Unión Internacional de Telecomunicaciones

UIT-R

Sector de Radiocomunicaciones de la UIT

Recomendación UIT-R BT.1852-1

(10/2016)

Sistemas de acceso condicional para la radiodifusión digital

Serie BT

Servicio de radiodifusión (televisión)

Unión Internacional de Telecomunicaciones

Prólogo

El Sector de Radiocomunicaciones tiene como cometido garantizar la utilización racional, equitativa, eficaz y económica del espectro de frecuencias radioeléctricas por todos los servicios de radiocomunicaciones, incluidos los servicios por satélite, y realizar, sin limitación de gamas de frecuencias, estudios que sirvan de base para la adopción de las Recomendaciones UIT-R.

Las Conferencias Mundiales y Regionales de Radiocomunicaciones y las Asambleas de Radiocomunicaciones, con la colaboración de las Comisiones de Estudio, cumplen las funciones reglamentarias y políticas del Sector de Radiocomunicaciones.

Política sobre Derechos de Propiedad Intelectual (IPR)

La política del UIT-R sobre Derechos de Propiedad Intelectual se describe en la Política Común de Patentes UIT-T/UIT-R/ISO/CEI a la que se hace referencia en el Anexo 1 a la Resolución UIT-R 1. Los formularios que deben utilizarse en la declaración sobre patentes y utilización de patentes por los titulares de las mismas figuran en la dirección web http://www.itu.int/ITU-R/go/patents/es, donde también aparecen las Directrices para la implementación de la Política Común de Patentes UIT-T/UIT-R/ISO/CEI y la base de datos sobre información de patentes del UIT-R sobre este asunto.

Series de las Recomendaciones UIT-R

(También disponible en línea en http://www.itu.int/publ/R-REC/es)

Series	Título
BO	Distribución por satélite
BR	Registro para producción, archivo y reproducción; películas en televisión
BS	Servicio de radiodifusión (sonora)
BT	**Servicio de radiodifusión (televisión)**
F	Servicio fijo
M	Servicios móviles, de radiodeterminación, de aficionados y otros servicios por satélite conexos
P	Propagación de las ondas radioeléctricas
RA	Radioastronomía
RS	Sistemas de detección a distancia
S	Servicio fijo por satélite
SA	Aplicaciones espaciales y meteorología
SF	Compartición de frecuencias y coordinación entre los sistemas del servicio fijo por satélite y del servicio fijo
SM	Gestión del espectro
SNG	Periodismo electrónico por satélite
TF	Emisiones de frecuencias patrón y señales horarias
V	Vocabulario y cuestiones afines

***Nota**: Esta Recomendación UIT-R fue aprobada en inglés conforme al procedimiento detallado en la Resolución UIT-R 1.*

Publicación electrónica
Ginebra, 2017

RECOMENDACIÓN UIT-R BT.1852-1

Sistemas de acceso condicional para la radiodifusión digital

(Cuestión UIT-R 49-1/6)

(2009-2016)

Cometido

En la presente Recomendación se describen principios destinados a facilitar el desarrollo de métodos eficaces de acceso condicional para la radiodifusión digital que utilizan o bien trenes de transporte MPEG-2 o bien protocolos de transporte de medios MPEG (MMTP). Además, se proporciona información sobre protección fiable de los servicios de radiodifusión contra el acceso no autorizado.

Palabras clave

Acceso condicional, sistema de aleatorización, control de acceso, protección del contenido, tren de transporte MPEG-2, MMT

La Asamblea de Radiocomunicaciones de la UIT,

considerando

a) que hay una creciente demanda en muchos países en lo que se refiere a la protección de los programas de radiodifusión contra la recepción no autorizada;

b) que un método eficaz para garantizar dicha protección de los paquetes del tren de transporte MPEG-2, multiplexado de acuerdo con la Recomendación UIT-T H.222.0, consiste en implementar sistemas de radiodifusión de acceso condicional;

c) que un método eficaz para garantizar dicha protección de los paquetes del MMTP, creados con arreglo a la Recomendación UIT-R BT.2074, consiste en implementar sistemas de radiodifusión de acceso condicional;

d) que se han diseñado y están funcionando ejemplos de sistemas de acceso condicional para la televisión terrenal digital, la televisión por cable digital, la televisión por satélite digital y la televisión IP (protocolo Internet), así como para servicios de sonido, multimedios y de datos;

e) que hay muchos casos de implementación de sistemas de radiodifusión digital basados en las Recomendaciones pertinentes de las Series BT y BO, tal como la Recomendación UIT-R BO.1516 para los sistemas de radiodifusión digital por satélite;

f) que es conveniente limitar el número de sistemas de acceso condicional distintos teniendo en cuenta a la vez los diferentes requisitos de los diversos servicios de radiodifusión y sistemas de transmisión;

g) que introduciendo desde el principio el mayor número posible de elementos comunes de acceso condicional en los receptores se obtiene el mayor potencial para que el público en general acceda a servicios protegidos con unos equipos de coste reducido;

h) que los sistemas de acceso condicional proporcionan protección y que los titulares de derechos de propiedad intelectual, suministradores de programas y proveedores de servicios desean la existencia de redes de radiodifusión/distribución altamente seguras para permitir la protección de sus programas mediante el control de acceso,

recomienda

1 que los sistemas de acceso condicional para los servicios de radiodifusión digital que protegen o bien los paquetes del tren de transporte MPEG-2, o bien los paquetes del MMTP:

– proporcionen los servicios disponibles únicamente a los receptores autorizados;

– compartan el mayor número de elementos comunes en el receptor;

– se diseñen de acuerdo con los principios fundamentales indicados en el Anexo 1.

NOTA 1 – En el Anexo 2 figuran ejemplos de implementaciones de sistemas de acceso condicional para la radiodifusión digital.

Anexo 1

Principios fundamentales para el diseño de sistemas de acceso condicional para la radiodifusión digital

1 Introducción

Los principios descritos en este Anexo deben facilitar el desarrollo de sistemas de acceso condicional eficaces para la radiodifusión digital, que sean convenientes tanto para los abonados como para los proveedores del servicio, garantizando una protección de la información fiable contra el acceso no autorizado.

Los principios se aplican generalmente a la distribución de servicios de televisión digital, a los servicios de radiodifusión sonora y a los servicios multimedios y de radiodifusión de datos. Estos principios se aplican a la distribución del paquete del tren de transporte de la Recomendación UIT-T H.222.0 y del paquete del MMTP a los consumidores a través de distintos medios, tales como sistemas terrenales digitales, sistemas de cable digitales, sistemas de satélites digitales y sistemas de radiodifusión IP (protocolo Internet).

2 Referencias normativas

Recomendación UIT-T H.222.0 | ISO/CEI 13818-1 – Tecnología de la información – Codificación genérica de imágenes en movimiento e información de audio asociadas: Sistemas.

Recomendación UIT-R BT.2074 – Configuración de servicio, protocolo de transporte de los medios e información de señalización para los sistemas de radiodifusión MMT.

3 Términos, definiciones y abreviaturas

3.1 Términos y definiciones

Aleatorización en la radiodifusión digital

Codificación cifrada del contenido de radiodifusión incluida la imagen/el sonido/los datos para impedir la recepción no autorizada de la información en formato no criptado. Esta codificación cifrada es un proceso especificado bajo el control del sistema de acceso condicional (extremo emisor).

Desaleatorización en la radiodifusión digital

Decodificación cifrada del contenido de radiodifusión incluida la imagen/el sonido/los datos para permitir la recepción de la información en formato no criptado. Esta decodificación cifrada es un proceso especificado bajo el control del sistema de acceso condicional (extremo receptor).

Acceso condicional

Un usuario accede a un servicio protegido interactuando a través de una funcionalidad de acceso condicional en el receptor. Si en la sesión se satisfacen todas las condiciones de acceso, se concede la autorización, se libera la clave de decodificación cifrada y se recupera el contenido.

La autentificación del abonado, la confirmación de cuenta y la validad de la disponibilidad del servicio u otros parámetros de control del programa activan la clave del criptado/descriptado de la sesión para permitir a ésta concluir el proceso de autorización.

Control de acceso condicional

La función del control de acceso condicional en el extremo emisor consiste en generar la información de control de aleatorización y las «claves» de criptado asociadas al servicio.

La función del control de acceso condicional en el extremo receptor consiste en producir la información de control de la desaleatorización junto con las «claves» asociadas al servicio.

Criptado y descriptado

Son términos utilizados para métodos que se emplean a fin de proteger (e interpretar) parte de la información en los «mensajes relativos al acceso» que deben transmitirse desde el extremo emisor al extremo receptor sobre las funciones de control de acceso condicional.

Punto de origen

Se trata del punto en un sistema de distribución donde el programa u otro contenido se convierte por primera vez en una señal con su formato de radiodifusión/distribución final. Marca el inicio de la protección de extremo a extremo. El contenido de entrada puede tomar cualquier forma y no necesariamente una forma perceptible para los seres humanos. No es necesario que la entrada de contenido sea inteligible.

NOTA 1 – Los titulares de derechos de propiedad intelectual, los proveedores de servicio y los distribuidores constituyen una amplia jerarquía de muchos puntos de origen posibles en un flujo de información dirigido al consumidor y, por consiguiente, en el flujo del contenido aleatorizado y las claves de criptado para el consumidor. El punto de origen debe comenzar con un titular de derechos de propiedad intelectual o un productor. En la práctica, la mayoría de los puntos de origen serán simplemente los puntos de entrada dondequiera se encuentren en el sistema por motivos comerciales y operacionales. Si bien puede haber muchos de estos puntos de entrada, cada uno de ellos es único e independiente y en él puede mantenerse la información de forma coherente en cualquier formato hasta el consumidor.

Punto de presentación

Es el punto donde el programa u otro contenido toma por última vez la forma de una señal en un sistema de distribución antes de convertirse en una forma perceptible para los seres humanos en la pantalla y los altavoces del receptor. Señala la salida de la protección.

Contenido

Se trata de cualquier forma de datos digitales que puede adquirir y presentar un dispositivo.

Servicio

Se trata de uno o más flujos de datos destinados a ser presentados conjuntamente.

Protección del servicio

Se trata de la protección de un servicio de manera que sólo los dispositivos autorizados pueden recibirlo y decodificarlo.

3.2 Abreviaturas

AES Norma de criptación avanzada (*advanced encryption standard*)

CBC Concatenación de bloques (*cipher block chaining*)

CTR Contador (*counter*)

CRC Verificación por redundancia cíclica (*cyclic redundancy check*)

DES Norma de criptado de datos (*data encryption standard*)

ECM Mensaje de control de autorización (*entitlement control message*)

EMM Mensaje de gestión de autorización (*entitlement management message*)

Km Clave maestra (*master key*)

Ks Clave de aleatorización (*scrambling key*)

Kw Clave de trabajo (*work key*)

MAC Código de autenticación de mensaje (*message authentication code*)

MMT Transporte de medios MPEG (*MPEG media transport*)

MMTP Protocolo de transporte de medios MPEG (*MPEG media transport protocol*)

OFB Realimentación de salida (*output feedback*)

RMP Gestión y protección de los derechos (*rights management and protection*)

4 Descripción general de un sistema de acceso condicional

Existe dos funciones fundamentales que llevan a cabo los sistemas de acceso condicional para la radiodifusión digital: aleatorización y control de acceso. Son componentes distintas, y en muchos casos independientes, en un sistema de acceso condicional y cada una de ellas constituye un proceso de información diferente.

4.1 Modelo de referencia

El acceso condicional exige *aleatorizar* la información antes de difundirla. Este proceso se obtiene mediante una codificación cifrada para transmitir el tren de bits.

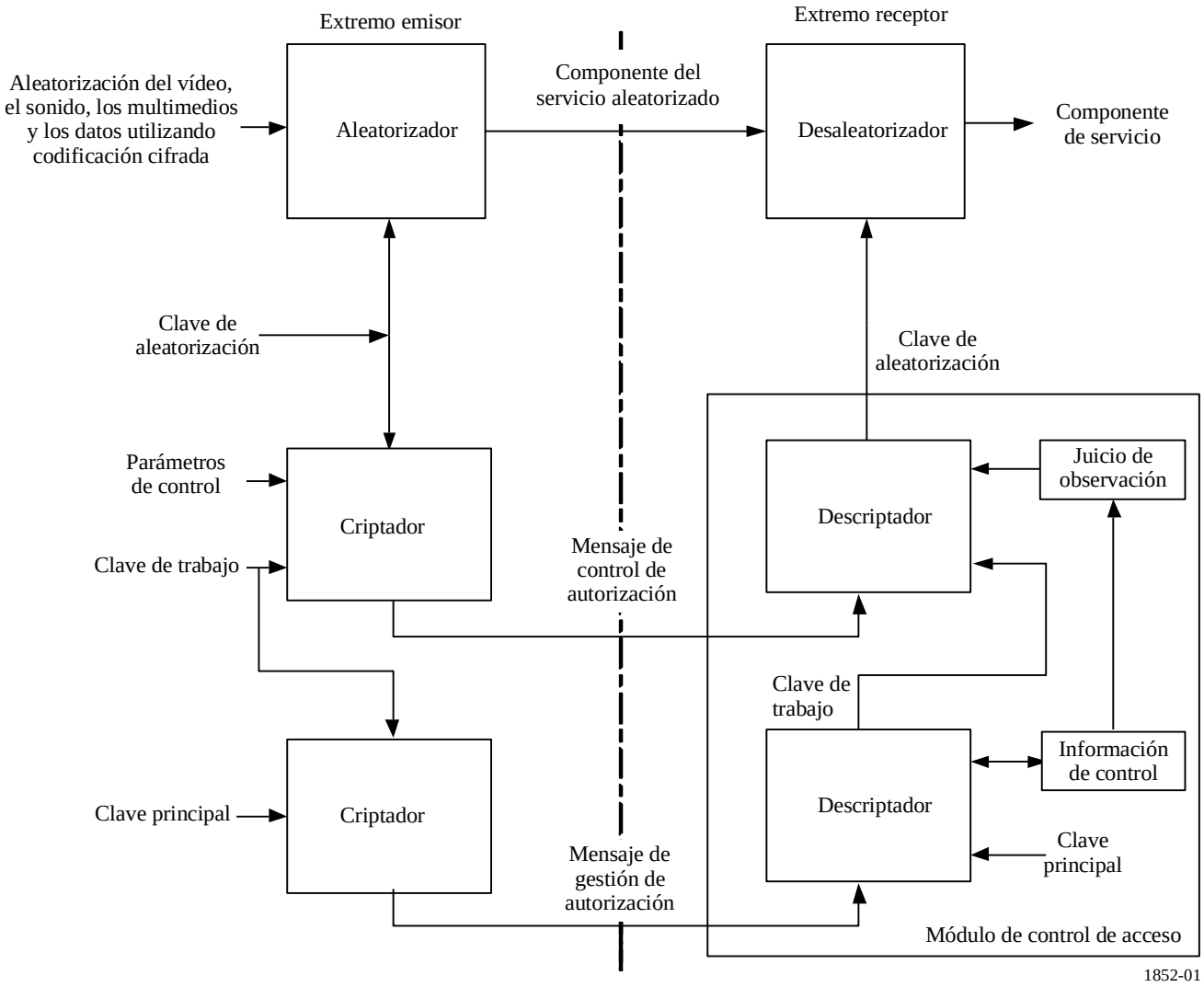
El proceso de desaleatorización en el extremo receptor requiere la misma decodificación de cifrado (en este caso el procedimiento de desaleatorización) para recuperar el tren de bits original.

A fin de proporcionar esta secuencia y garantizar el sincronismo entre los procesos de emisión y recepción, las condiciones de codificación de cifrado se controlan mediante datos transmitidos desde el codificador de cifrado al decodificador de acuerdo con un protocolo especial.

La estructura detallada de este proceso se representa en la Fig. 1.

FIGURA 1

Ejemplo de diagrama de bloques de un sistema de acceso condicional para la radiodifusión digital



4.2 Aleatorización

Se trata del proceso de proteger algunos o todos los componentes de un servicio para impedir el acceso no autorizado utilizando codificación cifrada bajo el control del sistema de acceso condicional en el extremo emisor.

4.3 Control de acceso

Se trata de una disposición de información para permitir a los usuarios autorizados desaleatorizar el servicio protegido. La disponibilidad de esta información viene controlada por el sistema de acceso condicional.

Entre el transmisor y el receptor o receptores, esta información se estructura en mensajes especiales, que pueden multiplexarse en el propio tren de bits de radiodifusión o pueden distribuirse por algún otro medio tal como una línea de telecomunicaciones.

En el extremo o extremos de recepción estos mensajes son interpretados por el sistema de control de acceso para controlar la desaleatorización de las partes autorizadas a partir del tren de bits recibidos en el receptor o receptores autorizados.

5 Requisitos de usuario

5.1 Potencia antipirateo de un cifrado para el aleatorizador y desaleatorizador

Debe probarse adecuadamente el cifrado utilizado en los bloques del aleatorizador y desaleatorizador para constatar su capacidad antipirateo. Se recomienda un cifrado seleccionado entre las normas internacionales.

5.2 Seguridad

La seguridad de un sistema es el grado de dificultad que encuentra un usuario no autorizado para acceder al servicio protegido.

– *Desaleatorización de la señal sin referencia al proceso de control de acceso*. Es una función de la naturaleza de los servicios y el método de aleatorización. Casi todos los servicios de radiodifusión de televisión, audio y datos revisten un carácter digital y, en consecuencia, permitirán la aplicación de procesos de aleatorización muy seguros.

– *Obtención de la clave de control de acceso de una forma no autorizada*. Se trata de una función de seguridad de los algoritmos de criptado de la clave.

5.3 Selección de un algoritmo de aleatorización común o privado

El acceso está disponible a cualquier usuario autorizado que reúna las condiciones de acceso a través de un algoritmo de aleatorización común (universal) o privado.

La utilización de un algoritmo de aleatorización común implica una desaleatorización común para todos los receptores, basada en un algoritmo de aleatorización normalizado, independientemente del medio de distribución utilizado; ello permite unos equipos flexibles y de coste inferior y seguiría posibilitando la competencia a través de implementaciones específicas al proveedor del servicio.

La utilización de un algoritmo de aleatorización privado supone que el proceso de desaleatorización debe llevarse a cabo en los receptores que implementen únicamente un algoritmo específico.

5.4 Modos de acceso

Un sistema de acceso condicional puede soportar una cierta gama de modos de acceso, por ejemplo:

– disponibilidad de periodo (suscripción del servicio) – la autorización va desde un instante de inicio a un instante final;

– elemento de programa o servicio (adquisición de un evento) – la disponibilidad se refiere a un elemento de servicio específico, se utilice o no en su totalidad;

– tasa de servicio (basada en testigo) – la tasa o utilización del crédito es proporcional a la duración de la utilización y/o el valor del servicio implicado;

– emisión libre – el servicio está protegido pero se proporciona el acceso de manera gratuita.

Los modos de acceso deben ser variables con respecto a varios parámetros, por ejemplo:

– hora;

– varios segmentos del servicio;

– grupos de usuarios destinatarios.

5.5 Normalización de los equipos

Para lograr la máxima economía en la fabricación de los equipos receptores y simplificar la gestión y el mantenimiento:

– debe normalizarse el equipo común de manera que admita el mayor número de opciones de servicio posible;

– se necesita una arquitectura de receptor del usuario para soportar los requisitos de funcionalidad de acceso condicional del sistema de acceso condicional seleccionado. Dependiendo del sistema elegido, la funcionalidad puede requerir un soporte tal como funcionalidad de seguridad incorporada o desmontable (por ejemplo, tarjeta inteligente).

5.6 Gestión de acceso

La definición de acceso condicional se basa en el concepto formal de *autorización* al acceso, que puede implementarse de varias formas. Una *autorización* permite a su titular acceder al servicio correspondiente. Debe evitarse una utilización poco económica de los recursos debido a los gastos generales de gestión o transmisión.

5.7 Impedimento de las interrupciones del servicio

Deben evitarse interrupciones debido a una adquisición errónea o no fiable de los datos de control de acceso.

6 Mensajes de control de autorización (ECM)

Los ECM proporcionan la clave de aleatorización para desaleatorizar el servicio protegido.

El acceso a la clave de aleatorización en los ECM se controla mediante las autorizaciones, o derechos, proporcionadas en los EMM.

Normalmente los ECM aparecen en el tren de radiodifusión junto con el servicio protegido.

Generalmente las claves de aleatorización se cambian con frecuencia para minimizar los daños causados por una fuga de la clave de aleatorización.

El contenido de los ECM es específico del sistema.

7 Mensajes de gestión de autorización (EMM)

El procesamiento de un mensaje de gestión de autorización valida o proporciona la autorización necesaria para desaleatorizar el servicio protegido. Un EMM puede contener una clave de trabajo que proporciona el criptado y descriptado de la clave de aleatorización. Los mensajes y/o las claves de trabajo dirigidas a receptores individuales están criptadas. El criptado puede utilizar la clave principal que puede estar almacenada en el dispositivo de recepción.

En los sistemas de acceso condicional para la radiodifusión digital, los mensajes de gestión de autorización se distribuyen mediante radiodifusión o por otros medios.

– La distribución mediante los servicios de radiodifusión se conoce como «direccionamiento por el aire». El ciclo de tiempo asociado con la distribución de las claves difundidas puede reducirse aplicando los principios de criptado de clave compartida. Los mensajes de gestión de autorización también pueden distribuirse por otros medios.

– La distribución por otros medios normalmente se realiza mediante una conexión punto a punto, proporcionando de esta forma una medida de seguridad adicional para garantizar que sólo tienen acceso a los mensajes los dispositivos autorizados.

A continuación figura un ejemplo de funcionamiento:

En el caso de pago, por unidad de tiempo o por programa, los mensajes de gestión pueden transportar un código de coste criptado, transmitido como parte del servicio. El crédito puede residir en el receptor y puede tomar la forma de testigos de dinero criptado transmitidos como parte del servicio de direccionamiento por el aire. Alternativamente, el crédito puede tomar la forma de testigos de dinero almacenados distribuidos por otros medios. El pago consiste en reducir el crédito almacenado de acuerdo con el código de coste recibido.

El contenido del EMM es específico al sistema.

8 Funcionalidad de control de acceso del receptor

En el extremo receptor, el acceso condicional puede introducirse de varias formas, incluidas las siguientes:

Tipo 1: La funcionalidad de seguridad (que puede incluir el algoritmo de criptado de clave y las claves principales) y la funcionalidad de desaleatorización están incorporadas en el receptor.

Tipo 2: La funcionalidad de seguridad es desmontable (por ejemplo, tarjeta inteligente) y la funcionalidad de desaleatorización se incorpora en el receptor.

Tipo 3: La seguridad y la funcionalidad de desaleatorización son desmontables; todas las funciones que llevan a cabo la restauración del tren de datos de entrada se implementan en un módulo desmontable que se comunica con el receptor a través de una interfaz normalizada (por ejemplo, una interfaz común); en este caso puede utilizarse cualquier receptor con dicha interfaz.

Cuando se solicite, la funcionalidad de seguridad verifica las condiciones y, si se cumplen, proporciona la clave de aleatorización al descriptor. Estas condiciones pueden incluir:

– un requisito de periodo de tiempo, estando situada la fecha del parámetro de control entre las fechas de inicio y finalización del parámetro de autorización;

– un requisito de precio por el cual puede proporcionarse una autorización únicamente si se acepta pagar una tasa por el módulo de seguridad.

Un sistema de acceso condicional puede realizar una transacción que implique la funcionalidad de seguridad que incluye diferentes etapas, tales como:

– instrucciones preliminares, si están presentes (por ejemplo, contraseña, aceptación de usuario, etc.);

– instrucciones de funcionamiento que utilizan el módulo de seguridad;

– procesamiento del resultado (por ejemplo, distribución de la palabra de aleatorización).

Anexo 2 (informativo)

Ejemplos de implementación de un sistema de acceso condicional para la radiodifusión digital

CUADRO 1

Ejemplos de implementación

Referencia en el Anexo 1	Sistema «Roscrypt»	Sistema «CAS-R»	«ARIB B61-CAS»	«CEI 62455 con sistemas DVB»
§ 4 Tipo de cifrado para el aleatorizador y el desaleatorizador	Basado en la Norma Estatal de la Federación de Rusia 28147-89	MULTI2 (ISO/CEI 9979).	– AES (longitud de clave de 128 bits) (ISO/CEI 18033-3) – Camellia (longitud de clave de 128 bits) (ISO/CEI 18033-3)	DVB-CSA o AES-128 (obligatorio para los dispositivos); también DES, 3DES y MULTI2 son posibles (opcional para los dispositivos)
§ 4 Proceso de aleatorización	Transición multietapa cíclica basada en registradores de desplazamiento que utilizan polinomios de 64º grados Basado en algoritmos no lineales y es prácticamente una secuencia aleatoria (no tiene forma analítica)	a) Para secuencias codificadas de 64 bits, la codificación original se sustituye con otra cadena de código binario que utiliza variables de 64 y 256 bits b) Para cadenas de código de menos de 64 bits, el método descrito en a) se utiliza para generar una serie de secuencias codificadas seudoaleatorias que se combinan con objeto de crear una señal aleatorizada	– Para los paquetes de tren de transporte MPEG-2, se utiliza el modo CBC+OFB – Para los paquetes de MMTP, se utiliza el modo CTR	DVB-CSA: de acuerdo con ETSI ETR-289; AES-128: de acuerdo con FIPS PUB 197:2001 utilizando modo ECB o CBC; DES o 3DES: de acuerdo con FIPS PUB 46-3:1999 y FIPS PUB 81:1980; MULTI2 de acuerdo con ISO/CEI 9979
§ 4 Sincronización del proceso de aleatorización	Sincronización mutua de secuencia aleatoria y circuitos de conformación del tren DVB	La información asociada en los ECM (programa e información de control), EMM (información individual), mensajes comunes EMM y mensajes individuales EMM se utiliza para sincronizar el proceso de aleatorización	La información asociada en los ECM (programa e información de control), EMM (información individual), mensajes comunes EMM y mensajes individuales EMM se utiliza para sincronizar el proceso de aleatorización	Odd_even_flag e initial_vector se incluyen en el mensaje del tren de clave que proporciona la clave de criptación de tráfico para facilitar la sincronización. Los valores correspondientes de los bits de transport_scrambling_control y pes_scrambling_control indican la clave que va a utilizarse en un instante determinado

CUADRO 1 (*continuación*)

Referencia en el Anexo 1	Sistema «Roscrypt»	Sistema «CAS-R»	«ARIB B61-CAS»	«CEI 62455 con sistemas DVB»
§ 6 Mensajes de control de autorización (ECM)	Contenido de los ECM: – Identificador de clave de trabajo – Clave de aleatorización (par/impar) – Contador criptado y redundancia estructural del tren DVB con suma de control criptográfica o reserva asignada adicional	Sección ECM y su arquitectura básica de la carga útil ECM: – Toda la sección ECM está sujeta a una CRC – La carga útil de los ECM consta de una parte fija que se transmite siempre y una parte variable cuyo contenido varía según el objetivo de transmisión – Sólo la información de función ECM necesaria se inserta en la parte variable de los ECM	Sección ECM y arquitectura básica de la carga útil ECM: – Toda la sección ECM está sujeta a una CRC – La carga útil de los ECM consta de una parte fija que se transmite siempre y una parte variable cuyo contenido varía según el objetivo de transmisión – Sólo la información de función ECM necesaria se inserta en la parte variable de los ECM	Los ECM transportan un mensaje del tren de clave que incluye campos para cursar la siguiente información: – content_key_index – odd_even_flag – cipher mode – next_initial_vector – encrypted_traffic_key_material – traffic_key_lifetime – timestamp – access_criteria_descriptors – permissions_category – encrypted_programme encryption key – programme_CID_extension – programme_MAC – service_CID_extension – service_MAC Existen factores que determinan cuáles de estos campos se incluyen en un mensaje del tren de clave particular; por ejemplo, si el proveedor de servicio desea permitir el acceso según el programa

CUADRO 1 (*continuación*)

Referencia en el Anexo 1	Sistema «Roscrypt»	Sistema «CAS-R»	«ARIB B61-CAS»	«CEI 62455 con sistemas DVB»
Clave principal	256 bits	La longitud de la clave principal depende del operador de servicios	La longitud de la clave principal depende del operador de servicios	No existe una «clave principal» como tal. La protección de las claves de criptado del servicio (SEK) o de las claves de criptado del programa (PEK) se basa en claves RSA que tienen 1 024, 2 048 ó 4 096 bits, dependiendo de la autoridad de certificación. En el modo de radiodifusión, la clave de criptado correspondiente de 128 bits (IEK) desempeña un cometido similar y se deriva de un conjunto de claves que pueden suministrarse al receptor durante el registro. La protección del conjunto de claves se basa en las claves RSA de 1 024, 2 048 ó 4 096 bits
§ 6 Cambio de clave y bandera de aleatorización	La clave de la aleatorización se cambia cuando es necesario. Se utilizan los cuatro estados de la bandera de aleatorización	Las claves de aleatorización (par/impar) se cambian normalmente cada dos segundos	Las claves de aleatorización (par/impar) se cambian cada más de un segundo	La clave de criptado de tráfico cambia frecuentemente, desde una vez por minuto hasta una vez por segundo

CUADRO 1 (*continuación*)

Referencia en el Anexo 1	Sistema «Roscrypt»	Sistema «CAS-R»	«ARIB B61-CAS»	«CEI 62455 con sistemas DVB»
§ 7 Mensaje de gestión de autorización (EMM)	Contenido del EMM: – Número de protocolo – Identificador del grupo del radiodifusor – Clave de trabajo – Identificador de programa – Identificador de módulo de seguridad – Derechos de acceso – Contador de criptado y suma de control criptográfica – Se utiliza redundancia estructural del tren DVB o reservas asignadas adicionalmente.	La sección EMM puede transportar múltiples cargas útiles – Toda la sección EMM está sujeta a detección de error por CRC – La carga útil EMM consta de una parte fija que siempre se transmite y una parte variable cuyo contenido varía según el objetivo de transmisión – Únicamente la información funcional EMM necesaria se inserta en la parte variable del EMM La ID de la tarjeta (6 bytes) y la longitud de byte de información asociada (1 byte) se envían al principio de la parte fija del EMM (parte sin criptar). El receptor filtra esta área para identificar las cargas útiles EMM dirigidas a sí mismo	La sección EMM puede transportar múltiples cargas útiles – Toda la sección EMM está sujeta a detección de error por CRC – La carga útil EMM consta de una parte fija que siempre se transmite y una parte variable cuyo contenido varía según el objetivo de transmisión – Únicamente la información funcional EMM necesaria se inserta en la parte variable del EMM La ID del dispositivo (8 bytes) en caso de RMP, o la ID del módulo (6 bytes) en caso de CAS, y la longitud de byte de información asociada (1 byte) se envían al principio de la parte fija del EMM (parte sin criptar). El receptor filtra esta área para identificar las cargas útiles EMM dirigidas a sí mismo	En modo interactivo, se utilizan los objetos de derecho OMA DRM 2.0 en vez de los mensajes de gestión de autorización para conceder los derechos y las claves de criptado del servicio (SEK) o las claves de criptado del programa (PEK) a los receptores. Se distribuyen a través de un canal de interactividad En modo radiodifusión, se utiliza la versión binaria especial (denominada BCRO) de estos objetos de derecho

CUADRO 1 (*fin*)

Referencia en el Anexo 1	Sistema «Roscrypt»	Sistema «CAS-R»	«ARIB B61-CAS»	«CEI 62455 con sistemas DVB»
§ 8 Funcionalidad de control de acceso	Se encuentra dentro del módulo de acceso condicional (CAM) o integrada en el STB	Tipo 2: El módulo de seguridad es desmontable y el módulo de desaleatorización está integrado en el receptor	Tipo 1: Los módulos de seguridad y desaleatorización están integrados en el receptor Tipo 2: El módulo de seguridad es desmontable y el módulo de desaleatorización está integrado en el receptor	Se prevé el Tipo 1 pero no se han descartado otras implementaciones
Contador de criptado y suma de control criptográfica	ECM, EMM	Se incluye un MAC (código de autentificación de mensajes) en los paquetes de ECM y EMM	Se incluye un MAC (código de autentificación de mensajes) en los mensajes ECM y EMM El MAC también puede agregarse a cada paquete de MMTP	Se incluye un MAC en los mensajes del tren de clave y los objetos de derechos de modo de radiodifusión. Los objetos de derechos de modo interactivo se protegen con una firma
§ 8 Funcionalidad de seguridad	Se encuentra en el interior del módulo de acceso condicional (CAM) o incorporado en el STB	Autentificación mutua entre la tarjeta inteligente y el receptor	Autentificación mutua entre la tarjeta inteligente y el receptor para los Tipos 1 y 2 En el caso del Tipo 1, la seguridad del sistema de control de acceso puede mantenerse y mejorarse mediante su descarga y actualización	La implementación no está determinada en la norma. Las reglas de cumplimiento y robustez vienen fijadas por la autoridad de control

1 Descripción del sistema «Roscrypt»

Se ha implementado actualmente en Rusia un sistema de acceso condicional (CAS) «Roscrypt» en conexión con la conversión a la radiodifusión de TV digital. El sistema «Roscrypt» está diseñado para proteger los trenes de datos DVB contra la recepción no autorizada. Posee una amplia gama de utilización con distintas cadenas DVB de radiodifusión por satélite y terrenal y flexibilidad en la gestión de sus abonados.

El sistema «Roscrypt» consta de:

– el *aleatorizador*, que lleva a cabo un criptado de los componentes del tren de transporte DVB preseleccionado; puede funcionar de manera autónoma o bajo control de un PC;

– un *módulo CAM*, insertado en la ranura de la interfaz común (CI) del receptor para desaleatorizar los componentes seleccionados;

– un *módulo de seguridad*, que cuenta con una unidad de adaptación multimedios incorporada.

El equipo necesario para el funcionamiento del sistema de control común y supervisión está instalado en el extremo emisor.

«Roscrypt» resuelve los siguientes problemas:

– limitación de la radiodifusión dentro de la zona del país para proteger los derechos de los propietarios del programa de forma que sea una radiodifusión limitada;

– protección de la radiodifusión empresarial y departamental contra el acceso no autorizado;

– organización de la radiodifusión comercial.

«Roscrypt» tiene en cuenta las características concretas de las cadenas protegidas contra el acceso no autorizado.

1.1 Características funcionales y técnicas del «Roscrypt»:

– El modelo de funcionamiento común del «Roscrypt» CAS se ilustra en la Fig. 1 del Anexo 1.

– *Algoritmo de aleatorización*: Existen dos algoritmos de aleatorización privados incorporados en el aleatorizador y desaleatorizador del «Roscrypt» CAS. El operador puede modificar en cualquier instante el algoritmo de aleatorización en vigor.

– *Claves de seguridad*: En el CAS «Roscrypt» se utilizan las siguientes claves:

  – La clave de aleatorización y la clave de funcionamiento que proporcionan la aleatorización/desaleatorización del contenido.

  – La base de las claves principales únicas que proporcionan el cifrado ECM (clave de funcionamiento) y el control de acceso por parte del abonado.

  – El grupo de claves de programa que permite aislar a los abonados de los diferentes operadores entre sí y la división de todos los abonados según un criterio determinado.

  – Los operadores pueden cambiar rápidamente las claves sin distribución física y electrónica.

– *Modo de acceso*: Existen dos modos de acceso para gestionar de manera eficaz a los abonados: disponibilidad de periodo y elemento de programa y servicio.

  – Parámetros de modo de acceso: el tiempo de gestión de abonado es de 1 000 abonados por segundo; el número de abonados no está limitado; el número de componentes de aleatorización es 150; el grupo de usuarios destinatarios es 64 000.

– *EMM y ECM*: La estructura de las señales EMM y ECM está de conformidad con los § 6 y 7 del Anexo 1.
  – Hay un contador criptado y una suma de control criptográfica en el extremo de cada paquete EMM y ECM.
  – Para la distribución de las órdenes de gestión (EMM y ECM) pueden utilizarse recursos adicionales de la anchura de banda del tren DVB y reservas de velocidad estructural (redundancia estructural) del tren de transporte DVB.
– *Equipo de recepción*: En el extremo receptor son posibles dos tipos de sistema de acceso condicional «Roscrypt»:
  – Un módulo de seguridad que incluye un algoritmo de descriptado de clave de las claves de seguridad y un módulo desaleatorizador incorporado en la unidad de adaptación multimedios.
  – Un módulo de acceso condicional (CAM) que incluye módulos de seguridad y desaleatorización que comunican con el receptor a través de una interfaz común (CI normalizada) desmontable. El módulo CAM puede restaurar componentes aleatorizados del tren de transporte de entrada simultáneamente.

1.2 Otros:

– Un solo equipo transmisor entre «Roscrypt» puede cifrar el contenido de varios proveedores independientes. Esta propiedad se utiliza para grandes operadores de radiodifusión por satélite y terrenal.
– El sistema de control común y supervisión permite controlar el acceso de los abonados al contenido.
– El sistema de control común y supervisión permite un funcionamiento centralizado a distancia y la supervisión del conjunto de equipos de transmisión «Roscrypt» a lo largo de toda la red. Esta propiedad se utiliza para grandes operadores de radiodifusión por satélite y terrenal.

2 Descripción del sistema «CAS-R»

2.1 Objetivo del sistema

ARIB STD-B25 aborda un sistema de control de acceso condicional para su utilización en la radiodifusión digital y define las especificaciones de aleatorización y de información asociada así como las especificaciones de recepción correspondientes para un sistema que proporciona control durante la recepción de la señal (denominado en adelante «CAS-R»).

Esta norma especifica los sistemas CAS para los sistemas de radiodifusión digital terrenal y por satélite utilizados actualmente en Japón.

2.2 Requisitos del CAS-R y sus sistemas deliberativos

ARIB STD-B25 especifica los sistemas CAS para que cumplan los siguientes requisitos:

1) Máximo número de abonados:

   El sistema puede ampliarse a fin de proporcionar funciones de gestión de cliente para todos los hogares en una zona de cobertura.

2) Vida útil del sistema:

El sistema puede gestionarse suportando medios de radiodifusión aplicables.

3) Antipiratería:

El sistema ofrece funcionalidad de seguridad avanzada y puede tomar medidas si sufre un ataque contra la seguridad.

4) Los sistemas son aplicables a todos los sistemas de radiodifusión digital en una zona específica.

5) Tipos de recepción:

a) Recepción en tiempo real incluido el tren A/V y la reducción de datos utilizando formato de fichero (CAS-R).

b) Recepción almacenada (recepción en tiempo no real).

c) Recepción grabada (incluida la recepción reservada).

6) El sistema puede aplicarse a las siguientes estructuras de tarifa; plana/por nivel, pago por visión (PPV por impulsos (IPPV)) y gratuito.

2.3 Requisito del módulo de seguridad

1) Criptado de la información asociada:

El sistema de criptado utiliza arquitectura de tres capas con equivalente DES y claves privadas. Desde la perspectiva de la implementación en una tarjeta inteligente, el sistema de criptado debe incorporar un programa compacto y habilitar un procesamiento a alta velocidad utilizando al menos un microcontrolador de 8 bits.

2) Funcionalidad de administración:

El sistema puede cambiar el protocolo de criptado para contrarrestar los ataques de los piratas.

3) Debe implementarse una autentificación mutua entre la tarjeta inteligente y el receptor:

Cuando se utiliza la tarjeta inteligente CAS para eliminar a los receptores que no responden a los derechos de protección de información en las aplicaciones que utilizan este sistema de acceso condicional como tecnología de protección de derechos para la radiodifusión digital, se proporciona un sistema para la autentificación mutua entre esta tarjeta inteligente y el receptor.

2.4 En el siguiente documento figura una descripción detallada del sistema

Las especificaciones del sistema de acceso condicional ARIB STD B-25 aparecen en: http://www.arib.or.jp/english/html/overview/doc/6-STD-B25v5_0-E1.pdf.

3 Descripción del sistema CAS de segunda generación basado en ARIB STD-B61 (ARIB B61-CAS)

3.1 Características del sistema

En la norma ARIB STD-B61 se especifica un sistema de aleatorización, un sistema de protección del contenido y un sistema de descarga de programas CAS para la radiodifusión digital de la índole del sistema CAS de segunda generación. Los sistemas CAS de segunda generación presentan las siguientes características:

– soportan trenes de transporte MPEG-2 y MMT como protocolo de transporte de medios subyacente;
– soportan Camellia y AES con una longitud de 128 bits como algoritmo de cifrado;
– soportan la transmisión segura de la información asociada, y
– tienen la capacidad de mantener y mejorar constantemente el nivel de seguridad de un sistema de control de acceso mediante un mecanismo de descarga de programas CAS.

3.2 Requisitos del sistema

1) El subsistema de aleatorización presenta el siguiente requisito:
   – El subsistema proporciona una funcionalidad de seguridad avanzada y puede adoptar medidas en caso de ataque contra la seguridad.
2) El subsistema de información asociada presenta los siguientes requisitos:
   – La información asociada adopta, en la medida de lo posible, un formato común.
   – La información destinada a los receptores individuales puede transmitirse.
   – La información asociada puede transmitirse de forma segura.
   – La seguridad del sistema de control del acceso puede mantenerse y mejorarse constantemente.

3.3 Subsistema de aleatorización

En el subsistema de aleatorización, se seleccionan dos algoritmos de cifrado a fin de mantener un alto nivel de seguridad sistémica, a saber: Camellia o AES con una longitud de 128 bits. Ambos algoritmos se utilizan para paquetes de MMTP y de tren de transporte MPEG-2.

En el caso de los trenes de transporte MPEG-2, la unidad de aleatorización es un paquete de tren de transporte MPEG-2 sin el encabezamiento correspondiente. Habida cuenta de que los paquetes de tren de transporte MPEG-2 tienen una longitud fija, los modos de concatenación de bloques (CBC) y realimentación de salida (OFB) se utilizan conjuntamente como modo de operación del algoritmo de cifrado. El algoritmo de cifrado se denomina Scramble_system_id en el descriptor de aleatorizador, que forma parte de la información de servicio.

En el caso de los MMT, la unidad de aleatorización es un paquete de MMTP sin el encabezamiento correspondiente. Habida cuenta de que los paquetes de MMTP tienen una longitud variable y relativamente extensa, el modo de contador (CTR) se utiliza como modo de operación del algoritmo de cifrado. El algoritmo de cifrado se denomina Scramble_system_id en el descriptor de aleatorizador, que forma parte de la información de señalización. La información de control de aleatorización se inserta en un campo de extensión de encabezamiento de paquete de MMTP, con miras a definir los siguientes tres estados de aleatorización: carga útil no aleatorizada, carga útil aleatorizada con clave par y carga útil aleatorizada con clave impar.

3.4 Subsistema de información asociada

Existen dos sistemas de control de recepción, a saber, el sistema CAS y el sistema de protección del contenido. Cada sistema tiene su propia información asociada.

El sistema CAS de segunda generación incluye un sistema de protección del contenido denominado «Sistema de gestión y protección de derechos» (RMP) para los servicios de radiodifusión hertziana, además del control de recepción. El sistema RMP permite a los organismos de radiodifusión distribuir una clave de aleatorización a cada receptor, que se utiliza para descriptar contenido.

Aunque el sistema RMP es casi idéntico al sistema CAS-R antes descrito, puede aplicarse tanto al MMT, así como a los trenes de transporte MPEG-2.

3.5 Arquitectura de tres capas y mensajes ECM/EMM

El sistema CAS de segunda generación utiliza la arquitectura de tres capas y los mensajes ECM/EMM descritos en el modelo de referencia.

En el caso de los trenes de transporte MPEG-2, el mensaje ECM proporciona información común a todos los receptores. La clave de aleatorización se halla en el ECM. El acceso a la clave de aleatorización del ECM se controla mediante autorizaciones o derechos proporcionados en el mensaje EMM. El EMM proporciona información a los receptores individuales y contiene la clave de trabajo.

En el caso de los MMT, el mensaje ECM proporciona información común a todos los receptores. La clave de aleatorización se halla en el ECM. El acceso a la clave de aleatorización del ECM se controla mediante autorizaciones o derechos proporcionados en el mensaje EMM. El EMM proporciona información a los receptores individuales y contiene la clave de trabajo. Los ECM y EMM vienen transportados en un mensaje de sección M2, cuya especificación figura en la Recomendación UIT-R BT.2074. El código de autentificación de mensajes (MAC) puede añadirse a cada paquete de MMTP, con objeto de que el receptor pueda comprobar la integridad y autenticidad del paquete.

3.6 Sistema CAS disponible para descarga

El sistema CAS de segunda generación incluye un CAS disponible para descarga, a fin de mantener constantemente la seguridad del sistema de control de acceso y dar soporte a nuevos servicios de radiodifusión. Los receptores pueden descargar de forma segura un programa CAS actualizado por medio de la radiodifusión y/o la banda ancha.

Para descargar un programa CAS mediante canales de radiodifusión, se utiliza una estructura principal de tres capas y un sistema de aleatorización. Un programa CAS en canales de radiodifusión está criptado con una clave de protección de canal de transmisión (Kt), que se distribuye a cada receptor utilizando un mensaje de control de descarga (DCM) y un mensaje de gestión de descarga (DMM).

Los programas CAS vienen criptados y firmados por su proveedor, con objeto de mantener la integridad y autenticidad del producto.

4 Descripción de los sistemas CEI 62455 con DVB

La norma CEI 62455 especifica un sistema normalizado para controlar el acceso a los servicios de radiodifusión basándose en el tren de transporte MPEG2. Dicha norma también especifica cómo puede utilizarse ese mismo sistema para controlar el acceso a los servicios de radiodifusión basados en el protocolo Internet (IP). Por consiguiente, la especificación es ampliamente aplicable a distintos sistemas de radiodifusión, incluidos sistemas en los que no puede lograrse la protección en los paquetes del tren de transporte MPEG2 (por ejemplo, servicios basados IP distribuidos a través de redes no basadas en MPEG2).

Para los sistemas de radiodifusión de acceso condicional, la norma CEI 62455 proporciona una interfaz plenamente especificada entre los extremos emisor y receptor. Utilizando esta interfaz los vendedores del servidor y el receptor pueden implementar independientemente el soporte de los sistemas de protección en vez de verse forzados a basarse en un solo vendedor de seguridad para facilitar la implementación tanto del servidor como del receptor. De esa forma, una incorporación del sistema evita depender de un vendedor de seguridad y permite cambiar el vendedor de un elemento del sistema de acceso condicional especificado sin cambiar los otros elementos o sus vendedores.

La especificación CEI 62455 cubre las siguientes capas del sistema, pero se hace referencia a especificaciones existentes siempre que es posible:

– capa de registro;
– capa de gestión de derechos;
– capa del tren de clave; y
– capa de tráfico.

La capa de gestión de derechos se basa en la norma de gestión de derechos digitales establecidas y ampliamente adoptada comercialmente de Open Mobile Alliance, OMA DRM 2.0. Esta capa es responsable de proporcionar los derechos y las restricciones correspondientes a los receptores así como las claves a largo plazo; es decir, la clave de criptado del servicio (SEK) o la clave de criptado de programa (PEK), dependiendo de si el acceso se otorga mediante suscripción o según el programa.

En el modo interactivo, es decir cuando está disponible un canal de comunicación bidireccional entre el receptor y el proveedor de servicio, se utiliza OMA DRM 2.0. Para un funcionamiento de radiodifusión unidireccional en ausencia de un canal de interacción, el sistema se ha mejorado con versiones binarias de ahorro de anchura de banda de los objetos de derechos OMA DRM 2.0 (llamado objeto de derechos codificados binario, o BCRO) y un método para proteger estos BCRO cuando se distribuyen a través de una canal de radiodifusión. El direccionamiento de los BCRO incluye varios modos de direccionamiento que reducen más la anchura de banda necesaria para distribuir los objetos de derechos. El método de protección se basa en el criptado de radiodifusión de cero mensajes que garantiza que una ruptura de la seguridad en un solo receptor no proporciona acceso a claves o derechos otorgados a los otros receptores. La utilización de la anchura de banda de radiodifusión está muy optimizada.

El teclado necesario para el funcionamiento en modo radiodifusión se concede al receptor durante el registro para el servicio por el canal de radiodifusión. A fin de registrarse para un servicio, el usuario sólo necesita comunicar el número de dispositivo único (UDN) del receptor al proveedor del servicio que puede verificar el certificado del receptor a partir de una base de datos de certificado. El certificado contiene la clave pública del receptor que se utiliza para proteger el teclado durante el tránsito.

Para proteger un tren de transporte MPEG-2, el criptado (aleatorización) del contenido real del servicio utiliza cifrados populares tales como DVB-CSA o AES-128 como especifica la norma CEI 62455. Esta norma también especifica el soporte de otras normas de criptado, tales como IPsec, SRTP y ISMAcryp – para facilitar una protección basada en el paquete del tren de transporte no MPEG2.

A fin de facilitar un cambio frecuente en las claves de criptado de tráfico (TEK) utilizadas para proteger el contenido del servicio, CEI 62455 especifica una capa del tren de clave que funciona entre la capa de gestión de derechos y la capa de tráfico. El sistema soporta la concesión de acceso

al mismo tren a través de los objetos de derecho de servicio y programa. Si el proveedor de servicio desea activar un acceso programa a programa en el caso de que el programa también sea disponible por suscripción, el mensaje del tren de clave transportará una PEK criptada con la SEK además de la TEK criptada por la PEK. La capa del tren de clave puede transportar alguna otra información tales como criterios de acceso o un valor permissions_category que puede utilizarse para seleccionar entre distintos derechos en el objeto de derechos del servicio, relativos al fragmento particular del tren al que se aplica el mensaje del tren de clave. Ello hace posible tener distintos derechos para diferentes programas aun cuando el acceso se base en la suscripción a un servicio que consta de múltiples programas consecutivos.

Apéndice 1
al Anexo 2

Bibliografía

– Recomendación UIT-R BT.810 – Sistemas de radiodifusión de acceso condicional.

– ARIB STD-B25: Especificaciones de un sistema de acceso condicional para la radiodifusión digital.

– ARIB STD-B61: Especificaciones de un sistema de acceso condicional (segunda generación) y de un sistema de descarga de programa CAS para la radiodifusión digital.

– CEI 62455: Acceso al servicio basado en el protocolo Internet (IP) y en el tren de transporte (TS).