UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T H.233

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

(07/95)

TRANSMISIÓN DE SEÑALES NO TELEFÓNICAS

SISTEMAS CON CONFIDENCIALIDAD PARA SERVICIOS AUDIOVISUALES

Recomendación UIT-T H.233

(Anteriormente «Recomendación del CCITT»)

PREFACIO

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

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

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución N.° 1 de la CMNT (Helsinki, 1 al 12 de marzo de 1993).

La Recomendación UIT-T H.233 ha sido revisada por la Comisión de Estudio 15 (1993-1996) del UIT-T y fue aprobada por el procedimiento de la Resolución N.° 1 de la CMNT el 10 de julio de 1995.

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.

ÍNDICE

Recomendación H.233

SISTEMA CON CONFIDENCIALIDAD PARA SERVICIOS AUDIOVISUALES

(revisada en 1995)

1 Alcance

Un sistema de privacidad consta de dos partes, el mecanismo de confidencialidad o proceso de cifrado de los datos, y un subsistema de gestión de claves.

Esta Recomendación describe la parte de confidencialidad de un sistema de privacidad adecuado para su utilización en los servicios audiovisuales de banda estrecha conformes con las Recomendaciones H.221, H.230, y H.242. Aunque en un sistema de privacidad así se necesita un algoritmo de cifrado, la especificación de dicho algoritmo no se incluye aquí: el sistema prevé más de un algoritmo específico.

El sistema de confidencialidad es aplicable a los enlaces punto a punto entre terminales o entre un terminal y una unidad de control multipunto (MCU, *multipoint control unit*); puede extenderse al funcionamiento multipunto, en el que no existe descifrado en el MCU, pero este punto será objeto de estudio ulterior.

2 Referencias normativas

Las Recomendaciones y demás referencias siguientes 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 demás referencias son objeto de revisiones, por lo que se preconiza que todos los usuarios de la presente Recomendación investiguen la posibilidad de aplicar las ediciones más reciente de las Recomendaciones y demás referencias citadas a continuación. Se publica regularmente una lista de las Recomendaciones UIT-T actualmente vigentes.

[1] Recomendación UIT-T H.221 (1993), *Estructura de trama para un canal de 64 a 1920 kbit/s en teleservicios audiovisuales*.

[2] Recomendación UIT-T H.242 (1993), *Sistema de establecimiento de comunicación entre terminales audiovisuales por canales digitales de hasta 2 Mbit/s*.

[3] Recomendación UIT-T H.230 (1995), *Señales de control e indicación con sincronismo de trama para sistemas audiovisuales*.

[4] Recomendación X.208 del CCITT (1988), *Especificación de la notación de sintaxis abstracta uno (NSA 1)*.

3 Abreviaturas

A los efectos de esta Recomendación, se utilizan las siguientes abreviaturas:

BAS	Señal de asignación de velocidad binaria (*bit-rate allocation signal*) – véase [1]
CRC4	Verificación por redundancia cíclica de 4 bits (*4-bit cyclic redundancy check*) – véase [1]
ECS	Señal de control de encripción (*encryption control signal*) – véase [1]
FAS	Señal de alineación de trama (*frame alignment signal*) – véase [1]
H.221	«Estructura de trama/entramado H.221» – véase [1]
ILC	Identificador, longitud, contenido (*identifier, length, content*)
IV	Vector de inicialización (*initialization vector*)
LSB	Bit menos significativo (*least significant bit*)
MCU	Unidad de control multipunto (*multipoint control unit*)
MLP	Canal lógico «MLP» (*multi-layer protocol "MLP" logical channel*) – véase [1]

MSB Bit más significativo (*most significant bit*)

SE Intercambio de sesión (*session exchange*)

SV Variable de partida (*starting variable*)

AIM Códigos de control e indicación (*control* & *indication codes*) – véase [3]

AIA Códigos de control e indicación (*control* & *indication codes*) – véase [3]

VIS Códigos de control e indicación (*control* & *indication codes*) – véase [3]

4 Propiedades del sistema especificado

4.1 Confidencialidad

1) La confidencialidad es independiente de otros servicios de privacidad proporcionados por el sistema; las claves se proporcionan por otros mecanismos tales como el descrito en el proyecto de Recomendación sobre autenticación y gestión de claves, o pueden introducirse manualmente.

2) Es aplicable a las señales audiovisuales entramadas según la Recomendación H.221, a velocidades de transferencia de $p \times 64$ kbit/s, donde p toma cualquier valor de 1 a 30. De acuerdo con la Recomendación H.221, la propia estructura de trama no está cifrada.

3) Se da confidencialidad a todas las transmisiones de audio, vídeo y datos, puesto que estas señales se cifran juntas bajo la misma clave (esto incluye actualmente datos MLP, de acuerdo con el Anexo A/H.221, aunque este aspecto queda en estudio).

4) El sistema es independiente del algoritmo de cifrado utilizado; algunos algoritmos han sido proporcionados, y podrían añadirse otros.

5) El mecanismo de confidencialidad es capaz de funcionar en llamadas punto a punto, y también en llamadas multipunto en las que se permite descifrado en la MCU (la denominada «MCU encargada»).

4.2 Especificación de algoritmos

La especificación de algoritmos no se incluye en esta Recomendación, que prevé una amplia gama de algoritmos de cifrado. Las especificaciones deben hallarse en otro lugar (véase 5.2) y contener los siguientes detalles:

– longitudes del vector de inicialización y de las claves de sesión;

– generación de la variable de partida a partir del vector de inicialización.

5 El mecanismo de confidencialidad

5.1 Descripción de la operación

La Figura 1 da un diagrama de bloques de un cifrador de enlace. Consta de un bloque cifrador y un bloque descifrador. El cifrador toma los datos de usuario y los cifra para formar datos cifrados. El descifrador toma los datos cifrados y los descifra para obtener los datos de usuario.

Dos canales conectan el cifrador y el descifrador. Uno se utiliza para transmitir los datos de usuario cifrados. El segundo es un canal no cifrado, llamado señal de control de cifrado (ECS, *encryption control signal*), y se utiliza para transmitir información de control del cifrador al descifrador. Aunque estos dos canales se muestran físicamente por separado, en la práctica se multiplexan en un único tren de datos.

Se utilizan técnicas de cifrado de tren aditivo (véase 5.2).

Las claves son proporcionadas por otros mecanismos y se presentan al mecanismo de confidencialidad a medida que se requieren. Son utilizadas por el cifrador y el descifrador de manera síncrona con los datos, y por el canal de control se envía la bandera de sincronización de carga de claves (véase L en el quinto guión del apartado 1) en 5.1.3).

El cifrado de datos es controlado desde el cifrador: la bandera de cifrado ON/OFF se envía por el canal de control para indicar cuándo se cifran los datos. El descifrador responde a esta bandera y descifra los datos cuando se le solicita.

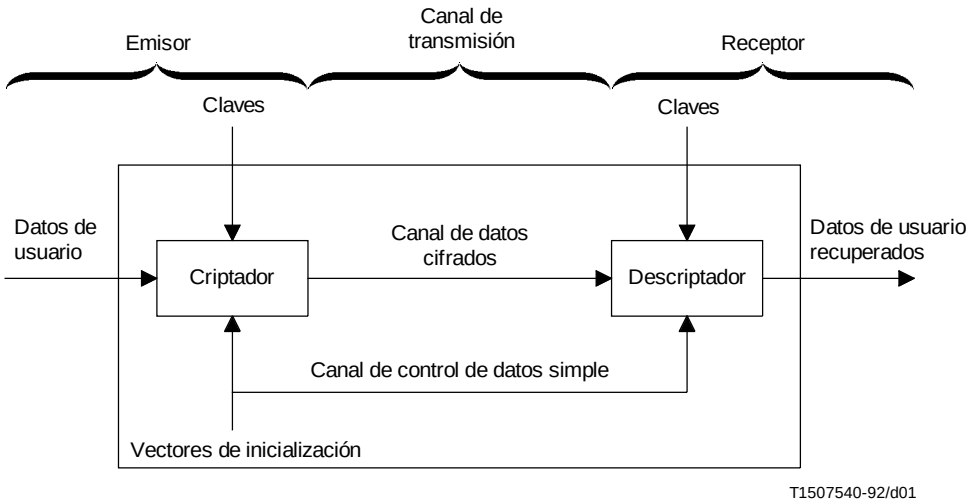


FIGURA 1/H.233

Diagrama de bloques de un criptador de enlace

5.1.1 Control e indicación dentro de la trama Rec. H.221

Para indicar la presencia de un sistema de confidencialidad dentro de un terminal, debe transmitirse el código BAS «Capacidad de cifrado». Si esta capacidad es señalizada desde ambos extremos de un enlace, puede abrirse el canal de señal de control del cifrado (ECS, *encryption control signal*) en cada sentido mediante la instrucción BAS Encrypt-on; se puede cerrar el canal ECS con la instrucción Encrypt-off, pero debe ir precedida por la transmisión de una bandera Encryption-off dentro del propio canal (ver a continuación). Si un terminal recibe la instrucción BAS Encrypt-off sin recibir primero la bandera Encryption-off, se indicará al usuario que puede haber intrusión o funcionamiento incorrecto del sistema de confidencialidad.

En los casos en que se utilice una señal entramada Rec. H.221 en un sentido solamente, el canal ECS puede ser activado sin utilizar el mecanismo de capacidad: el mecanismo para asegurar que el extremo receptor puede descifrar el algoritmo elegido, etc., cae entonces fuera del alcance de esta Recomendación.

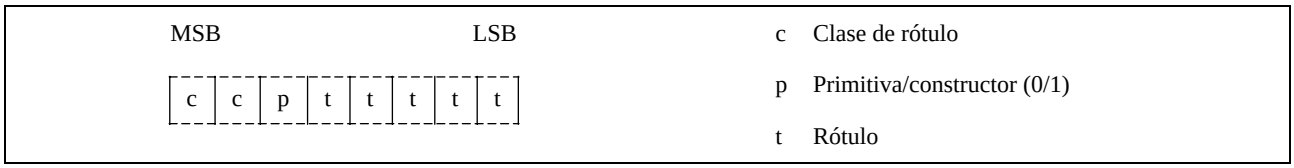
5.1.2 Formatos de mensaje

Los mensajes utilizados por el sistema de cifrado para la distribución y autenticación de claves se formatan en una forma identificador, longitud, contenido (ILC, *identifier, length, content*) nidificada, que se describe en la Recomendación X.208 [4]. La longitud puede codificarse en forma corta o forma larga. No se utilizará la forma indefinida indicada en [4].

A continuación figura una breve descripción de algunas de las definiciones de la Recomendación X.208 [4] utilizadas en esta propuesta.

5.1.2.1 Identificador

Un identificador es un octeto, cuya estructura es la que se presenta a continuación.



La clase de rótulo define el tipo de identificador, que será 10 u 11 (según el contexto) para los identificadores definidos en esta Recomendación.

El bit de primitiva/constructor (P) indica si el contenido es una primitiva o si se compone de elementos nidificados.

El rótulo de 5 bits define unívocamente el identificador (según su clase).

Por tanto, todos los identificadores de esta Recomendación tienen la forma de octeto: 10 P t_1 t_2 t_3 t_4 t_5 u 11 P t_1 t_2 t_3 t_4 t_5.

5.1.2.2 Longitud

La longitud especifica la longitud de octetos del contenido y es de naturaleza variable.

La forma corta tiene un octeto de longitud y se utilizará con preferencia a la forma larga cuando L es menor que 128. El bit 8 tiene el valor cero y los bits 7-1 codifican L como un número binario sin signo, cuyos MSB y LSB son el bit 7 y el bit 1, respectivamente.

La forma larga tiene una longitud de 2 a 127 octetos y se utiliza cuando L es superior o igual a 128 y menor que 2 a la potencia 1008. El bit 8 del primer octeto tiene el valor uno. Los bits 7-1 del primer octeto codifican un número inferior en una unidad al tamaño de la longitud en octetos, como número binario sin signo cuyos MSB y LSB son el bit 7 y el bit 1, respectivamente. El propio L se codifica como un número binario sin signo, cuyos MSB y LSB son el bit 8 del segundo octeto y el bit 1 del último octeto, respectivamente. Este número binario será codificado en el menor número posible de octetos, sin octetos de cabecera que contengan el valor 0.

5.1.2.3 Cadena de bits

Una cadena de bits en forma primitiva tiene ocho bits por octeto y va precedida por un octeto que codifica el número de bits no utilizados en el octeto final del contenido – de cero a siete – como número binario sin signo, cuyos MSB y LSB son el bit 8 y el bit 1, respectivamente.

5.1.3 Canal ECS no cifrado

El sistema de confidencialidad exige la utilización de un canal de control no cifrado entre el cifrador y el descifrador. Sólo se necesita un canal de control por sistema de cifrado de enlace. El mismo canal de control se utiliza en asociación con el cifrado del audio, vídeo y cualesquiera datos que puedan estar presentes.

El contenido del canal ECS se estructura en bloques de 128 bits, síncronos con la multitrama H.221 (véase la Figura 2); por tanto, el primer bit del bloque es el bit 8 del octeto 17 de la trama número 0 en una multitrama. Existen dos tipos de bloques: intercambio de sesión (SE, *session exchange*) y vector de inicialización (IV, *initialization vector*). La información contenida dentro de un bloque IV surte efecto desde el comienzo de la siguiente multitrama, y sigue siendo efectiva hasta que se envía otro IV. El canal ECS debe siempre contener sea un bloque IV o un bloque SE, cabe señalar que, según la definición de ciertos algoritmos, se puede cargar repetidamente el mismo IV; la decisión de hacerlo o no depende del compromiso entre un restablecimiento más rápido después de un error y una seguridad adicional.

	Bit número														
	0	1	2	3	4	5	6	7	8	9	10	11	| 12-119	|	120-127
Tipo SE	0	n	n	s	s	s	s	s	e	e	e	e	| mensaje	|	de reserva
	Bit número														
	0	1	2	3	4	5	6	7	8	9	10	11	| 12-107	|	108-127
Tipo IV	1	n	n	A	C	C	L	s	e	e	e	e	| IV	|	de reserva

FIGURA 2/H.233

Bloques de canales de control

El bloque contiene lo siguiente:

1) Encabezamiento (12 bits), compuesto por:
   - Bit 0 para seleccionar el tipo: 0 = SE (intercambio de sesión)
     1 = IV (vector de inicialización)
   - Bits 1 y 2 para identificar los bloques de una secuencia multibloque
     00 para un único bloque, no seguido por bloques relacionados
     01 para el bloque N.° 1 de una secuencia de varios bloques
     10 para un bloque intermedio de una secuencia
     11 para el último bloque de una secuencia
   - Bit 3 del bloque tipo IV para indicar cifrado activado (on)/desactivado (off) (A):
     1 = ON, 0 = OFF
   - Bits 4 y 5 del bloque tipo IV para dar la longitud de IV (CC):
     00 = 64 bits + 32 bits de corrección de errores
     01, 10, 11 reservados
   - Bit 6 del bloque tipo IV: reservado para sincronización de carga de claves (L)
   - Todos los demás bits: de reserva puestos a «0»
   - Bits 8-11: corrección de errores para los bits 0-7
2) Bloques SE: 108 bits estructurados como $9 \times (8$ bits de información + 4 bits de corrección de errores)

   Bloques IV: vector de inicialización del sistema o parte del mismo (64 bits), con protección contra errores (32 bits).
3) Bloques SE: 8 bits de reserva

   Bloques IV: 20 bits de reserva – proporcionan un intervalo para que el sistema actúe sobre la información recibida, y pueden también proporcionar mejora futura.

5.1.3.1 Bloques de intercambio de sesión

En los bloques de tipo SE, los 116 bits que siguen al encabezamiento de bits $8 + 4$ están estructurados como $9 \times (8 + 4) + 8$, donde los últimos 8 bits no se utilizan, y las 9 palabras son cada una 8 bits de información con 4 bits de corrección de errores. En el receptor, los bits de información (procedentes de más de un bloque si así se indica en el encabezamiento) se forman para componer un tren, compuesto de mensajes sobre autenticación y gestión de claves, más dos mensajes adicionales P8, P9 definidos a continuación para las capacidades e instrucciones de algoritmo.

Los 12 bits de las palabras de cola no utilizadas del bloque SE deben ponerse a cero.

Capacidades de algoritmo (P8)

Nombre del mensaje: esta es la información disponible sobre los algoritmos de descifrado (P8).

Identificador del mensaje: 1 1 P t_1 t_2 t_3 t_4 t_5 = 11000000.

Contenido: [número 3-255] [más bytes] en el que el primer byte da el número de los bytes siguientes. Cada conjunto de tres bytes indica un mecanismo de descifrado disponible mediante valores como identificadores de medios, identificadores de algoritmo e identificadores de parámetro listados a continuación. Por ejemplo, un terminal capaz de decodificar DES y FEAL transmitiría el mensaje P8 {[11000000][00000110][00000000] [00000010][00000000][00000000][00000001][00000000]}.

Instrucción de algoritmo (P9)

Nombre del mensaje: esta es la información del algoritmo en uso (P9).

Identificador del mensaje: 1 1 P t_1 t_2 t_3 t_4 t_5 = 11000001.

Significado: cuando el bit encryption-ON es el próximo conjunto en el encabezamiento IV, el algoritmo utilizado es el especificado aquí en este mensaje.

Contenido: bytes del esquema de cifrado (mismos valores que en el mensaje de capacidad P8).

Identificadores de medios

Se utiliza un byte para identificar cuáles son los elementos de la señal audiovisual que se cifran. Cada bit de este byte corresponde al medio siguiente:

1er	bit (LSB):	audio 0 = cifrado, 1 = no cifrado
2º	bit:	vídeo 0 = cifrado, 1 = no cifrado
3er	bit:	LSD 0 = cifrado, 1 = no cifrado
4º	bit:	HSD 0 = cifrado, 1 = no cifrado
5º	bit:	reservado para MLP, puesto a «0»
6º	bit:	reservado para H-MLP, puesto a «0»
7º	bit:	reservado para uso futuro, puesto a «0»
8º	bit (MSB):	reservado para uso futuro, puesto a «0»

[00000000] indica que la señal multiplexada (excepto FAS, BAS y ECS) está criptada. Los procedimientos para otros casos están en estudio.

Identificadores de algoritmo

Se utiliza un byte para identificación de algoritmo. La definición del algoritmo incluye la especificación completa sobre cómo se obtiene el tren de cifrado a partir de la clave vigente y el valor IV. Actualmente hay identificados varios algoritmos; deben utilizarse los siguientes códigos:

MSB LSB	
0 0 0 0 0 0 0 0	No asignado. Reservado para uso futuro
0 0 0 0 0 0 0 1	«FEAL» (véase A.1) – ISO/CEI 9979 algorithm register No. 0010
0 0 0 0 0 0 1 0	«DES» (véase A.2), modo 1 – ISO/CEI 9979 algorithm register No. 0004
0 0 0 0 0 0 1 1	Reservado para «DES» (véase A.2), modo 2
0 0 0 0 0 1 0 0	Reservado para «DES» (véase A.2), modo 3
0 0 0 0 0 1 0 1	B-CRYPT – ISO/CEI 9979 algorithm register No. 0001
0 0 0 0 0 1 1 0	IDEA – ISO/CEI 9979 algorithm register No. 0002
0 0 0 0 0 1 1 1	BARAS (ETSI)
Otros valores	No asignados. Reservados para uso futuro

Identificadores de parámetro

Se utiliza un byte para identificar los parámetros de los algoritmos de cifrado que se definen en 5.2. El valor por defecto es [00000000], que puede utilizarse cuando el algoritmo no necesita valores de parámetro. En el Anexo A se indican los parámetros operacionales de cada método de cifrado.

El equipo debe proporcionar el descifrado de al menos uno de los algoritmos identificados; si se indica más de una capacidad, puede entonces dejarse al operador del sistema la selección del algoritmo necesario para el cifrado de la información transmitida.

Otros mensajes

P1 Nombre del mensaje: no se puede cifrar.

Significado: el enviador de este mensaje no utilizará un sistema de cifrado.

Identificador del mensaje: 1 0 P t_1 t_2 t_3 t_4 t_5 = 10000001.

Contenido: este mensaje no tiene contenido.

P2 Nombre del mensaje: Falla el arranque del sistema de cifrado.

Significado: el enviador de este mensaje no ha podido hacer arrancar su sistema de cifrado. Esto podría deberse a un fallo en el intercambio de claves, pero por razones de seguridad, no se da ninguna indicación en el mensaje de la causa del fallo.

Identificador del mensaje: 1 0 P t_1 t_2 t_3 t_4 t_5 = 100000010.

Contenido: este mensaje no tiene contenido.

Si resulta necesario enviar P1 o P2, o si se recibe cualquiera de estos mensajes, se proporcionará una indicación al usuario. Los medios de esa indicación y las acciones subsiguientes se dejan al arbitrio del realizador.

5.1.3.2 Vectores de inicialización

La longitud por defecto del IV es 64 bits. La longitud, incluida corrección de errores, es de 96 bits. Pueden transmitirse longitudes IV mayores utilizando más de un bloque. El bit más significativo se transmite primero, es decir, el bit 12 del (primer) bloque de tipo IV.

5.1.3.3 Protección contra errores de la información del canal de control

La información transmitida vía el canal de control debe protegerse contra los errores. Se utiliza para ello un código Hamming [12,8]. Las matrices generadora y de comprobación de paridad se dan en la Figura 3.

El mismo esquema se utiliza para los encabezamientos, los mensajes de intercambio de sesión y los vectores de inicialización. En cada caso, un byte de 8 bits va seguido por cuatro bits de corrección de errores.

El IV se divide en 8 bytes, cada uno de los cuales tiene 4 bits de paridad asignados, lo que en el caso por defecto hace una longitud total IV más paridad de 96 bits.

Matriz generada	Matriz de comprobación de paridad
100000001110 010000000111 001000001010 000100000101 000010001011 000001001100 000000100110 000000010011	1110 0111 1010 0101 1011 1100 0110 0011 1000 0100 0010 0001

T1507550-92/d02

FIGURA 3/H.233

Matrices de corrección de errores

5.2 Método de cifrado de la transmisión

Esta subcláusula trata del cifrado de audio, vídeo y cualesquiera datos asociados. El cifrado sólo tendrá lugar si se establece la alineación de multitrama H.221.

El sistema de cifrado realiza las mismas funciones independientemente de la velocidad de transferencia. Pueden cifrarse cualquier tren de información de usuario o la totalidad de esos trenes. El sistema de cifrado no necesita información sobre la asignación de capacidades entre estas diversas formas de información de usuario, ya que cripta los datos después de la multiplexación y descripta los datos antes de la demultiplexación. Los dos sentidos de transmisión son independientes: se puede cifrar uno o ambos, y utilizar algoritmos diferentes.

El orden temporal de cifrado sigue el de la transmisión en un tren serie bit a bit. Los datos deben cifrarse antes de que tenga lugar ningún cálculo CRC4. Los cálculos CRC4 se efectúan entonces en los datos cifrados, asegurándose de que a cualesquiera redes asociadas se les presente un código CRC4 válido.

Se crea en ambos terminales un tren de cifrado a partir de los valores vigentes de la clave y del vector de inicialización; este tren se combina en el cifrador con los bits que han de cifrarse por adición en módulo 2, y en el descifrador los bytes cifrados se añaden en módulo 2 al mismo tren de cifrado para recuperar la información de liberación del usuario.

Los vectores de inicialización (IV) se crean en forma aleatoria en el cifrador y se envían al descifrador a través del ECS. Se utilizan síncronamente con los datos que han de cifrarse o descifrarse. Proporcionan un método para resincronizar el cifrador y el descifrador periódicamente.

NOTA – Debe prestarse atención al orden de los bits IV cargados en el cifrador y el descifrador, según el algoritmo elegido.

Si se pierde la sincronización, los datos se corromperán hasta que se reciba un nuevo IV. El periodo para la transmisión IV viene determinado por la magnitud de la pérdida de datos que puede ser tolerada hasta que se obtiene resincronización.

Cada bit dentro del canal se trata por el sistema de cifrado de una de las tres maneras siguientes (véase el Apéndice I):

a) se genera y aplica el tren de cifrado: información de usuario (audio, vídeo, datos);

b) se genera el tren de cifrado, pero no se aplica: FAS y BAS en los canales iniciales y adicionales (véase la Recomendación H.221) y ECS; el tren de cifrado no es almacenado ni sometido a retardo para uso posterior, pero se pierde, y no se utiliza para cifrar ninguna información siguiente;

c) no se genera ningún tren de cifrado: si la salida de terminal a línea incluye canales que no forman parte de la velocidad de transferencia especificada en la instrucción BAS pertinente (por ejemplo, TS0 y/o TS16 de una conexión a velocidad primaria, u otros canales no transmitidos extremo a extremo), no se genera para estos bits ningún tren de cifrado.

En la transmisión a 56 kbit/s descrita en el Anexo B/H.221, se genera tren de cifrado para el octavo subcanal, pero solamente se utilizan los primeros 7 bits para la adición en módulo 2 a la señal de septeto.

En la transmisión restringida a 128 kbit/s o a velocidad superior, se genera tren de cifrado, pero no se aplica al octavo bit de relleno en cada intervalo de tiempo.

5.3 Procedimiento para la utilización del sistema

Cuando un terminal desea empezar el cifrado, habiendo recibido la capacidad «encrypt» (véase la Recomendación H.221) en el juego de capacidades del terminal distante, abre el canal ECS y transmite el mensaje (o mensajes) P8. Al recibir el mensaje (o mensajes) P8 desde el extremo distante, comprueba si hay algunos algoritmos/modos compatibles: si no los hay, envía el mensaje P1; si hay compatibles, envía un mensaje P9 para identificar el algoritmo/modo que se utilizará, e inicia entonces la transmisión de bloques IV. En el Apéndice II se presentan ejemplos de procedimientos para una sesión de cifrado.

P2 puede ser utilizado en procedimientos de recuperación de fallo (queda en estudio).

6 Cifrado del canal MLP

Queda en estudio.

Anexo A

Algoritmos de cifrado y sus parámetros

(Este anexo forma parte integrante de la presente Recomendación)

A.1 FEAL

Se crea un tren de cifrado en ambos terminales a partir de los valores vigentes de la clave y del vector de inicialización utilizando FEAL-8 (FEAL de 8 rondas con clave de 64 bits) en modo realimentación de salida (OFB, *output feeback*) definido en ISO 8372. En la referencia [A1] se dan detalles del algoritmo FEAL. Este tren se combina en el cifrador con los bits que han de cifrarse por adición en módulo 2, y en el descifrador, los bits cifrados se añaden en módulo 2 al mismo tren de cifrado para recobrar la información de liberación de usuario (véase la Figura A.1).

La variable de partida (SV, *starting variable*) es idéntica al vector de inicialización (IV, *initialization vector*). IV se carga al comienzo de cada multitrama.

De los 64 bits de salida del algoritmo de cifrado, los 8 primeros bits del lado MSB se utilizan para adición en módulo 2 bit a bit a los 8 bits del bloque de señal audiovisual; el primer bit del bloque de cifrado se añade en módulo 2 al primer bit del bloque de señal, y el bit resultante se transmite primero a través del canal, el segundo bit del bloque de cifrado se añade en módulo 2 al segundo bit del bloque de señal y el bit resultante se transmite a continuación a través del canal, y así sucesivamente. Si se transmiten los 8 bits, se genera y utiliza para cifrado el siguiente ciclo del tren de cifrado.

A.2 DES

El algoritmo DES y los métodos para aplicar el tren de cifrado al tren de datos se describen en la referencia [A2].

DES modo 1 utiliza uno de los dos métodos designados OFB-8 y OFB-64. La variable de partida (SV) es idéntica al vector de inicialización (IV). El identificador de parámetro se fija así:

Valor de campo		Modo OFB	Número de bits
MSB	LSB		
0000	0000	OFB-8	8
0000	0001	OFB-64	64

Todos los demás valores del identificador de parámetro se reservan para ulterior estudio.

DES modo 2 y DES modo 3 quedan para ulterior estudio.

A.3 IDEA

El algoritmo de cifrado de bloque IDEA funciona con bloques de entrada y salida de 64 bits y está controlado por una clave de 128 bits. Se define en la referencia [A3].

El modo de funcionamiento para producir el tren de cifrado es retroalimentación de salida OFB-8, *output feed back OFB*, conforme a ISO 8372. La variable de partida es idéntica al vector de inicialización (IV).

El método para aplicar el tren de cifrado al tren de datos es fundamentalmente el correspondiente a OFB definido en ISO 8372. Los ocho bits del tren de cifrado que se utilizan para cifrar los ocho bits del tren de datos son los bits más a la izquierda del bloque de salida de 64 bits que se describen en la Figura 1 de la referencia [A3].

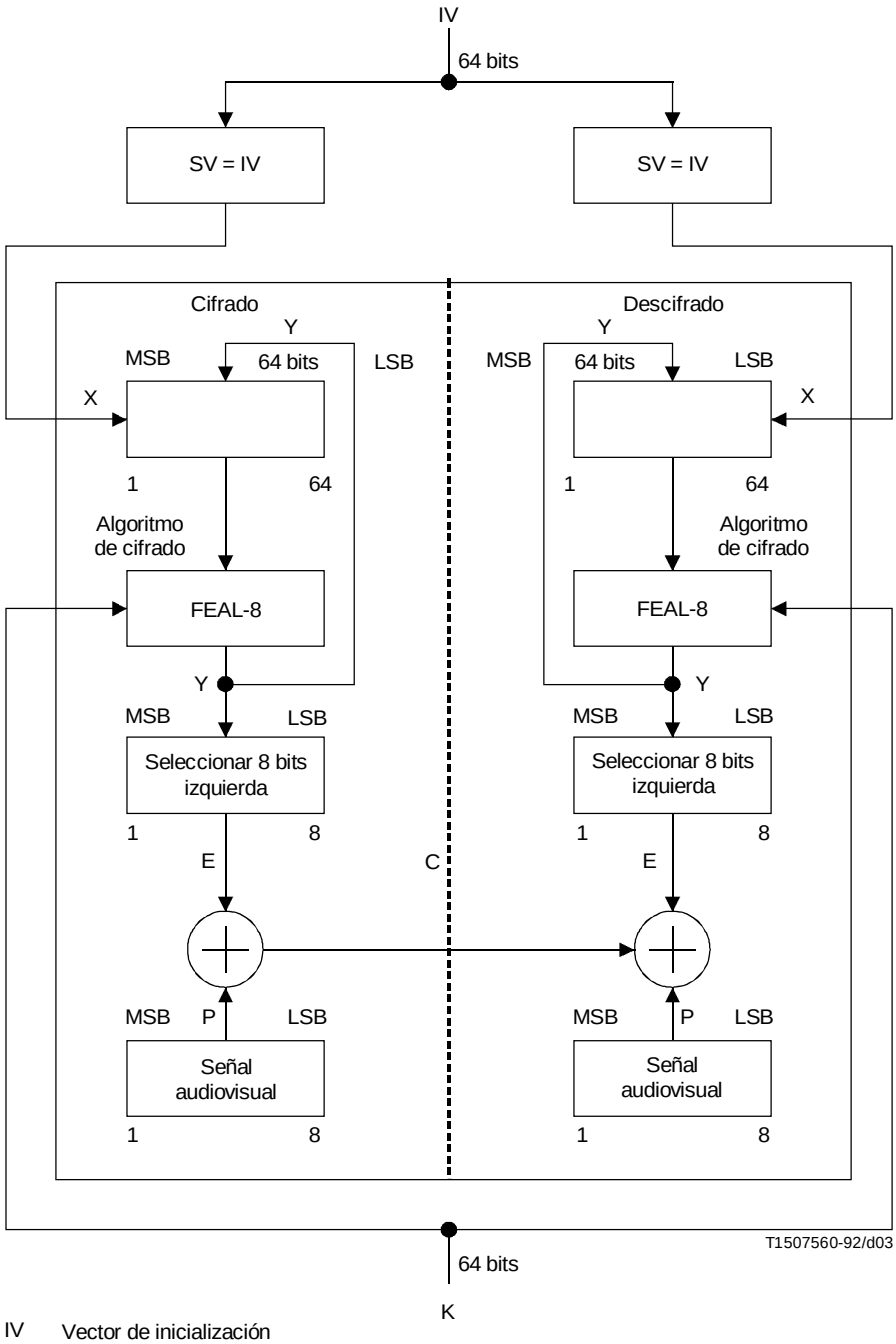
El parámetro identificador (véase 5.1.3.1) se pone a [0000 0000] en este modo. Otros modos de funcionamiento, como encadenamiento de bloque de cifrado o retroalimentación de cifrado descritos en ISO 8372 precisan más estudio.

Referencias normativas

[A1] ISO/CEI 9979 Resgistration No. 0010 (FEAL).

[A2] ISO/CEI 9979 Registration No. 0004 (*data encryption standard*).

[A3] ISO/CEI 9979 Registration No. 0002 (IDEA).



IV Vector de inicialización
K Clave (*key*)
SV Vector de partida

FIGURA A.1/H.233

Operación en modo realimentación de salida para FEAL

Apéndice I

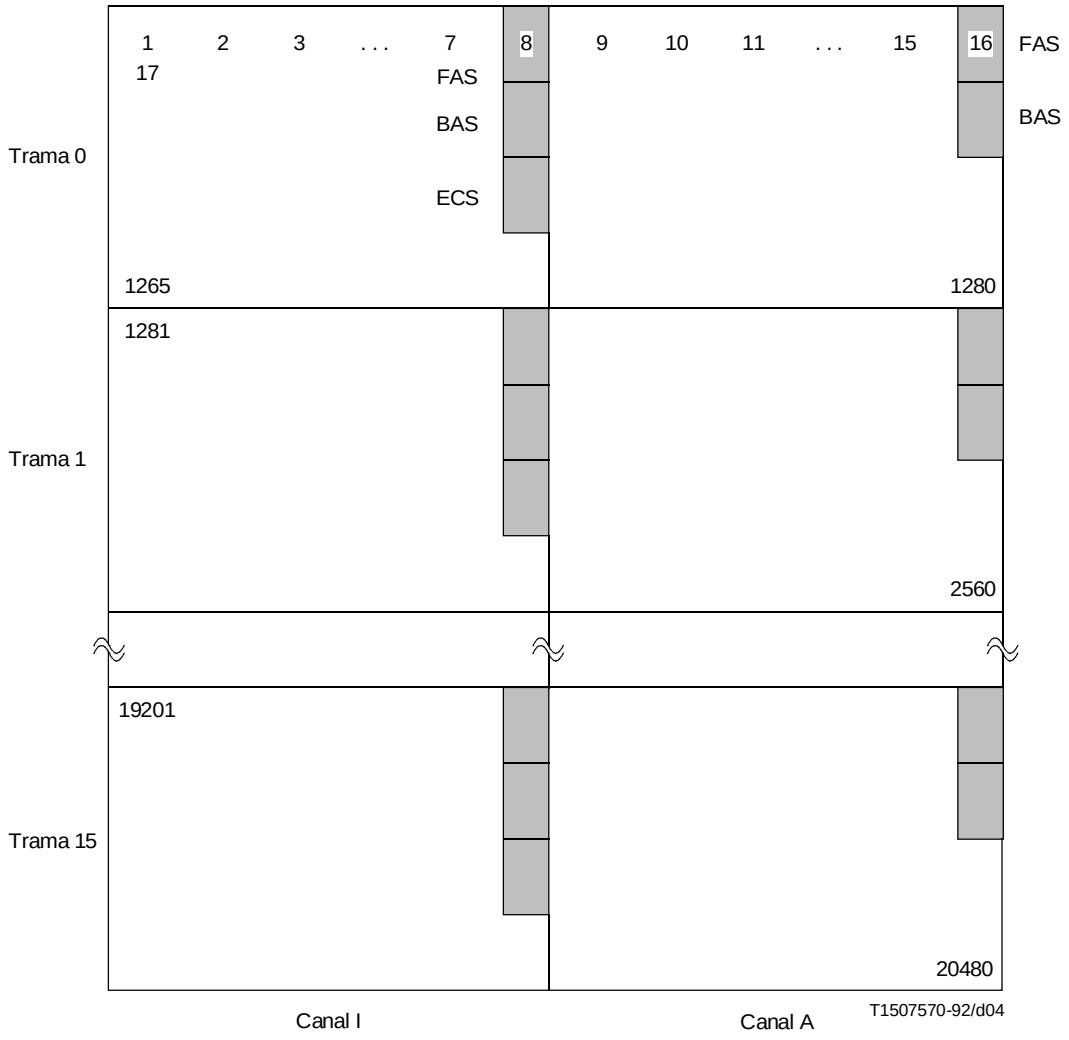
Cifrado y descifrado para dos canales B

(Este apéndice no forma parte integrante de la presente Recomendación)

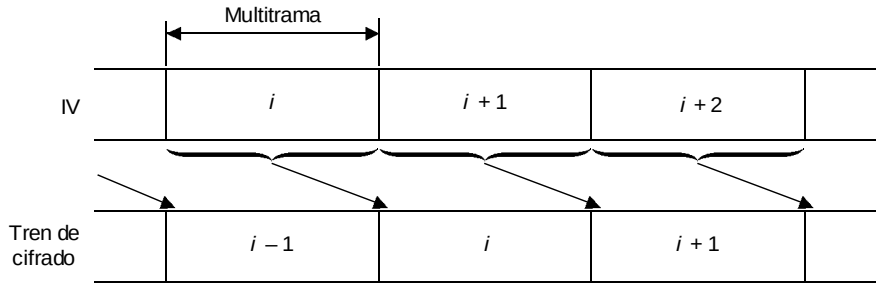
Este apéndice ilustra cómo funciona el cifrado/descifrado H.233.

– Se genera un tren de cifrado para todos los bits.

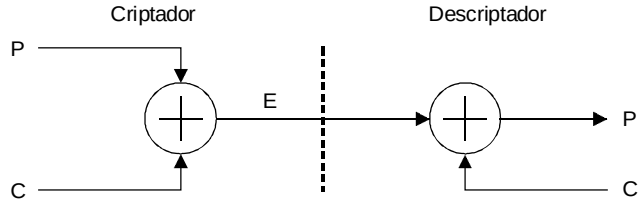
– Se añade un tren de cifrado a todos los bits, salvo a la parte sombreada.



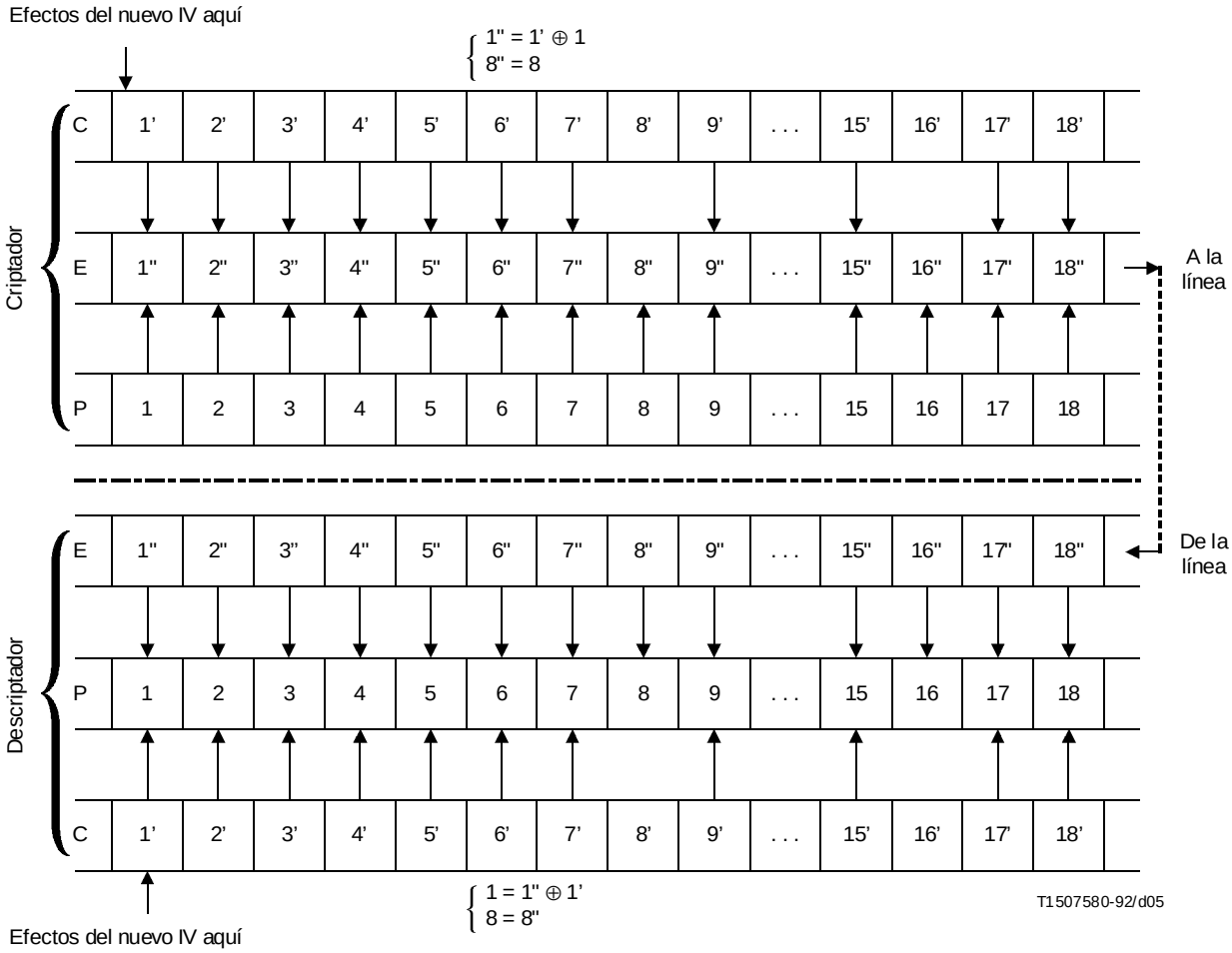
Numeración de bits y bits no cifrados en una multitrama para dos canales B



Generación de tren de cifrado a partir de un nuevo IV



Tren de cifrado aditivo



P Texto claro
C Tren de cifrado
E Texto cifrado

Apéndice II

Procedimiento para comunicaciones audiovisuales con privacidad

(Este apéndice no forma parte integrante de la presente Recomendación)

Cuando en una sesión de comunicación audiovisual se necesita privacidad, ésta se consigue mediante la aplicación de las Recomendaciones H.233 y H.234 y otras Recomendaciones de la serie H. Puesto que los elementos necesarios de los procedimientos de comunicación se definen en varias Recomendaciones, este apéndice proporciona ejemplos para un conjunto de procedimientos con referencia a dichas Recomendaciones.

Existen dos posibilidades para iniciar la privacidad en una comunicación audiovisual:

1) la llamada ha sido establecida y está en curso cuando los participantes deciden activar el cifrado;

2) la decisión de activar el cifrado se comunica antes del establecimiento de la llamada por medios externos, de forma que no se produce la comunicación audiovisual hasta que el mecanismo de confidencialidad es plenamente operativo.

Los Cuadros II.1 y II.2 que se ofrecen a continuación, centrados en los aspectos de privacidad, corresponden a los dos casos, respectivamente. Los procedimientos se enumeran por orden temporal cuando se utiliza el esquema Diffie Hellman ampliado para la distribución de las claves.

Al invocar una comunicación con privacidad, se prestará especial atención al momento en que se cifran las señales audiovisuales. A pesar de que no se ha normalizado ningún método particular, el diseño de terminal deberá comprender las disposiciones adecuadas para tener en cuenta el margen de unos segundos o más que se requiere antes de iniciar la comunicación segura.

Una manera de conseguirlo es permitir la comunicación cifrada hasta que se disponga de las señales cifradas (escenario 1), y otra, silenciar totalmente las señales audiovisuales hasta ese momento (escenario 2). En cualquiera de los dos casos, se indicará explícitamente el estado de cifrado a los usuarios mediante una luz u otro medio.

CUADRO II.1/H.233

Caso de invocación de la privacidad después del establecimiento de la llamada

Orden temporal	Procedimiento	Mensaje	Canal utilizado	Referencias y Notas
1	Establecer la llamada	BC/LLC/HLC	Canal D	Rec. Q.939
2	Trayecto audio libre; enviar AIM si silenciado; indicar al usuario si audio entrante silenciado; caso contrario, indicar audio saliente no cifrado	AIM	BAS	Rec. H.230
3	Intercambio de capacidad ECS (Nota 1)	Encrypt-cap	BAS	Rec. H.242
4	Abrir canal ECS (Nota 1)	Encrypt-on	BAS	Rec. H.242
5	Identificación de los algoritmos de cifrado disponibles	P8	Rec. H.233	
6	Identificación de los sistemas de gestión de claves comunes	P0	ECS(SE)	Rec. H.234
7	Se conoce el método de gestión de claves; elegir el algoritmo de cifrado	–	(Local)	
8	Enviar el algoritmo elegido para intercambio de claves de sesión y comunicaciones audiovisuales	P9		Rec. H.233 (Nota 2)

CUADRO II.1/H.233 *(fin)*

Caso de invocación de la privacidad después del establecimiento de la llamada

Orden temporal	Procedimiento	Mensaje	Canal utilizado	Referencias y Notas
9	Intercambio de valores de prima, raíz primitiva y resultados intermedios	P3, P4	ECS(SE)	Rec. H.234
10	Cálculo de *clave*; r1, r2 y R12	–	(Local)	Rec. H.234
11	Presentación del código de comprobación de 64 bits como 16 cifras hexadecimales	(Local)	(Local)	Rec. H.234
12	Presentación verbal (punto a punto) o comprobar información de código de la MCU (multipunto) del código de comprobación de 64 bits – si audio está silenciado, la comprobación verbal puede posponerse hasta después de activar el cifrado	16 cifras hexadecimales	Principal (punto a punto) o ECS (multipunto)	Rec. H.234
13	Transmisión del vector de inicialización y del número cifrado aleatorio de 4N bits	P6	ECS(SE)	Rec. H.234 (Nota 3)
14	Cifrado activado y vector de inicialización	A y IV en ECS	ECS(IV)	Rec. H.233
15	Indicar salida cifrada; desactivar silenciado, si no es automático; comprobación verbal si se necesita y no se ha efectuado todavía	AIA 16 cifras hexadecimales	(Local) BAS Canal principal	Rec. H.230, Rec. H.234
16	Comunicaciones audiovisuales cifradas	Audio, vídeo, etc.	Canal principal	
17	Silenciar audio, suprimir vídeo	AIM, VIS	BAS	Rec. H.230
18	Cifrado desactivado	A en ECS	ECS(IV)	Rec. H.233
19	Cerrar canal ECS (Nota 4)	Encrypt-off	BAS	Rec. H.242
20	Liberar la llamada	–	Canal D	Rec. Q.939

NOTAS

1 Como parte de los procedimientos de fase de inicialización de modo y establecimiento de modo común definidos en la Recomendación H.242.

2 El algoritmo de cifrado y los modos descritos en el Anexo A se utilizan generalmente para el intercambio de claves de sesión y las comunicaciones audiovisuales.

3 El número aleatorio de 4N bits se cifra mediante el algoritmo de cifrado determinado en el procedimiento 8 con la *clave* determinada en el procedimiento 10 y el vector de inicialización obtenido en este procedimiento.

4 Como parte de los procedimientos de fase de terminación de la comunicación definidos en la Recomendación H.242.

CUADRO II.2/H.233

Caso de decisión de la privacidad antes del establecimiento de la llamada

Orden temporal	Procedimiento	Mensaje	Canal utilizado	Referencias y Notas
0	Decisión de utilizar la privacidad entre las dos partes		Medios externos	(Nota 1)
1	Establecer la llamada	BC/LLC/HLC	Canal D	Rec. Q.939
2	Silenciar audio, suprimir vídeo; indicar al usuario si audio entrante silenciado o vídeo suprimido	AIM, VIS	BAS	Rec. H.230

CUADRO II.2/H.233 *(fin)*

Caso de decisión de la privacidad antes del establecimiento de la llamada

Orden temporal	Procedimiento	Mensaje	Canal utilizado	Referencias y Notas
3	Intercambio de capacidad ECS (Nota 2)	Encrypt-cap	BAS	Rec. H.242
4	Abrir canal ECS (Nota 2)	Encrypt-on	BAS	Rec. H.242
5	Identificación de los algoritmos de cifrado disponibles	P8	ECS(SE)	Rec. H.233
6	Identificación de los sistemas de gestión de claves comunes	P0	ECS(SE)	Rec. H.234
7	Se conoce el método de gestión de claves; elegir el algoritmo de cifrado	–	(Local)	
8	Enviar el algoritmo elegido para intercambio de claves de sesión y comunicaciones audiovisuales	P9		Rec. H.233 (Nota 3)
9	Intercambio de valores de prima, raíz primitiva y resultados intermedios	P3, P4	ECS(SE)	Rec. H.234
10	Cálculo de *clave*, re1, r2 y R12	–	(Local)	Rec. H.234
11	Presentación del código de comprobación de 64 bits como 16 cifras hexadecimales	(Local)	(Local)	Rec. H.234
12	(Si es multipunto) información de código de comprobación de 64 bits de la MCU	16 cifras hexadecimales	ECS	Rec. H.234
13	Transmisión del vector de inicialización y del número cifrado aleatorio de 4N bits	P6	ECS(SE)	Rec. H.234 (Nota 4)
14	Cifrado activado y vector de inicialización	A y IV en ECS	ECS(IV)	Rec. H.233
15	Indicar salida cifrada; desactivar silenciado audio, desactivar supresión vídeo; (si es punto a punto) presentación verbal del código de comprobación de 64 bits	AIA, VIA 16 cifras hexadecimales	(Local) BAS Canal principal	Rec. H.230
16	Comunicaciones audiovisuales cifradas	Audio, vídeo, etc.	Canal principal	
17	Silenciar audio, suprimir vídeo	AIM, VIS	BAS	Rec. H.230
18	Cifrado desactivado	A en ECS	ECS(IV)	Rec. H.233
19	Cerrar canal ECS (Nota 5)	Encrypt-off	BAS	Rec. H.242
20	Liberar la llamada	–	Canal D	Rec. Q.939

NOTAS

1 Fuera del alcance de la normalización.

2 Como parte de los procedimientos de fase de inicialización de modo y establecimiento de modo común definidos en la Recomendación H.242.

3 El algoritmo de cifrado y los modos descritos en el Anexo A se utilizan generalmente para el intercambio de claves de sesión y las comunicaciones audiovisuales.

4 El número aleatorio de 4N bits se cifra mediante el algoritmo de cifrado determinado en el procedimiento 8 con la *clave* determinada por el procedimiento 10 y el vector de inicialización obtenido en este procedimiento.

5 Como parte de los procedimientos de fase de terminación de la comunicación definidos en la Recomendación H.242.