UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T J.96

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

(03/2001)

SERIE J: REDES DE CABLE Y TRANSMISIÓN DE PROGRAMAS RADIOFÓNICOS Y TELEVISIVOS, Y DE OTRAS SEÑALES MULTIMEDIOS

Servicios digitales auxiliares para transmisiones de televisión

Procedimiento técnico para asegurar la privacidad en la transmisión internacional a larga distancia de señales de televisión MPEG-2 de conformidad con UIT-T J.89

Recomendación UIT-T J.96

(Anteriormente Recomendación del CCITT)

RECOMENDACIONES UIT-T DE LA SERIE J

REDES DE CABLE Y TRANSMISIÓN DE PROGRAMAS RADIOFÓNICOS Y TELEVISIVOS, Y DE OTRAS SEÑALES MULTIMEDIOS

Recomendaciones generales	J.1–J.9
Especificaciones generales para transmisiones radiofónicas analógicas	J.10–J.19
Características de funcionamiento de los circuitos radiofónicos	J.20–J.29
Equipos y líneas utilizados para circuitos radiofónicos analógicos	J.30–J.39
Codificadores digitales para señales radiofónicas analógicas	J.40–J.49
Transmisión digital de señales radiofónicas	J.50–J.59
Circuitos para transmisiones de televisión analógica	J.60–J.69
Transmisiones de televisión analógica por líneas metálicas e interconexión con radioenlaces	J.70–J.79
Transmisión digital de señales de televisión	J.80–J.89
Servicios digitales auxiliares para transmisiones de televisión	**J.90–J.99**
Requisitos operacionales y métodos para transmisiones de televisión	J.100–J.109
Sistemas interactivos para distribución de televisión digital	J.110–J.129
Transporte de señales MPEG-2 por redes de transmisión de paquetes	J.130–J.139
Mediciones de la calidad de servicio	J.140–J.149
Distribución de televisión digital por redes locales de abonados	J.150–J.159
IPCablecom	J.160–J.179
Varios	J.180–J.199
Aplicación para televisión digital interactiva	J.200–J.209

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

Recomendación UIT-T J.96

Procedimiento técnico para asegurar la privacidad en la transmisión internacional a larga distancia de señales de televisión MPEG-2 de conformidad con UIT-T J.89

Resumen

Esta Recomendación constituye una norma común para un sistema de acceso condicional de transmisión internacional a larga distancia de televisión digital de acuerdo con el perfil profesional MPEG (4:2:2).

En el anexo A se exponen además implementaciones prácticas.

Orígenes

La Recomendación UIT-T J.96, preparada por la Comisión de Estudio 9 (2001-2004) del UIT-T, fue aprobada por el procedimiento de la Resolución 1 de la AMNT el 9 de marzo de 2001.

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

ÍNDICE

Recomendación UIT-T J.96

Procedimiento técnico para asegurar la privacidad en la transmisión internacional a larga distancia de señales de televisión MPEG-2 de conformidad con UIT-T J.89

1 Alcance

Esta Recomendación constituye una norma común para un sistema de acceso condicional de transmisión internacional a larga distancia de televisión digital de acuerdo con el perfil profesional MPEG (4:2:2).

En el anexo A se exponen además implementaciones prácticas.

2 Referencias

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.

2.1 Referencias normativas

[1] UIT-T H.222.0 (2000) | ISO/CEI 13818-1:2000, *Tecnología de la información – Codificación genérica de imágenes en movimiento e información de audio asociada: Sistemas.*

[2] ETSI ETR 162 (1995), *Digital Video Broadcasting (DVB); Allocation of Service Information (SI) codes for DVB systems.*

[3] ETSI ETR 289 (1996), *Digital Video Broadcasting (DVB); Support for use of scrambling and conditional access (CA) within digital broadcasting systems.*

[4] ETSI EN 300 468, *Digital Video Broadcasting (DVB); Specification for Service Information (SI) in DVB systems.*

[5] UIT-T J.81 (1993), *Transmisión de señales de televisión digitales con codificación de componentes para las aplicaciones con calidad de contribución al tercer nivel jerárquico de la Recomendación UIT-T G.702.*

[6] UIT-T J.89 (1999), *Mecanismo de transporte para señales de televisión digital codificadas por componente que utilizan MPEG-2 4:2:2P@ML, incluidos todos los elementos de servicio para contribución y distribución primaria.*

[7] EBU Tech3290 (2000), *Basic Interoperable Scrambling System (BISS).*

2.2 Referencia bibliográfica

– OKAPI: BOUCQUEAU (J.M.), SERRET (J.), QUISQUATER (J.J.) and MACQ (B.): *Security in Multimedia Teleservices in Multimedia Telecommunications Services; Cost 237 – Final Report, Springer, September 1999, pp. 348-373.*

3 Términos y definiciones

En esta Recomendación se definen los términos siguientes:

3.1 Aleatorización: Alteración de las características de una señal de vídeo/audio/datos para evitar la recepción no autorizada en forma clara. La alteración es un proceso especificado bajo el control del sistema de acceso condicional (extremo emisor).

3.2 Desaleatorización: Restablecimiento de las características de una señal de vídeo/audio/datos para hacer posible la recepción en forma clara. El restablecimiento es un proceso especificado bajo el control del sistema de acceso condicional (extremo receptor).

4 Abreviaturas

En esta Recomendación se utilizan las siguientes siglas.

3DES	DES triple (*triple DES*)
ABC	Claves A, B y C de DES (*DES keys A, B, C*)
ACS	Sistema de control de acceso (*access control system*)
Bit	Contracción de las palabras "dígito binario" (*a contraction of the words "binary digit"*)
bslbf	Cadena de bits, bits izquierdo primero (*bit string, left bit first*)
CA	Acceso condicional (*conditional access*)
CAT	Tabla de acceso condicional (*conditional access table*)
CD	Dispositivo controlador (*controller device*)
CK	Clave común (*common key*)
CSA	Algoritmo de aleatorización común (*common scrambling algorithm*)
CW	Palabra de control (*control word*)
DES	Norma de criptación de datos (*data encryption standard*)
DSNG	SNG digital (*digital SNG*)
ECB	Libro de códigos electrónico (*electronic codebook*)
ECM	Mensaje de control de título (*entitlement control message*)
EDE	Codificación, decodificación, codificación (*encode, decode, encode*)
EMM	Mensaje de gestión de títulos (*entitlement management message*)
KE	Depósito de claves (*key escrow*)
lsb	Bit menos significativo (*least significant bit*)
LSB	Byte menos significativo (*least significant byte*)
MD	Dispositivo gestor (*manager device*)
MH	Encabezamiento de mensaje (*message header*)
msb	Bit más significativo (*most significant bit*)
MSB	Byte más significativo (*most significant byte*)
NMC	Centro de gestión de la red (*network management centre*)
OKAPI	Núcleo abierto para acceso a servicios interactivos interoperables protegidos (*open kernel for access to protected interoperable interactive services*)

Octet Secuencia de 8 bits que representan un grupo de datos o una palabra (*a sequence of 8 bits operated on as a data group or word*)

PCMCIA Asociación internacional de fabricantes de tarjetas de memoria de computador personal (*personal computer memory card international association*)

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

PMT Tabla de correspondencia de programas (*program map table*)

PRG Generador de secuencias seudoaleatorias (*pseudo-random (sequence) generator*)

PSI Información específica de programa (*program specific information*)

RPCP Red pública con conmutación de paquetes

RTPC Red telefónica pública conmutada

SAM Módulo de autorización de aleatorización (*scrambling authorization module*)

SK Clave de sesión (*session key*)

SNG Periodismo electrónico por satélite (*satellite news gathering*)

SM Módulo de seguridad (*security module*)

SW Palabra de sesión (*session word*)

TTP Tercera parte confiable (*trusted third party*)

uimsbf Entero sin signo, bit más significativo primero (*unsigned integer, most significant bit first*)

Word Grupo o secuencia de bits tratados de manera conjunta

5 Visión general del sistema

La Recomendación UIT-T J.89, que define el mecanismo de transporte para señales de televisión digital codificadas por componente utilizando MPEG-2 4:2:2P@ML, incluidos todos los elementos de servicio, se utiliza mucho en la actualidad para contribución y distribución primaria y también para las aplicaciones SNG de UIT-R SNG.1421.

Se emplea un sistema de acceso condicional, necesario para asegurar la privacidad en la transmisión de televisión internacional a larga distancia, para permitir a los usuarios autorizados a desaleatorizar los componentes de un servicio. Además, en las aplicaciones SNG quizás se requiera un sistema simplificado basado en una clave fija.

La información necesaria para la desaleatorización puede ser introducida manualmente en el decodificador mediante una "palabra de control" local fija como en la parte A de la figura 1, mediante palabras de control locales variables prealmacenadas a las que se accede a través de una contraseña o clave de sesión (parte B de la figura 1) o mediante palabras proporcionadas por el sistema de acceso condicional que se resume en la parte C de la figura 1.

La figura 1 ilustra los procesos de aleatorización.

En la presente Recomendación, se supone que se utiliza el algoritmo de aleatorización común (CSA, *common scrambling algorithm*) del grupo DVB (radiodifusión digital de señales de vídeo, *digital video broadcasting*), incluyendo la modificación para aplicaciones DSNG. Para utilizar el algoritmo se ha de firmar un acuerdo de no divulgación con el ETSI, incluido el pago de un canon no recurrente (para los detalles al respecto, acudir a www.etsi.org y hacer clic en **security algorithms and codes** bajo el epígrafe **Publication and Products**).

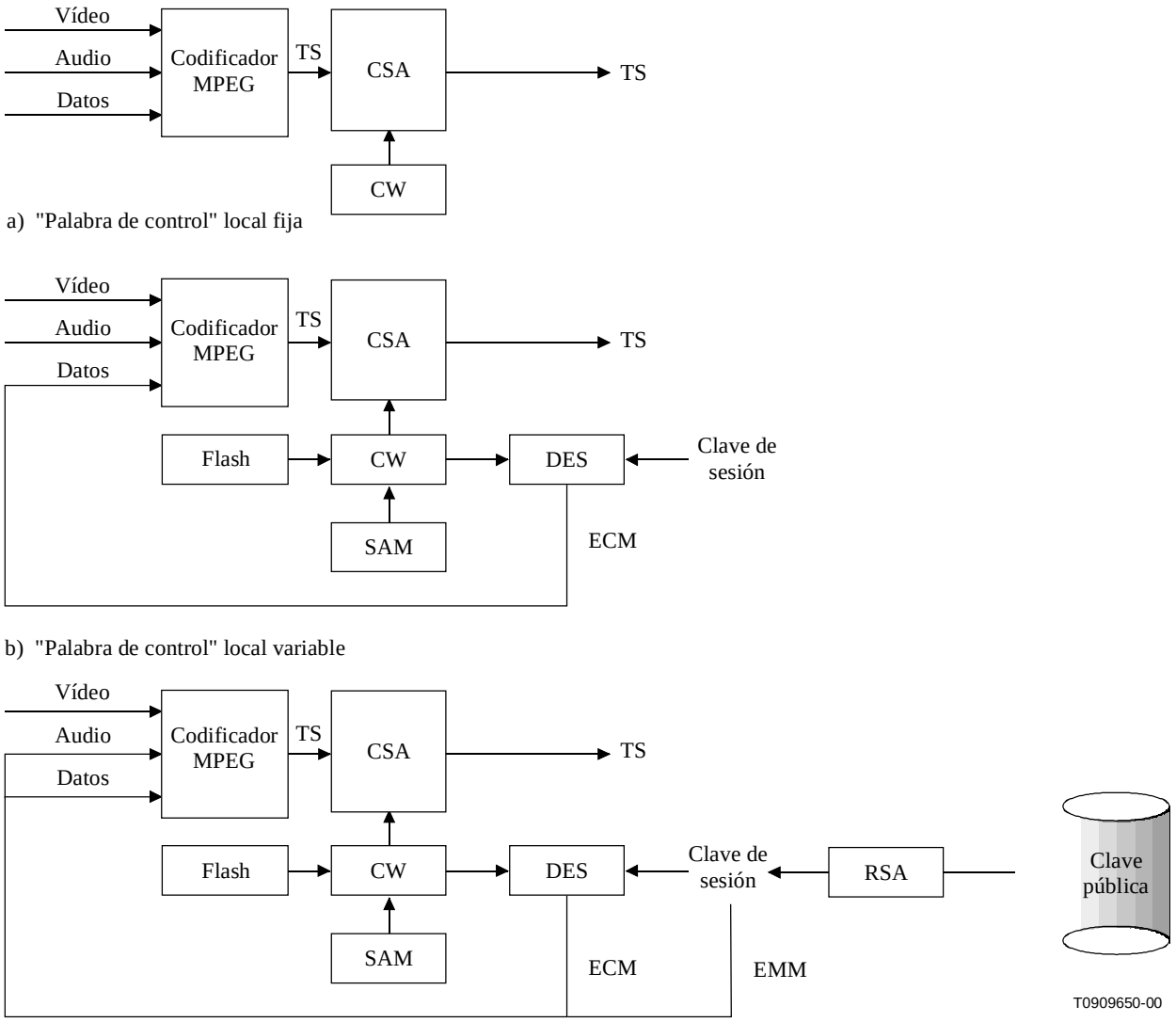


Figura 1/J.96 – Descripción general de los procesos de aleatorización/desaleatorización

Las tres implementaciones ilustradas en la figura 1 se describen en los anexos A y B.

6 Aplicación en el entorno MPEG/DVB

Aleatorización

La aleatorización es un proceso utilizado para hacer una información incomprensible a los receptores no autorizados durante la transmisión de dicha información.

El CSA utiliza claves comunes para inicializar el proceso de aleatorización/desaleatorización en cada paquete de transporte. Las claves comunes se generan a partir de las palabras de control (CW, *control words*) que son enviadas en el tren.

La aleatorización se puede hacer a nivel de transporte o a nivel de paquetes de tren elemental paquetizado (PES, *packetized elementary stream*).

Las palabras de control pueden evolucionar a lo largo del tiempo, con una duración denominada "criptoperiodo". Para sincronizar los receptores, se designan como "CW impar" o "CW par". Cada paquete aleatorizado indica, mediante los bits de "transport_scrambling_control" (control de aleatorización de transporte), si ha sido o no aleatorizado y la paridad de la CW en curso. El criptoperiodo puede variar desde unos segundos (CAS principal) hasta la duración de una transmisión completa ("palabra de control fija" para DSNG).

Acceso condicional

El sistema de acceso condicional (CAS, *conditional acces system*) consta de los elementos que permiten a los receptores autorizados obtener las palabras de control para desaleatorizar la información.

Esos elementos son normalmente los mensajes de control de título (ECM, *entitlement control messages*) y los mensajes de gestión de títulos (EMM, *entitlement management messages*) que son radiodifundidos en el tren de transporte. La sintaxis de la parte privada del ECM y el EMM depende del CAS.

El ECM contiene por lo general un criptograma de palabras de control (CW) y criterios de acceso. Su contenido varía con un periodo igual al criptoperiodo.

Para DSNG, si la CW es constante por cada transmisión, el ECM puede ser sustituido por cualquier medio fuera de banda para precisar que CW será utilizada durante toda la transmisión.

6.1 Especificaciones del MPEG y ETR 289

6.1.1 Aleatorización

El grupo de experto en imágenes en movimiento (MPEG, *moving picture experts group*) ha definido los bits de Transport_Scrambling_Control de los encabezamientos de los paquetes de transporte. El ETR 289 [3] ha especificado estos bits como se muestra en el cuadro 1.

Cuadro 1/J.96 – Valores de los bits transport_scrambling_control

Valor	Descripción
00	Sin aleatorización de cabida útil de los paquetes del TS
01	Reservado para utilización futura por el Grupo DVB
10	Paquetes del TS aleatorizados con clave par
11	Paquetes del TS aleatorizados con clave impar

NOTA – En Europa todos los CAS tienen que utilizar este algoritmo (a disposición del ETSI, que lo guarda con el compromiso de no revelarlo).

6.1.2 PSI/SI

La Organización Internacional de Normalización (ISO) ha definido un identificador de paquetes (PID, *packet identifier*) = 0x01 reservado a la tabla de acceso condicional. Su contenido es utilizado por el receptor para encontrar los PID de los EMM.

En el cuadro 2 (cuadro 2-27 en [1]) se indica la sintaxis de la tabla de acceso condicional (CAT).

Cuadro 2/J.96 – Tabla de acceso condicional

Sintaxis	N.º de bits	Mnemotécnico
CA_section() {		
table_id	**8**	**uimsbf**
section_syntax_indicator	**1**	**bslbf**
'0'	**1**	**bslbf**
reserved	**2**	**bslbf**
section_length	**12**	**uimsbf**
reserved	**18**	**bslbf**
version_number	**5**	**uimsbf**
current_next_indicator	**1**	**bslbf**
section_number	**8**	**uimsbf**
last_section_number	**8**	**uimsbf**
for (i = 0; i < N; i++) {		
descriptor()		
}		
CRC_32	**32**	**rpchof**
}		

En el cuadro 3 (cuadro 2-51 en [1]) se indica la sintaxis del descriptor de acceso condicional (CA_Descriptor).

Cuadro 3/J.96 – Descriptor de acceso condicional

Sintaxis	N.º de bits	Mnemotécnico
CA_descriptor() {		
descriptor_tag	**8**	**uimsbf**
descriptor_length	**8**	**uimsbf**
CA_system_ID	**16**	**uimsbf**
reserved	**3**	**bslbf**
CA_PID	**13**	**uimsbf**
for (i = 0; i < N; i++) {		
private_data_byte	**8**	**uimsbf**
}		
}		

La ISO ha definido la tabla de correspondencia de programas (PMT, *program map table*) en la que los receptores pueden utilizar CA_Descriptors para encontrar los PID de los ECM. Véase el cuadro 4 (cuadro 2-28 en [1]).

Cuadro 4/J.96 – Tabla de correspondencia de programas

Sintaxis	N.º de bits	Mnemotécnico
TS_program_map_section() {		
table_id	**8**	**uimsbf**
section_syntax_indicator	**1**	**bslbf**
'0'	**1**	**bslbf**
reserved	**2**	**bslbf**
section_length	**12**	**uimsbf**
program_number	**16**	**uimsbf**
reserved	**2**	**bslbf**
version_number	**5**	**uimsbf**
current_next_indicator	**1**	**bslbf**
section_number	**8**	**uimsbf**
last_section_number	**8**	**uimsbf**
reserved	**3**	**bslbf**
PCR_PID	**13**	**uimsbf**
reserved	**4**	**bslbf**
program_info_length	**12**	**uimsbf**
for (i = 0; i < N; i++) {		
descriptor()		
}		
for (i = 0; i < N1; i++) {		
stream_type	**8**	**uimsbf**
reserved	**3**	**bslbf**
elementary_PID	**13**	**uimsnf**
reserved	**4**	**bslbf**
ES_info_length	**12**	**uimsbf**
for (i = 0; i < N2; i++) {		
descriptor()		
}		
}		
CRC_32	**32**	**rpchof**
}		

En 300 468 [4] ha especificado un bit free_CA_mode (modo CA libre) en la tabla de descripción de servicio (SDT, *service description table*) y en la tabla de información de eventos (EIT, *event information table*). Ese bit se ha de fijar cuando el acceso a un componente por lo menos es controlado por un CA_System (sistema de acceso condicional) (véase 5.2.4 de [4]).

6.1.3 Mensajes de acceso condicional

La sintaxis de la tabla de mensajes de CA y los valores de Table_Id (identificador de tabla) se muestran en los cuadros 5 y 6 (cuadros 3 y 4, respectivamente, en [4]. El valor de CA_section_length (longitud de sección de CA) está limitado a 253 (tamaño de sección máximo = 256 bytes).

Cuadro 5/J.96 – Sintaxis de la tabla de mensajes CA (CMT)

Sintaxis	Nº de bits	Identificador
CA_message_section() {		
table_id	**8**	**uimsbf**
section_syntax_indicator	**1**	**bslbf**
DVB_reserved	**1**	**bslbf**
ISO_reserved	**2**	**bslbf**
CA_section_length	**12**	**uimsbf**
for (i = 0; I < N; i++) {		
CA_data_byte	**8**	**bslbf**
}		
}		

Cuadro 6/J.96 – Atribución de identificadores de tabla

Valor de table_id	Descripción
0x00 – 0x02	Especificado por el MPEG
0x03 – 0x3F	Reservado para el MPEG
0x40 – 0x72	Especificado por V2-SI
0x73 – 0x7F	Reservado para el Grupo DVB
0x80	CA_message_section, ECM
0x81	CA_message_section, ECM
0x82 – 0x8F	CA_message_section, sistema de CA privado
0x90 – 0xFE	privado
0xFF	Reservado para la ISO

6.2 Especificaciones de DSNG

Lo que sigue se basa en los cuatro modos definidos por UIT-T J.81:

– modo 0: sin aleatorización;

– modo 1: los componentes son aleatorizados mediante una sola CW fija;

– modo 2: todos los componentes del programa son aleatorizados mediante una CW única;

– modo 3: los componentes son aleatorizados mediante más de una CW.

El ETSI ha de entregar un CA_System_Id (identificador de sistema CA) con un valor comprendido entre 0x1 y 0xff (sistemas de CA normalizados) de acuerdo con [2].

En los modos 1 a 3, la aleatorización se aplicará a nivel de tren de transporte (TS).

En todos los modos, si están presentes ECM y/o EMM, deberán cumplir [3], por lo que se refiere a la longitud máxima de sección de 256 bytes, sintaxis de sección y valores de table_id (identificador de tabla).

6.2.1 Modo 0

No hay aleatorización. Los dos bits de Transport_Scrambling_Control se ponen a cero.

Pueden estar presentes una CAT y un tren de EMM si es necesario transmitir derechos a programas planificados en modo 1 a 3 (contenido pendiente de definición).

En la PMT no hay CA_descriptors (descriptores de CA). Ningún ECM en el tren.

6.2.2 Modo 1

Se fija el primer bit de Transport_Scrambling_Control. El segundo puede variar en las fronteras del evento durante la transmisión. La CW utilizada pertenece a una lista de palabras de control presente en el equipo de aleatorización y desaleatorización.

Pueden estar presentes una CAT y un tren de EMM, si es necesario.

En la PMT hay un CA_descriptor (descriptor de CA) a nivel de programa. A continuación se da un ejemplo:

Sintaxis	N.º de bits	Mnemotécnico
CA_descriptor() {		
descriptor_tag = 0x09	**8**	**uimsbf**
descriptor_length = 0x07	**8**	**uimsbf**
CA_system_ID = 0x0001 to 0x00ff (t.b.d)	**16**	**uimsbf**
reserved	**3**	**bslbf**
CA_PID = dummy value	**13**	**uimsbf**
Mode_id = 0x01	**8**	**uimsbf**
Odd_CW_index	**8**	**uimsbf**
Even_CW_index	**8**	**uimsbf**
}		

Mode_id (identificador de modo) = 0x01 indica al receptor que no necesita recibir ningún ECM (en este modo, no está presente ningún tren de ECM, CA_PID tiene un valor ficticio) y los bytes siguientes dan el CW_index (índice de CW).

Se utilizan odd_CW_index (índice de CW impar) y even_CW_index (índice de CW par) para seleccionar una CW en la lista de palabras de control (CW) almacenada en el receptor.

Cualquier cambio del valor de CW_index será señalado por un número de versión nueva en la PMT. Tratando correctamente las CW impares y pares se puede "cambiar" las CW "fijas" en las fronteras de un evento con transiciones sin discontinuidades o cambiar una lista CW en el receptor y el aleatorizador (lista actual, lista siguiente).

6.2.3 Modos 2 y 3

Se fija el primer bit de Transport_Scrambling_Control. El segundo varía durante la transmisión e indica al desaleatorizador qué CW se está utilizando (impar o par).

Pueden estar presentes una CAT y un tren de EMM, si es necesario.

En la PMT puede haber un CA_descriptor a nivel de programa, dando un ECM_pid (identificador de paquete de ECM) para todos los componentes del programa. CA_descriptors adicionales pueden estar presentes a nivel de componente. En este caso, reemplazan el valor que ha sido especificado a nivel de programa, sólo para el componente de que se trate.

Ejemplo 1: modo 2, todos los componentes son aleatorizados con la CW1 :

– bien un CA_Desc a nivel de programa con el ECM_PID_1; o

– bien un CA_Desc a nivel de componente con ECM_PID_1 para cada componente.

Ejemplo 2: modo 3, vídeo y sonido 1 aleatorizados con la CW1, sonido 2 con la CW2 y sonido 3 con la CW3:

– un CA_Desc a nivel de programa con el ECM_PID_1; y

– un CA_Desc a nivel de audio 2 con el ECM_PID_2; y

– un CA_Desc a nivel de audio 3 con el ECM_PID_3.

6.2.4 Resumen

El cuadro que sigue presenta de forma resumida los ítems presentes durante una transmisión:

Ítem	Modo 0	Modo 1	Modo 2	Modo 3
Transport_Scrambling_Control	**00**	**Constante 10 u 11**	**Alternativo 10/11**	**Alternativo 10/11**
CAT	**Opcional**	**Opcional**	**Opcional**	**Opcional**
EMM	**Opcional**	**Opcional**	**Opcional**	**Opcional**
CA_Descriptor(s) in PMT	**No**	**Sí**	**Sí**	**Sí**
ECM	**No**	**No**	**Sí**	**Sí**

ANEXO A

Implementación práctica que permite la interoperabilidad

A.1 Introducción

A.1.1 Visión general

En este anexo se proponen los mecanismos adicionales requeridos que requiere el acceso condicional para hacer posible la interoperabilidad de los equipos de DSNG de los distintos fabricantes.

Sólo el modo 1 es obligatorio (aleatorización de palabra de control fija).

A.1.2 Nomenclatura

A lo largo de este anexo, el término "aleatorizador" se refiere a los mecanismos que, de manera general, han de cumplir la especificación del algoritmo de aleatorización común (CSA).

A lo largo de este anexo, el término "módulo aleatorizador" se refiere a los súper mecanismos de aleatorización que han de cumplir la especificación del algoritmo de aleatorización común (CSA).

NOTA – Para obtener la especificación del CSA se ha de firmar un acuerdo de no divulgación con el ETSI, incluido el pago de un canon no recurrente (para los detalles al respecto, acudir a www.etsi.org y hacer clic en **Security algorithms and codes** bajo el epígrafe **Publication and Products**).

A lo largo de este anexo, el término "SAM" se refiere al módulo de autorización de aleatorización que ha de cumplir la especificación del algoritmo de aleatorización común (CSA).

A lo largo de este anexo, el término "clave de sesión" se refiere a la clave que es única y constante mientras dura la transmisión. Puede ser una CW fija utilizada para aleatorizar el tren de transporte directamente o, añadiendo un cierto grado de confusión, la clave utilizada para aleatorizar las CW cambiantes dentro de los mensajes de control del derecho a la prestación.

A lo largo de este anexo, el término "palabra de sesión" se refiere a la palabra a partir de la cual se obtiene la clave de sesión; es decir, la palabra de sesión no se utiliza directamente en el proceso de aleatorización, sino que se transforma mediante un mecanismo en una clave de sesión.

A.1.3 Requisitos de seguridad

El modelo DSNG requiere la entrada directa de una palabra de sesión en el transmisor y el receptor para controlar el acceso a la transmisión. El emisor y el receptor (o los receptores) de la transmisión comparten la palabra de sesión, de tal manera que sólo las partes pretendidas recibirán la transmisión, lo que se resume de la siguiente manera:

1) Palabra de sesión introducida en la unidad DSNG en el terreno.

2) Palabra de sesión introducida en los decoficadores de receptor integrado (IRD, *integrated receiver decoder)* de recepción.

3) Si las palabras de sesión son iguales, los IRD pueden descriptar el mensaje radiodifundido.

4) Si las palabras de sesión son diferentes, no se recibe el mensaje radiodifundido.

Los requisitos de seguridad para sistemas de contribución fija son algo diferentes del modelo DSNG. El intercambio seguro de claves de sesión es fundamental para esos sistemas, y puede conseguirse. En el caso de sistemas fijos que requieren interoperabilidad con unidades DSNG, se pueden emplear sistemas de control externo para hacer posible la transmisión de mensajes de gestión de títulos (los EMM) de manera tal que el intercambio de claves de sesión entre los sitios de transmisión y recepción se haga de manera segura. Este modelo funciona con sitios de transmisión que forman parte de la red fija, pero cuando los sitios de recepción aceptan una transmisión procedente de una unidad DSNG, el funcionamiento ha de retornar al método de entrada directa descrito más arriba.

NOTA – Para obtener la especificación del CSA se ha de firmar un acuerdo de no divulgación con el ETSI, incluido el pago de un canon no recurrente (para los detalles al respecto, acudir a www.etsi.org y hacer clic en **Security algorithms and codes** bajo el epígrafe **Publication and Products**).

A.2 Requisitos funcionales

A.2.1 Modos de funcionamiento

El aleatorizador ha de poder soportar los cuatro modos de funcionamiento siguiente:

- modo 0: sin aleatorización;
- modo 1: todos los componentes son aleatorizados mediante una CW fija;
- modo 2: todos los componentes son aleatorizados mediante una sola secuencia de palabras de control (CW). El módulo aleatorizador fija una CW a partir de la secuencia para la duración del criptoperiodo;
- modo 3: cada componente puede ser aleatorizado mediante una secuencia de palabras de control (CW) diferente como en el modo 2.

El aleatorizador deberá implementar las operaciones de súper aleatorización definidas en la especificación del algoritmo de aleatorización común (CSA). El mecanismo aleatorizador se aplicará a nivel de transporte solamente.

Para soportar los diversos modos de funcionamiento, el aleatorizador ha de poder insertar trenes de ECM en el múltiplex y esos trenes deberán estar convenientemente identificados dentro de la PMT. La utilización de trenes de EMM no tiene aplicación en los modos de funcionamiento descritos en la presente Recomendación, sin embargo, los equipos compatibles con DSNG puede utilizar esos trenes cuando se empleen en una arquitectura de red fija.

En el múltiplex para los modos 1, 2 y 3 deberá haber una tabla de acceso condicional (CAT), aunque esté vacía, ya que no estarán presentes trenes de EMM. Una vez más, los equipos compatibles con DSNG empleados dentro de un sistema de red fija que utilicen trenes de EMM deberán identificarlos convenientemente dentro de la CAT.

El aleatorizador que sólo soporte un subconjunto de los modos de funcionamiento definidos deberá hacerlo de acuerdo con una jerarquía impuesta. El aleatorizador que soporte el modo 2, deberá soportar también los modos 0 y 1. De manera similar, el aleatorizador que soporte el modo 3, deberá soportar también los modos 0, 1 y 2.

A.2.2 Modo 0

El aleatorizador ha de poder inhabilitar la operación aleatorizadora. En este modo no habrá CA_descriptor en la PMT ni tren de ECM. Los bits de Transport_Scrambling_Control de los paquetes de transporte se pondrán a "00".

A.2.3 Modo 1

A.2.3.1 Visión general

En este modo, el aleatorizador utiliza la palabra de control (CW) fija mientras dura la transmisión. El operador introducirá una palabra de sesión, que es transformada en la clave de sesión (SK, *session key*) para que la utilice el módulo aleatorizador. Los términos "palabra de sesión" y "clave de sesión" son, en este modo, sinónimos de los términos "palabra de control" y "clave común" de la especificación del algoritmo de aleatorización común (CSA), respectivamente. En la figura A.1 se da una visión general.

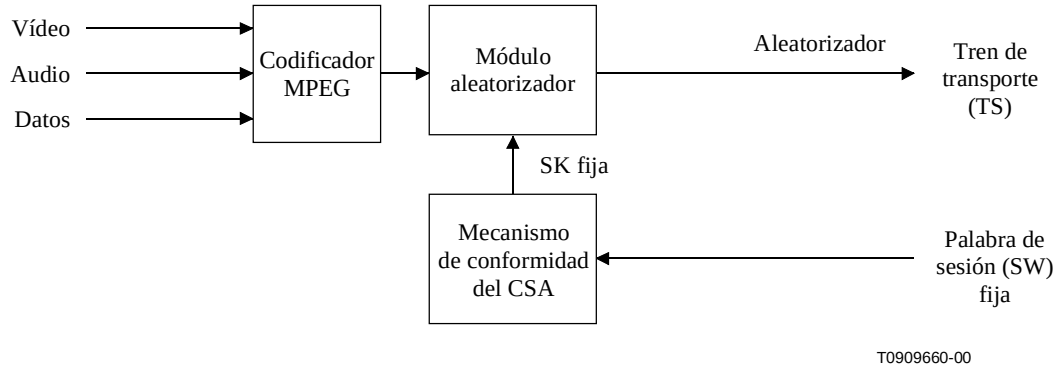


Figura A.1/J.96 – Visión general: Modo 1

La palabra de sesión (SW) es una palabra de 48 bits que el aleatorizador transforma en una clave de sesión (SK) de 64 bits utilizando el mecanismo de conformidad definido como parte de la especificación del CSA.

El aleatorizador establece primero la correspondencia entre la SW de 48 bits y la CW de 64 bits, antes de aplicar el mecanismo de conformidad CSA. En el cuadro A.1 se da la correspondencia de bytes entre la CW de 48 bits y la SW de 64 bits.

Cuadro A.1/J.96 – Correspondencia entre SW y CW fija

CW de 64 bits	SW de 48 bits
CW(1)	SW(1)
CW(2)	SW(2)
CW(3)	SW(3)
CW(4)	(Nota 1)
CW(5)	SW(4)

Cuadro A.1/J.96 – Correspondencia entre SW y CW fija *(fin)*

CW de 64 bits	SW de 48 bits
CW(6)	SW(5)
CW(7)	SW(6)
CW(8)	(Nota 2)
NOTA 1 – CW(4) es obtenida a partir de SW(1)..SW(6) por el mecanismo de conformidad del CSA. NOTA 2 – CW(8) es obtenida a partir de SW(1)..SW(6) mediante el mecanismo de conformidad del CSA.	

En este modo habrá un CA_descriptor en la PMT, presente a nivel de programa, pero no habrá tren de ECM. Se asigna un ID (identificador) de sistema CA único para identificar el modo 1.

Los bits Transport_Scrambling_Control de los paquetes de transporte deberán ponerse a "10".

La entrada manual de la SW se hará en hexadecimal, introduciendo primero los dígitos del cuarteto más significativo, es decir, de izquierda a derecha según se ve en la notación hexadecimal.

Por ejemplo, 0xA13DBC42908F, se introduciría en la secuencia siguiente: A,1,3,D,B,C,4,2,9,0,8,F.

Deberá estar prevista además la entrada a distancia de la SW, aunque la especificación de esta interfaz queda fuera del alcance de la presente Recomendación.

El aleatorizador deberá asegurar que la SK utilizada por el módulo aleatorizador no puede ser cambiada más de 10 veces en un periodo de 5 minutos y que entre cada dos cambios transcurre un mínimo de 10 segundos.

A.2.3.2 Descriptor de CA

En el cuadro A.2 se define el CA_descriptor, que debe estar presente en la PMT para soportar el modo 1.

Cuadro A.2/J.96 – Descriptor de acceso condicional: Modo 1

Sintaxis	N.º de bits	Identificador
CA_descriptor() {		
descriptor_tag	**8**	**uimsbf**
descriptor_length	**8**	**uimsbf**
CA_system_ID	**16**	**uimsbf**
Reserved	**3**	**bslbf**
CA_PID	**13**	**uimsbf**
}		

Semántica:

CA_system_ID (identificador de sistema de acceso condicional): Éste es un campo de 16 bits que indica el tipo de sistema de CA aplicable para los trenes de ECM asociados. El valor de este campo para el modo 1 es 0x2600 [2].

CA_PID (identificador de paquete de acceso condicional): Éste es un campo de 13 bits que indica el PID de los paquetes del tren de transporte que deberán contener la información de ECM. Para el modo 1, no se requiere información de ECM, por lo que este campo contendrá el valor 0x1FFF.

A.2.4 Modos 2 y 3

A.2.4.1 Visión general

En estos modos, el aleatorizador utiliza una CW variable para una transmisión determinada (modo 2), o para los componentes de una transmisión (modo 3). En la figura A.2 se da una visión general de los modos 2 y 3.

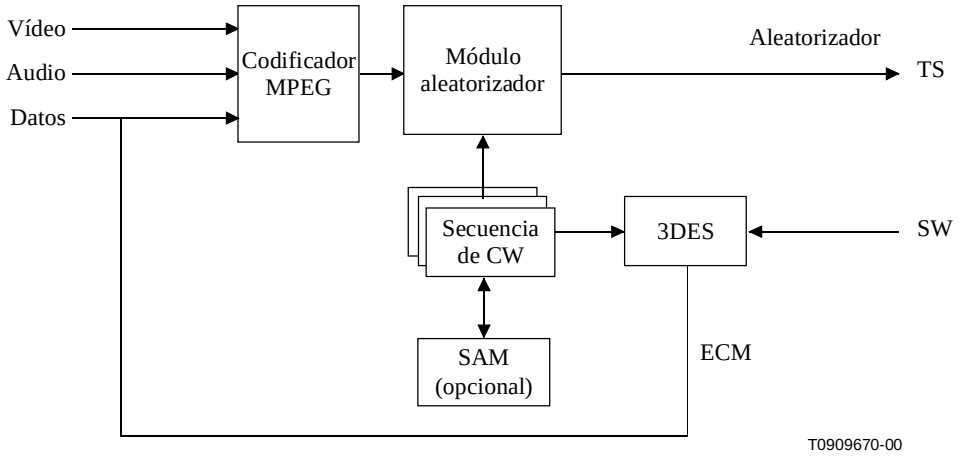


Figura A.2/J.96 – Visión general de los modos 2 y 3

Para soportar los modos 2 y 3, deben producirse por adelantado secuencias de CW que se atengan a las especificaciones del grupo DVB y almacenarlas localmente en el aleatorizador, por ejemplo, en un dispositivo de memoria FLASH (impulso). El aleatorizador fijará la CW siguiente de la secuencia de CW en el módulo aleatorizador para la duración conocida como el criptoperiodo (normalmente, algunos segundos). Las CW deberán ser criptadas y transmitidas dentro de un tren de ECM, protegido por la clave de sesión. El SAM, si está presente, sólo llevará a cabo la autenticación de las CW pero no la generación de CW.

Las CW serán criptadas utilizando la DES en el modo 3DES de EDE con ABC sin encadenamiento (ECB) y un tamaño de clave de 168 bits. Para que este algoritmo sea exportable, sólo 56 bits de la clave deberán ser la palabra de sesión dependiente del operador, mientras que los otros 112 bits deberán ser constantes.

En el modo 2 habrá un CA_descriptor en la PMT, presente a nivel de programa, que identifique el tren de ECM para la secuencia de CW. En el modo 3 habrá un CA_descriptor en la PMT, presente para cada componente, que identifique el tren de ECM para la secuencia de CW de ese componente (véase la nota). Se asigna un ID de sistema de CA único para identificar ambos modos, el 2 y el 3. Los dos modos se distinguen solamente por la posición de los CA_descriptors en la PMT como se describe más arriba.

NOTA – En el modo 3, deberá ser posible introducir una palabra de sesión separada por cada componente que requiera control del derecho a la prestación específico.

Para ambos modos, los bits Transport_Scrambling_Control de los paquetes de transporte se deben poner a "10" o a "11" dependiendo de si utiliza clave par o clave impar, respectivamente.

A.2.4.2 Criptación de la palabra de control

La clave de sesión de 168 bits utilizada para la encriptación 3DES de la CW se obtiene como sigue:

1) con una palabra de sesión de 56 bits proporcionada por el operador;

2) con un depósito de claves (KE, *key escrow*) de 112 bits;

3) concatenando **1** y **2** y utilizando los 168 bits resultantes como clave de sesión para la criptación 3DES.

SK(167..0) = [KE & SW]

Es decir, el KE aporta los bits más significativos de la SK, y la SW los bits menos significativos de la SK.

- SK(167..56) = KE(111..0)
- SK(55..0) = SW(55..0)
- Si KE = 0x00000000000000000000000000000 y SW = 0x11223344556677, SK = 0x00000000000000000000000000011223344556677.

A continuación se muestra la correspondencia entre la SK y la clave 3DES con ABC. Se señala que la SK utiliza notación científica (es decir, msb = 55, lsb = 0) mientras que la 3DES utiliza notación de la FIPS (es decir, msb = 1, lsb = 56).

Cuadro A.3/J.96 – Correspondencia entre SK y clave 3DES

	A(1..56)	**B(1..56)**	**C(1..56)**
Modo DES	E	D	E
Clave de sesión	SK(167..112)	SK(111..56)	SK(55..0)

La norma permite hasta 256 opciones de KE, de tal manera que durante una transmisión se puede utilizar un KE particular para asegurar la sesión. La opción de KE se identifica dentro del campo fixed_bits_option (opción de bits fijos) del ECM, con lo que un desealeatorizador puede seleccionar el mismo KE que ha utilizado el aleatorizador de la transmisión.

A efectos de interoperabilidad es fundamental que el aleatorizador y el desealeatorizador compartan el mismo KE en cualquier sesión determinada. La aplicación específica de las opciones de KE queda fuera del alcance de la presente. No obstante, para que sea posible una auténtica interoperabilidad, se asigna el valor de KE "00000000000000000000000000000" al campo fixed_bits_option = "0x00" (valor por defecto).

En el cuadro A.4 se muestra la correspondencia entre la CW y el bloque de cifras de 3DES. Se señala que la CW utiliza notación científica (es decir, msb = 63, lsb = 0) mientras que 3DES utiliza notación de la FIPS (es decir, msb = 1, lsb = 64).

Cuadro A.4/J.96 – Correspondencia entre CW y bloque de cifras de 3DES

3DES(1) <= CW(63)	3DES(33) <= CW(31)
3DES(2) <= CW(62)	3DES(34) <= CW(30)
3DES(3) <= CW(61)	3DES(35) <= CW(29)
3DES(4) <= CW(60)	3DES(36) <= CW(28)
3DES(5) <= CW(59)	3DES(37) <= CW(27)
3DES(6) <= CW(58)	3DES(38) <= CW(26)
3DES(7) <= CW(57)	3DES(39) <= CW(25)
3DES(8) <= CW(56)	3DES(40) <= CW(24)
3DES(9) <= CW(55)	3DES(41) <= CW(23)
3DES(10) <= CW(54)	3DES(42) <= CW(22)
3DES(11) <= CW(53)	3DES(43) <= CW(21)

Cuadro A.4/J.96 – Correspondencia entre CW y bloque de cifras de 3DES *(fin)*

3DES(12) <= CW(52)	3DES(44) <= CW(20)
3DES(13) <= CW(51)	3DES(45) <= CW(19)
3DES(14) <= CW(50)	3DES(46) <= CW(18)
3DES(15) <= CW(49)	3DES(47) <= CW(17)
3DES(16) <= CW(48)	3DES(48) <= CW(16)
3DES(17) <= CW(47)	3DES(49) <= CW(15)
3DES(18) <= CW(46)	3DES(50) <= CW(14)
3DES(19) <= CW(45)	3DES(51) <= CW(13)
3DES(20) <= CW(44)	3DES(52) <= CW(12)
3DES(21) <= CW(43)	3DES(53) <= CW(11)
3DES(22) <= CW(42)	3DES(54) <= CW(10)
3DES(23) <= CW(41)	3DES(55) <= CW(9)
3DES(24) <= CW(40)	3DES(56) <= CW(8)
3DES(25) <= CW(39)	3DES(57) <= CW(7)
3DES(26) <= CW(38)	3DES(58) <= CW(6)
3DES(27) <= CW(37)	3DES(59) <= CW(5)
3DES(28) <= CW(36)	3DES(60) <= CW(4)
3DES(29) <= CW(35)	3DES(61) <= CW(3)
3DES(30) <= CW(34)	3DES(62) <= CW(2)
3DES(31) <= CW(33)	3DES(63) <= CW(1)
3DES(32) <= CW(32)	3DES(64) <= CW(0)

A.2.4.3 Mensaje de control de título

El ECM tiene el aspecto de una sección definida por UIT-T H.222.0 | ISO/CEI 13818-1 [1]. En el cuadro A.5 se da el formato de mensaje de un ECM como parte de esta Recomendación.

Cuadro A.5/J.96 – Sección mensaje de control del derecho a la prestación

Sintaxis	N.º de bits	Identificador
entitlement_control_message_section() {		
table_id	**8**	**uimsbf**
section_syntax_indicator	**1**	**bslbf**
DVB_reserved	**1**	**bslbf**
ISO_reserved	**2**	**bslbf**
CA_section_length	**12**	**uimsbf**
fixed_bits_option	**8**	**uimsbf**
even_cw_encrypted	**64**	**bslbf**
odd_cw_encrypted	**64**	**bslbf**
for (i = 0; i < N; i++) {		
CA_data_byte	**8**	**bslbf**
}		
}		

Semántica

table_id (identificador de tabla): Este campo puede tomar el valor de 0x80 ó 0x81 para identificarla como una sección del ECM. Cuando el valor del table_id cambia, indica un cambio del contenido del ECM.

fixed_bits_option (opción bits fijos): Este campo identifica la opción depósito de claves del conjunto de bits fijos, cuyo valor por defecto es "0x00".

even_cw_encrypted (palabra de control par criptada): Se trata de la CW par criptada de acuerdo con 3DES.

odd_cw_encrypted (palabra de control impar criptada): Se trata de la CW impar criptada de acuerdo con 3DES.

La temporización de la ejecución de un ECM nuevo equivale a establecer un equilibrio entre fiabilidad y seguridad. Si el mensaje se ejecuta con suficiente antelación con respecto al criptoperiodo al que está asociado, el sistema resulta más fiable. Para alcanzar un equilibrio adecuado, la cadencia de repetición de los ECM debe ser de 10 por segundo y la ejecución no debe ser impuesta sino que ha de estar sujeta a limitaciones con un criptoperiodo de 500 ms como mínimo. Así pues, el ECM relativo a un criptoperiodo nuevo debe ejecutarse con un adelanto de al menos el criptoperiodo mínimo.

La ejecución de un ECM nuevo debe ser tal que el receptor pueda procesarlo a tiempo para el próximo criptoperiodo. Si se prima la fiabilidad con respecto a la seguridad, el ECM de un determinado criptoperiodo puede ejecutarse durante todo el criptoperiodo previo.

A.2.4.4 Descriptor de CA

En el cuadro A.6 se define el CA_descriptor, que debe estar presente en la PMT para soportar los modos 2 y 3.

Cuadro A.6/J.96 – Descriptor de acceso condicional: Modos 2 y 3

Sintaxis	N.º de bits	Identificador
CA_descriptor() {		
descriptor_tag	**8**	**uimsbf**
descriptor_length	**8**	**uimsbf**
CA_system_ID	**16**	**uimsbf**
Reserved	**3**	**bslbf**
CA_PID	**13**	**uimsbf**
}		

Semántica

CA_system_ID (identificador de sistema de CA): Este campo de 16 bits indica el tipo de sistema de CA aplicable a los trenes de ECM asociados. El valor de este campo para los modos 2 y 3 es 0x2601. Un CA_system_ID identifica ambos modos; los modos se distinguen por la ubicación del o de los CA_descriptor(s) dentro de la PMT.

CA_PID (identificador de paquete de CA): Este campo de 13 bits indica el PID de los paquetes del tren de transporte que contendrán la información del ECM.

APÉNDICE I

Descripción general de un sistema de acceso condicional abierto basado en OKAPI

El acceso al control de la secuencia de aleatorización se asegura utilizando la infraestructura de clave pública (PKI, *public key infrastructure*), que es un sistema abierto para aplicaciones criptográficas.

I.1 Criptosistemas de claves públicas

La noción de criptografía de claves públicas fue introducida por Diffie y Hellman. Los sistemas de claves públicas difieren de los sistemas convencionales en que ya no hay un secreto único compartido por un par de usuarios. Más bien, cada usuario tiene su propio material de clave. Además, el material de clave de cada usuario se divide en dos componentes, uno privado y otro público. El componente público genera una transformación pública *E*, y el componente privado genera una transformación privada *D*. En analogía con el caso convencional, *E* y *D* podrían denominarse funciones de criptación y descriptación respectivamente. Esa denominación, no obstante, resulta imprecisa: en un sistema dado se puede tener $D(E(M)) = M$, $E(D(M)) = M$, o ambas cosas.

Un requisito consiste en que *E* debe ser una función trampilla unidireccional. Lo de unidireccional se refiere al hecho de que *E* ha de ser fácil de calcular a partir del material de claves públicas pero difícil de transponer a menos que se posea la *D* correspondiente, o de manera equivalente, el material de claves privadas que genera *D*. El componente privado produce así una trampilla que hace que el problema de transponer *E* parezca difícil desde el punto de vista del criptoanalista, pero fácil para el poseedor (único legitimado) de *D*. La trampilla puede ser por ejemplo, el conocimiento de la factorización de un entero.

Se señala que las funciones trampilla empleadas como transformación pública en los sistemas de claves públicas sólo son una subclase de la clase de funciones unidireccionales.

Se señala además que la dicotomía público/privado de *E* y *D* en los sistemas públicos no tiene analogía en un criptosistema convencional. En este último, tanto E_k como D_k están parametrizadas mediante una clave única *k*. Por ello, si E_k es conocida, se puede suponer que *K* ha quedado comprometida, por lo que puede suponerse que también D_k es conocida, o viceversa. Por ejemplo, en DES, tanto *E* como *D* se calculan básicamente mediante el mismo algoritmo público a partir de una clave común; de esa manera, *E* y *D* son, ambas, conocidas o desconocidas, dependiendo de si la clave ha quedado o no comprometida.

Los criptosistemas de claves públicas ofrecen por lo menos la misma seguridad que las claves secretas. Su principal inconveniente es el tiempo de computación, unas mil veces superior. Pero esos sistemas presentan una ventaja importante: la fácil aplicación del sistema de gestión de claves.

Con independencia de si se utiliza un criptosistema de claves públicas o convencional, es preciso que los usuarios puedan obtener las claves de otros usuarios. Esto crea, de alguna manera, un problema de tipo circular: para comunicarse de forma segura por canales inseguros, los usuarios deben intercambiar primero información de claves. Si no hay alternativa a los canales inseguros, el intercambio seguro de información de claves presenta básicamente el mismo problema de seguridad que la comunicación segura subsiguiente.

En los criptosistemas convencionales, es posible romper ese círculo vicioso de varias maneras. Puede suponerse, por ejemplo, que dos usuarios tienen la capacidad de comunicar por un canal seguro suplementario, tal como un servicio de correo. En este caso, ocurre a menudo que el canal seguro resulte costoso, sea inadecuado, de anchura de banda baja y lento; además, el uso del correo no se puede considerar verdaderamente seguro. Una alternativa consistiría en que los dos usuarios intercambiaran información de claves a través de una autoridad central. Pero el recurso a una autoridad central tiene varios inconvenientes.

En los sistemas de claves públicas, el problema de la gestión de las claves es más sencillo debido al carácter público del material de claves intercambiado entre usuarios, o entre un usuario y una autoridad central. Además, las alternativas al canal inseguro pueden ser más sencillas; por ejemplo, podría ser suficiente un sistema de correo físico, sobre todo si se envía información redundante a través del canal (electrónico) inseguro. De todos modos, la manera más eficaz de gestionar las claves en un criptosistema asimétrico es mediante un esquema de certificación.

I.2 Tecnología de certificados

Una de las primeras cuestiones que se plantean cuando se diseña un protocolo basado en claves públicas es la de su arquitectura de certificados.

En el IETF una nueva tecnología de certificados, la SPKI, ha sido diseñada recientemente.

Los certificados SPKI son certificados de autorización centrados en la *clave*. No establecen ninguna vinculación entre un nombre y una clave, sino que, por el contrario, expresan directamente una delegación de autorización en una clave pública. En la terminología SPKI, las claves públicas se denominan "principales". Un principal es una entidad que puede manifestar algún tipo de autoridad firmando y/o descifrando alguna información. Un principal actúa además como nombre único universal por sí mismo, pero para simplificar y reducir el volumen de datos procesados, se acepta también una porción troceada de forma segura del principal como identificador único.

Mientras que la SPKI también soporte certificados de identidad, el OKAPI sólo utiliza los certificados de autoridad. Los certificados de autoridad de la SPKI son expedidos inicialmente por la entidad verificadora. La autoridad delegada exacta se puede precisar fácilmente con rótulos significativos de texto libre definidos por el verificador.

Para dar al sistema un cierto grado de flexibilidad, la autoridad delegada en un principal puede ser delegada nuevamente por éste en otro principal. Este mecanismo se facilita añadiendo el campo "propagación" al certificado original. Se considera que los certificados SPKI no son únicos (en el sentido de que contienen toda la información que necesitan todas las entidades), y en teoría se tiene que expedir un certificado diferente para abarcar cada una de las autoridades delegadas.

Cuando una entidad alegue ante un verificador estar investida de cierta autoridad, deberá aportar todos los certificados que el verificador necesite. También es preciso que la entidad alegadora ordene esos certificados de tal manera que si uno de ellos necesita que otro certificado esté validado, este último haya sido ya procesado. Al final, el verificador reducirá la cadena de certificados a un certificado del tipo:

(Expedidor = el mismo, Sujeto = entidad alegadora, Autoridad = X, alguna limitación de tiempo).

SPKI introduce dos nuevas metodologías para tratar el tema de la revocación de certificados: la verificación en línea[1] y el certificado de revalidación de certificado (CRC, *certificate revalidation certificate*). En la primera, el verificador está obligado a ponerse en contacto con el expedidor (o una tercera entidad) cada vez que el certificado ha de ser verificado. En la segunda, la entidad alegadora está obligada a ponerse en contacto con el expedidor (o una tercera entidad) para obtener un CRC, y reenviar a continuación el CRC y el certificado original al verificador. Naturalmente, el CRC sólo es válido durante un periodo de tiempo determinado.

OKAPI decidió utilizar el método de revalidación porque tiene las ventajas siguientes:

- No es necesario publicar largas listas de certificados de revalidación (CRL, *certificate revalidation list*).
- No hace falta ponerse en contacto con el expedidor para cada verificación. Una vez obtenido un CRC, se puede utilizar hasta que concluya su periodo de validez.

---

[1] Revalidación de una sola vez en terminología de SPKI.

- Es fácil ajustar el momento en que entra en vigor el certificado de revalidación.
- La expedición de un certificado de revalidación de certificado se puede controlar de manera estricta. Sólo se ha de proporcionar al propietario principal del certificado original.

SPKI hizo un planteamiento a base de Internet del problema de la representación de datos. Los certificados SPKI se representan mediante expresiones S canónicas [4]. Las expresiones S son sencillas, fáciles de interpretar y (hasta cierto punto) legibles por las personas. Además suponen una tara muy pequeña con respecto a los datos reales que contienen. En el proyecto SPKI del IETF se dice que "*Una expresión S canónica es aquella que contiene cadenas binarias de bytes cada una de las cuales tiene una longitud y una puntuación "() []" dadas para las listas constitutivas. La longitud de una cadena de bytes es un número decimal ASCII no negativo, sin dígitos "0" delanteros, terminada por ":". Además se requiere, según dicho proyecto, que no haya listas vacías y que el primer elemento de la lista sea una cadena de bytes (definida más abajo). Esta forma es, indica por último, la representación única de una expresión S que se utiliza como entrada en todas las funciones de troceado y firma*." Naturalmente, las expresiones S se pueden utilizar también a efectos de almacenamiento y transmisión. Para ayudar al lector a comprender las expresiones S, e ilustrar la sencillez de las mismas, a continuación se dan algunos ejemplos de S canónicas (entre comillas):

- "(10:no antes de 19:1998-01-19_17:00:00)"
- "(11:saludo)"
- "(4:esta(2:es(1:a(5:válida)(12:expresión-s))))"

I.3 Funcionamiento práctico con OKAPI

I.3.1 Introducción

Hay dos clases de sitios:

– El centro de gestión de la red, que incluye un dispositivo de control y un dispositivo de gestión.

– Cada sitio de comunicación, que incluye uno o varios dispositivos de acceso condicional.

El centro de gestión de la red es único para cada red. Se encarga de la gestión de los recursos de la misma, de la atribución de canales disponibles [se propone un enlace directo entre la planificación (TPP) y la gestión del CAS] y de la sincronización entre transmisores y receptores. El NMC podría ampliar fácilmente sus responsabilidades a nuevos servicios, tales como los de identificación mediante marcas de agua.

Hay varios sitios de comunicación. Cada uno de ellos podría transmitir y/o recibir, al mismo tiempo, uno o más programas de televisión aleatorizados. En cada uno de esos sitios hay por lo menos un dispositivo de acceso condicional que gestiona varios transmisores y varios receptores.

Cabe considerar una tercera clase de sitio. Un sistema que requiere una autoridad de certificación para la personalización de las tarjetas inteligentes. Por motivos de seguridad, este sistema especializado fuera de línea podría situarse fuera del NMC.

Las características principales del sistema son:

– la gestión centralizada de los intercambios de programas de televisión;

– la capacidad de seleccionar/autorizar receptores muy rápidamente, casi en tiempo real;

– una interfaz hombre-máquina sencilla en el centro de gestión de la red y en los sitios de comunicación;

– no es necesaria la conexión permanente entre el centro de gestión de la red y los sitios de comunicación;

– un grado de protección muy alto frente a la piratería de los programas de televisión transmitidos vía redes abiertas, por ejemplo, por satélite;

– una amplia gama de oportunidades de nuevos servicios cuya seguridad se basa en las características del CAS;
– una serie de modos que permiten un alto nivel de protección, incluso con medios limitados en el sitio.

Por otra parte, los sitios de comunicación no conectados directamente con el centro de gestión de la red pueden transmitir y/o recibir, de todos modos, programas de televisión aleatorizados.

En la figura I.1 y en las cláusulas subsiguientes, la expresión centro de gestión de la red se abrevia normalmente a NMC, y la expresión dispositivo de acceso condicional, a CAD (*conditional access devices*).

La utilización de una tarjeta inteligente en el centro de gestión de la red es facultativa.

Para transmitir y recibir en cada sitio de comunicación se utilizan una o más tarjetas inteligentes.

Es preciso hacer una importante distinción aclaratoria entre transmisiones y programas.

Una transmisión se caracteriza por:
– un satélite u otro canal de comunicación;
– un sitio de comunicación utilizado como transmisor;
– uno o más sitios de comunicación utilizados como receptor(es);
– una fecha y una hora de comienzo y terminación;
– un conjunto de componentes de televisión que incluyen sonido(s), visión y datos.

Un programa se caracteriza por:
– un nombre del programa;
– una o más transmisiones;
– una clave de autorización;
– uno o más criterios de acceso.

En consecuencia, una transmisión se puede utilizar para radiodifundir uno o más programas y un programa se puede transmitir mediante una o más transmisiones.

Se consideran tres comportamientos diferentes:
– el del centro de gestión de la red;
– el del transmisor de un sitio de comunicación cuando utiliza uno de sus codificadores;
– el del receptor de un sitio de comunicación cuando utiliza uno de sus decodificadores.

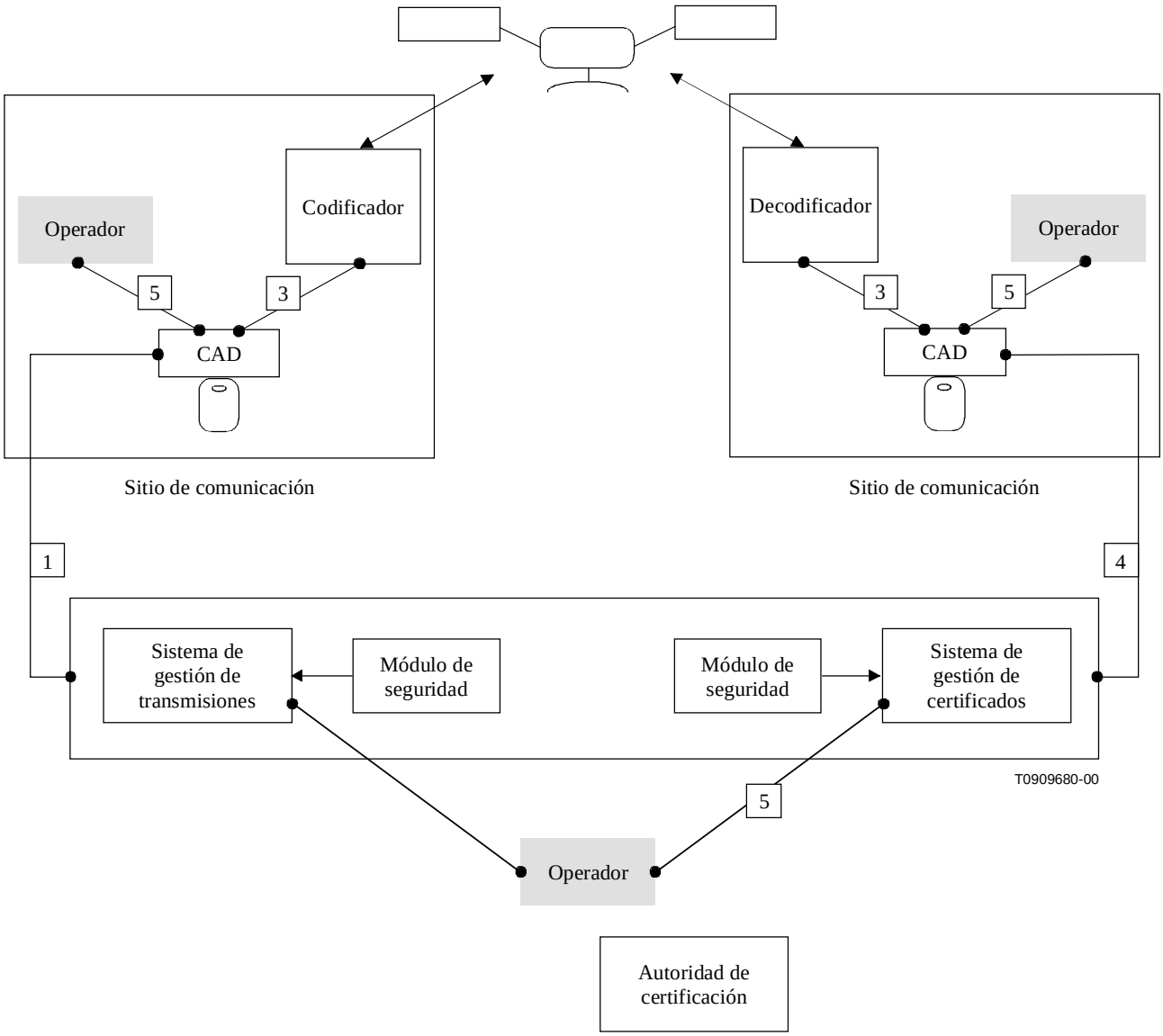


Figura I.1/J.96 – Arquitectura de la red

I.3.2 Funcionalidad del centro de gestión de la red

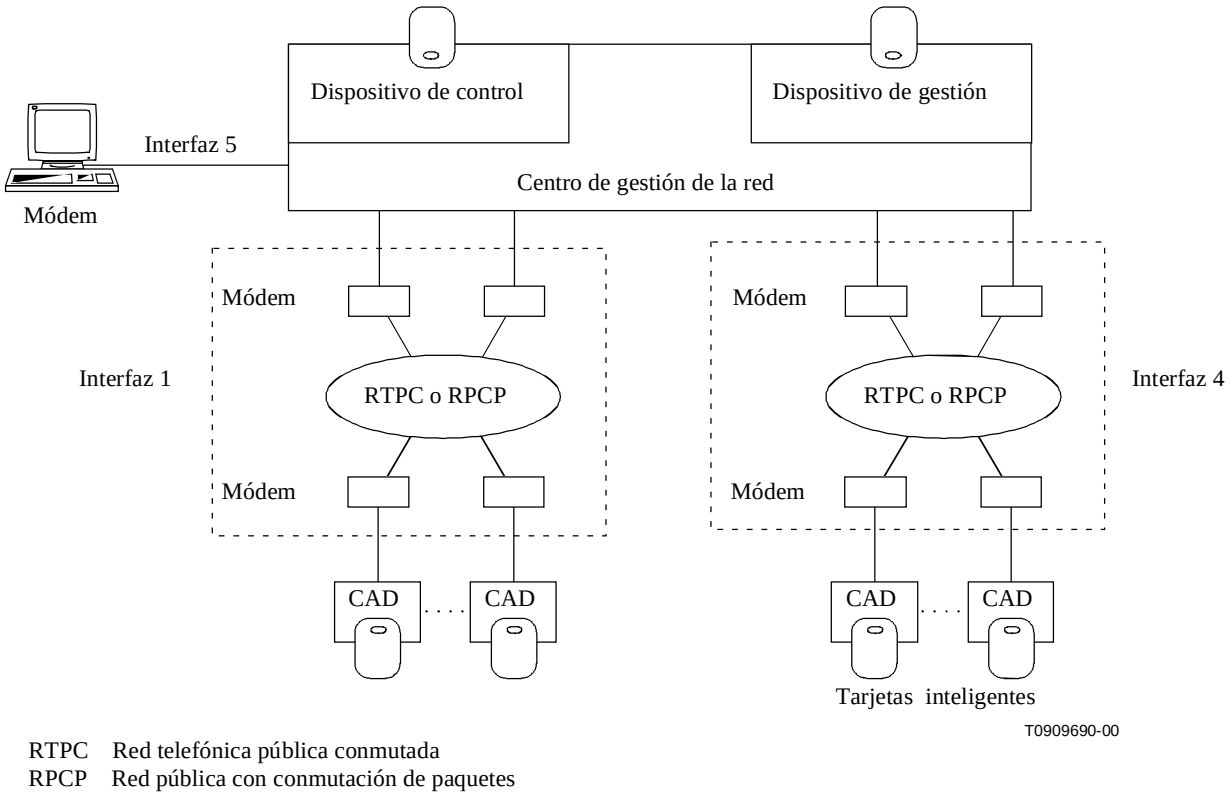
Corresponde al NMC asegurar que el transmisor y todos los receptores autorizados reciben la clave de autorización correcta y los justificantes del derecho de acceso correctos antes de la transmisión del programa. También es de la responsabilidad del NMC actualizar periódicamente las claves de autorización por motivos de seguridad. Para hacer esto, el NMC elabora y envía los ECM y los EMM.

El NMC también garantiza la supervisión de todas las tarjetas inteligentes correspondientes, al desempeñar su cometido de TTP.

El NMC gestiona una guía de claves pública; en el futuro cabría considerar soluciones tales como UIT-T X.500 | ISO/CEI 9594-1.

Al NMC incumbe decidir respecto al escenario aplicado (procedimiento bidireccional, procedimiento unidireccional, testigos y palabra de control local).

La figura I.2 da la representación esquemática de un NMC.



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

Figura I.2/J.96 – Centro de gestión de la red (NMC)

I.3.2.1 Generación de ECM

El NMC ha de generar los ECM. A tal fin, crea palabras de control, las cifra utilizando en su caso una tarjeta inteligente y genera los ECM correspondientes. Cada ECM se protege mediante una suma de control criptográfica calculada por medios criptográficos. Durante la transmisión, se envía periódicamente un ECM nuevo. Los ECM son enviados al CAD del transmisor a través de la interfaz 1.

Una manera inmediata de implementar el esquema consiste en crear periódicamente ECM y enviarlos "en línea" al CAD del transmisor. Esa implementación supone que durante toda la transmisión el NMC permanece conectado al CAD del transmisor. Además, el NMC, que dirige todos los transmisores, habrá de generar varios conjuntos de mensajes ECM (tantos como canales haya en funcionamiento en cada momento) y enviarlos al mismo tiempo.

La utilización de ficheros cíclicos de ECM elimina esa constricción. Dichos ficheros contienen tantos ECM como se necesiten para la duración estimada de la transmisión. Si la transmisión dura más de lo previsto, el último ECM debe construirse de manera que vaya seguido del primer ECM del mismo fichero, para poder circular a través del mismo conjunto de mensajes ECM.

El NMC podría generar un grupo de ficheros cíclicos de ECM antes de que se detecte necesidad alguna y enviarlos al CAD por adelantado, o en el último momento antes de una transmisión.

El envío de varios ficheros cíclicos de ECM por adelantado al CAD hará que éste quede preparado para funcionar casi de inmediato, incluso en el caso de transmisiones de televisión impulsivas (planificadas en el último minuto) o en el caso de un transmisor transportable aislado.

El aspecto más innovador del CAS OKAPI está en los EMM para los que se explotan plenamente las facilidades de la PKI. De acuerdo con DSNG219, debería considerarse la protección de la transmisión mediante un EMM único sin tener en cuenta ningún ECM.

Hay que insistir en que el sistema propuesto ganaría en eficacia vinculando estrechamente la planificación con la protección de la transmisión.

I.3.2.2 Generación de EMM

El NMC tiene que generar también los EMM para distribuir claves y derechos a la prestación de las tarjetas inteligentes especificadas.

Uno de los EMM es para el transmisor: permitirá al CAD del transmisor (con la ayuda de su tarjeta inteligente) descifrar la palabra de control de todos los ECM antes referidos.

Los demás EMM son para los receptores. Permitirán a las tarjetas inteligentes autorizadas de los CAD de los receptores descifrar la palabra de control de los ECM anteriores. Hay dos maneras diferentes de transmitir los EMM:

– directamente, utilizando la interfaz 4 (vía teléfono, X.25, VSAT, conexión directa) con el CAD correspondiente de cada receptor;
– mediante su radiodifusión a todos los receptores vía codificador del transmisor y canal de satélite.

Los EMM pueden ser generados por adelantado y almacenados localmente o a distancia en las tarjetas inteligentes. Esto es algo que corresponde al escenario de los testigos.

I.3.2.3 Supervisión de tarjetas inteligentes y certificados asociados

El NMC gestiona el contenido de cada tarjeta inteligente, con el soporte en su caso de una autoridad externa, si el CA está deslocalizado.

Si se utiliza pago por visión sin previo aviso, el NMC supervisa las compras de tarjetas inteligentes.

El NMC tiene una base de datos para saber el contenido de todas las tarjetas inteligentes y disponer de información detallada sobre todos los CAD (ubicación, clave pública de las tarjetas inteligentes, etc.). La clave privada asociada a cada tarjeta inteligente PODRÍA ser conocida a este nivel.

Si en una tarjeta inteligente no queda más memoria, el NMC tiene que despejarla eliminando las claves obsoletas y los derechos a prestación caducados.

I.3.2.4 Expedición de tarjetas inteligentes

El NMC genera escenarios de expedición (descripción de todas las claves y todos los parámetros que se han de inscribir en cada tarjeta) a petición de su operador. Esos escenarios se envían a un dispositivo expedidor, que inicializa las tarjetas. El dispositivo expedidor devuelve al NMC un conjunto de tarjetas y un fichero informe. Este último se utiliza para actualizar la base de datos del NMC. Una autoridad de certificación garantiza la expedición de las tarjetas inteligentes. Corresponde a un computador personal especializado, asegurado físicamente. La autoridad de certificación PODRÍA estar situada en el NMC.

I.3.2.5 Interfaz hombre-máquina

La interfaz hombre-máquina deberá constar de:

– una petición de transmisión;
– una descripción de todas las referencias de transmisión descritas más arriba;
– una consulta y una actualización de la base de datos;
– una supervisión periódica de las tarjetas configuradas para visión por pago sin previo aviso;
– un diario de las alarmas (una tarjeta inteligente se ha agotado o está fuera de servicio, hay problema de conexión con un CAD, etc.).

En el NMC se tendrá que desarrollar la interfaz hombre-máquina (MMI, *man-machine interface*) con las personas afectadas. Para identificar rápidamente cualquier problema, deberán estar accesibles varios registros cronológicos.

I.3.3 Implementación de los CAD

La actuación del CAD del transmisor consiste en:

– mantener el enlace con el NMC (por ejemplo, verificación del funcionamiento del servidor del NMC enviándole señales periódicas);

– autenticar (primer nivel) el emisor de los EMM;

– transmitir el (los) EMM pertinente(s) a su(s) tarjeta(s) inteligente(s) para almacenar nueva(s) clave(s) y nuevo(s) derecho(s) a la prestación;

– transmitir periódicamente un ECM a su tarjeta inteligente para obtener como respuesta la CW correspondiente que habrá que dar al codificador para que aleatorice el programa de televisión;

– transmitir periódicamente al codificador un ECM para que sea radiodifundido a los decodificadores;

– si es necesario, transmitir también los EMM al codificador para que sean enviados a los decodificadores.

La actuación del CAD del receptor consiste en:

– mantener el enlace con el NMC (por ejemplo, verificación del funcionamiento del servidor del NMC enviándole señales periódicas);

– autenticar (primer nivel) el emisor de los EMM;

– obtener los EMM pertinentes a partir del decodificador o del enlace directo con el NMC y transmitirlos a su(s) tarjeta(s) inteligente(s) para almacenar nueva(s) clave(s) y nuevo(s) derecho(s) a la prestación;

– obtener periódicamente los ECM a partir del decodificador y enviarlos a su tarjeta inteligente para obtener como respuesta las palabras de control correspondientes, y devolver al decodificador esas palabras de control.

I.3.3.1 Caso de estación de transmisor aislado

"Aislado" significa que no hay ninguna conexión entre el CAD del transmisor y el NMC en el momento de la transmisión. Tal podría ser el caso, por ejemplo, de una unidad especial informadora de noticias cuya estación del transmisor es sumamente móvil. Cualquier transmisor deberá poder funcionar de este modo en caso de emergencia.

En este contexto, todavía es posible asegurar la transmisión de programas de televisión. Para ello, el CAD del transmisor ha de ser cargado por adelantado (utilizando un disquete, una tarjeta de memoria de la PCMCIA o la propia tarjeta inteligente) con un fichero cíclico de ECM. Lo único que tiene que hacer entonces el operador del transmisor es seleccionar el fichero cíclico de ECM apropiado.

En el caso de una transmisión en la que intervengan estaciones conectadas y estaciones aisladas, deberá aplicarse el escenario de testigos. Dicho escenario está siendo patentado.

Este modo es muy apropiado cuando se utiliza el pago por visión sin aviso previo. Las tarjetas inteligentes de los receptores almacenarán automáticamente el número del programa (con el acuerdo del operador del receptor). El NMC comprobará más tarde el contenido de las tarjetas.

I.3.4 Implementación de la interfaz 1

La interfaz 1 conecta el NMC con el CAD del transmisor. La inicializa el NMC.

Se intercambian los mensajes y las instrucciones siguientes:

– Mensajes ECM: La implementación recomendada consiste en un fichero cíclico de ECM que computa el NMC y lo transmite por adelantado al CAD del transmisor junto con la referencia del programa de televisión que utilizará esos ECM. Otra implementación consistiría en enviar un ECM "en línea" cada 8,2 segundos.

– Mensajes EMM: La implementación recomendada consiste en un fichero de EMM que computa el NMC y lo transmite por adelantado al CAD del transmisor. Es posible otra implementación utilizando la interfaz 4 para el direccionamiento de cada receptor.

La interfaz 2 se puede implementar en la red telefónica pública conmutada, o en la red pública con conmutación de paquetes, o incluso en un disquete o una tarjeta de memoria de PCMCIA.

I.3.5 Implementación de la interfaz 4

La interfaz 4 conecta el NMC con una tarjeta inteligente, a través de un CAD. La inicializa el CAD.

Se utiliza sobre todo para la supervisión de las tarjetas inteligentes conectadas al CAD. La vigilancia de las tarjetas consiste en:

– comprobar el pago por visión sin aviso previo almacenado en la tarjeta;

– despejar la memoria de sólo lectura, eléctricamente programable y borrable (EEPROM, *electrically erasable programmable read-only memory*) de la tarjeta. Si en una tarjeta ya no queda memoria, el NMC elimina las autorizaciones antiguas.

Además, como se ha indicado más arriba, se puede utilizar la interfaz 4 para enviar mensajes EMM.

La interfaz 4 se puede implementar utilizando la red telefónica pública conmutada o la red pública con conmutación de paquetes.

La información de entrada en el sistema es almacenada en la tarjeta inteligente en un bloque de facilidades ad hoc. La llamada la inicia el CAD tras recibir un EMM para la activación del módem.

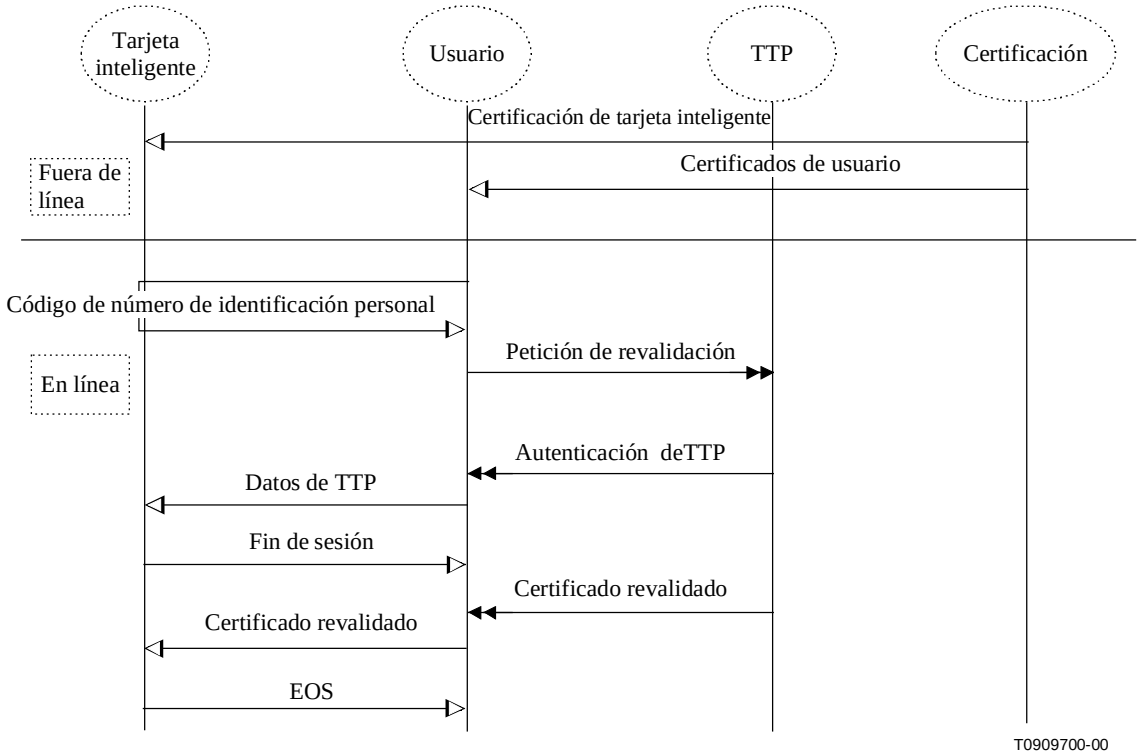
I.3.6 Principales protocolos bidireccionales

Se pueden presentar protocolos correspondientes a cada modo. En lo que sigue se expone el diagrama de la secuencia de los protocolos más importantes, considerando que se dispone de un canal de datos de baja velocidad binaria bidireccional entre el dispositivo de gestión y los sitios de comunicación. Esos protocolos preparan el camino para la realización de una gestión más fácil, así como la prestación de una amplia gama de servicios nuevos, y una política de recuperación más sencilla.

I.3.6.1 Revalidación de certificados

Para facilitar, entre otras cosas, la inclusión de un usuario en una lista de usuarios sospechosos, el controlador deberá revalidar periódicamente los certificados en las tarjetas inteligentes de los sitios de comunicación. Mientras la gestión no es de la competencia exclusiva del NMC, esta fase es mucho menos importante. La base de datos de claves públicas del TTP (controlador) es la misma que para la gestión.

En la figura I.3, el TTP representa UN cometido del controlador. El usuario es responsable de la tarjeta inteligente (el que conoce el código de número de identificación personal) en el sitio de comunicación.



Las flechas negras dobles representan los mensajes; las flechas blancas simples representan flujos de datos.

Figura I.3/J.96 – Diagrama de la secuencia de revalidación de certificados

Para otros servicios que compartan la seguridad del CAS, se podrían introducir otros TTP. En Internet están apareciendo ahora servidores de certificados de SPKI que se pueden utilizar en el comercio electrónico, las redes privadas virtuales, etc. Para ello es necesaria una certificación recíproca entre tercera parte confiable (TTP, *trusted third part*) y que se inicie de este modo con el acuerdo del NMC, con lo que se evita cualquier deterioro de la seguridad.

I.3.6.2 Petición de justificante de títulos

En la figura I.4 se muestran los mensajes en el caso de canal bidireccional entre el NMC y los sitios de comunicación. Las notaciones son las mismas que en la cláusula anterior.

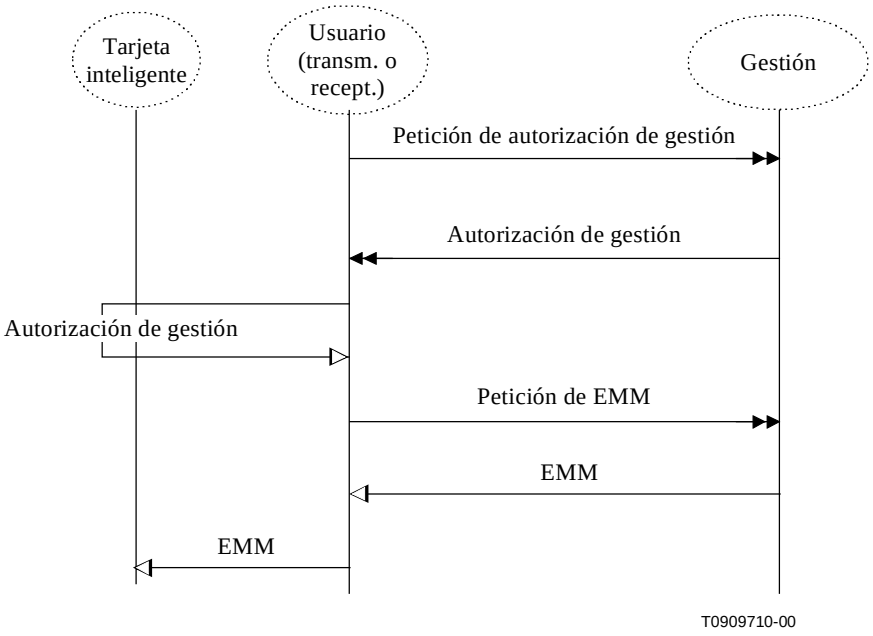


Figura I.4/J.96 – Petición de justificante de títulos

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

Ginebra, 2001