UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

# UIT-T H.233

(11/2002)

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

SERIE H: SISTEMAS AUDIOVISUALES Y MULTIMEDIOS

Infraestructura de los servicios audiovisuales – Aspectos de los sistemas

# Sistemas con confidencialidad para servicios audiovisuales

Recomendación UIT-T H.233

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.399 |
| 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 |

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

# Recomendación UIT-T H.233

## Sistemas con confidencialidad para servicios audiovisuales


**Resumen**

Esta Recomendación describe la parte de confidencialidad de un sistema de privacidad adaptado a los servicios audiovisuales de banda estrecha conformes a las Recomendaciones UIT-T H.320, H.221, H.230 y H.242. Si bien se requiere un algoritmo de criptación para el sistema de privacidad, la especificación de los algoritmos no se incluye aquí: el sistema no se limita a un determinado algoritmo. En el anexo A se definen algunos de estos algoritmos y sus parámetros. Un sistema de privacidad consta de dos partes: el mecanismo de confidencialidad o proceso de criptación de los datos, y un subsistema de gestión de claves que se describe en la Rec. UIT-T H.234.

Esta versión revisada de la Rec. UIT-T H.233 introduce varias correcciones y aclaraciones a la versión original y, lo que es más importante, explica la utilización de la criptación DES triple y AES que se aplica de acuerdo con las Recomendaciones de la serie H.320.



**Orígenes**

La Recomendación UIT-T H.233, revisada por la Comisión de Estudio 16 (2001-2004) del UIT-T, fue aprobada por el procedimiento de la Resolución 1 de la AMNT el 29 de noviembre de 2002.

## 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.

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

# ÍNDICE

# Recomendación H.233

## Sistema con confidencialidad para servicios audiovisuales

### 1 Alcance

Un sistema de privacidad consta de dos partes, el mecanismo de confidencialidad o proceso de criptación 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 conforme a las Recomendaciones UIT-T H.221, H.230, y H.242. Si bien este sistema de privacidad necesita un algoritmo de criptación, la especificación de dicho algoritmo no se incluye aquí: el sistema no se limita a un determinado algoritmo.

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 hay descriptación en el MCU, pero este punto queda en estudio.

### 2 Referencias normativas

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

[1] Recomendación UIT-T H.221 (1999), *Estructura de trama para un canal de 64 a 1920 kbit/s en teleservicios audiovisuales*.

[2] Recomendación UIT-T H.242 (1999), *Sistema para el establecimiento de comunicaciones entre terminales audiovisuales con utilización de canales digitales de hasta 2 Mbit/s*.

[3] Recomendación UIT-T H.230 (1999), *Señales de control e indicación con sincronismo de trama para sistemas audiovisuales*.

[4] Recomendación UIT-T X.680 (2002), *Tecnología de la información – Notación de sintaxis abstracta uno: Especificación de la notación básica*.

[5] Recomendación UIT-T H.234 (2002), *Sistema de autenticación y de gestión de las claves de criptación para los servicios audiovisuales*.

[6] ISO 8732:1988, *Banking – Key management (wholesale)*.

### 3 Abreviaturas

En esta Recomendación se utilizan las siguientes siglas.

AIA Indicación de audio activo (*audio indicate active*) (códigos de control e indicación, *control & indication codes*) (véase [3])

AIM Indicación de audio silenciado (*audio indicate muted*) (códigos de control e indicación, *control & indication codes*) (véase [3])

BAS Señal de asignación de velocidad binaria (*bit-rate allocation signal*) (véase [1])

CRC4 Verificación por redundancia cíclica de cuatro bits (*4-bit cyclic redundancy check*) (véase [1])

ECS Señal de control de criptación (*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 protocolo multicapa (*MLP logical channel*) (véase [1])

MSB Bit más significativo (*most significant bit*)

OFB Realimentación de salida (*output feedback*)

SE Intercambio de sesión (*session exchange*)

SV Variable de partida (*starting variable*)

TOFB Realimentación de salida del algoritmo TDEA (*TDEA output feedback*)

VIS Indicación de vídeo suprimido (*video indicate suppressed*) (códigos de control e indicación, *control and 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 las proporcionan otros mecanismos tales como el descrito en la Rec. UIT-T H.234 sobre autenticación y gestión de claves, o pueden introducirse manualmente.

2) Es aplicable a las señales audiovisuales entramadas según la Rec. UIT-T 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 Rec. UIT-T H.221, los canales de señal de alineación de trama (FAS, *frame alignment signal*), de señal de asignación de velocidad binaria (BAS, *bit-rate allocation signal*) y de señal de control de criptación (ECS, *encryption control signal*) de la estructura de trama no están criptados.

3) Todas las transmisiones de audio, vídeo y datos son confidenciales, puesto que estas señales se criptan juntas bajo la misma clave (esto incluye actualmente datos MLP, de conformidad con el anexo A/H.221, aunque este aspecto queda en estudio).

4) El sistema es independiente del algoritmo de criptación utilizado; acepta algunos algoritmos, y podrían añadirse otros.

5) El mecanismo de confidencialidad puede funcionar en llamadas punto a punto, y también en llamadas multipunto cuando se puede (descriptar) en la MCU ("MCU confiable").

## 4.2 Especificación de algoritmo

La especificación de algoritmos no se incluye en esta Recomendación, que prevé muchos algoritmos de criptación. Las especificaciones pueden estar definidas en el anexo A o en otros documentos (véase 5.2) y deben 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 del funcionamiento

La figura 1 es un diagrama lógico de un criptador de enlace. Consta de un bloque criptador y un bloque descriptador. El criptador cifra los datos de usuario. El descriptador descifra estos datos para obtener los datos de usuario.

Se necesitan dos canales para conectar el criptador y el descriptador. Uno se utiliza para transmitir los datos de usuario cifrados. El segundo es un canal no cifrado, llamado señal de control de criptación (ECS), y se utiliza para transmitir información de control del criptador al descriptador. Aunque estos dos canales se muestran físicamente separados, en la práctica se multiplexan en una única estructura de trama señalada en la Rec. UIT-T H.221.

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 criptador y el descriptador 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 5.1.3).

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

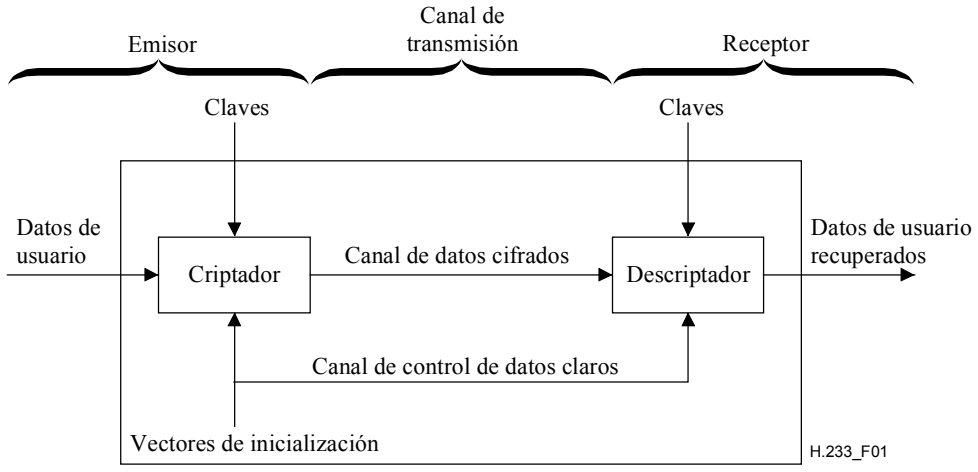



**Figura 1/H.233 – Diagrama lógico de un criptador de enlace**

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

Para indicar la presencia de un sistema de confidencialidad dentro de un terminal, debe transmitirse el código BAS "Capacidad de criptación". Si esta capacidad es señalizada desde ambos extremos de un enlace, puede abrirse el canal de señal de control de criptación (ECS) 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 antes de recibir 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 H.221 en un sentido solamente, el canal ECS puede ser activado sin utilizar el mecanismo de capacidad: por tanto, el mecanismo para asegurar que el extremo receptor puede descriptar el algoritmo elegido, etc., está fuera del alcance de esta Recomendación.

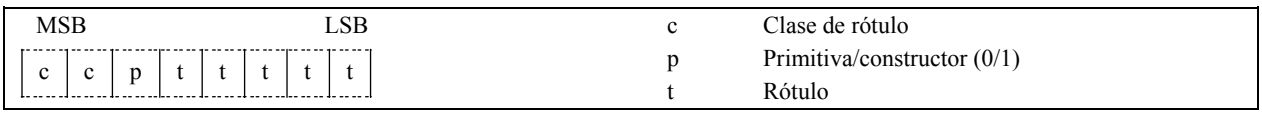
### 5.1.2 Formatos de mensaje

Los mensajes utilizados por el sistema de criptación para la distribución y autenticación de claves tienen un formato anidado de identificador, longitud, contenido (ILC, *identifier, length, content*) que se describe en la Rec. UIT-T X.680 [4]. La longitud puede codificarse en forma corta o forma larga. No se utilizará la forma indefinida indicada en [4].

A continuación se describen someramente algunas de las definiciones de la Rec. UIT-T X.680 [4] utilizadas en esta propuesta.

#### 5.1.2.1 Identificador

Un identificador es un octeto que tiene la siguiente estructura:




La clase de rótulo define el tipo de identificador y toma el valor de 10 u 11 (según el contexto).

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

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 un componente más o menos largo.

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 128 o superior, 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 criptador y el descriptador. Sólo se necesita un canal de control por sistema de criptación de enlace. El mismo canal de control se utiliza en asociación con la criptación de 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 es efectiva desde el comienzo de la siguiente multitrama, y sigue siendo efectiva hasta que se envía otro IV. El canal ECS debe contener siempre sea un bloque IV o un bloque SE. Obsérvese 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 mayor seguridad.

| | 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) Cabecera (12 bits), compuesta 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 #1 de una secuencia de varios bloques
     10 para un bloque intermedio de una secuencia
     11 para el último bloque de una secuencia
   - Bits 3-7 del bloque tipo SE: de reserva (s) puestos a "0".
   - Bit 3 del bloque tipo IV para indicar criptación activada (on)/desactivada (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)
   - Bit 7 del bloque tipo IV: de reserva (s) puesto a "0"
   - Bits 8-11: corrección de error (e) para los bits 0-7
2) Bloques SE: 108 bits estructurados como 9 × (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 a la cabecera de 8 + 4 bits están estructurados como 9 × (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 la cabecera) 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.

##### 5.1.3.1.1 Capacidades de algoritmo (P8)

| | |
|---|---|
| Nombre de mensaje: | Información disponible sobre los algoritmos de descriptación (P8). |
| Identificador de mensaje: | 1 1 P $t_1$ $t_2$ $t_3$ $t_4$ $t_5$ = 1100 0000 |
| Significado: | Identifica la lista de algoritmos que el terminal puede descriptar. |
| 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 descriptación disponible, mediante los siguientes valores de identificadores de medios, identificadores de algoritmos e identificadores de parámetros. |

Por ejemplo, un terminal capaz de decodificar DES y FEAL transmitiría el mensaje P8 {[11000000][00000110][00000000] [00000010][00000000][00000000][00000001][00000000]}.

##### 5.1.3.1.2 Instrucción de algoritmo (P9)

| | |
|---|---|
| Nombre de mensaje: | Información del algoritmo en uso (P9). |
| Identificador de mensaje: | 1 1 P $t_1$ $t_2$ $t_3$ $t_4$ $t_5$ = 1100 0001 |
| Significado: | Cuando el bit "criptación activada" se pone a 1 en la cabecera IV, el algoritmo utilizado es el especificado aquí en este mensaje. |
| Contenido: | Bytes del esquema de criptación (mismos valores que en el mensaje de capacidad P8). |

##### 5.1.3.1.3 Identificadores de medios

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

1er bit (LSB): audio 0 = criptado, 1 = no criptado

2º bit: vídeo 0 = criptado, 1 = no criptado

3er bit: LSD 0 = criptado, 1 = no criptado

4º bit: HSD 0 = criptado, 1 = no criptado

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 quedan en estudio.

#### 5.1.3.1.4 Identificadores de algoritmo

Se utiliza un byte para identificación de algoritmo. La definición del algoritmo especifica completamente 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 – ISO/CEI 9979 algoritmo registro N.° 0010 |
| 0 0 0 0 0 0 1 0 | DES Modo 1 – ISO/CEI 9979 algoritmo registro N.° 0004 |
| 0 0 0 0 0 0 1 1 | TDEA – NIST FIPS PUB 46-3 |
| 0 0 0 0 0 1 0 0 | Reservado |
| 0 0 0 0 0 1 0 1 | B-CRYPT – ISO/CEI 9979 algoritmo registro N.° 0001 |
| 0 0 0 0 0 1 1 0 | IDEA – ISO/CEI 9979 algoritmo registro N.° 0002 |
| 0 0 0 0 0 1 1 1 | Reservado para BARAS (ETSI) |
| 0 0 0 0 1 0 0 0 | AES – UIST FIPS PUB 197 |
| Otros valores | No asignados. Reservados para uso futuro. |

#### 5.1.3.1.5 Identificadores de parámetro

Se utiliza un byte para identificar los parámetros de los algoritmos de criptación 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 criptación.

El equipo debe descriptar 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 la criptación de la información transmitida.

#### 5.1.3.1.6 Otros mensajes

| | |
|---|---|
| Nombre de mensaje: | No se puede criptar (P1). |
| Identificador de mensaje: | 1 0 P $t_1$ $t_2$ $t_3$ $t_4$ $t_5$ = 1000 0001 |
| Significado: | El remitente de este mensaje no utilizará un sistema de criptación. |
| Contenido: | Este mensaje no tiene contenido. |

| | |
|---|---|
| Nombre de mensaje: | No se ha puesto en marcha el sistema de criptación (P2). |
| Identificador de mensaje: | 1 0 P $t_1$ $t_2$ $t_3$ $t_4$ $t_5$ = 1000 0010 |
| Significado: | El remitente de este mensaje no ha podido poner en marcha su sistema de criptación. Podría deberse a un fallo en el intercambio de claves, pero no se da ninguna indicación de la causa del fallo en el mensaje, por razones de seguridad. |
| 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 implementador.

| | |
|---|---|
| Nombre de mensaje: | Mensaje de canal desocupado (SE_NULL). |
| Identificador de mensaje: | 1 1 P $t_1$ $t_2$ $t_3$ $t_4$ $t_5$ = 1101 1111 |
| Significado: | El remitente de este mensaje rellena el canal ya que no tiene otro mensaje para enviar. |
| Contenido: | Este mensaje no tiene contenido. |

Se transmitirá SE_NULL cuando el remitente no tenga capacidades, instrucciones o mensajes IV que transmitir. Podría suceder durante un intercambio de información suplementaria que no se puede transmitir simultáneamente. Por ejemplo, intercambios de conjuntos de capacidades de distintos tamaños, o un intercambio de claves con el algoritmo Diffie-Hellman.

#### 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 por el canal de control debe protegerse contra 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 cabeceras, mensajes de intercambio de sesión y 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<br>010000000111<br>001000001010<br>000100000101<br>000010001011<br>000001001100<br>000000100110<br>000000010011 | 1110<br>0111<br>1010<br>0101<br>1011<br>1100<br>0110<br>0011<br>1000<br>0100<br>0010<br>0001 |

H.233_F03

**Figura 3/H.233 – Matrices de corrección de errores**

### 5.2 Método de criptación de la transmisión

Esta cláusula trata de la criptación de audio, vídeo y cualesquiera datos asociados. La criptación sólo tendrá lugar si se establece la alineación de multitrama H.221.

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

El orden temporal de criptación sigue el de la transmisión en un tren serie bit a bit. Los datos deben criptarse antes de que tenga lugar un cálculo CRC4. Los cálculos CRC4 se efectúan entonces en los datos criptados para que el código CRC4 que se presenta a las redes sea 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 criptador con los bits que han de criptarse por adición en módulo 2, y en el descriptador los bytes criptados 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 criptador y se envían al des criptador a través del ECS. Se utilizan síncronamente con los datos que se van a criptar o descriptar. Proporcionan un método para resincronizar el criptador y el descriptador periódicamente.

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

Si se pierde la sincronización, los datos estarán alterados 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.

El sistema de criptación trata todos los bits del canal 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 Rec. UIT-T H.221) y ECS; el tren de cifrado no es almacenado ni mantenido para uso posterior; se pierde y no se utiliza para criptar 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 un 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 un 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 va a empezar a criptar, habiendo recibido la capacidad "encrypt" (véase la Rec. UIT-T H.221) en el juego de capacidades del terminal distante, abre el canal ECS y transmite el mensaje (o mensajes) P8. Mientras espera la recepción de un mensaje P8, el terminal rellena el canal ECS con un mensaje SE_NULL. Al recibir el mensaje (o mensajes) P8 desde el extremo distante, comprueba si hay 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, decide las claves comunes que utilizará el algoritmo de criptación, e inicia entonces la transmisión de bloques IV. El procedimiento de gestión de claves se ejecuta de conformidad con la Rec. UIT-T H.234. En el apéndice II se presentan ejemplos de procedimientos para una sesión de criptación.

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

## 6 Criptación del canal MLP

Queda en estudio.

# Anexo A

# Algoritmos de criptación y sus parámetros

## A.1 Alcance

Este anexo define los algoritmos de criptación para los que se asignaron identificadores de algoritmo en 5.1.3.1.4. La definición de los algoritmos y sus parámetros especifica cómo se obtiene el tren de cifrado a partir de la clave actual y del valor IV.

## A.2 Referencias normativas

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

[A2] ISO/CEI 9979 Registration No. 0004 (Data Encryption Standard).

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

[A4] NIST Federal Information Processing Standard (FIPS) Publication 46-3 (Triple Data Encryption Algorithm)

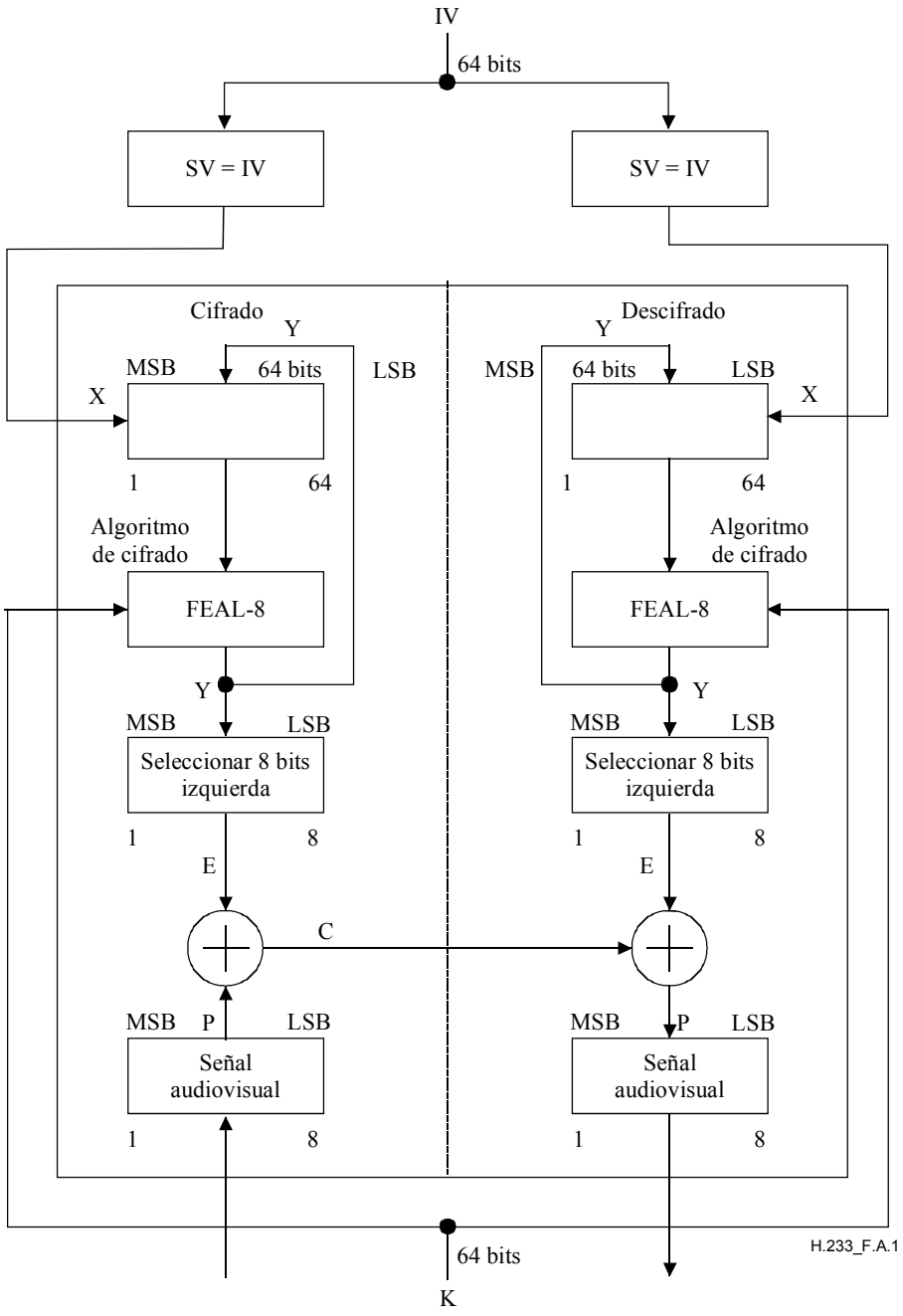
[A5] NIST Federal Information Processing Standard (FIPS) Publication 197 (Advanced Encryption Standard).

## A.3 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 ocho rondas con clave de 64 bits) en modo realimentación de salida (OFB, *output feedback*) definido en ISO 8372. En la referencia [A1] se dan detalles del algoritmo FEAL. Este tren se combina en el criptador con los bits que se van a criptar por adición en módulo 2, y en el descriptador los bits criptados 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). Este vector IV se carga al comienzo de cada multitrama.

De los 64 bits de salida del algoritmo de cifrado, los ocho primeros bits del lado MSB se utilizan para adición en módulo 2 bit a bit a los ocho 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 ocho bits, se genera el siguiente ciclo del tren de cifrado y se utiliza para criptación.




C Tren de cifrado
E Criptación
IV Vector de inicialización
K Clave
P Texto claro
SV Vector de partida

**Figura A.1/H.233 – Operación en modo realimentación de salida para FEAL**

## A.4 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 quedan en estudio.

## A.5 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].

Para producir el tren de cifrado se utiliza el método de realimentación de salida OFB-8, conforme a ISO 8372. La variable de partida es idéntica al vector de inicialización (IV).

El método utilizado para aplicar el tren de cifrado al tren de datos es fundamentalmente el método para 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 identificador de parámetro (véase 5.1.3.1.5) se pone a [0000 0000] en este modo. Otros modos de funcionamiento, como encadenamiento de bloque de cifrado o realimentación de cifrado descritos en ISO 8372 quedan en estudio.

## A.6 TDEA

El algoritmo TDEA (o DES triple) y los métodos de aplicación del tren de cifrado al tren de datos se describen en la referencia [A4].

Tanto la entrada como la salida del TDEA consisten en secuencias de 64 bits. En algunas ocasiones se hablará de bloques para referirse a estas secuencias, y de longitud para referirse al número de bits que contienen. La clave de cifrado del algoritmo TDEA consiste en 112 ó 168 bits que forman un agrupamiento de dos o tres claves DES de 56 bits distintas.

El tren de cifrado se produce por el método de realimentación de salida TOFB-64. La variable de partida (SV) es idéntica al vector de inicialización (IV). El identificador de parámetro se fija como sigue:

| Valor de campo MSB | Tamaño de la clave en bits |
|---|---|
| 00 | 112 |
| 01 | 168 |

| Valor de campo LSB | Modo de funcionamiento | Número de bits |
|---|---|---|
| 000000 | Reservado | |
| 000001 | TOFB-64 | 64 |

Los seis bits LSB representan los métodos de aplicación del tren de cifrado.

Los dos bits MSB representan el tamaño de la clave de cifrado que se utiliza para iniciar el algoritmo TDEA.

Otros valores del identificador de parámetro quedan en estudio.

Ejemplo: TDEA-168 con TOFB de 64 bits será 0100 0001.

## A.7 AES

Los métodos de aplicación del tren de cifrado al tren de datos con AES se definen en la referencia [A5].

Tanto la entrada como la salida del algoritmo AES consisten en secuencias de 128 bits. Algunas veces se hablará de bloques para referirse a estas secuencias, y de longitud para referirse al número de bits que contienen. La clave de cifrado para el algoritmo AES es una secuencia de 128, 192 ó 256 bits que se puede designar con los siguientes términos "AES-128", "AES-192" y "AES-256" respectivamente.

La variable de partida (SV) es idéntica a la longitud del vector de inicialización (IV), que tendrá una longitud de 128 bits. El identificador de parámetro se fija como sigue:

| Valor de campo MSB | Tamaño de la clave en bits |
|---|---|
| 00 | 128 |
| 01 | 192 |
| 10 | 256 |

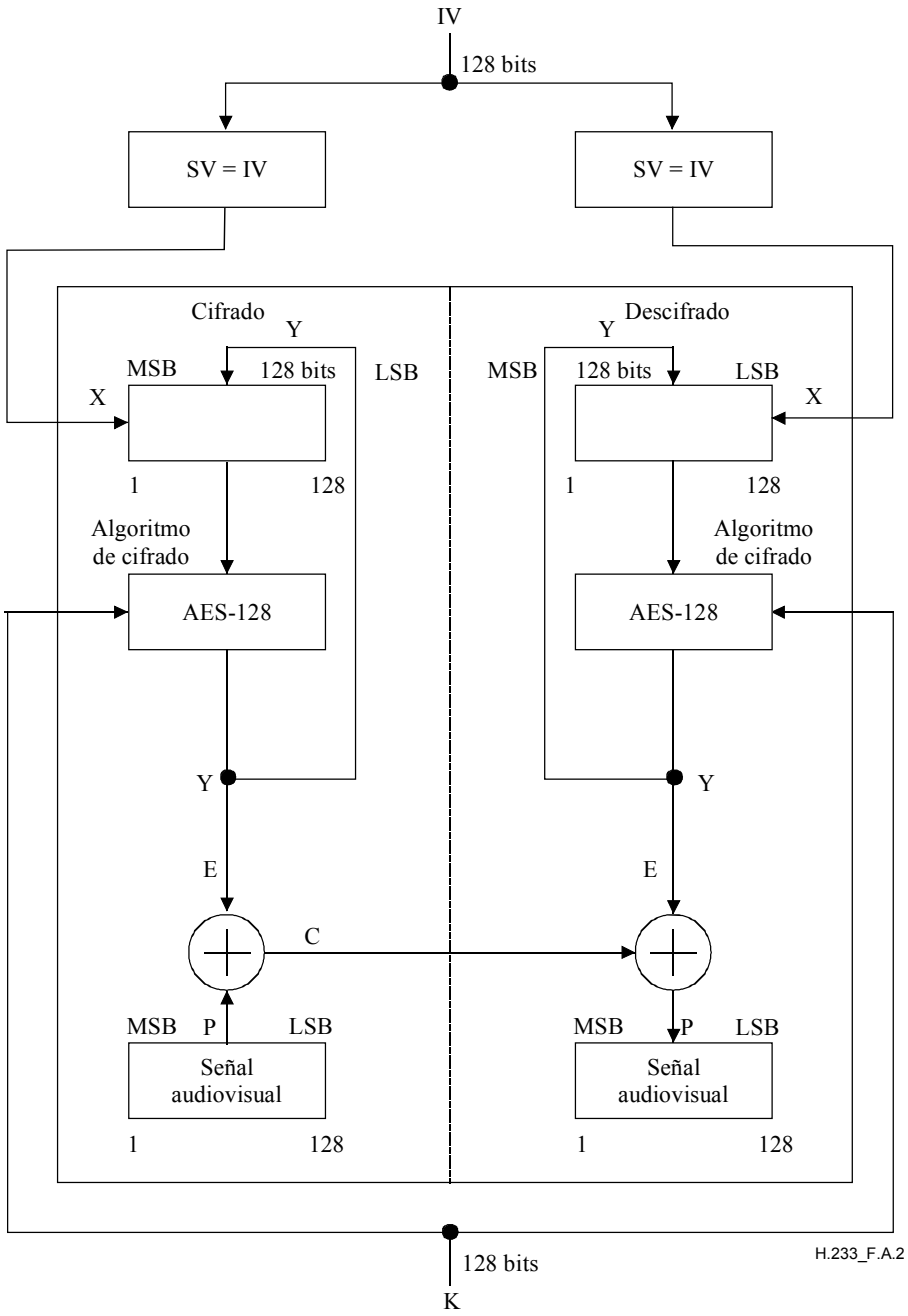
| Valor de campo LSB | Modo de funcionamiento | Número de bits |
|---|---|---|
| 000000 | Reservado | |
| 000001 | OFB-128 | 128 |

Los seis bits LSB representan los métodos de aplicación del tren de cifrado.

Los dos bits MSB representan el tamaño de la clave de cifrado que se utiliza para iniciar AES.

Otros valores del identificador de parámetro quedan en estudio.

Ejemplo: AES-128 con OFB de 128 bits será 0000 0001.




C Tren de cifrado
E Criptación
IV Vector de inicialización
K Clave
P Texto claro
SV Vector de partida

**Figura A.2/H.233 – Funcionamiento con realimentación de salida (OFB) para AES-128**

# Apéndice I

## Criptación y descriptación para 2 × canales B

Este apéndice ilustra el funcionamiento de la criptación/descriptación 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.

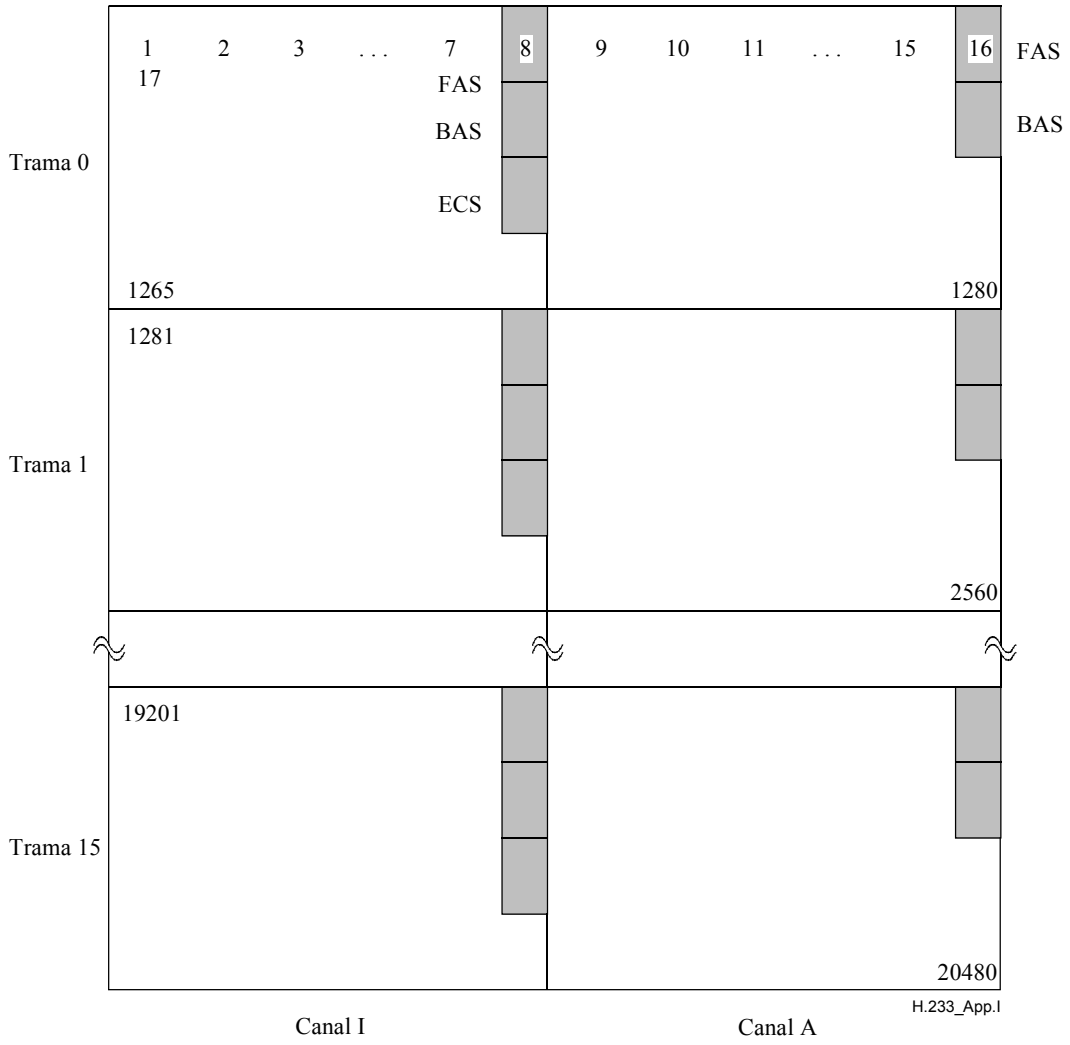
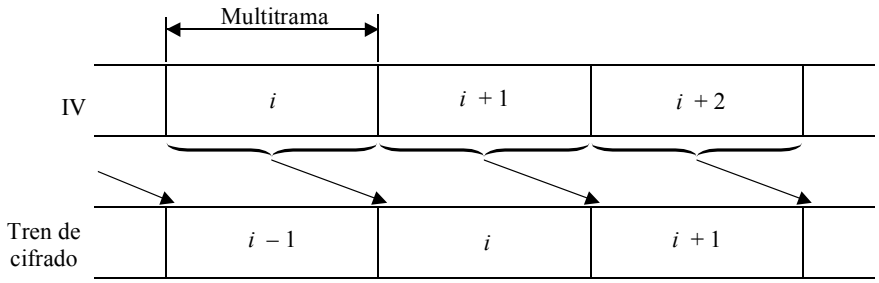
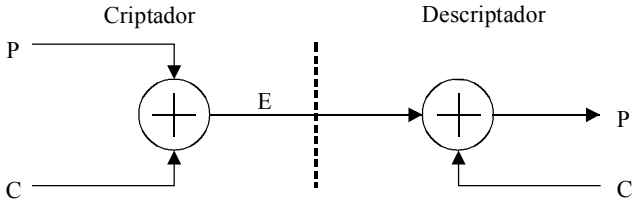


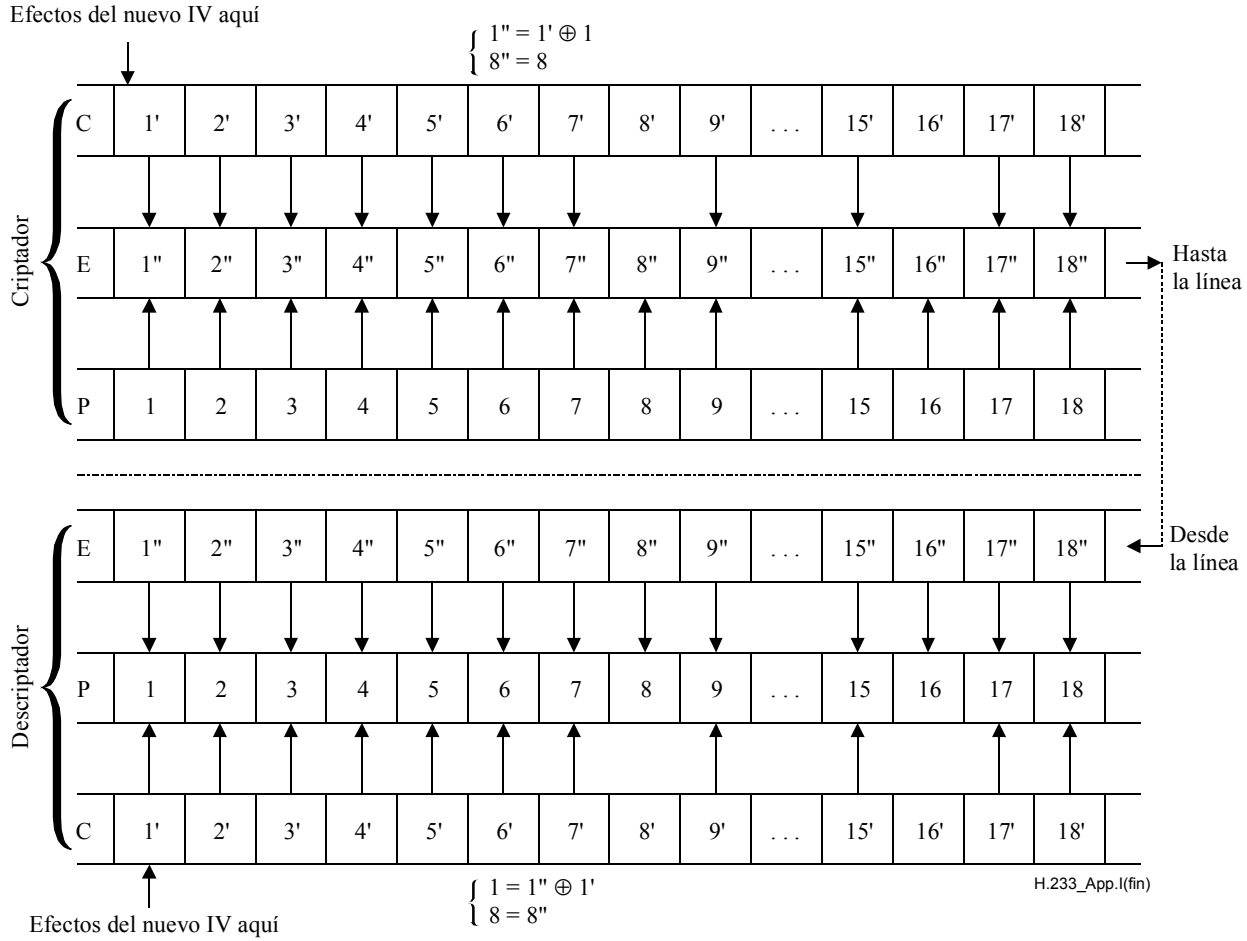

**Figura I.1/H.233 – Numeración de bits no cifrados en una multitrama para dos canales B**




Generación de tren de cifrado a partir de un nuevo IV




Tren de cifrado aditivo




C Tren de cifrado
E Texto criptado
P Texto claro

**Figura I.2/H.233 – Procesos de criptación y descriptación**

# Apéndice II

## Procedimiento para comunicaciones audiovisuales con privacidad

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 el procedimiento de privacidad en una comunicación audiovisual:

1) la comunicación ha sido establecida y está en curso cuando los participantes deciden activar la criptación;
2) la decisión de activar la criptación se comunica antes del establecimiento de la comunicación por medios externos: la comunicación audiovisual sólo se produce después de activar el mecanismo de confidencialidad.

Los cuadros II.1 y II.2 destacan los aspectos de privacidad y 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 criptan las señales audiovisuales. No se ha normalizado ningún método particular, pero es necesario que el terminal admita un margen de unos segundos o más que se requiere antes de iniciar la comunicación segura.

Una manera de conseguirlo es permitir la comunicación no criptada hasta que se disponga de señales criptadas (escenario 1), y otra, silenciar totalmente las señales audiovisuales hasta ese momento (escenario 2). En los dos casos se indicará explícitamente el estado de criptación a los usuarios mediante una luz o de otra forma.

**Cuadro II.1/H.233 – Caso de invocación de privacidad después del establecimiento de la comunicación**

| Orden temporal | Procedimiento | Mensaje | Canal utilizado | Referencias y notas |
|---|---|---|---|---|
| 1 | Establecer la comunicación | BC/LLC/HLC | Canal D | Rec. UIT-T Q.939 |
| 2 | Trayecto audio libre; enviar AIM si silenciado; indicar al usuario si audio entrante silenciado; caso contrario, indicar audio saliente no criptado | AIM | BAS | Rec. UIT-T H.230 |
| 3 | Decisión de comunicar con privacidad entre las dos partes | | Medios externos | (Nota 5) |
| 4 | Intercambio de capacidad ECS (nota 1) | Encrypt-(cap) | BAS | Rec. UIT-T H.242 |
| 5 | Abrir canal ECS (nota 1) | Encrypt-on | BAS | Rec. UIT-T H.242 |
| 6 | Identificación de los algoritmos de criptación disponibles | P8 | Rec. UIT-T H.233 | |
| 7 | Identificación de los sistemas de gestión de claves comunes | P0 | ECS(SE) | Rec. UIT-T H.234 |
| 8 | Se conoce el método de gestión de claves; elegir el algoritmo de criptación | – | (Local) | |

**Cuadro II.1/H.233 – Caso de invocación de privacidad después del establecimiento de la comunicación**

| Orden temporal | Procedimiento | Mensaje | Canal utilizado | Referencias y notas |
|---|---|---|---|---|
| 9 | Enviar el algoritmo elegido para intercambio de claves de sesión y comunicaciones audiovisuales | P9 | | Rec. UIT-T H.233 (Nota 2) |
| 10 | Intercambio de valores preparatorios, raíz primitiva y resultados intermedios | P3, P4 | ECS(SE) | Rec. UIT-T H.234 |
| 11 | Cálculo de *clave*; r1, r2 y R12 | – | (Local) | Rec. UIT-T H.234 |
| 12 | Presentación del código de comprobación de 64 bits como 16 cifras hexadecimales | (Local) | (Local) | Rec. UIT-T H.234 |
| 13 | Presentación verbal (punto a punto) o información de código de comprobación de la MCU (multipunto) o el código de comprobación de 64 bits – si audio está silenciado, la comprobación verbal puede posponerse hasta después de activar la criptación | 16 cifras hexadecimales | Principal (punto a punto) o ECS (multipunto) | Rec. UIT-T H.234 |
| 14 | Transmisión del vector de inicialización y del número criptado aleatorio de 4N bits | P6 | ECS(SE) | Rec. UIT-T H.234 (Nota 3) |
| 15 | Criptación activada y vector de inicialización | A y IV en ECS | ECS(IV) | Rec. UIT-T H.233 |
| 16 | Indicar salida criptada; 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. UIT-T H.230, Rec. UIT-T H.234 |
| 17 | Comunicaciones audiovisuales criptadas | Audio, vídeo, etc. | Canal principal | |
| 18 | Silenciar audio, suprimir vídeo | AIM, VIS | BAS | Rec. UIT-T H.230 |
| 19 | Criptación desactivada | A en ECS | ECS(IV) | Rec. UIT-T H.233 |
| 20 | Cerrar canal ECS (nota 4) | Encrypt-off | BAS | Rec. UIT-T H.242 |
| 21 | Liberar la llamada | – | Canal D | Rec. UIT-T Q.939 |

NOTA 1 – Forma parte de los procedimientos de fase de inicialización de modo y establecimiento de modo común definidos en la Rec. UIT-T H.242.

NOTA 2 – El algoritmo y el modo de criptación descritos en el anexo A se utilizan generalmente para el intercambio de claves de sesión y las comunicaciones audiovisuales.

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

NOTA 4 – Forma parte de los procedimientos de fase de terminación de la comunicación definidos en la Rec. UIT-T H.242.

NOTA 5 – Fuera del alcance de la normalización.

**Cuadro II.2/H.233 – Caso de decisión de privacidad antes del establecimiento de la comunicación**

| Orden temporal | Procedimiento | Mensaje | Canal utilizado | Referencias y notas |
|---|---|---|---|---|
| 0 | Decisión de comunicar con privacidad entre las dos partes | | Medios externos | (Nota 1) |
| 1 | Establecer la comunicación | BC/LLC/HLC | Canal D | Rec. UIT-T Q.939 |
| 2 | Silenciar audio, suprimir vídeo; indicar al usuario si audio entrante silenciado o vídeo suprimido | AIM, VIS | BAS | Rec. UIT-T H.230 |
| 3 | Intercambio de capacidad ECS (nota 2) | Encrypt-(cap) | BAS | Rec. UIT-T H.242 |
| 4 | Abrir canal ECS (Nota 2) | Encrypt-on | BAS | Rec. UIT-T H.242 |
| 5 | Identificación de los algoritmos de criptación disponibles | P8 | ECS(SE) | Rec. UIT-T H.233 |
| 6 | Identificación de los sistemas de gestión de claves comunes | P0 | ECS(SE) | Rec. UIT-T H.234 |
| 7 | Se conoce el método de gestión de claves; elegir el algoritmo de criptación | – | (Local) | |
| 8 | Enviar el algoritmo elegido para intercambio de claves de sesión y comunicaciones audiovisuales | P9 | | Rec. UIT-T H.233 (Nota 3) |
| 9 | Intercambio de valores preparatorios, raíz primitiva y resultados intermedios | P3, P4 | ECS(SE) | Rec. UIT-T H.234 |
| 10 | Cálculo de *clave*, re1, r2 y R12 | – | (Local) | Rec. UIT-T H.234 |
| 11 | Presentación del código de comprobación de 64 bits como 16 cifras hexadecimales | (Local) | (Local) | Rec. UIT-T H.234 |
| 12 | (Si es multipunto) información de código de comprobación de 64 bits de la MCU | 16 cifras hexadecimales | ECS | Rec. UIT-T H.234 |
| 13 | Transmisión del vector de inicialización y del número criptado aleatorio de 4N bits | P6 | ECS(SE) | Rec. UIT-T H.234 (Nota 4) |
| 14 | Criptación activada y vector de inicialización | A y IV en ECS | ECS(IV) | Rec. UIT-T H.233 |
| 15 | Indicar salida criptada; 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. UIT-T H.230 |
| 16 | Comunicaciones audiovisuales criptadas | Audio, vídeo, etc. | Canal principal | |
| 17 | Silenciar audio, suprimir vídeo | AIM, VIS | BAS | Rec. UIT-T H.230 |
| 18 | Criptación desactivada | A en ECS | ECS(IV) | Rec. UIT-T H.233 |

**Cuadro II.2/H.233 – Caso de decisión de privacidad antes del establecimiento de la comunicación**

| Orden temporal | Procedimiento | Mensaje | Canal utilizado | Referencias y notas |
|---|---|---|---|---|
| 19 | Cerrar canal ECS (nota 5) | Encrypt-off | BAS | Rec. UIT-T H.242 |
| 20 | Liberar la llamada | – | Canal D | Rec. UIT-T Q.939 |

NOTA 1 – Fuera del alcance de la normalización.

NOTA 2 – Forma parte de los procedimientos de fase de inicialización de modo y establecimiento de modo común definidos en la Rec. UIT-T H.242.

NOTA 3 – El algoritmo y el modo de criptación descritos en el anexo A se utilizan generalmente para el intercambio de claves de sesión y las comunicaciones audiovisuales.

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

NOTA 5 – Forma parte de los procedimientos de fase de terminación de la comunicación definidos en la Rec. UIT-T H.242.

## SERIES DE RECOMENDACIONES DEL UIT-T

| | |
|---|---|
| Serie A | Organización del trabajo del UIT-T |
| Serie B | Medios de expresión: definiciones, símbolos, clasificación |
| Serie C | Estadísticas generales de telecomunicaciones |
| Serie D | Principios generales de tarificación |
| Serie E | Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos |
| Serie F | Servicios de telecomunicación no telefónicos |
| Serie G | Sistemas y medios de transmisión, sistemas y redes digitales |
| **Serie H** | **Sistemas audiovisuales y multimedios** |
| Serie I | Red digital de servicios integrados |
| Serie J | 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 | RGT y mantenimiento de redes: sistemas de transmisión, circuitos telefónicos, telegrafía, facsímil y circuitos arrendados internacionales |
| Serie N | Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión |
| Serie O | Especificaciones de los aparatos de medida |
| Serie P | Calidad de transmisión telefónica, instalaciones telefónicas y redes locales |
| Serie Q | Conmutación y señalización |
| Serie R | Transmisión telegráfica |
| Serie S | Equipos terminales para servicios de telegrafía |
| Serie T | Terminales para servicios de telemática |
| Serie U | Conmutación telegráfica |
| Serie V | Comunicación de datos por la red telefónica |
| Serie X | Redes de datos y comunicación entre sistemas abiertos |
| Serie Y | Infraestructura mundial de la información y aspectos del protocolo Internet |
| Serie Z | Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación |

Impreso en Suiza
Ginebra, 2003