un cifrado de bloque en el modo CBC para criptar cabidas útiles de paquetes RTP. El tamaño de un IV es igual al tamaño de bloque para el cifrado de bloque correspondiente. Por ejemplo, el tamaño IV para DES y 3-DES es 64 bits, mientras que para AES es 128 bits.

Para el caso CBC, el IV se construirá a partir de los primeros *B* octetos (donde *B* es el tamaño de bloques) de: número de secuencia (Seq#) concatenado y el Timestamp. Esto forma el patrón, *SSTTTT*, donde *SS* es el Seq# RTP de 2 octetos y *TTTT* es la indicación de tiempo RTP de 4 octetos. Este esquema se repetirá hasta que se hayan generado *B* octetos, truncando siempre que sea necesario. Por ejemplo, los IV de 64 y 128 bits podrían contener *SSTTTTSS* y *SSTTTTSSTTTTSSTT*, respectivamente. Nótese que el IV generado de esta manera puede producir un esquema de clave considerado "débil" en ciertos algoritmos.

9.3.1.2 Vector de inicialización EOFB

El vector inicial IV único para cada paquete RTP en el modo EOFB se calculará de la siguiente manera:

Se asocia cada paquete RTP con un índice *i* de paquete de 48 bits implícito, como se define en [SRTP], donde $i = 2^{16} \times \text{ROC} + \text{SEQ}$, y para el que SEQ es el número de secuencia tomado del encabezamiento RTP y ROC el contador de incremento de 32 bits cuántas veces el número de secuencia SEQ ha vuelto a 65535.

Para comenzar, el contador de incremento ROC se fijará a cero. Cada vez que el SEQ llega al módulo 2^{16}, el remitente incrementará ROC en un módulo 2^{32}.

El vector inicial IV se calcula como ($i \parallel T$ [$\parallel i \parallel T \parallel \ldots$]) con el índice *i* de 48 bit y el indicador de tiempo *T* de 32 bit tomados del encabezamiento RTP concatenado varias veces hasta que se llena completamente el tamaño de bloques. El símbolo || indica concatenación.

NOTA – El contador de recomienzo y el IV se mantienen y calculan localmente en cada extremo par, y no se transmiten.

Si hay paquetes perdidos o reordenados, el receptor debería calcular un índice *i* mediante:

$i = 2^{16} \times v + \text{SEQ}$, donde *v* se escoge del conjunto {ROC-1, ROC, ROC+1} modulo 2^{32}, de tal manera que sea el más cercano respecto al valor $2^{16} \times \text{ROC} + s_l$ (en el sentido de 2^{48}) donde s_l es el número de secuencia mantenido en el receptor. Tras haber procesado el paquete utilizando el índice así calculado, el receptor decidirá si hay que actualizar s_l y ROC. Por ejemplo, un método simple (pero no muy resistente a los errores) consiste en simplemente fijar s_l a SEQ (si SEQ > s_l) y, si el valor v = ROC + 1 ha sido utilizado, actualizar ROC a *v*; en [SRTP, sección 3.2.1] se puede encontrar más información al respecto.

9.3.2 Relleno

Los modos ECB y CBC procesan siempre el tren de entrada un bloque cada vez, pero CFB y OFB pueden procesar la entrada en cualquier número de octetos, N ($\leq B$); 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 bloques incompletos ECB y CBC; sin relleno para CFB y EOFB.

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

[RTP], sección 5.1 describe un método de relleno en el cual la cabida útil se rellenará hasta un múltiplo de bloque. El último octeto se fijará 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 soportarán 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.

9.3.3 Protección de RTCP

La aplicación de técnicas criptográficas a los elementos RTCP queda en estudio.

9.3.4 Tren de cabida útil seguro

Las redes basadas en H.323 suelen utilizar, por ejemplo para la transmisión mediante módem en el IP, señalización H.245 para establecer y negociar un canal de datos de banda local y RTP para la paquetización de un tren de cabida útil múltiple (MPS, *multiple payload stream*).

En el caso de un tren de medios único con un solo tipo de cabida útil o FEC para otro canal, el tipo de cabida útil dinámica en **encryptionSync** reemplazará el tipo de cabida útil por defecto.

Para los trenes de encapsulamiento (es decir, codificación de redundancia o FEC codificada según RFC 2198) el tipo de cabida útil dinámico en **encryptionSync** reemplazará el tipo de cabida útil de encapsulamiento.

Para los trenes de cabida útil múltiple se ignorará el tipo de cabida útil dinámico en la **syncFlag** de **encryptionSync**, y se utilizarán en su lugar los tipos de cabida útil (facultativos) en el (los) **multiplePayloadStreamElement**(s).

En el procedimiento mejorado de actualización de clave, se utilizará la **encryptionUpdateCommand** para distribuir nuevo material clave de sesión (véase 8.6.2). **multiplePayloadStream** se utiliza solamente cuando se debe reotorgar una clave a un tren de cabida útil múltiple, en cuyo caso se ignorará el tipo de cabida útil dinámico en **EncryptionSync**.

9.3.5 Interfuncionamiento con J.170

Queda en estudio.

9.4 DES triple en modo CBC exterior

La DES triple de 168 bits en modo CBC exterior, como se ilustra en la figura 10, *debería* utilizarse dentro de este perfil de seguridad. En la figura, cada k_i se refiere a una clave de 56 bits. Habrá que utilizar una clave de 56 bits diferente dentro de cada bloque de criptación (E, *encryption*) y descriptación (D, *decryption*). Aparentemente ninguna de las 64 claves débiles para DES ocasione alguna debilidad dentro de la DES triple. Sin embargo, las implementaciones conformes a este perfil deberían rechazar la clave si se trata de una clave DES débil (véase RFC 2405).

En [Schneier] y (RFC 2405) puede encontrarse más información sobre DES triple.

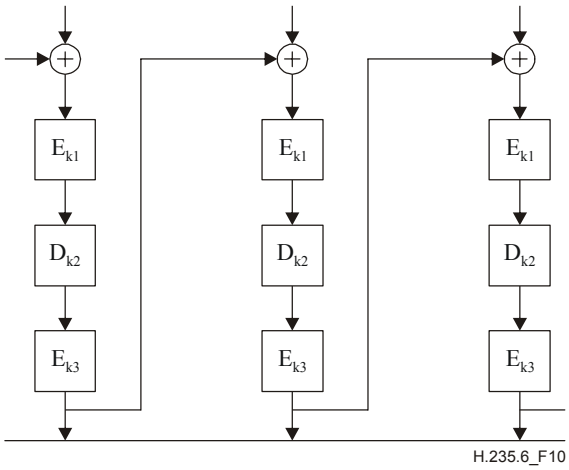


Figura 10/H.235.6 – Criptación DES triple en modo CBC exterior

9.5 Algoritmo DES que funciona en modo EOFB

Se puede criptar la voz utilizando el algoritmo DES que funciona en el modo de encadenamiento de bloque cifrado de tren EOFB. El modo EOFB permite aprovechar los paralelismos entre las implementaciones. Si se funciona en dicho modo, se recomienda tanto por motivos de calidad de funcionamiento como de seguridad, retroalimentar el bloque criptado completo (es decir, todos los 64 bits para DES, por ejemplo con $n = j = 64$). No obstante, puesto que este modo no proporciona el encadrenamiento entre los bloques y los bits, puede ser susceptible a ataques particulares dependiendo de las propiedades estadísticas de los datos de texto básico de entrada. Es decir, se debería efectuar una actualización de clave (véase 8.6) regularmente y, en todo caso, antes de que regrese el valor inicial. En 9.3.1.2 se describe el cálculo del valor inicial.

9.6 DES triple en el modo EOFB exterior

En este perfil de seguridad se puede utilizar la DES triple de 168 bits en modo EOFB exterior, como se muestra en la figura 11. En la figura, cada k_i representa una clave de 56 bits. Hay que utilizar una clave de 56 bits diferente dentro de cada bloque de criptación (E, *encryption*) y descriptación (D, *decryption*). Aparentemente, ninguna de las 64 claves débiles para DES debilita la DES triple. Sin embargo, las implementaciones conformes a este perfil deberían rechazar la clave si se trata de una clave DES débil [RFC 2405].

En [Schneier] y [RFC 2405] puede encontrarse más información sobre DES triple.

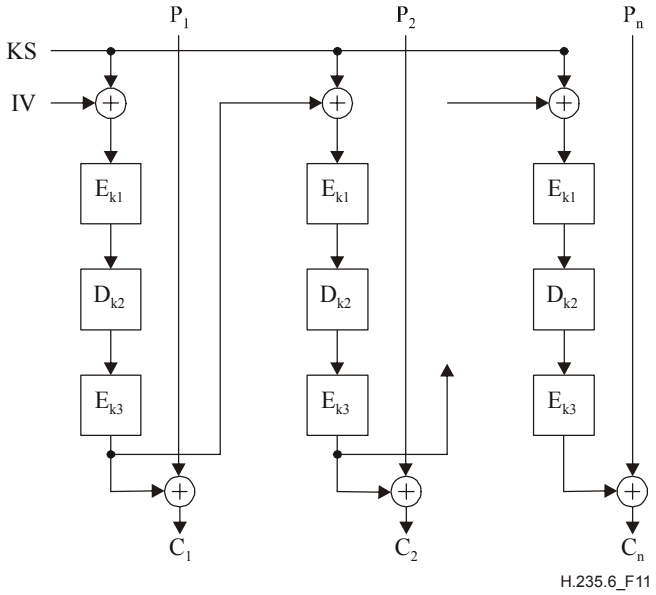


Figura 11/H.235.6 – Criptación DES triple en modo EOFB exterior

10 Interceptación lícita

Queda en estudio (véase [LI]).

11 Lista de identificadores de objeto

En el cuadro 6 se listan todos los OID referenciados (véase también [OIW] y [WEBOIDs]). No hay identificadores de objeto para H.235v1 [Rec. UIT-T H.235v1] ni para H.235v2 [Rec. UIT-T H.235v2].

Cuadro 6/H.235.6 – Identificadores de objeto

Referencia de identificador de objeto	Valor(es) de identificador de objeto	Descripción
"DHdummy"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 40} {itu-t (0) recommendation (0) h (8) 235 version (0) 3 40}	Se proporciona explícitamente el grupo DH no estándar.
"DH1024"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 43} {itu-t (0) recommendation (0) h (8) 235 version (0) 3 43}	Grupo DH de 1024 bits
"DH1536"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 44}	Grupo DH de 1536 bits
"X"	{iso(1) member-body(2) us(840) rsadsi(113549) encryptionalgorithm(3) 2}	Criptación vocal utilizando compatible con RC2 (56 bits) o compatible con RC2 en modo CBC y grupo DH de 512 bits.
"X1"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 27}	Criptación vocal que utiliza el RC2-compatible (56 bits) o RC2-compatible en modo EOFB y grupo DH de 512 bits.
"Y"	{iso(1) identified-organization(3) oiw(14) secsig(3)	Criptación vocal utilizando DES (56 bits) en modo CBC

Cuadro 6/H.235.6 – Identificadores de objeto

Referencia de identificador de objeto	Valor(es) de identificador de objeto	Descripción
	algorithm(2) descbc(7)}	y grupo DH de 512 bits.
"Y1"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 28}	Criptación vocal que utiliza el DES (56 bits) en modo EOFB y grupo DH de 512 bits con retroalimentación de 64 bits.
"Z1"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 29}	Criptación vocal que utiliza el DES triple (168 bits) en el modo EOFB exterior y grupo DH de 1024-bits con retroalimentación de 64 bits.
"Z2"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 30}	Criptación vocal que utiliza AES (128 bits) en el modo EOFB y grupo DH de 1024 bits.
"Z3"	{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) 3 nistAlgorithm(4) aes(1) cbc(2)}	Criptación vocal que utiliza AES (128 bits) en el modo CBC y grupo DH de 1024 bits.
"Z"	{iso(1) identified-organization(3) oiw(14) secsig(3) algorithm(2) desEDE(17)}	Criptación vocal utilizando DES triple (168 bits) en modo CBC exterior y grupo DH de 1024 bits.

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. Las figuras I.1 a I.5 ilustran la técnica.

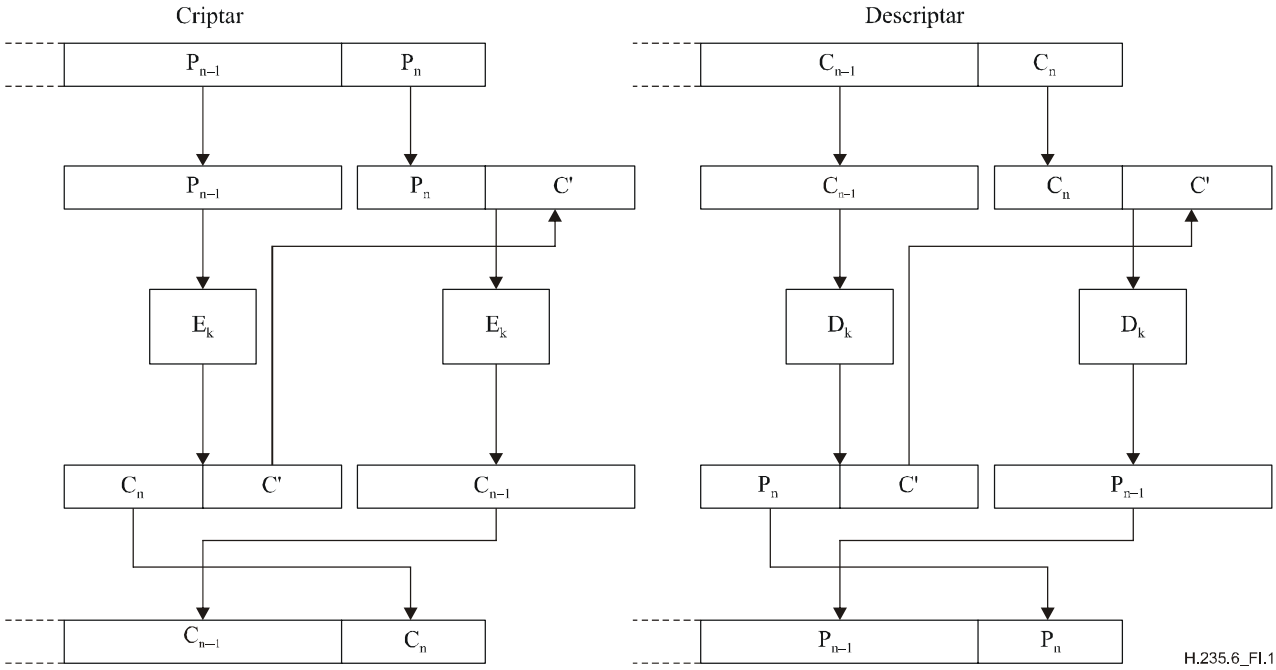


Figura I.1/H.235.6 – Apropiación de texto cifrado en modo ECB

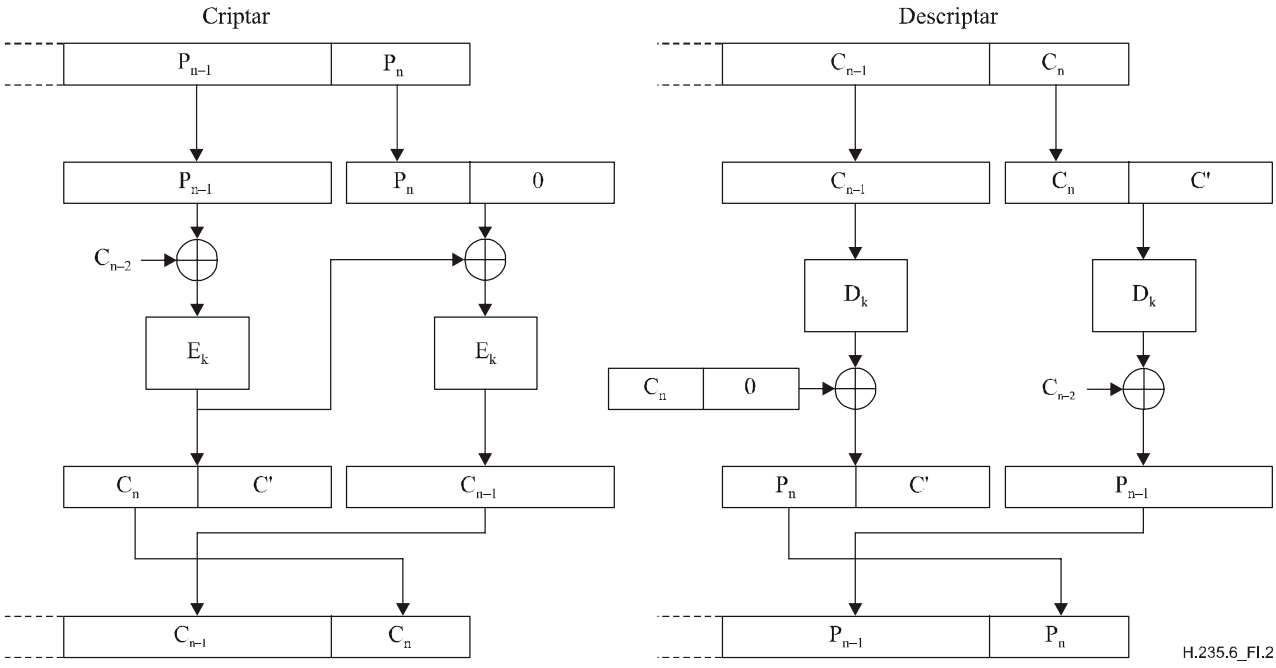


Figura I.2/H.235.6 – Apropiación de texto cifrado en modo CBC

NOTA – Para la apropiación de texto cifrado en los modos ECB o CBC es necesario que la cabida útil transporte al menos un bloque completo. Las implementaciones que utilicen apropiación de texto cifrado en el modo ECB o los modos CBC deberían garantizar que la cabida útil siempre transporta al menos un bloque criptado; por ejemplo, escogiendo adecuadamente la tasa de muestreo/paquetización o mediante la selección del algoritmo de criptación adecuado.

Cuando la cabida útil ocupe más de un bloque, el vector inicial (IV) se utilizará como el bloque anterior de texto cifrado cuando se aplique la apropiación de texto cifrado en el modo CBC.

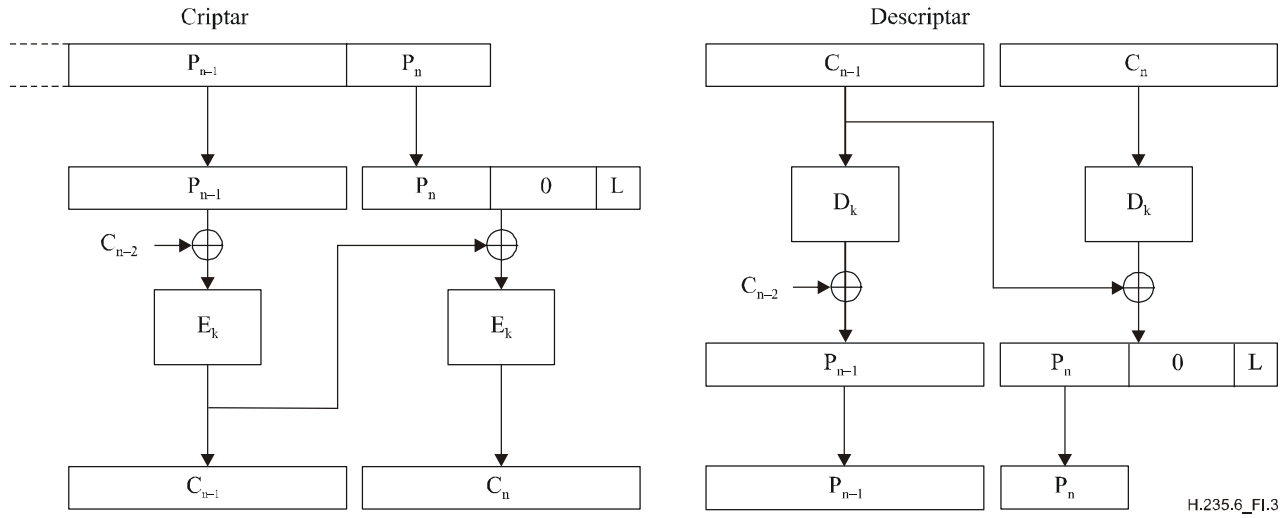


Figura I.3/H.235.6 – Relleno de ceros en modo CBC

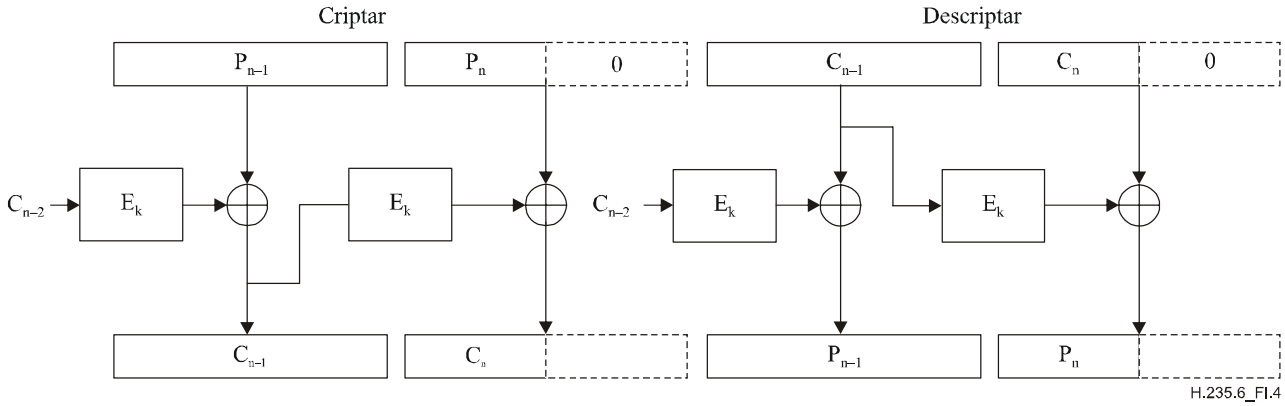
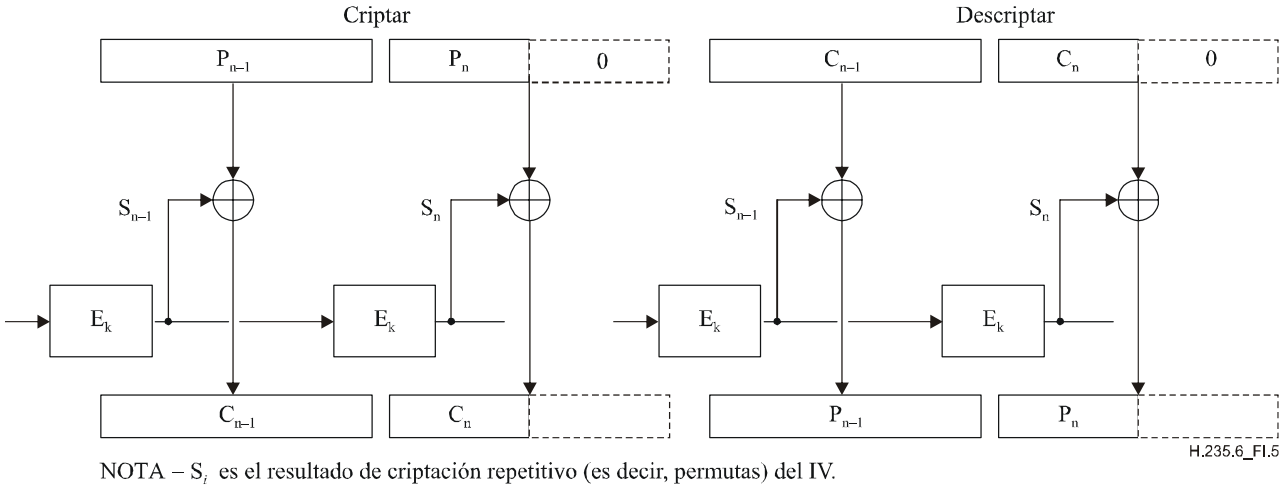


Figura I.4/H.235.6 – Relleno de ceros en modo CFB



NOTA – S_i es el resultado de criptación repetitivo (es decir, permutas) del IV.

Figura I.5/H.235.6 – Relleno de ceros en modo OFB

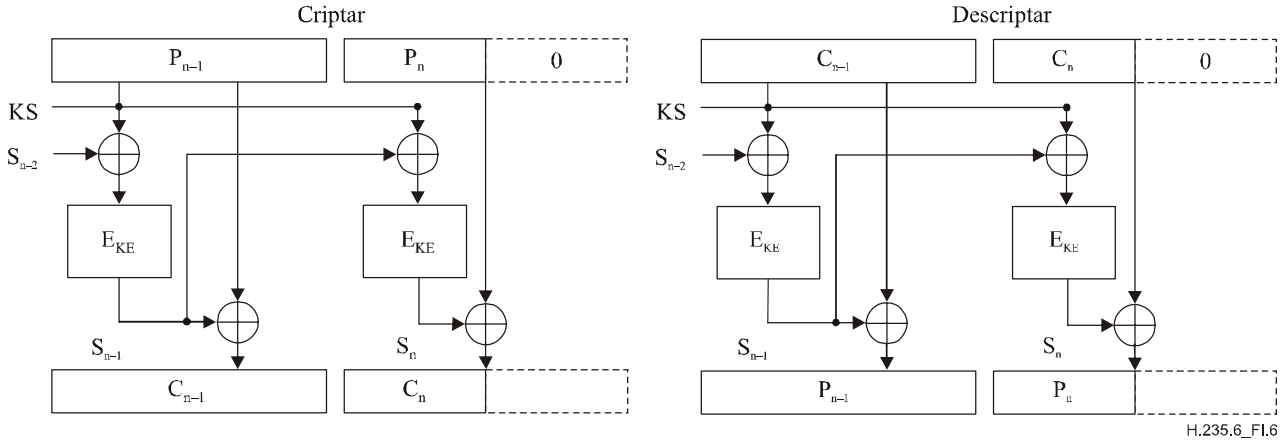


Figura I.6/H.235.6 – Modo EOFB con relleno de ceros

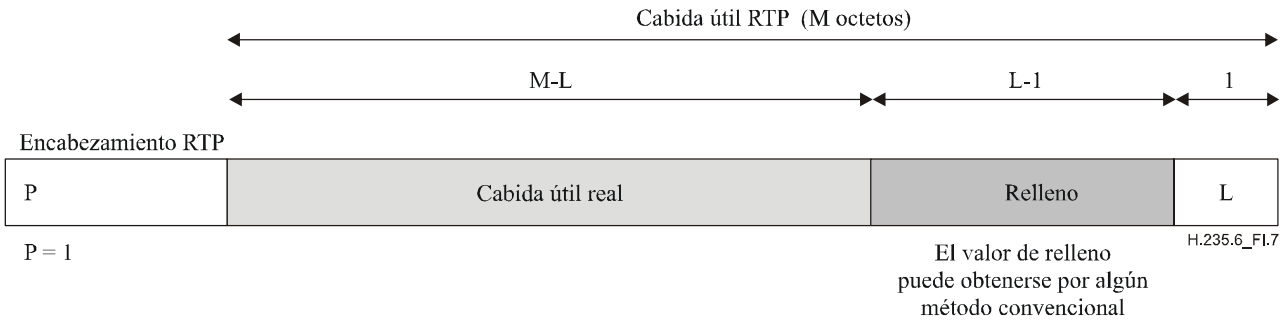


Figura I.7/H.235.6 – Relleno prescrito por RTP

I.2 Nuevas claves

Un MC realiza los procedimientos indicados en 8.5/H.323 para sacar a un participante de una conferencia. El terminal director puede generar nuevas claves de criptación para los canales lógicos (y no distribuirlas a la parte eliminada). Así se evita que la parte eliminada supervise los trenes de medios.

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