UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T J.91

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

(08/94)

TRANSMISIONES RADIOFÓNICAS Y DE TELEVISIÓN

MÉTODOS TÉCNICOS PARA ASEGURAR LA PRIVACIDAD DE LAS TRANSMISIONES INTERNACIONALES DE TELEVISIÓN A LARGA DISTANCIA

Recomendación UIT-T J.91

(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 J.91 ha sido preparada por la Comisión de Estudio 9 (1993-1996) del UIT-T y fue aprobada por el procedimiento de la Resolución N.° 1 de la CMNT el 22 de agosto de 1994.

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

RESUMEN

Esta Recomendación constituye una norma común para un sistema de acceso condicional a transmisiones internacionales de televisión digital de larga distancia de acuerdo con la Recomendación J.81[1)]. Traza primeramente un panorama de los sistemas de acceso condicional, en el que se describen las categorías de los mensajes de acceso condicional que han de transmitirse. Se especifica, por otra parte, un protocolo de transporte basado en tramas HDLC para los mensajes de acceso condicional enviados por el canal CA1 de la Recomendación J.81.

Asimismo, se describe una arquitectura de todo el sistema de transmisión, lo que incluye las características de acceso condicional. Esta arquitectura difiere de la arquitectura de los sistemas tradicionales de televisión de pago, ya que hace resaltar la necesidad de establecer una autoridad de control de acceso que no esté situada en el lugar donde se encuentran los transmisores.

Se modelan los principales equipos e interfaces de acceso condicional que se requieren para explotar el sistema de acceso condicional, se describen las funcionalidades de estos equipos e interfaces y se proponen ciertas realizaciones en función de la aplicación. Por último, se presentan realizaciones prácticas con arreglo al nivel de seguridad y funcionalidad requerido por las distintas aplicaciones.

1) La Recomendación J.81 era anteriormente la Recomendación UIT-R CMTT.723.

Recomendación J.91

MÉTODOS TÉCNICOS PARA ASEGURAR LA PRIVACIDAD DE LAS TRANSMISIONES INTERNACIONALES DE TELEVISIÓN A LARGA DISTANCIA

(Ginebra, 1994)

El UIT-T,

considerando

(a) que debido a su propia naturaleza las señales radioeléctricas se reciben por un gran número de receptores sin identificar y en el caso de las transmisiones internacionales de televisión por satélites de telecomunicaciones, pueden recibir e interpretar las señales las estaciones a las que no está destinada la información;

(b) que el número de estaciones capaces de recibir tales señales aumenta constantemente;

(c) que el acceso no deseado a la señal transmitida se facilita cuando en la radiodifusión se emplean características técnicas similares a las utilizadas en transmisión;

(d) que la Recomendación J.81 que define el códec de reducción de la velocidad binaria a utilizar en aplicaciones con calidad de contribución para el tercer nivel jerárquico de la Recomendación G.702, tiene en cuenta la necesidad de establecer un sistema de acceso condicional,

recomienda

que los métodos técnicos utilizados para asegurar la privacidad de las transmisiones internacionales de televisión digitales a larga distancia de acuerdo con la Recomendación J.81, que utilizan técnicas de radiocomunicación, tengan las siguientes características.

1 Consideraciones generales

La presente Recomendación UIT-T constituye una norma común de un sistema de acceso condicional a las transmisiones internacionales de televisión digital a larga distancia de acuerdo con la Recomendación J.81.

Se definen las interfaces y equipos necesarios para el funcionamiento del sistema de acceso condicional y se especifica un protocolo de transporte de los mensajes de acceso condicional en el canal CA1 de la Recomendación J.81.

En los anexos aparecen realizaciones prácticas.

2 Referencias

- Recomendación J.81, *Transmisión de señales de televisión digitales con codificación de componentes para las aplicaciones con calidad de contribución a las velocidades binarias del tercer nivel jerárquico de la Recomendación G.702*.
- EN 50094: 1992, *Sistema de control de acceso para la familia MAC/Paquetes, EUROCRYPT*.
- ISO 7816-1:1987, *Tarjetas de identificación – Tarjetas de circuitos integrados con contactos – Parte 1: Características físicas*.
- ISO 7816-2:1988, *Tarjetas de identificación – Tarjetas de circuitos integrados con contactos – Parte 2: Dimensiones y situación de los contactos*.
- ISO/CEI 7816-3:1989, *Tarjetas de identificación – Tarjetas de circuitos integrados con contactos – Parte 3: Señales electrónicas y protocolos de transmisión*.

3 Términos y definiciones

En la presente Recomendación se utilizan las siguientes definiciones:

aleatorización se define como la alteración de las características de una señal de imagen/sonido/datos para impedir la recepción no autorizada en forma clara. Esta alteración es un proceso específico bajo el control del sistema de acceso condicional (extremo emisor).

desaleatorización se define como la restauración de las características de una señal de imagen/sonido/datos para permitir la recepción en forma clara. Esta restauración es un proceso específico bajo el control del sistema de acceso condicional (extremo receptor).

4 Abreviaturas

En la presente Recomendación se utilizan las siguientes abreviaturas:

ACS	Sistema de control de acceso (*access control system*)
Bit	Dígito binario [contracción de las palabras (*binary digit*)]
CA	Dirección de abonado (*customer address*)
CA1	Canal de acceso condicional 1 (parte del múltiplex de servicio del códec) (*conditional access channel 1*)
CA2	Canal de acceso condicional 2 (parte del múltiplex de servicio del códec) (*conditional access channel 2*)
CAD	Dispositivo de acceso condicional (*conditional access device*)
CD	Dispositivo controlador (*controller device*)
CI	Identificador de instrucción (*command identifier*)
CIW	Palabra identificación de soporte (*container identification word*)
CMSM	Modelo de seguridad principal de control (*control major security module*)
CW	Palabra de control *(control word)*
ECM	Mensaje de control de autorización (*entitlement control message*)
ECW	Palabra de control par (*even control word*)
EEPROM	Memoria de sólo lectura programable y borrable eléctricamente (circuito integrado) (*electrically erasable programmable read only memory) (integrated circuit)*
EMM	Mensaje de gestión de autorización (*entitlement management message*)
HDLC	Control de alto nivel para enlace de datos (*high level data link control*)
IW	Palabra de inicialización, cargada en los generadores de secuencia seudoaleatoria para desaleatorizar (*initialization word*)
LI	Indicador de longitud (*length indicator*)
MD	Dispositivo gestor (*manager device*)
MH	Encabezamiento de mensaje (*message header*)
MMSM	Módulo de seguridad principal de gestión (*management major security module*)
NMC	Centro de gestión de red (*network management centre*)
Octeto	Secuencia de 8 bits considerada como una palabra o un grupo de datos
OCW	Palabra de control impar (*odd control word*)
PCMCIA	Asociación internacional de tarjetas de memoria de ordenador personal (*personal computer memory card international association*)

PPI	Identificador de paridad de fase, que indica la CW que debe utilizarse para desaleatorizar (*phase parity identifier*)
PRG	Generador de secuencia seudoaleatoria (*pseudo-random generator*)
RPCP	Red pública con conmutación de paquetes
RTPC	Red telefónica pública con conmutación
UA	Dirección única (*unique address*)
USM	Módulo de seguridad de usuario (*user security module*)
SA	Dirección compartida (*shared address*)
Palabra	Grupo o secuencia de bits que se tratan conjuntamente

5 Descripción general del sistema

Un sistema de acceso condicional tiene por objeto permitir a usuarios autorizados desaleatorizar los componentes de un servicio.

En la Recomendación J.81 se especifican los procesos de aleatorización y desaleatorización, que se resumen en 5.1. Estos procesos se llevan a cabo por los codificadores y decodificadores, respectivamente.

La información necesaria para desaleatorizar puede introducirse manualmente en el decodificador (es decir, la palabra de control local) o puede proporcionarla el sistema de acceso condicional descrito en 5.2.

Entre el transmisor y el receptor o receptores esta información se estructura en mensajes de seguridad multiplexados con la propia señal en los canales CA1 y CA2 (véase la cláusula 12/J.81). Estos mensajes se extraen de la señal por los decodificadores y se interpretan por el sistema de acceso condicional en el receptor o receptores autorizados para controlar la desaleatorización de los componentes del servicio.

5.1 Descripción general de los procesos de aleatorización/desaleatorización

En la Figura 1 se representan los procesos de aleatorización/desaleatorización.

El acceso condicional exige que las señales de televisión se aleatoricen mediante el codificador antes de su transmisión. Este proceso se controla mediante una secuencia de aleatorización obtenida a partir de un generador seudoaleatorio.

El proceso de desaleatorización en los decodificadores exige la correspondiente secuencia (en este caso la secuencia de desaleatorización) para recuperar la señal original.

Con objeto de obtener esta secuencia y asegurar el sincronismo entre el transmisor y el receptor o receptores, la condición de arranque del generador seudoaleatorio se controla mediante una palabra de inicialización.

El acceso condicional a un servicio es equivalente, de hecho, a un acceso condicional a la palabra de inicialización, que se obtiene mediante una combinación del modificador de inicialización y la palabra de control.

El modificador de inicialización se utiliza para producir una nueva palabra de inicialización en cada soporte de televisión, como se define en la Recomendación J.81. El modificador de inicialización, denominado CIW en la Recomendación J.81, se transmite sin codificar por el canal CA2.

Independientemente de los procesos de aleatorización/desaleatorización, el sistema de acceso condicional crea parejas de palabras de control activo. Cada pareja consiste en una palabra de control par (ECW), válida para los bloques pares, y una palabra de control impar (OCW), válida para los bloques impares. La paridad del bloque transmitido viene dada por el indicador PPI en el canal CA2 (véase 12/J.81).

La palabra de control es el elemento básico de seguridad. Su valor arbitrario permanece constante durante cualquier bloque de los soportes de TV, (65 534 soportes de TV, lo que corresponde a 8,2 segundos). El codificador recibe criptogramas de las palabras de control y los transmite al decodificador o decodificadores a través del canal CA1.

5.2 Descripción general del sistema de acceso condicional

El cometido del sistema de acceso condicional consiste en crear para cada nueva transmisión una nueva secuencia de palabras de control y distribuir de forma exclusiva cada secuencia a los usuarios pertinentes (un transmisor y uno o más receptores, de acuerdo con la configuración de la transmisión). Para ello, el sistema de acceso condicional crea, transmite y utiliza mensajes de acceso condicional.

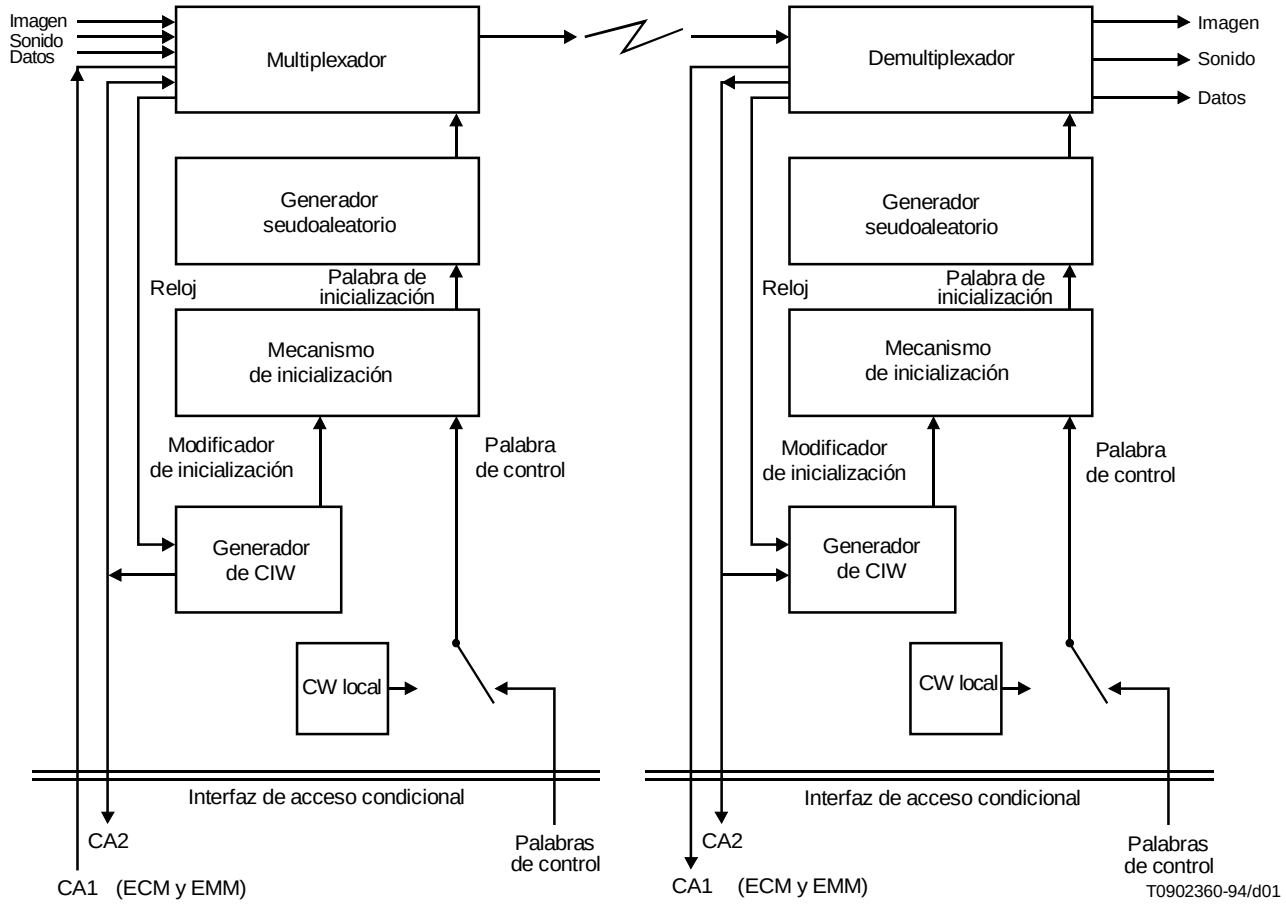


FIGURA 1/J.91

Procesos de aleatorización/desaleatorización

Para lograr la seguridad de los mensajes de acceso condicional, se utilizan dos conjuntos de mecanismos criptográficos, a saber:

- El cifrado y descifrado del bloque se emplean para asegurar la privacidad (por ejemplo, para las palabras de control y las contraseñas en criptogramas).

- El cálculo y la verificación de la suma de control criptográfica se emplean para asegurar la integridad (por ejemplo, para mensajes de autentificación).

El cifrado de bloque y el cálculo de la suma de control criptográfica se realizan mediante los módulos de seguridad principales.

El descifrado de bloque y la verificación de la suma de control criptográfica se realizan mediante los módulos de seguridad de usuario.

Un control de suma criptográfico debe proteger cada mensaje de acceso condicional donde están presentes uno o más criptogramas. Al recibir tal mensaje, cualquier módulo de seguridad debe determinar la validez de la suma de control criptográfica antes de continuar el proceso. En consecuencia, el descifrado de cualquier criptograma viene condicionado por una verificación positiva de la integridad de todo el mensaje de acceso condicional.

En cualquier sistema de acceso condicional, se necesita una autoridad responsable que genere las palabras de control y calcule y transmita sus criptogramas. Dicha autoridad posee y utiliza en exclusividad los módulos de seguridad principales.

En la mayoría de los sistemas de televisión por pago tradicionales, existe un organismo que desempeña a la vez el cometido de autoridad responsable y de ente transmisor. En la presente Recomendación, la autoridad y el ente transmisor son dos organismos distintos por las siguientes razones:

- Es muy conveniente una distribución de los módulos de seguridad principales.
- Debe centralizarse la gestión del intercambio internacional de programas de televisión (por ejemplo, en la EBU).

En consecuencia, el transmisor y el receptor o receptores únicamente tienen y utilizan los módulos de seguridad de usuario.

El sistema de acceso condicional emplea dos categorías de mensajes de acceso condicional: mensajes de control de autorización (ECM) y mensajes de gestión de autorización (EMM).

El canal CA1 se dedica a la transmisión de los mensajes del transmisor al receptor o receptores. La longitud media de los mensajes de acceso condicional es de unos 300 bits. Si se utiliza un sistema de protección contra errores (por ejemplo, un código Golay) puede duplicarse esta longitud. Se envía un ECM al menos cada 8,2 segundos. Si el ECM se repite cada segundo, se dispone aproximadamente de 7 kbit/s para enviar 10 EMM por segundo.

Cada mensaje de acceso condicional consiste en una cadena de parámetros opcionales. Uno de los parámetros se dedica a transportar uno o más criptogramas y otro parámetro se dedica a cursar una suma de control criptográfica.

5.2.1 Mensajes de control de autorización (ECM)

Los ECM están destinados a proporcionar las palabras de control a todos los usuarios autorizados y solamente a ellos. Por consiguiente, el parámetro esencial de cada ECM es uno o más criptogramas de palabras de control.

Los ECM pueden comenzar con uno o más criterios de acceso. De ser así, el módulo de seguridad de usuario debe validar al menos uno de esos criterios de acceso antes de continuar el proceso del mensaje.

El último parámetro de cada ECM debe ser una suma de control criptográfica para proteger todo el mensaje.

5.2.2 Mensajes de gestión de autorización (EMM)

Los EMM tienen por objeto proporcionar a los módulos de seguridad de usuario correspondientes las autorizaciones y contraseñas apropiadas, que se utilizan para descifrar los criptogramas de las palabras de control transmitidas en los ECM.

Los parámetros principales de los EMM son las direcciones del módulo de seguridad de usuario, las autorizaciones, los criptogramas de la contraseña y, por último, una suma de control criptográfica para proteger todo el mensaje.

6 Establecimiento de modelos de interfaces y equipos

En la Figura 2 se representa un modelo de interfaces basado en la descripción general anterior.

La parte superior de la figura representa la autoridad responsable. El dispositivo de gestión y el dispositivo de control pueden no estar situados en el mismo lugar.

La parte inferior de la Figura 2 representa a los usuarios; en principio cada usuario es capaz de transmitir y recibir.

6.1 Lista de interfaces

- *Interfaz 1* – Esta interfaz asegura la transmisión de los EMM desde el dispositivo de gestión al dispositivo de control. Estos EMM se utilizarán para configurar los módulos de seguridad de usuario implicados en el intercambio de programas de televisión planificado.
- *Interfaz 2* **–** Esta interfaz asegura la transmisión de mensajes (EMM seguidos de ECM) desde la autoridad responsable (dispositivo de control) al transmisor (dispositivo de acceso condicional). La transmisión (como máximo a 8 kbit/s) puede llevarse a cabo en tiempo real por un canal especializado o por una línea telefónica. La transmisión puede efectuarse de forma alternativa mediante un disquete enviado por correo previamente, los mensajes (EMM y ECM) se procesan por el dispositivo de acceso condicional para su inserción en el canal CA1.
- *Interfaz 3* **–** Esta interfaz conecta los módulos de seguridad a diversos dispositivos tales como los dispositivos de acceso condicional, en el caso de los usuarios y los dispositivos de control y de gestión, en el caso de la autoridad responsable. Una posible realización del módulo de seguridad es la tarjeta inteligente. En este caso, la interfaz viene especificado en las series de la Norma Internacional ISO/CEI 7816.

– *Interfaz 4* **–** Esta interfaz conecta los dispositivos de acceso condicional de los usuarios a los codificadores y decodificadores. Viene especificado en la Recomendación J.81.

– *Interfaz 5* – Esta interfaz conecta los módulos de seguridad de usuario de los usuarios al dispositivo de gestión, a través de los dispositivos de acceso condicional. La información consultada en los módulos de seguridad de usuario puede utilizarse a efectos estadísticos y económicos. La interfaz 5 puede realizarse utilizando la red telefónica pública con conmutación o la red pública con conmutación de paquetes.

– *Interfaz 6* **–** Esta interfaz permite el diálogo con el operador local. Consiste en una interfaz hombre-máquina para los dispositivos de control y de gestión así como para cada dispositivo de acceso condicional.

Los detalles de las realizaciones (protocolo, realización física) de las interfaces 1, 2, 5 y 6 dependen de la aplicación y no se indican en la presente Recomendación.

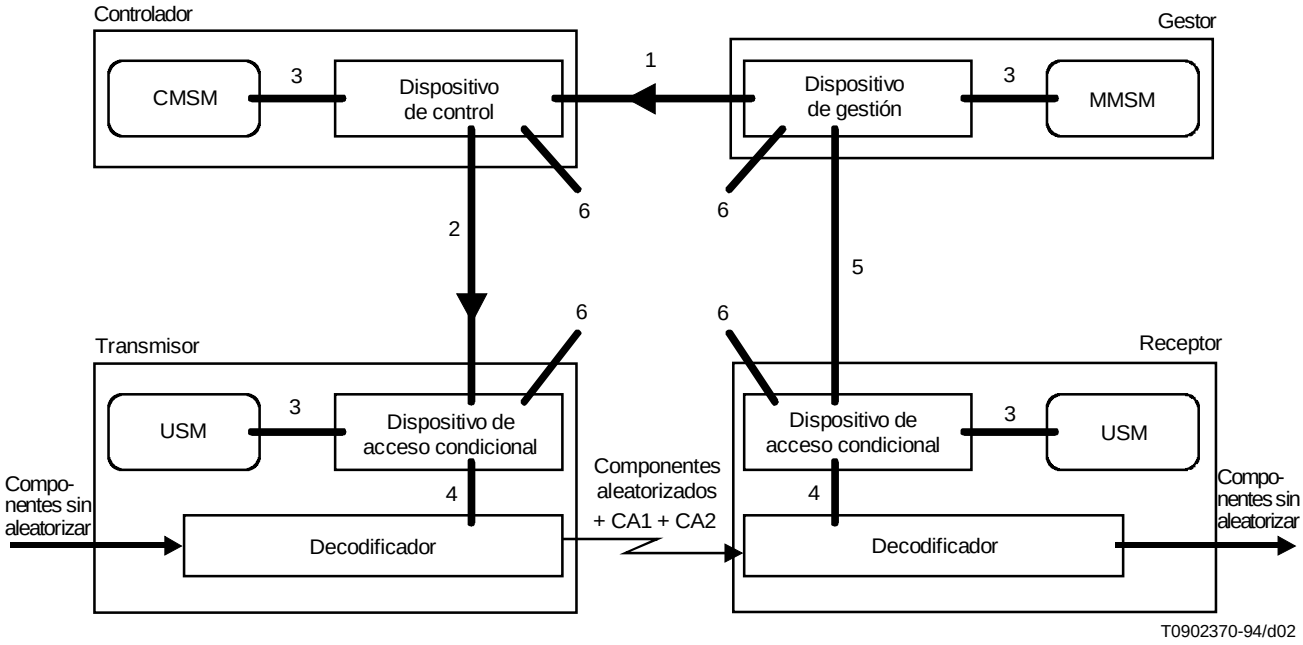


FIGURA 2/J.91

Modelos de interfaces

6.2 Lista de equipos

En la Recomendación J.81 se describen los codificadores y decodificadores.

Los módulos de seguridad principales de control y de gestión (capaces de realizar el cifrado de bloque y el cálculo de la suma de control criptográfica) se utilizan para determinar, respectivamente, los ECM y los EMM.

El módulo de seguridad de usuario (capaz de realizar el cifrado de bloque y la verificación de suma de control criptográfica únicamente) se emplea para interpretar los ECM y los EMM. Almacena las autorizaciones y las contraseñas de su usuario para descifrar los criptogramas de las palabras de control. Puede almacenar igualmente los accesos reales del usuario al sistema en caso de un sistema de visión de pago por cómputo de impulsos.

Cualquier módulo de seguridad puede realizarse como una tarjeta inteligente. En este caso, los módulos de seguridad principales se denominan a veces «tarjetas madre» y los módulos de seguridad de usuario «tarjetas hija».

El dispositivo de gestión se conecta a uno o más módulos de seguridad principales de gestión, que determinan los EMM, los cuales se envían al usuario a través del dispositivo de control. Si el número de usuarios es de unos pocos miles, el dispositivo de gestión puede consistir en un ordenador personal.

El dispositivo de control genera aleatoriamente las palabras de control y construye los ECM con la ayuda de sus módulos de seguridad principales de control. Estos ECM, así como los EMM comunicados por el dispositivo de gestión, se envían al transmisor. Si el número de usuarios es de unos pocos miles, el dispositivo de control puede consistir en un ordenador personal.

El dispositivo de acceso condicional se conecta a uno o más codificadores o decodificadores y a uno o más módulos de seguridad de usuario. En el extremo codificador, este dispositivo genera el canal CA1 que transporta los EMM y los ECM al receptor o receptores. El dispositivo de acceso condicional recibe los EMM y selecciona aquéllos dirigidos a su módulo o módulos de seguridad. Recibe igualmente los ECM que se procesan por los módulos de seguridad de usuario.

El «sistema de control de acceso» (ACS) descrito en la Recomendación J.81 corresponde a la combinación de un dispositivo de acceso condicional con uno o más módulos de seguridad de usuario.

7 Protocolo de transporte de los mensajes de acceso condicional en el canal CA1

Los mensajes de acceso condicional se difunden por el canal CA1 a la velocidad binaria nominal de 8 kbit/s (véase la Recomendación J.81).

Hasta ahora se han descrito dos tipos de mensajes de acceso condicional: los ECM y los EMM.

Según el modo de encripción (véase 12.7.3/J.81), puede haber

- ningún ECM (modos 0 y 1);
- un nuevo ECM cada bloque (modo 2);
- varios nuevos ECM cada bloque (modo 3).

En el modo 3, cada ECM se asociará con los componentes a los que se aplica.

Los EMM pueden enviarse a

- *Todos los usuarios* – En este caso se denomina EMM-G y se envían sin dirección;
- *Un grupo de usuarios* – En este caso, se denominan EMM-S y se envían con una dirección compartida (SA, 24 bits);
- *Un usuario único* – En este caso, se denominan EMM-U y se envían con una dirección única (UA, 36 bits).

Los ECM y los EMM se protegen con algoritmos criptográficos. La referencia del algoritmo criptográfico utilizado se envía junto con el mensaje.

Los mismos ECM y EMM deben enviarse varias veces [por ejemplo, el ECM se cambia cada bloque (8,2 s), pero el mismo ECM puede repetirse cada segundo para disminuir el retardo de adquisición]. Debe establecerse un mecanismo para permitir a los receptores distinguir entre los nuevos mensajes de acceso condicional y los mensajes repetidos.

7.1 Trama de transmisión

La estructura de trama descrita en 9.2.4/J.81 se utiliza para transmitir los mensajes de acceso condicional. Se basa en una estructura de trama HDLC.

La trama de transmisión, representada en la Figura 3, se compone de la siguiente información:

- una bandera de comienzo (INICIO): «01111110»;
- un encabezamiento de mensaje (MH): 2 octetos;
- un mensaje de acceso condicional: n octetos;
- un CRC detector de errores de 16 bits (FCS: Secuencia de verificación de trama): 2 octetos;
- una bandera de finalización, idéntica a la de comienzo (FIN): 1 octeto.

Para evitar la imitación de las banderas por los datos, HDLC define un método para suprimir largas cadenas de unos en los datos o zonas de CRC.

En cada octeto transmitido, el bit 0 es el menos significativo y se envía en primer lugar, de acuerdo con la especificación HDLC. Sin embargo, entre los octetos, el que se envía en primer lugar es el más significativo.

Después de la bandera de finalización, la línea HDLC vuelve al modo «inactivo».

INICIO	MH	Mensaje de acceso condicional	CRC	FIN
1 octeto	2 octetos	n octetos	2 octetos	1 octeto

FIGURA 3/J.91

Estructura de trama

Los 2 octetos MH se codifican como se describe en los Cuadros 1 y 2.

Los mensajes no reconocidos por el receptor deben ignorarse.

En el modo de encripción 3 (véase 12.7.3/J.81), pueden enviarse en una sola trama varios ECM precedidos por sus encabezamientos de mensaje asociados.

CUADRO 1/J.91

Codificación del encabezamiento de mensaje en los mensajes de acceso condicional

b_{16}	b_{15}	b_{14}	b_{13}	b_{12} b_7	b_6 b_1	Significado
0	0	0	0	Reservados	Véase el Cuadro 2	ECM
0	0	Otro valor		Reservados	Véase el Cuadro 2	Reservado para un máximo de 3 tipos especiales de ECM
0	1	0	0	Reservados	1 1 1 1 1 1	EMM-U
0	1	0	1	Reservados	1 1 1 1 1 1	EMM-S
0	1	1	0	Reservados	1 1 1 1 1 1	EMM-G
Cualquier otro valor				Reservados	1 1 1 1 1 1	Reservado para un máximo de 9 tipos de EMM
NOTA – Los bits b_{12} a b_7 se reservan para su uso futuro y se ponen a 0.						

CUADRO 2/J.91

Significado de los bits b_6 a b_1 del encabezamiento de mensaje de los ECM

b_6	b_5	b_4	b_3	b_2	b_1	Significado
0	0	0	0	0	0	Reservados
0	X	X	X	X	1	El componente T viene determinado por el ECM
0	X	X	X	1	X	El componente A viene determinado por el ECM
0	X	X	1	X	X	El componente T′ viene determinado por el ECM
0	X	1	X	X	X	El componente A′ viene determinado por el ECM
0	1	X	X	X	X	El componente V viene determinado por el ECM
Cualquier otro valor						Reservados

7.2 Contenido del mensaje de acceso condicional

7.2.1 Identificador de instrucción (CI)

Todos los ECM y EMM contienen un campo de identificador de instrucción (CI) de 8 bits que describe el formato que ha de utilizar el campo de mensaje y el tipo de algoritmo criptográfico utilizado. En la Figura 4 se indica su codificación.

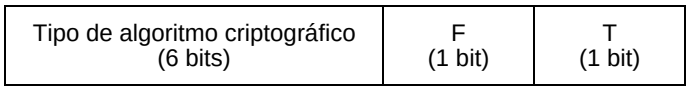


FIGURA 4/J.91

Codificación del identificador de instrucción (CI)

NOTAS

1 Tipo de algoritmo criptográfico (6 bits) – Este parámetro se utiliza para identificar de forma simultánea hasta 64 tipos de algoritmos criptográficos. El módulo de seguridad de usuario del receptor sólo puede interpretar y procesar los mensajes cuyo tipo de algoritmo se adapte al del módulo de seguridad de usuario.

2 F es un bit que describe el formato del campo de datos del mensaje.

a) F = 1 – El campo de datos está estructurado en el formato variable definido por EUROCRYPT.

b) F = 0 – Reservado para futura utilización.

3 T es el bit de conmutación. Se mantiene en el mismo estado mientras el contenido del mensaje no varía. Se utiliza en los EMM-G y en los ECM para indicar una modificación en el contenido de la información de estos mensajes. No tiene significado en los EMM-U y los EMM-S.

7.2.2 Contenido del ECM

En la Figura 5 se representa el contenido de un ECM antes de su inserción en una trama.

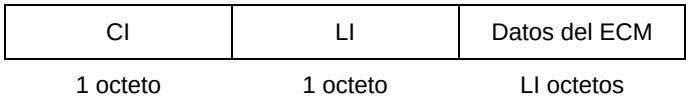


FIGURA 5/J.91

Mensaje ECM

7.2.3 Contenido del EMM

En la Figura 6 se representa el contenido de un EMM antes de su inserción en una trama.

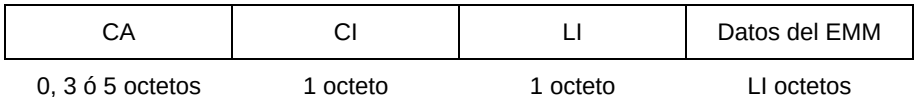


FIGURA 6/J.91

Mensaje EMM

Todos los EMM, salvo el EMM-G, comienzan por una dirección de abonado (CA). La longitud del campo CA es:

- 40 bits para el EMM-U – En este caso, los 4 primeros bits se ponen a 0 y los 36 bits restantes transportan la UA (dirección única);
- 24 bits para el EMM-S – En este caso, CA transporta los 24 bits de la dirección compartida (SA).

8 Realizaciones prácticas

En la práctica, las funcionalidades descritas anteriormente pueden realizarse de diversas formas, desde el establecimiento de palabras de control local únicamente a través de sistemas de acceso condicional patentados, para redes pequeñas o de configuración sencilla, hasta sistemas de acceso condicional completamente caracterizados y comercialmente disponibles que pueden utilizarse en un entorno de red abierta o cuando tanto el número de abonados a la red como la variedad de funciones de control de acceso necesarias son elevados.

En el Anexo A se describe el funcionamiento con palabra de control local. En el Anexo B se indica el funcionamiento con el sistema de acceso condicional EUROCRYPT[2)] que cubre todas las funciones señaladas en el párrafo anterior; otros sistemas que puedan aparecer se incluirán en futuros anexos.

Anexo A

Funcionamiento con palabra de control local

(Este anexo es parte integrante de esta Recomendación)

A.1 Realización práctica con palabra de control local

Pueden utilizarse palabras de control local. Ello significa que el codificador en el emplazamiento de comunicación para la transmisión utiliza únicamente una palabra de control durante toda la transmisión. Dicha palabra de control debe introducirse en el codificador por el operador del transmisor. Con objeto de desaleatorizar la señal en el emplazamiento de comunicación para su recepción, el decodificador debe conseguir la misma palabra de control del operador del receptor.

Dicha realización supone una nueva acción específica del operador. Aunque esta realización es mucho menos segura desde el punto de vista de control de acceso, sería en realidad totalmente independiente de los dispositivos de gestión y de control y del CAD, y podría coexistir fácilmente con un sistema de control de acceso.

Anexo B

Funcionamiento con EUROCRYPT[3)]

(Este anexo es parte integrante de esta Recomendación)

B.1 Introducción

El presente anexo describe una realización práctica que utiliza el sistema de acceso condicional EUROCRYPT normalizado completamente caracterizado donde las funcionalidades de los diversos módulos de seguridad las proporciona la familia de tarjetas inteligentes PC2.

EUROCRYPT es un sistema de acceso condicional normalizado por UTE (EN 50094, 1992) y utilizado actualmente para controlar el acceso a las señales D2MAC/paquetes. Especifica a los ECM y los EMM.

La familia PC2 de tarjetas inteligentes consiste en módulos de seguridad desarrollados para llevar a cabo las funciones de seguridad de EUROCRYPT. Existen varias categorías de tarjetas inteligentes PC2 (véase la Figura B.2):

- las tarjetas madre de gestión PC2 proporcionan las funciones de los módulos de seguridad principales de gestión;
- las tarjetas madre de control PC2 proporcionan las funciones de los módulos de seguridad principales de control;
- las tarjetas hija PC2 proporcionan las funciones de los módulos de seguridad de usuario.

---

2) EUROCRYPT se encuentra normalizado por UTE (EN 50094, 1992).

3) EUROCRYPT se encuentra normalizado por UTE (EN 50094, 1992).

Hay dos tipos de emplazamientos:

- el centro de gestión de red que incluye un dispositivo de control y un dispositivo de gestión;
- cada emplazamiento de comunicación incluye uno o varios dispositivos de acceso condicional.

El centro de gestión de red es único en la red y es el responsable de la gestión de los recursos de la red, de la atribución de los canales disponibles y de la sincronización entre transmisores y receptores.

Hay varios emplazamientos de comunicación. Cada uno de ellos puede transmitir y/o recibir simultáneamente uno o más programas de televisión aleatorizados. En cada emplazamiento, existe al menos un dispositivo de acceso condicional que gestiona varios transmisores y varios receptores.

Las principales características del sistema son las siguientes:

- gestión centralizada del intercambio de programas de televisión;
- posibilidad de seleccionar/autorizar receptores muy rápidamente, casi en tiempo real;
- interfaz hombre-máquina sencilla en el centro de gestión de red y en los emplazamientos de comunicación;
- no tiene necesidad de conexión permanente entre el centro de gestión de red y los emplazamientos de comunicación;
- protección muy elevada contra la piratería de los programas de televisión transmitidos por redes abiertas, tales como satélites.

Además, los emplazamientos de comunicación que no están conectados directamente al centro de gestión de red pueden, no obstante, transmitir y/o recibir programas de televisión aleatorizados.

La Figura B.1 ilustra la red considerada desde el punto de vista de control de acceso. En la Figura B.1 y en las cláusulas siguientes, se denomina NMC al centro de gestión de red y CAD a los dispositivos de acceso condicional.

Las tarjetas madre PC2 son necesarias únicamente en el centro de gestión de red.

Para transmitir y recibir en cada emplazamiento de comunicación se utilizan una o más tarjetas hija PC2.

B.1.1 Programas y transmisiones

Debe distinguirse claramente entre transmisiones y programas:

Una transmisión se caracteriza por:

- un satélite u otro canal de comunicación;
- un emplazamiento de comunicación utilizado como transmisor;
- uno o más emplazamientos de comunicaciones utilizados como receptor o receptores;
- una fecha y hora de inicio y de finalización;
- un conjunto de componentes de televisión, incluyendo las señales sonoras, de imagen y de datos.

Un programa se caracteriza por:

- un nombre del programa;
- una o más transmisiones;
- una contraseña de autorización;
- uno o más criterios de acceso.

En consecuencia, puede utilizarse una transmisión para difundir uno o más programas y un programa puede transmitirse a través de una o más transmisiones.

Se consideran tres comportamientos distintos:

- el comportamiento del centro de gestión de red;
- el comportamiento del transmisor de un emplazamiento de comunicación cuando utiliza uno de sus codificadores;
- el comportamiento del receptor de un emplazamiento de comunicación cuando utiliza uno de sus decodificadores.

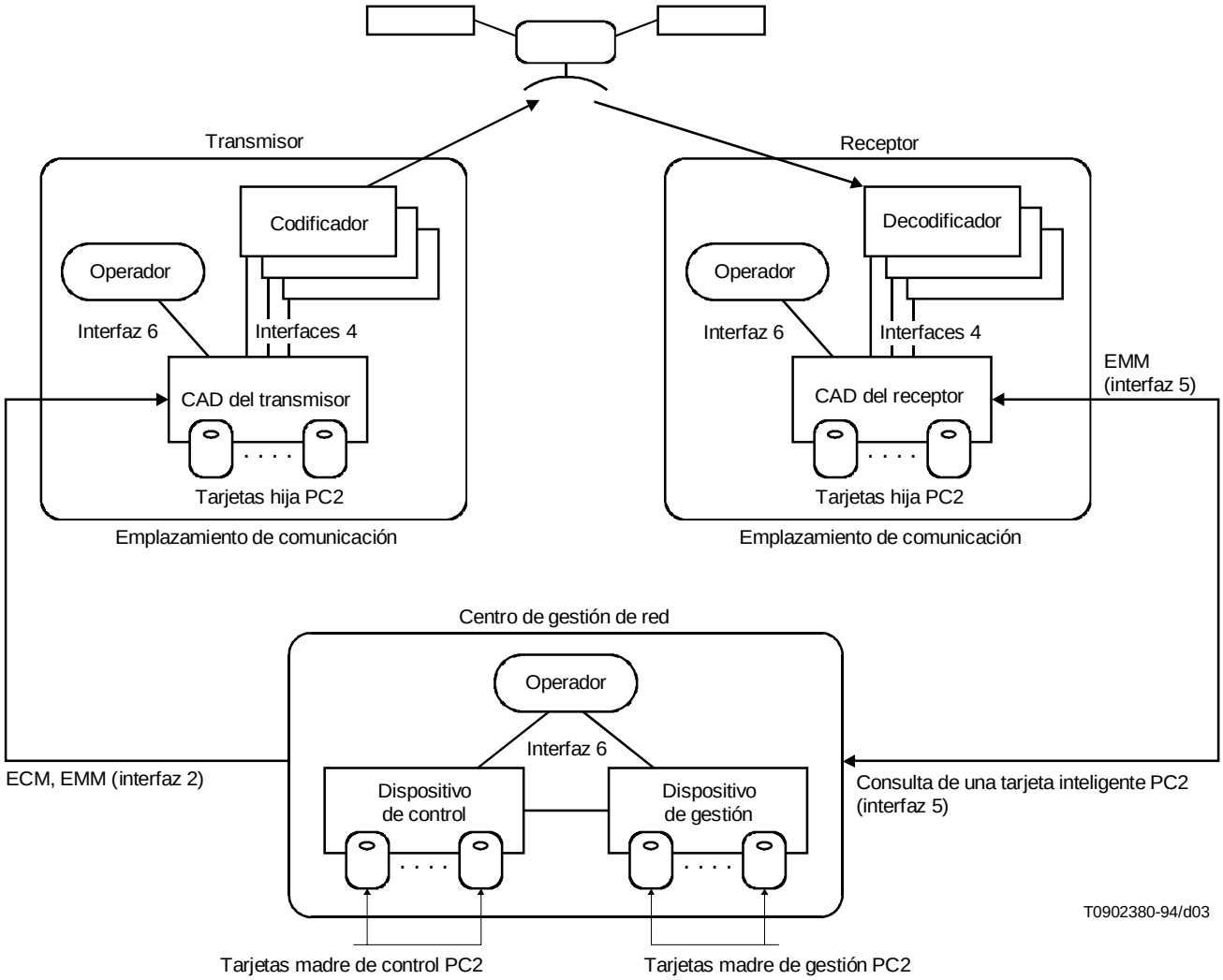


FIGURA B.1/J.91

Arquitectura de la red

B.2 Funcionalidades del centro de gestión de red (NMC)

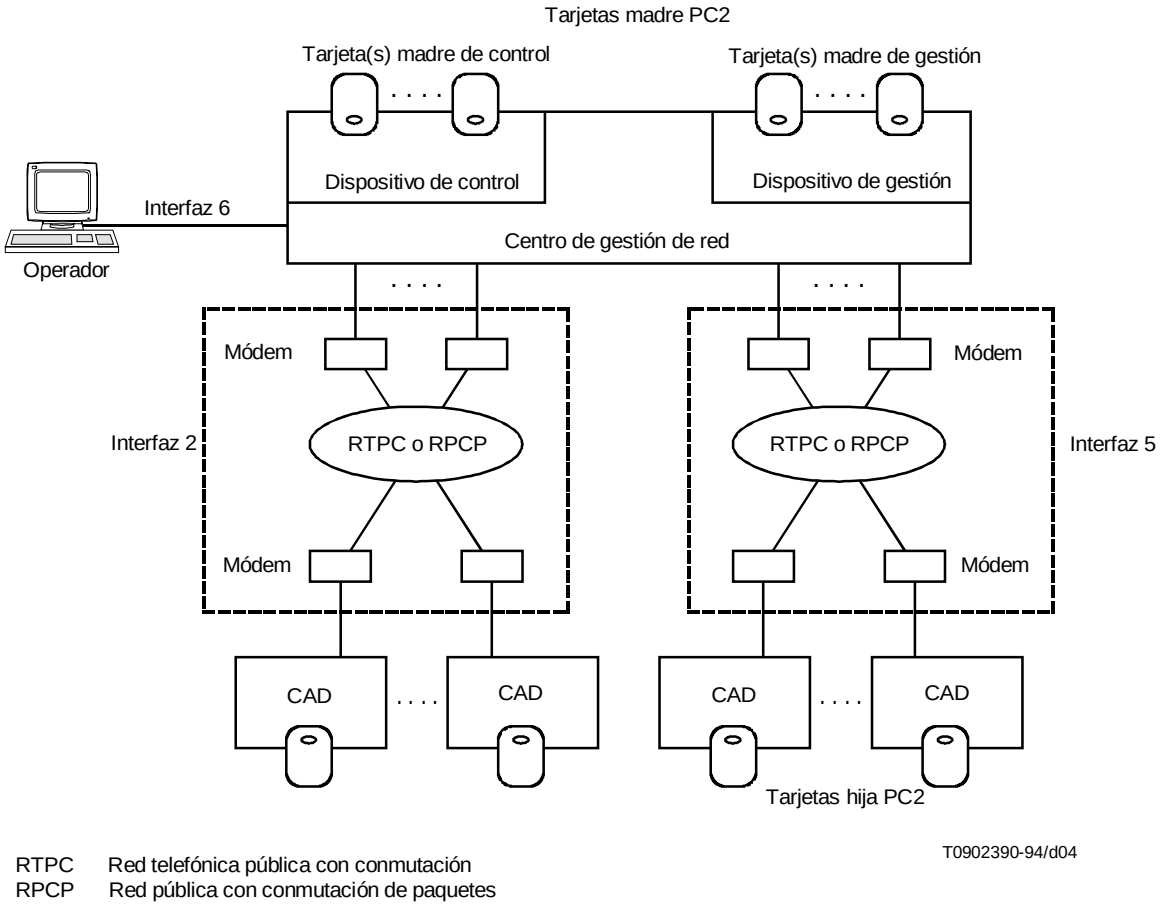
Corresponde al NMC asegurar que el transmisor y todos los receptores autorizados consiguen la contraseña de autorización y las autorizaciones de acceso correctas antes de transmitir el programa. También es responsabilidad del NMC la actualización periódica de las contraseñas de autorización por razones de seguridad. Para ello, el NMC crea y transmite los ECM y los EMM.

El NMC controla igualmente la emisión de todas las tarjetas inteligentes del sistema y asegura la supervisión de todas las tarjetas hija.

En la Figura B.2 se representa esquemáticamente el NMC.

B.2.1 Generación de los ECM

El NMC debe generar los ECM. Para ello, establece las palabras de control, cifra dichas palabras de control utilizando una tarjeta madre y crea los correspondientes ECM. Cada ECM se protege mediante una suma de control criptográfica calculada por su tarjeta madre. Durante la transmisión, se utiliza un nuevo ECM cada 8,2 segundos. Los ECM se envían al CAD del transmisor a través de la interfaz 2



RTPC Red telefónica pública con conmutación
RPCP Red pública con conmutación de paquetes

FIGURA B.2/J.91

Centro de gestión de red (NMC)

Un modo inmediato de llevar a cabo el proceso consiste en crear regularmente ECM y enviarlos «en línea» al CAD del transmisor. Dicha realización supone que durante toda la transmisión, el NMC permanece conectado al CAD del transmisor. Además, el NMC que excita todos los transmisores debe generar varios conjuntos de ECM (tantos como canales funcionen en ese instante) y enviarlos a la vez.

La utilización de ficheros cíclicos de ECM suprime ese inconveniente. Dichos ficheros contienen el número de ECM necesarios para la duración estimada de la transmisión. Si las transmisiones se superponen, el último ECM se construye de tal forma que puede ir seguido del primer ECM del mismo fichero para poder enlazar a través del mismo conjunto de ECM. Utilizando los ECM EUROCRYPT, un fichero de 16k octetos proporciona ECM para aproximadamente una hora de programa.

El NMC puede generar un conjunto de ficheros cíclicos ECM antes de que se identifique alguna necesidad y enviarlos al CAD con anticipación, o en el último momento antes de la transmisión.

El envío de varios ficheros cíclicos ECM con anterioridad al CAD facilita el funcionamiento casi inmediato, aun en el caso de transmisiones de televisión repentinas (planificadas en el último minuto) o en el caso de un transmisor transportable aislado.

B.2.2 Generación de los EMM

El NMC debe generar también los EMM para la distribución de contraseñas y autorizaciones a las tarjetas hija especificadas.

Un EMM es para el transmisor: permitirá al CAD del transmisor (con la ayuda de su tarjeta hija) descifrar la palabra de control de los ECM anteriores.

El resto de EMM son para los receptores. Permitirán a las tarjetas hija autorizadas de los CAD de los receptores descifrar la palabra de control de los ECM anteriores. Hay dos formas distintas de transmitir los EMM, a saber:

- pueden transmitirse directamente, utilizando la interfaz 5 (vía telefónica, X.25, conexión directa), al CAD correspondiente de cada receptor;
- pueden difundirse a todos los receptores a través del codificador del transmisor y el canal de satélite.

Se definen dos categorías de EMM: EMM-U y EMM-S.

Un EMM-U contiene la dirección única de una sola tarjeta hija. En consecuencia, la distribución de una autorización determinada a *n* tarjetas hija supone el cálculo y transmisión de *n* EMM-U.

Un EMM-S contiene la dirección compartida de un grupo de tarjetas hija. Un EMM-S puede direccionar hasta 256 tarjetas hija que comparten la misma contraseña de gestión. La utilización de EMM-S reduce el número medio de EMM que debe crear y transmitir una transmisión de televisión.

B.2.3 Supervisión de las tarjetas hija

El NMC controla el contenido de cada tarjeta hija.

Si se utiliza un sistema de televisión de pago por cómputo de impulsos, el NMC controla la adquisición de las tarjetas hija.

El NMC cuenta con una base de datos para conocer el contenido de cada una de las tarjetas inteligentes así como información detallada sobre todos los CAD (emplazamientos, tarjetas inteligentes, etc.).

Si una tarjeta hija tiene toda su memoria ocupada, el NMC debe limpiar dicha memoria suprimiendo las contraseñas y autorizaciones anticuadas. Si esta limpieza no es posible (tarjeta PC2-1), el NMC indica a su operador y al operador del CAD que cambie la tarjeta hija.

B.2.4 Emisión de tarjetas inteligentes

El NMC genera casos de emisión (descripción de todas las contraseñas y parámetros que deben escribirse en cada tarjeta) a petición de su operador. Dichos casos se envían a un dispositivo de emisión que inicializa las tarjetas, a continuación devuelve al NMC un conjunto de tarjetas y un fichero informe que se utiliza para actualizar la base de datos del NMC.

B.2.5 Interfaz hombre-máquina

La interfaz hombre-máquina consiste en:

- una petición de transmisión;
- una descripción de todas las referencias de transmisión descritas anteriormente;
- una consulta y una actualización de la base de datos;
- una revisión periódica de las tarjetas configuradas para los sistemas de televisión de pago por cómputo de impulsos;
- un diario de las alarmas (una tarjeta inteligente está completa o no funciona, existen problemas de conexión con un CAD).

B.3 Realización de los CAD

Las labores del CAD del transmisor consisten en:

- transmisión de los EMM pertinentes a su tarjeta o tarjetas hija para almacenar las nuevas contraseñas y autorizaciones;
- transmisión regular (cada 8,2 segundos) de un ECM a su tarjeta hija para obtener la correspondiente CW que debe darse al codificador para aleatorizar el programa de televisión;
- transmisión regular (cada segundo) al codificador de un ECM para su difusión a los decodificadores (a través del canal CA1 en el múltiplex de 34 Mbit/s);
- si es necesario, la transmisión igualmente de los EMM al codificador para su transmisión a los decodificadores (a través del canal CA1 en el múltiplex de 34 Mbit/s).

Las labores del CAD del receptor consisten en:

- obtener los EMM pertinentes del decodificador o del enlace directo con el NMC y transmitirlos a su tarjeta o tarjetas hija para almacenar las nuevas contraseñas y autorizaciones;
- obtener regularmente los ECM del decodificador y enviarlos a su tarjeta hija para obtener las correspondientes palabras de control y devolver al decodificador dichas palabras de control.

En la Figura B.3 se representa la arquitectura del CAD.

Los ECM y los EMM transmitidos en el canal CA1 pueden protegerse mediante un código Golay. En este caso, antes de la transmisión el transmisor debe proteger estos mensajes por un código Golay y en recepción cada receptor debe corregir los mensajes antes de procesarlos.

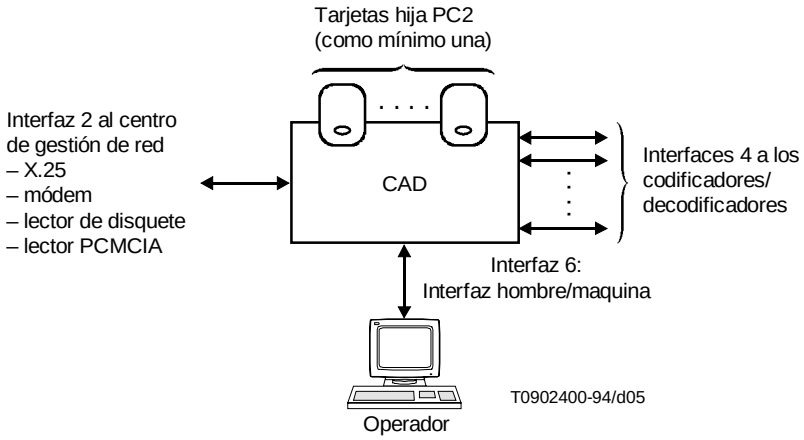


FIGURA B.3/J.91

Arquitectura del CAD

B.3.1 Caso de la estación transmisora aislada

«Aislada» significa que no hay conexión entre el CAD del transmisor y el NMC en el instante de la transmisión. Puede ser el caso, por ejemplo, de una unidad informativa de noticias especial en que la estación transmisora tiene gran movilidad. Cualquier transmisor debe ser capaz de funcionar de este modo en caso de emergencia.

En este contexto, aún es posible asegurar la transmisión de los programas de televisión. Para ello, debe cargarse previamente el CAD del transmisor (utilizando un disquete o una tarjeta de memoria PCMCIA) con un fichero cíclico ECM. En esas circunstancias, la única tarea del operador del transmisor consiste en seleccionar el fichero cíclico ECM adecuado.

Este modo es muy apropiado cuando se trata de sistemas de televisión de pago por cómputo de impulsos. Las tarjetas hija de los receptores almacenarán automáticamente el número del programa (con el acuerdo del operador del receptor). El NMC controlará posteriormente el contenido de las tarjetas.

B.4 Realización de la interfaz 2

La interfaz 2 conecta el NMC al CAD del transmisor. Se inicializa mediante el NMC.

Se intercambian los siguientes mensajes e instrucciones:

- ECM – La realización recomendada consiste en un fichero cíclico ECM establecido por el NMC y transmitido previamente al CAD del transmisor junto con la referencia del programa de televisión que utilizará estos ECM. Otra realización podría consistir en enviar un ECM «en línea» cada 8,2 segundos.
- EMM – La realización recomendada consiste en un fichero EMM establecido por el NMC y transmitido previamente al CAD del transmisor. Es posible otra realización utilizando la interfaz 5 para direccionar cada receptor.

La interfaz 2 puede realizarse sobre la red telefónica pública con conmutación o sobre la red pública con conmutación de paquetes, o incluso en un disquete o en la nueva tarjeta de memoria PCMCIA.

B.5 Realización de la interfaz 5

La interfaz 5 conecta el NMC a una tarjeta hija a través de un CAD. Se inicializa mediante el CAD.

Se utiliza fundamentalmente para supervisar las tarjetas hija conectadas al CAD. La supervisión de las tarjetas consiste en:

- verificar el sistema de pago mediante cómputos por impulsos almacenados en la tarjeta;
- limpiar la EEPROM de la tarjeta (únicamente las tarjetas PC2-2). Si una tarjeta no tiene memoria libre, el NMC suprime las autorizaciones caducas. Si no es posible efectuar la limpieza (tarjeta PC2-1), el NMC indica a su operador y al operador del CAD que cambie la tarjeta hija.

De forma adicional, como se ha indicado anteriormente, puede utilizarse la interfaz 5 para enviar los EMM.

El interfaz 5 puede realizarse utilizando la red telefónica pública con conmutación o la red pública con conmutación de paquetes.

La información registrada se almacena en la tarjeta hija en un bloque dispuesto al respecto. La llamada se inicia por el CAD tras recibir un EMM para activar el módem (véanse las especificaciones EUROCRYPT, Apéndice 2, § 11).

B.6 Ilustración del sistema que utiliza las características EUROCRYPT

Para determinar las palabras de control de un fichero cíclico de ECM asociado a una transmisión determinada, la tarjeta hija PC2 del receptor debe contener la contraseña de autorización correcta y al menos una autorización válida. Las contraseñas de autorizaciones son definidas por el NMC que envía los EMM para autorizar las tarjetas pertinentes. Para llevar a cabo esta acción, el NMC puede elegir entre los diversos modos de funcionamiento descritos más adelante.

Las abreviaturas utilizadas en este punto para representar el contenido de los ECM y los EMM vienen definidas en EUROCRYPT (EN 50094, 1992), donde aparecen más detalles sobre la utilización de EMM-U y EMM-S.

B.6.1 Dispositivo de control de acceso por actualización de la contraseña de autorización

Las contraseñas de autorización de todas las tarjetas pertinentes deben actualizarse antes de cada nuevo programa. El siguiente EMM-U tiene por objeto actualizar una contraseña de autorización en la tarjeta direccionada por UA:

EMM-U (37 octetos): UA, CI LI, PI LI PPID, PI LI IDUP, PI LI contraseña cifrada, PI LI HASH.

B.6.2 Dispositivo de control de acceso mediante abono

El NMC puede enviar abonos para tarjetas seleccionadas. Una tarjeta abonada tiene acceso a una categoría de programas durante un periodo determinado de tiempo. El siguiente EMM-U tiene por objeto incluir un abono en la tarjeta direccionada por la UA:

EMM-U (30 octetos): UA, CI LI, PI LI PPID, PI LI DATES+TH/LE, PI LI HASH.

B.6.3 Dispositivo de control de acceso por número de programa

El NMC puede asociar un número a cada programa (PNUMB). El siguiente EMM-U tiene por objeto incorporar una autorización asignando uno o más números de programas consecutivos a la tarjeta direccionada por la UA:

EMM-U (30 octetos): UA, CI LI, PI LI PPID, PI LI INUMB+FNUMB, PI LI HASH.

Una solución alternativa consiste en utilizar uno o más EMM-S precedidos de un EMM-G. La SA puede direccionar un grupo de hasta 256 tarjetas. Cada tarjeta en el grupo tiene un rango, que va de 1 a 256. Una tarjeta determinada en el grupo acepta o rechaza la acción según el valor que tome el bit *i*-ésimo de ADF, 1 ó 0:

EMM-G (15 octetos): CI LI, PI LI PPID, PI LI INUMB+FNUMB.

EMM-S (79 octetos): SA, CI LI, ADF, PI LI HASH.

Con un solo EMM-G + EMM-S, es posible enviar la autorización de forma selectiva a un grupo de 256 tarjetas. Este modo de acceso es muy interesante en el caso de programas planificados mucho tiempo antes de su transmisión.

B.6.4 Dispositivo de control de acceso mediante visión de pago por cómputo de impulsos a un número de programa

En este modo, los receptores no necesitan ningún EMM. Todos los receptores potenciales con la contraseña de autorización correcta pueden desaleatorizar el programa en el modo de pago en función del tiempo de observación (con el acuerdo del operador del receptor). La tarjeta memoriza la acción del operador. Este modo de acceso es muy conveniente para transmisiones urgentes.

B.6.5 ECM con los últimos tres criterios de acceso

El mismo programa puede utilizar conjuntamente diversos modos de acceso. En ese caso, varias clases de receptores acceden al mismo programa:

- los abonados tienen un acceso por abono;
- los usuarios inscritos tienen un acceso mediante el número de programa;
- los usuarios eventuales pueden tener acceso a un número de programa mediante un sistema de pago en función del tiempo de observación por cómputo de impulso.

El siguiente ECM propone el acceso por abono, por inscripción y mediante pago por cómputo de impulsos. La tarjeta verifica los criterios de acceso en orden hasta hallar una autorización válida:

ECM (53 octetos): CI LI, PI LI PPID, PI LI DATE+TH/LE, PI LI PNUMB, PI LI PNUMB+PPV-P, PI LI ECW/OCW, PI LI HASH.

Anexo C

Funcionamiento con otros sistemas

Este anexo queda en estudio.