MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

Secretaría de Estado de Telecomunicaciones
y para la Sociedad de la Información

TVad

Foro de la TV de Alta Definición

# ALTA DEFINICIÓN y ACCESO CONDICIONAL

***Versión 1.0***

Elaborado por

**Subgrupo de Normalización Técnica de la presentación**

**Grupo Técnico del Foro de la Televisión de Alta Definición en España**

Coordinado por
UNIVERSIDAD POLITÉCNICA DE MADRID

**Abril de 2008**

# Índice

# 1 OBJETIVO

El objetivo de este documento es establecer los elementos más significativos que relacionan alta definición y acceso condicional.

Realiza una disección de las tramas MPEG-2, revisa los fundamentos del acceso condicional, las arquitecturas simulcrypt y multicrypt, estudio de prestaciones y características de los sistemas de acceso condicional y una breve prospección de DVB-CPCM.

Es obvio que por su interés la Alta Definición es susceptible de pertenecer a ofertas audiovisuales cerradas o de pago por evento, y por tanto, de emplear métodos de acceso condicional. No obstante, la resolución de la imagen, la alta definición per se, no introduce ningún factor diferencial en el establecimiento de los sistemas de control de acceso a los contenidos.

De mayor interés resulta la protección y el marcado de contenidos de alta definición para el control de su consumo en el entorno doméstico. En esta línea se ha tratado de esbozar el tratamiento que se da a los contenidos en la nueva norma DVB-CPCM.

# 2 ANÁLISIS DE LAS TRAMAS MPEG-2

## 2.1 Anatomía del flujo de transporte MPEG-2 (MPEG-2 TS)

La señal de televisión digital se transmite como un flujo de datos codificado en MPEG-2 llamado flujo de transporte ("transport stream"), y denominado MPEG-2 TS. Cada flujo de transporte posee una tasa binaria de unos 40 Megabits por segundo para redes por cable o satélite y en el caso de España, con los parámetros en uso, es de 19,91 Megabits por segundo para redes terrestres. Estas tasas son suficientes para llevar 7 u 8 canales independientes de TV.

Cada flujo de transporte se compone de otros flujos conocidos como flujos elementales ("elementary streams"), que pueden llevar audio codificado en MPEG-2, video codificado en MPEG-2 o datos encapsulados en un flujo MPEG-2. Como muchos flujos elementales forman un flujo de transporte, cada uno de estos flujos elementales lleva asociado un identificador único, denominado PID ("packet identifier"), para poder identificarlo una vez que está multiplexado en el flujo de transporte.

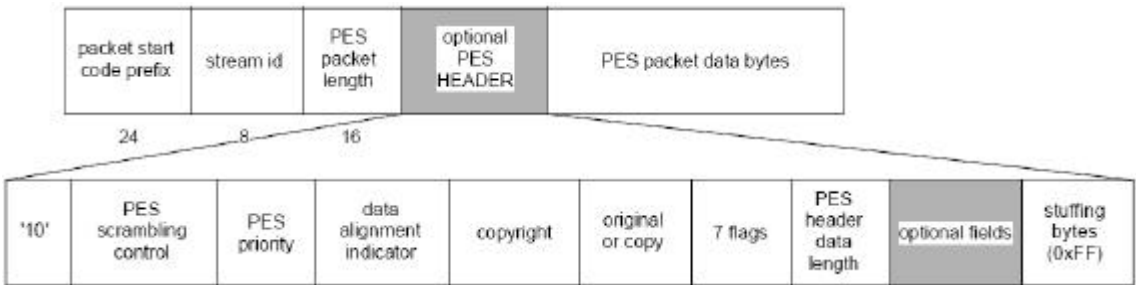
Cada flujo elemental debe llevar un PID diferente dentro de un mismo flujo de transporte. El PID está formado por 13 bits. Al ser este número tan elevado, lo que limita el número de flujos elementales que pueden ir en un mismo flujo de transporte es la tasa binaria ([1]).

**Construcción del flujo de transporte:**

El proceso desde el que tenemos varios programas hasta que formamos un flujo de transporte es el siguiente:

1) Codificamos el audio y el video de varios de programas en MPEG-2, obteniendo múltiples flujos elementales, cada uno formado únicamente por un solo canal de video o de audio (mono o estéreo).

2) A continuación hacemos paquetes de datos a partir de estos flujos, dando como resultado los PES ("packetised elementary stream"). Gráficamente, la estructura de un paquete PES es la siguiente:

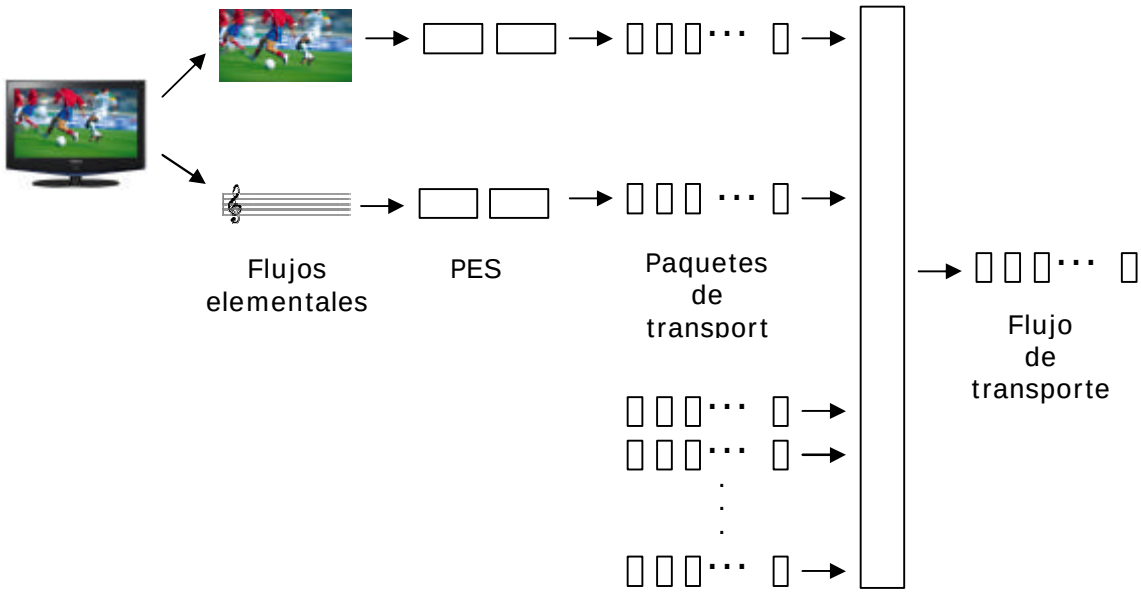



Fuente: ISO/IEC 13818-1 ([2])

3) Una vez realizado esto, dividimos los PES y los introducimos en paquetes de transporte, que forman el flujo de transporte. Un paquete PES es mayor que un paquete de transporte (188 Bytes), por lo que un PES entero irá alojado

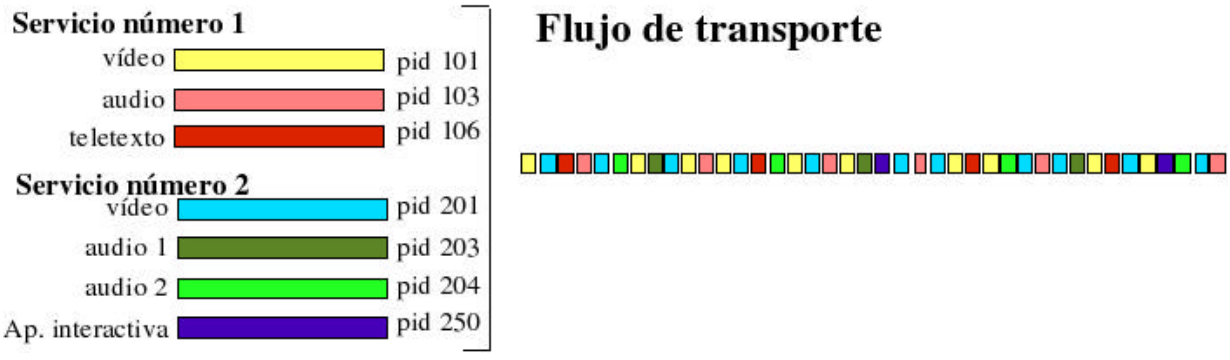
en varios paquetes de transporte. Este doble empaquetado tiene los siguientes objetivos: el empaquetado a nivel PES permite multiplexar flujos elementales en un flujo mayor, identificar el tipo de información contenida en el paquete y el tiempo en el que debe de ser decodificado y mostrado. Por otro lado, el empaquetado de transporte facilita la corrección de errores.

En la siguiente ilustración vemos de forma gráfica este proceso:




También es posible introducir datos en el flujo de transporte. MPEG-2 define para ello secciones privadas, que son partes reservadas para introducir datos.

Otra ilustración que muestra este proceso es la siguiente:



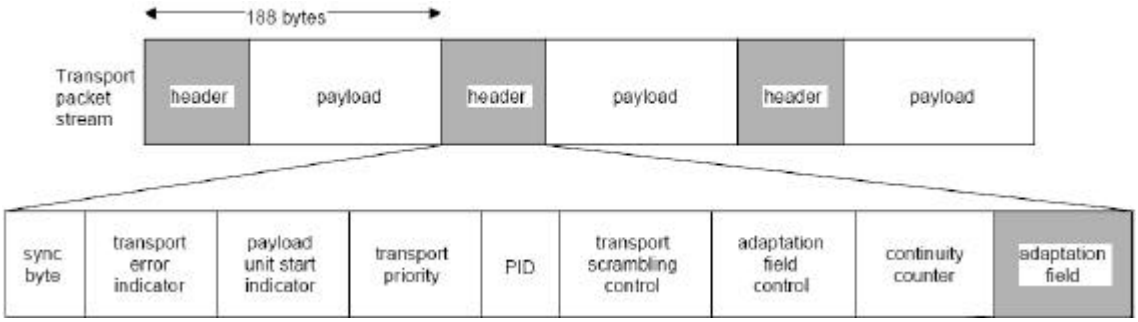

En ella podemos observar cómo un servicio está formado por diferentes flujos elementales, cada uno con su PID. Estos flujos se dividen en paquetes PES y a continuación se dividen en los paquetes de transporte, que se multiplexan y se envían dando lugar al flujo de transporte. También se puede apreciar cómo se da un ancho de banda mayor a los flujos elementales que lo necesitan, como por ejemplo el video.

Hay que tener cuidado a la hora de construir el flujo de transporte. No se deben de introducir los paquetes de transporte provenientes de diferentes flujos elementales a la ligera. Es necesario introducir los paquetes de cada flujo elemental en el orden correcto. Por otro lado, también hay que asegurarse de que le estamos dando una tasa binaria constante a cada flujo elemental para asegurarnos de que el receptor pueda descodificar los flujos evitando que se sature o que se quede parado.

Para la correcta decodificación del flujo de transporte es necesario introducir una información que nos permita identificar cada flujo elemental para poder reconstruirlo. Esta información, denominada Información de Servicio ("Service Information, SI"), se codifica como si se tratara de otro flujo elemental y se inserta en el flujo de transporte en el proceso de multiplexación.

La información de servicio es básicamente una base de datos sencilla que describe la estructura del flujo de transporte. Está formada por diferentes tablas que describen diferentes características del flujo de transporte y que se verán más adelante. Gracias a esta información el receptor es capaz de identificar que flujos son de audio, video o datos y tratarlos adecuadamente ([1]).

Gráficamente, el flujo de transporte queda como sigue:




Fuente: ISO/IEC 13818-1 ([2])

## 2.2 Nomenclatura tecnológica relacionada con el acceso condicional

Antes de pasar a describir las características del sistema de acceso condicional es necesario tener claras una serie de ideas y conceptos.

En la nomenclatura de televisión digital cada flujo de transporte se conoce también como un múltiplex. Cada múltiplex se emite en una sola frecuencia, y solamente un múltiplex se puede emitir en cada frecuencia.

En cada múltiplex, cada grupo de flujos elementales que forman un canal de TV se conoce como un servicio. El número de flujos elementales por servicio no tiene porque ser constante: se pueden transmitir varios flujos de audio correspondientes a varios idiomas, varios flujos de video correspondientes a diferentes ángulos de grabación…etc. Para referirnos a un servicio utilizaremos también el término de programa.

Dentro de cada servicio podemos tener también diferentes eventos. Un evento corresponde a los diferentes acontecimientos (por ejemplo, un concurso, una película, un noticiario… etc) que hay en un canal de TV.

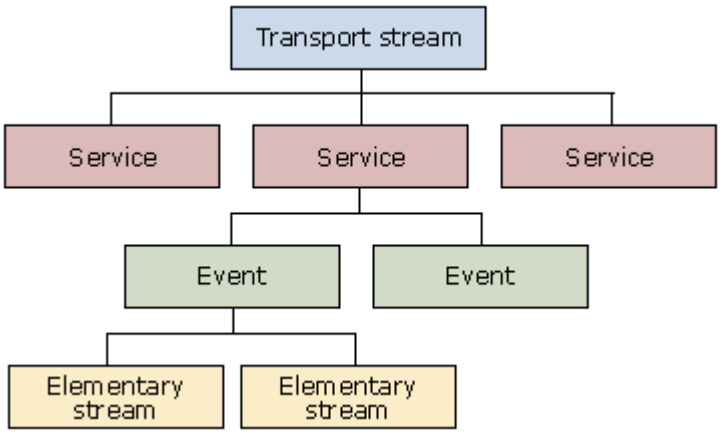
También es necesario definir otro concepto cuyo nombre en nomenclatura inglesa es el de "bouquet". Se trata de un conjunto de servicios agrupados de manera lógica, es decir, servicios que forman un mismo paquete pero que se están emitiendo en múltiplex diferentes. Este concepto surge ante el siguiente problema: si un gran difusor quiere ofrecer paquetes de servicios a los consumidores, lo primero que podría hacer es meter los servicios de cada paquete en un mismo múltiplex. Sin embargo, esta opción es muy poco flexible, limitada si queremos ofrecer más servicios en un bouquet de los que caben en un múltiplex, o derrochadora de recursos si queremos ofrecer menos servicios en un bouquet de los que caben en un múltiplex. Para ello se agrupan los servicios en los múltiplex de la manera más eficiente posible, y se definen estos paquetes lógicos llamados bouquets formados por servicios de diferentes múltiplex.

En la terminología de televisión digital surge también el concepto de red. Una red es un conjunto de flujos de transporte que comparten una información de servicio similar. Suelen ser difundidos por la misma compañía, y en consecuencia más de una red suele estar disponible en cualquier momento.

Resumiendo hasta ahora tenemos lo siguiente:

- Una red está compuesta por varios flujos de transporte difundidos por la misma entidad.
- Un flujo de transporte es un flujo MPEG-2 que contiene diferentes servicios (o programas).
- Cada servicio se corresponde con un canal de televisión, que es una sucesión de eventos seguidos uno detrás de otro.
- Cada evento es un acontecimiento de televisión, y está formado por varios flujos elementales.
- Cada flujo elemental es un flujo MPEG-2 empaquetado, que puede contener audio, video o datos.
- Diferentes servicios pertenecientes a un mismo múltiplex, o múltiplex diferentes, se pueden agrupar de forma lógica para formar un bouquet.

De manera gráfica podemos observar lo comentado anteriormente:




Fuente: Interactive TV web ([1])

Cada servicio de una red DVB puede ser identificado de manera única gracias a tres valores localizados en la información de servicio:

- Identificador de red de origen ("original network ID"): es el identificador de la red que difundió dicho servicio.
- Identificador de flujo de transporte ("transport stream ID"): permite identificar un flujo de transporte dentro de la red de origen.
- Identificador de servicio ("service ID"): permite identificar el servicio dentro del flujo de transporte.

El flujo de transporte DVB tiene dos identificadores para diferenciar entre la red de origen que produjo el flujo de transporte (por ejemplo, la BCC) y la red que está transmitiendo dicho flujo (por ejemplo, BSkyB). El primero es el identificador de la red de origen ("original network ID"), y el segundo es el identificador de red ("network ID") ([1]).

## 2.3 Información de servicio (DVB-SI)

Como se ha visto hasta el momento, un flujo de transporte contiene diferentes servicios, y a su vez cada servicio está formado por diferentes flujos elementales. El problema que surge ahora es como diferenciar qué es cada cosa.

La solución es un conjunto especial de flujos elementales que contienen una serie de tablas que forman una sencilla base de datos que describe la estructura del flujo de transporte, los servicios que hay dentro de él e información que los receptores de TV digital pueden mostrar al usuario tal como el nombre del servicio, horarios de eventos …etc. Todo flujo de transporte (DVB o no) debe llevar incluidas unas tablas que las especificación de MPEG-2 obliga. Además, DVB define unas tablas adicionales.

Estas tablas se difunden como flujos elementales dentro del flujo de transporte. Algunas están ligadas directamente a los servicios que hay en el flujo de transporte, mientras que otras son más generales y describen la estructura del flujo de transporte o proporcionan propiedades de la red ([1]).

## 2.4 Tablas de información de servicio y secciones

### Tablas de información de servicio

Las tablas que define el estándar MPEG-2 son:

- Tabla de Asociación de programas ("Program Asociation Table", PAT)
- Tabla de Mapas de Programa ("Program Map Table", PMT)
- Tabla de Acceso Condicional ("Condicional Access Table", CAT)
- Tabla de Información de Red ("Network Information Table", NIT)

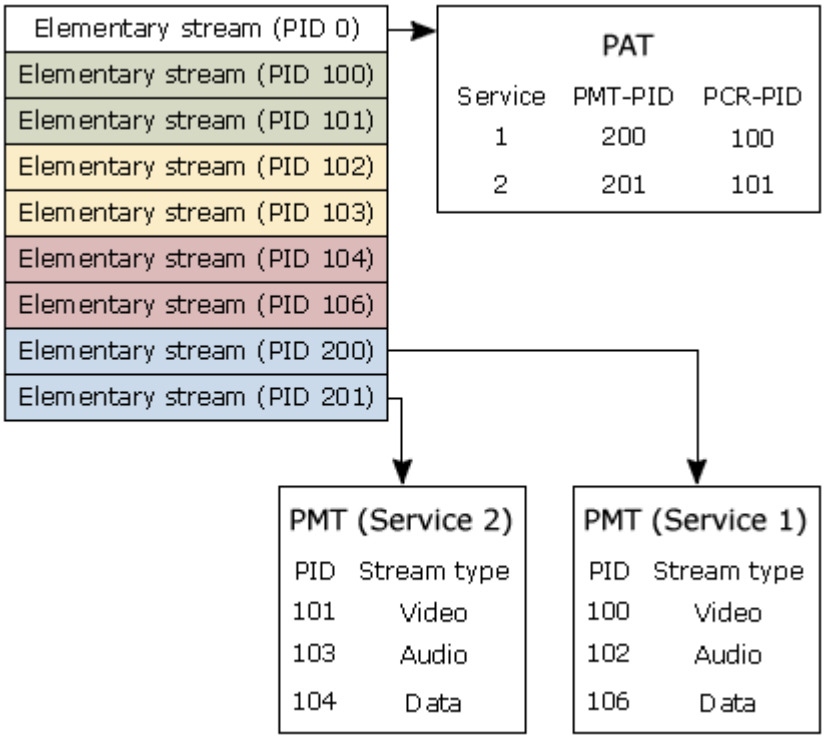
Las tablas que añade DVB son:

- Tabla de Información de Red ("Network Information Table", NIT)
- Tabla de Descripción de Servicio ("Service Description Table",SDT)
- Tabla de Información de Eventos ("Event Information Table", EIT)
- Tabla de Asociación de Bouquets( "Bouquet Association Table", BAT)
- Tabla de Tiempo y Fecha ("Time and Date Table", TDT)
- Tabla de Compensación de Tiempo( "Time Offset Table", TOT)

La PAT es la tabla fundamental de la información de servicio. Describe qué PID contiene la PMT de cada servicio así como el PID de la NIT en aquellas redes que la usan. La PAT siempre tiene el PID 0x0000.

La PMT describe cómo se reensambla un servicio a partir de sus flujos elementales. Describe todos los flujos de un servicio y anuncia cual de ellos contiene el reloj de referencia del programa ("Program Clock Reference"), elemento encargado de la sincronización entre los diferentes flujos del servicio. A las PMT´s no se les asigna un PID fijo. Existe una PMT por cada servicio dentro del flujo de transporte, y encontramos el PID de cada PMT dentro de la PAT.

Antes de continuar con el resto de tablas, veamos gráficamente la relación entre la PAT y la PMT de un flujo de transporte:




Fuente: Interactive TV web ([1])

La PAT siempre lleva el PID 0x0000. En ella podemos ver que hay dos servicios, el 1 cuya PMT tiene como PID el 200 y su PCR está en el flujo elemental 100, y el servicio 2, cuya PMT tiene asignado el PID 201 y su PCR está en el flujo elemental 101.

Analizando la PMT de cada servicio podemos ver que el servicio 1 está formado por tres flujos elementales cuyos PID´s son el 101 (que contiene video), el 103 (que contiene audio) y el 104 (que contiene datos). De igual manera el servicio 2 está formado también por tres flujos elementales cuyos PID´s son el 100 (que contiene video), el 102 (que contiene audio) y el 106 (que contiene datos).

Aunque en este ejemplo ambos servicios tienen los mismos flujos elementales, no siempre es así. Un servicio puede tener un número variable de flujos elementales correspondientes a varios canales de video, audio o datos.

La CAT describe qué sistema de acceso condicional se está utilizando en el flujo de transporte y proporciona información para decodificarlo. La CAT tiene asignado el PID 0x0001.

La NIT es una tabla opcional y sus contenidos son privados. Si existe, está estructurada en una o varias secciones privadas y se transporta dentro del TS bajo el PID 0x0010. Este valor se define en la PAT y tiene que estar asociado al program_number de valor 0x0000', que está reservado para este caso. DVB-SI define, especifíca, y estructura esta tabla para el caso concreto de las redes DVB.

En conjunto, la PAT, la CAT y la PMT se conocen como la Información Específica de Programa ("Program Specific Information", PSI), y están definidas por MPEG.

La NIT describe cómo están organizados los flujos de transporte en la red y describe algunas propiedades físicas de ésta. Contiene el nombre de la red, y el identificador de red. Este valor identifica a la red que está en ese momento dado difundiendo el flujo de transporte, y probablemente sea diferente del identificador de red de origen, si el flujo de transporte está siendo redifundido.

La SDT da información orientada al usuario sobre los servicios del flujo de transporte. Hay solamente una SDT en un flujo de transporte, y contiene la información de todos los servicios. Contiene información tal como el nombre del servicio, su identificador, el estado actual del servicio (iniciado, terminado, con inicio inmediato…etc) y si el servidio está cifrado o no. La SDT tiene asignado el PID 0x0011.

La EIT proporciona información sobre los horarios de los eventos de un servicio.
Incluye el nombre del evento, la hora de comienzo, la duración y el estado del evento. Esta tabla está realmente dividida en dos tablas: la "EIT-present/following", que contiene información sobre el evento en curso y los siguientes, y la "EIT-schedule", que contiene otra información sobre horarios. La "EIT-present/following" tiene asignado el PID 0x0012.

La BAT enumera y describe los servicios que forman un bouquet. No proporciona información mucho más detallada, ya que se puede extraer de otras tablas que forman la información de servicio. Tiene asignado el PID 0x0011.

La TDT y la TOT proporcionan una referencia de tiempo para el flujo. La TDT contiene la hora UTC (Universal/GMT), mientras que la TOT contiene esto último y además la compensación de tiempo en referencia a la hora UTC para la hora local. Tienen asignado el PID 0x0014.

Algunas de estas tablas, además de contener información sobre el flujo de transporte en el que están, pueden contener información de otros flujos de transporte. La NIT, la SDT y la EIT deben contener información sobre el flujo de transporte al que pertenecen, denominándose "NIT-actual", "SDT-actual" y "EIT-actual", pero dicho flujo de transporte puede tener versiones de estas tablas con información referente a otros flujos de transporte, en cuyo caso se denominarían "NIT-other", "SDT-other" y "EIT-other".

La PAT y PMT deben existir obligatoriamente por lo que define el estándar MPEG-2, mientras que la CAT sólo es obligatoria en el caso que existan servicios encriptados en el TS. La "NIT-actual", "SDT-actual", "EIT-present/following-actual" y la TDT también deben existir obligatoriamente por lo que define el estándar DVB. El resto de tablas son opcionales.

Aunque algunas tablas tengan que existir obligatoriamente, no quiere decir que tengan que estar rellenas. Muchos difusores, bien por pereza o bien por aprovechar al máximo la tasa binaria disponible dejan algunas tablas vacías.

Por otro lado, el contenido de las tablas de la información de servicio va cambiando. Para ello cada tabla tiene asociado un número de versión, que se incrementa al cambiar algo, y así el receptor sabe cual es la versión más actualizada de la tabla ([1]).

## Estructura de las tablas de servicio

Las tablas de servicio tienen estructuras muy similares. Todas empiezan por una cabecera, seguida de uno o varios bucles descriptores. Cada bucle descriptor

contiene uno o más descriptores, y cada descriptor proporciona la información de una fila de la tabla. Hay descriptores que llevan información general y aparecen en diferentes tablas.
Hay gran cantidad de descriptores. Los más importantes y utilizados son:

- "service_descriptor": Está en la SDT y proporciona el nombre y el tipo de servicio.
- "linkage_descriptor": Está en varias tablas y proporciona una referencia a una fuente de información sobre un elemento de la información de servicio. También proporciona una referencia a un sustituto del servicio si éste no está funcionando o está cifrado.
- "component_descriptor": Está en la EIT y da información sobre un flujo elemental tal como el tipo de contenido y el formato, y en algunos casos el idioma del flujo.
- "data_broadcast_id_descriptro": Está en la PMT y se utiliza para adjuntar la etiqueta de un componente a un flujo elemental de tal manera que los flujos se puedan identificar individualmente.
- "CA_identifier_descriptor": Está en varias tablas e identifica el sistema de cifrado que se está utilizando (si hay alguno) para un servicio o evento determinado.

## Secciones

Como las tablas de información pueden ser en ocasiones demasiado grandes como para enviarlas juntas, es necesario dividirlas para enviarlas dentro de los paquetes de transporte. Cada división se denomina sección, y se pueden utilizar no solo para enviar las tablas: también para todo tipo de información binaria.

Las secciones que contienen datos y no llevan audio ni video se denominan secciones privadas, aun cuando la información es conocida ([1]).

# 3 ACCESO CONDICIONAL: FUNCIONAMIENTO E IMPLEMENTACIÓN

## 3.1 Cifrado y descifrado del contenido

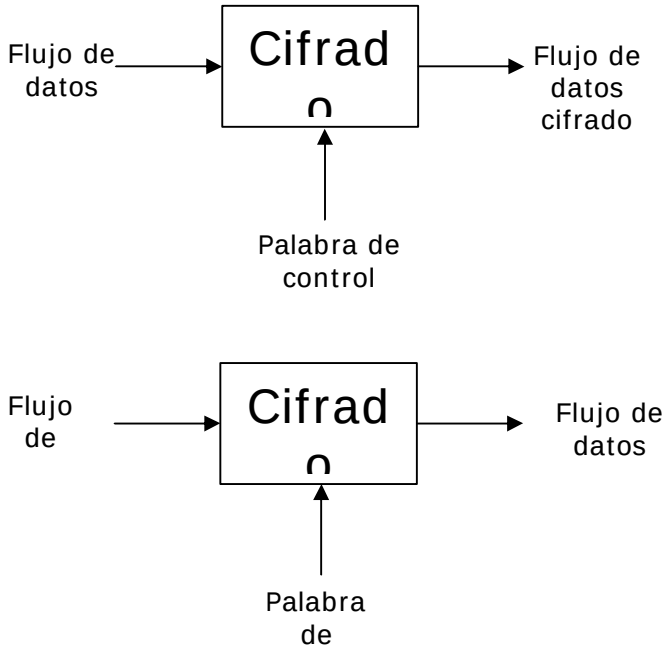
En múltiples ocasiones no queremos que se pueda acceder al contenido emitido de manera gratuita. Ya sea porque se trata de un contenido de pago, o porque queremos limitar el acceso a dicho contenido a unas regiones determinadas, es necesario disponer de un sistema de acceso condicional ("Conditional Access", CA). Las especificaciones definen la estructura de este sistema, pero los algoritmos de cifrado y descifrado dependen de cada proveedor. Estos algoritmos son privados y no se conoce su funcionamiento, aunque hay alguno abierto pero no conocido públicamente como el Algoritmo de Cifrado Común de DVB.

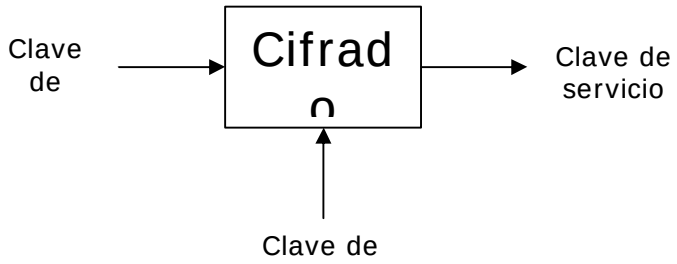
El cifrado se puede hacer a dos niveles: a nivel de flujo de transporte o a nivel de flujo elemental. Cuando trabajamos a nivel de flujo de transporte las cabeceras se dejan sin cifrar, y todo lo demás queda cifrado. Si trabajamos a nivel de flujo elemental ocurre lo mismo: las cabeceras se dejan sin cifrar para que el decodificador pueda manejar los contenidos correctamente. Más adelante analizaremos estas técnicas en detalle.

El proceso de cifrado recae en tres piezas clave de información:

- La palabra de control
- La clave de servicio
- La clave de usuario

La información se cifra con la palabra de control. La palabra de control se cifra con la clave de servicio, proporcionando un primer nivel de cifrado, y la clave de servicio se cifra con la clave de usuario.

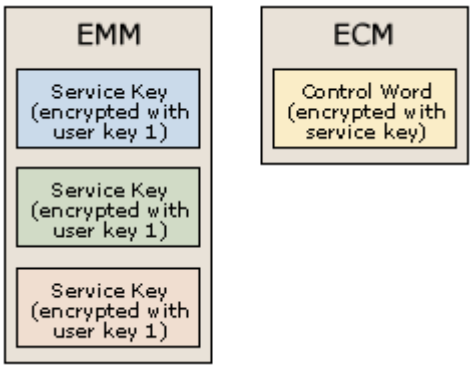





Cada servicio tiene una clave de servicio diferente. De esta manera podemos cifrar los servicios individualmente y dar acceso a unos y a otros no. Esta clave de servicio será común a todos aquellos usuarios que tengan contratado dicho servicio. Por otro lado cada usuario tiene en su decodificador una clave de usuario, única para él.

Para asegurarnos de que todos los usuarios que han pagado por un servicio puedan acceder a él, es necesario cifrar la clave de servicio con todas las diferentes claves de usuario que tengan acceso a ese contenido, y emitir todas las claves de servicio cifradas. En el descodificador de un usuario se analizará si la clave de servicio viene cifrada con su clave de usuario, y si es así, se procederá a la descodificación.

El sistema de acceso condicional dispone de dos tipos de mensajes para enviar esta información en el flujo de transporte. Estos mensajes de denominan "CA messages" y son de dos tipos: los ECM´s ("Entitlement Control Messages") y los ECM´s ("Entitlement management Messages"). En conjunto estos mensajes tiene la capacidad de controlar el acceso al contenido de los usuarios individuales o grupos de usuarios. La palabra de control cifrada se envía en los ECM´s, aproximadamente cada dos segundos, y las claves de servicio cifradas se envían en los EMM´s aproximadamente cada diez segundos.




Fuente: Interactive TV web ([1])

Una cosa que hay que tener en cuenta es que el proceso de cifrado/descifrado no tiene y no suele ser simétrico. Estamos asumiendo por simplicidad que las mismas claves se utilizan para cifrar y descifrar, pero esto no suele ser lo habitual.

Cuando a un receptor le llega un mensaje CA, se lo pasa al sistema de acceso condicional. Si es un EMM, el receptor comprueba si va dirigido a ese receptor, y si lo es, usará su clave de usuario para descifrar la clave de servicio.

A partir de entonces esa clave de servicio se utiliza para descifrar los ECMs que lleguen destinados para ese servicio y así recuperar la palabra de control. Una vez obtenida la palabra de control, puede empezar a descifrar el contenido.

Con el objetivo de generar los EMMs de manera adecuada, el sistema de CA necesita saber qué usuarios están autorizados a ver los diferentes eventos o servicios. El Sistema de Gestión de Suscriptores ("Subscriber Management System", SMS) se utiliza para fijar qué canales puede ver un usuario. Se trata de una gran base de datos de todos los usuarios conectado al sistema de facturación y al sistema de de CA. El SMS controla el sistema de CA decidiendo qué EMMs se deben generar y así permitir que cada usuario vea solo los contenidos a los que tiene acceso.

Los ECMs y los EMMs se difunden como parte del servicio. Los PIDs para el CA están enumerados en la CAT, y pueden usar diferentes PIDs para los ECMs y los EMMs ([1]).

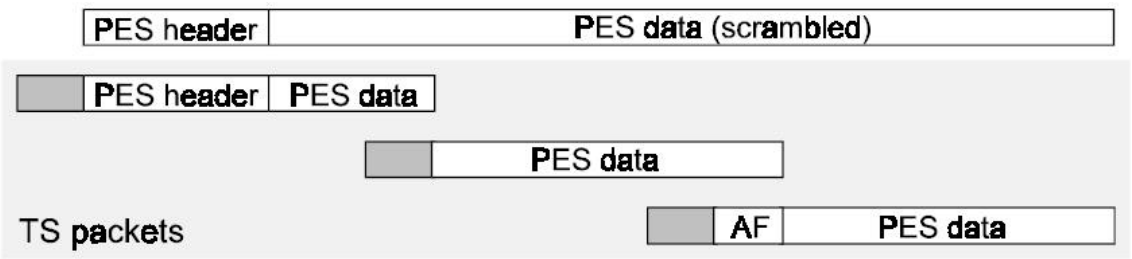
**Cifrado a nivel de flujo de transporte o de PES**

Como se ha dicho anteriormente, podemos cifrar la información a dos niveles. El más intuitivo es el nivel de flujo de transporte: la cabecera se deja sin cifrar, y la carga del paquete sí que se cifra.

El cifrado a nivel de PES es un poco más complejo. Cómo se indica en la ETR 289 ([3]), Este método requiere que la cabeza del PES no esté cifrada, y el resto del cuerpo sí. A continuación hay que dividir el paquete PES cifrado para introducirlo en los paquetes de transporte. Este proceso da lugar a tres tipos diferentes de paquetes de transporte según se reparta el PES:

- Un primer paquete de transporte con su propia cabecera (sin cifrar), la cabecera del PES (también sin cifrar) y la primera parte de la carga del PES cifrada. La cabecera del paquete PES no debe ocupar más de un paquete de transporte.
- Un número variable de paquetes de transporte, cada uno con 184 bytes del paquete PES. Cada bloque de 184 bytes está cifrado.
- Un último paquete que contiene el final del PES. Se pueden dar dos casos: que la parte que queda del PES sea exactamente de 184 bytes o no. Si es de 184 bytes se cifra de la misma manera que los anteriores. Si no es de esta longitud, el bloque del PES se alinea al final del paquete de transporte y se introduce un campo de adaptación ("Adaptation Field", AF) entre la cabecera del paquete de transporte y el último bloque del PES.

De manera esquemática:




Fuente: ETR 289 ([3])

Para evitar complejas implementaciones en los receptores de los usuarios es necesario seguir las siguientes recomendaciones:

- Solo se puede cifrar a un nivel: a nivel de flujo de transporte o de PES, pero nunca ambos simultáneamente.
- La cabecera de un paquete PES cifrado no debe de exceder 184 bytes.
- Ningún paquete de transporte que lleve bloques de un PES cifrado debe de llevar AF ("adaptation field"), a excepción de paquete que lleve el último bloque del PES, que lo llevará para alinear el bloque del PES al final del paquete de transporte.

Estas recomendaciones no se aplican cuando se trata de cifrado a nivel de flujo de transporte o con paquetes PES sin cifrar.

Si queremos cifrar secciones MPEG-2 tendremos que hacerlo a nivel de flujo de transporte e indicarlo en los bits de control de cifrado de los paquetes de transporte, ya que la sintaxis de MPEG-2 no nos permite incluir bits de control de cifrado en las secciones. No se pueden combinar secciones cifradas y no cifradas en un mismo paquete de transporte: es necesario separarlas. Para ello MPEG-2 define un mecanismo de relleno que se puede utilizar para crear paquetes de transporte con solo secciones cifradas o solo secciones no cifradas, rellenando el final del paquete de transporte con 0xFF.

Para controlar el proceso de cifrado, las especificaciones de MPEG-2 definen unos bits de control en la cabecera del los paquetes de transporte y en la cabecera de los paquetes PES. El significado de estos bits está solamente definido parcialmente, dejando algunos valores para futuros usos.

Valores de control para el flujo de transporte:

| Valor de los bits | Descripción |
|---|---|
| 00 | No hay cifrado a nivel de flujo de transporte |
| 01 | Reservado para usos futuros |
| 10 | Paquete de transporte cifrado con clave par |
| 11 | Paquete de transporte cifrado con clave impar |

Valores de control para el cifrado a nivel de PES:

| Valor de los bits | Descripción |
|---|---|
| 00 | No hay cifrado a nivel de paquetes PES |
| 01 | Reservado para usos futuros |
| 10 | Paquete PES cifrado con clave par |
| 11 | Paquete PES cifrado con clave impar |

## 3.2 Tabla de acceso condicional (CAT) y descriptores

La CAT proporciona la asociación entre uno o más sistemas CA, sus flujos de EMMs y cualquier parámetro especial relacionado con ellos. La tabla se divide en secciones, cuya sintaxis es la siguiente, como se especifica en [2]:

| Sintaxis de la sección CA | Nº de bits | Mnemónico |
|---|---|---|
| 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 |
| } | | |

Cada uno de los campos indica lo siguiente:

**table_id:** indica que se trata de una sección CA. Su valor en este caso es 0x01.

**section_syntax_indicator:** este indicador se debe de poner a 1.

**section_length:** los primeros dos bits de este indicador deben de ser '00'. Los otros 10 indican el número de bytes de la sección empezando inmediatamente después de este campo, e incluyendo el CRC. El valor de este campo no debe de exceder 1021.

**version_number:** este indicador indica el número de versión de la tabla CA entera. Este valor debe de incrementarse en 1 y en módulo 32 cuando hay cambios en la información de la tabla. Si el **current_next_indicator** vale 1, el **version_number** es el de la CAT en curso. Si **current_next_indicator** es 0, el **version_number** es el de la siguiente CAT.

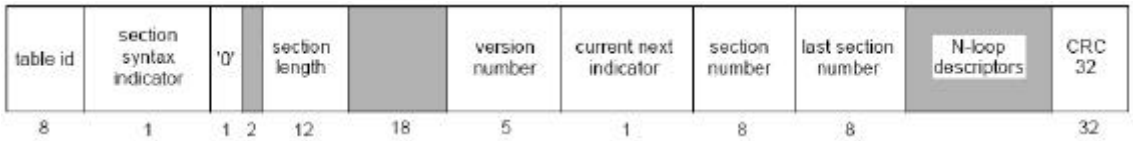
**current_next_indicator:** si vale 1, indica que la CAT enviada es aplicable. Si vale 0, quiere decir que la CAT enviada no es aun aplicable, pero que será la próxima en ser válida.

**section_number:** indica el número de sección dentro de la CAT. La primera sección de todas tendrá este valor a 0x00. Se debe incrementar en uno para cada nueva sección de la tabla.

**last_section_number:** especifica el número de la última sección de la CAT.

**CRC_32:** este valor es el de un código para detectar errores.

De manera gráfica la CAT queda como sigue:




Fuente: ISO/IEC 13818-1 ([2])

## Descriptor de acceso condicional

El descriptor de acceso condicional se utiliza para especificar información de gestión de acceso condicional como los EMMs y también para especificar información sobre flujos elementales como los ECMs ([2]). Este descriptor se utiliza en la TS_program_map_section y también en el program_stream_map. Si algún flujo elemental está cifrado, en descriptor de CA debe de estar presente para el programa que contiene ese flujo elemental. Por otro lado, si existe información relacionada con el sistema de acceso condicional dentro del flujo de transporte, también deberá haber un descriptor de acceso condicional en la CAT.

La sintaxis del descriptor es la siguiente:

| Sintaxis del descriptor de CA | Nº de bits | Mnemónico |
|---|---|---|
| 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 |
| } | | |
| } | | |

Los campos que forman el descriptor son los siguientes:

**descriptor_tag:** es un campo que identifica el descriptor. Para el descriptor de CA es el 9.

**descriptor_lenght:** indica el número de bytes que tiene el descriptor inmediatamente después de este campo.

**CA_system_ID:** indica el sistema de acceso condicional aplicable a los EMMs o ECMs asociados. En la ETR 162 ([4]) podemos encontrar las siguientes asignaciones:

| **CA_system_id values** | **CA system specifier** |
|---|---|
| 0x0000 | Reserved |

| | |
|---|---|
| 0x0001 to 0x00FF | Standardized systems |
| 0x0100 to 0x01FF | Canal Plus |
| 0x0200 to 0x02FF | CCETT |
| 0x0300 to 0x03FF | Deutsche Telecom |
| 0x0400 to 0x04FF | Eurodec |
| 0x0500 to 0x05FF | France Telecom |
| 0x0600 to 0x06FF | Irdeto |
| 0x0700 to 0x07FF | Jerrold/GI |
| 0x0800 to 0x08FF | Matra Communication |
| 0x0900 to 0x09FF | News Datacom |
| 0x0A00 to 0x0AFF | Nokia |
| 0x0B00 to 0x0BFF | Norwegian Telekom |
| 0x0C00 to 0x0CFF | NTL |
| 0x0D00 to 0x0DFF | Philips |
| 0x0E00 to 0x0EFF | Scientific Atlanta |
| 0x0F00 to 0x0FFF | Sony |
| 0x1000 to 0x10FF | Tandberg Television |
| 0x1100 to 0x11FF | Thomson |
| 0x1200 to 0x12FF | TV/Com |
| 0x1300 to 0x13FF | HPT - Croatian Post and Telecommunications |
| 0x1400 to 0x14FF | HRT - Croatian Radio and Television |
| 0x1500 to 0x15FF | IBM |
| 0x1600 to 0x16FF | Nera |
| 0x1700 to 0x17FF | BetaTechnik |
| 0x1800 to 0x18FF | Kudelski SA |
| 0x1900 to 0x19FF | Titan Information Systems |
| 0x2000 to 0x20FF | Telefónica Servicios Audiovisuales |
| 0x2100 to 0x21FF | STENTOR (France Telecom, CNES and DGA) |
| 0x2200 to 0x22FF | Tadiran Scopus |
| 0x2300 to 0x23FF | BARCO AS |
| 0x2400 to 0x24FF | StarGuide Digital Networks |

**CA_PID:** indica el PID de los paquetes del flujo de transporte que contienen los ECMs o los EMMs con la información para el sistema de acceso condicional especificado en el **CA_system_ID.**

Cuando el descriptor de CA está en una TS_program_map_section (table_id = 0x02) el CA_PID apunta a paquetes que contienen información de control de acceso al programa relacionado, tales como los ECMs. Su presencia como información de programa indica que se puede aplicar al programa entero.

Cuando, por otra parte, encontramos el descriptor de CA en una sección de CA, el CA_PID apunta a paquetes que contienen información de gestión y control de acceso, tales como los EMMs.

En la ETR 289 ([3]) se indican dos recomendaciones que deben cumplirse para el correcto funcionamiento del sistema de CA. Estas son:

- Todos los paquetes de transporte que tengan un PID igual al CA_PID dado en el descriptor de CA deben llevar solo información del sistema de CA. Ninguna información de CA puede ir en otro lugar.
- Dos proveedores de CA no deben tener los mismos valores de CA_PID en el mismo flujo de transporte.

## 3.3 Paquetes EMM y ECM

Como hemos ido diciendo, los paquetes EMM y los paquetes ECM son dos tipos de mensajes CA en donde va parte de la información necesaria para el sistema de CA. Los EMM y los ECM se transportan en mensajes de CA, y como se especifica en la ETR 289 ([3]) su sintaxis es la siguiente:

| Sintaxis de la tabla de mensaje de CA | 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 |
| } | | |
| } | | |

Las secciones de mensajes de CA se tratan como si fueran secciones privadas, tal y como se indica en ISO/IEC 13818-1 ([2]), a la hora de introducirlas en un flujo de transporte MPEG-2. Por otro lado, estas secciones no deben tener un tamaño superior a 256 bytes.

Los campos de la sección indican lo siguiente:

**table_id:** puede tomar los valores de la siguiente tabla ([3]):

| table_id | Descripción |
|---|---|
| 0x00 - 0x02 | MPEG specified |
| 0x03 - 0x3F | MPEG_reserved |
| 0x40 - 0x72 | V2-SI specified |
| 0x73 - 0x7F | DVB_reserved |
| 0x80 | CA_message_section, ECM |
| 0x81 | CA_message_section, ECM |
| 0x82 - 0x8F | CA_message_section, CA System private |
| 0x90 - 0xFE | private |
| 0xFF | ISO_reserved |

Hay dos valores posibles para el transporte de ECMs: 0x80 y 0x81. Cuando cambia este valor en una transmisión, quiere decir que ha habido un cambio en el contenido de los ECMs. Este cambio se puede utilizar para filtrar información de acceso condicional.

**section_syntax_indicator:** este bit debe de estar siempre fijado a 0.

**DVB_reserved:** este término indica que este campo se va a usar en el futuro para aplicaciones DVB y por lo tanto no se debe de utilizar para aplicaciones privadas.

**ISO_reserved:** este término indica que el valor de este campo se va a definir en el futuro para extensiones ISO y por lo tanto no está especificado por DVB.

**CA_section_length:** indica el número de bytes que siguen a este campo hasta el final de la sección.

**CA_data_byte**: este campo de 8 bits transporta información de CA privada. Los 17 primeros CA_data_bytes se pueden utilizar para realizar un filtrado de direcciones.

# 4 ARQUITECTURA DEL SISTEMA DE ACCESO CONDICIONAL

En la actualidad los proveedores de contenidos, los operadores de red y los fabricantes de equipos suelen ser entidades diferentes.

Sería ineficiente que un operador de red tuviera acuerdos únicamente con un proveedor de contenidos para distribuir su información. Dicho operador tenderá a distribuir los contenidos de varios proveedores. Para ello es necesario buscar una solución a la interoperabilidad de varios sistemas de acceso condicional que gestionan la información que está siendo difundida por un mismo operador de red. En respuesta a este problema surge Simulcrypt.

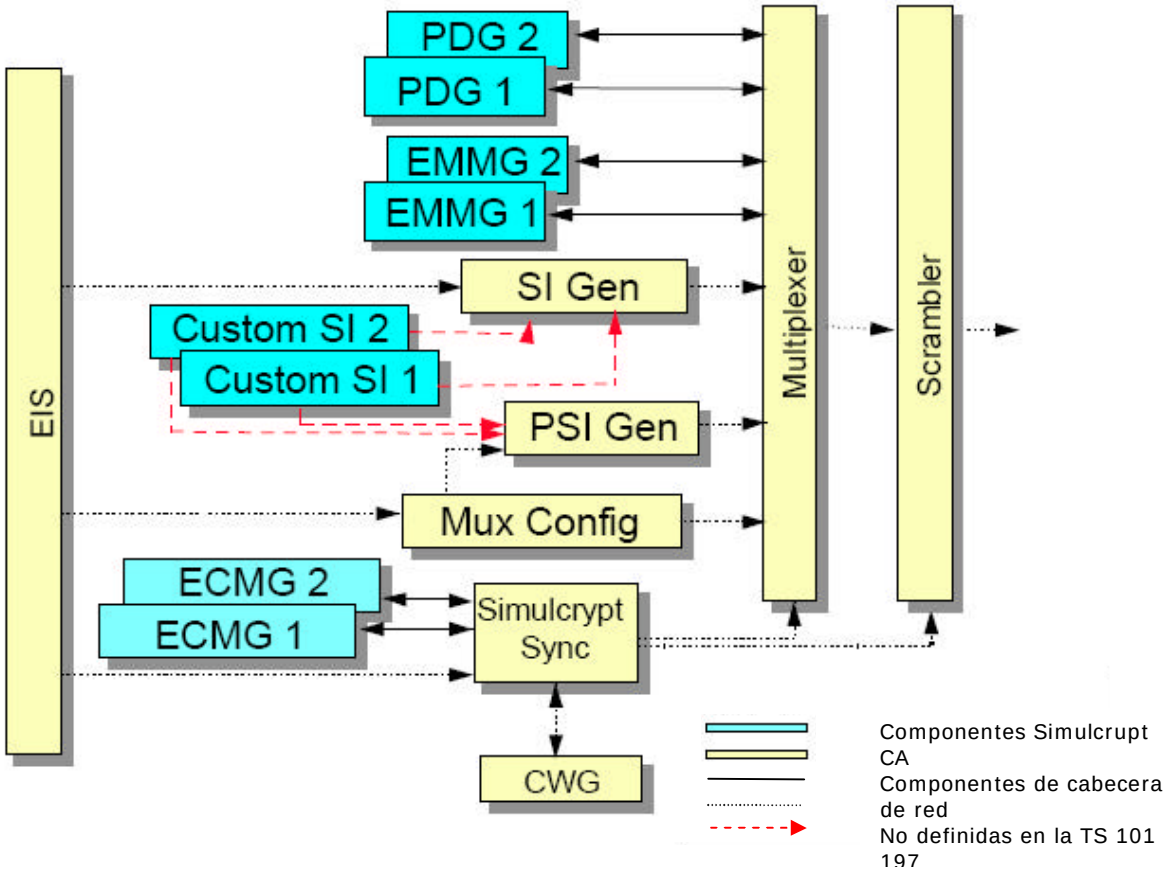
En Simulcrypt, el receptor-descodificador digital contiene únicamente un sistema de acceso condicional. No obstante, la información de más de un sistema de acceso condicional se puede insertar en las señales y los servicios que se van a emitir. De este modo, los receptores que utilizan cada uno un sistema de acceso condicional diferente pueden hacer uso de la correspondiente información de acceso condicional para descodificar la señal. Es necesario el acuerdo entre los distintos proveedores de servicios.

Por otro lado los fabricantes de equipos tienen que diseñar receptores que sean compatibles con el sistema de acceso condicional que utilizan los proveedores de contenidos. Esto implica que si un fabricante de equipos proporciona equipos a varios proveedores debe fabricar receptores diferentes que implementen los sistemas de CA adecuados. Podría pensarse en una solución alternativa: un mismo receptor para todos los sistemas de acceso condicional con una o varias interfaces comunes a la que añadir un módulo de CA.

Para ello surge Multicrypt, que es una técnica que consiste en intercambiar, en un receptor-descodificador digital, varios controles de acceso, gracias a uno o varios interfaces comunes. También permite a este terminal específico descodificar sucesivamente varios sistemas diferentes, en función del o de los elegidos. La ventaja de esta técnica es que los receptores-descodificadores pueden fabricarse en serie e integrar en última instancia el o los controles de acceso vigentes en el país donde son comercializados. La base del aparato permanece la misma. Sólo cambia el control de acceso. No sirve de nada enviar varias formas de codificación en la señal, como se necesita en el caso de Simulcrypt. En otras palabras, en Multicrypt, el receptor-descodificador digital es capaz de utilizar diversos sistemas de acceso condicional para descodificar los servicios procedentes de proveedores de servicios que utilizan distintos sistemas de acceso condicional. Esto se logra mediante la conexión del correspondiente módulo de acceso condicional al interfaz (interfaz común especificado por DVB) incorporado en el receptor.

## 4.1 Simulcrypt

Simulcrypt, en la TS 101 197 ([5]), define una arquitectura de cabecera de red que permite implementar un sistema que envía la información de CA de varios proveedores en un mismo flujo de transporte. El diagrama de bloques de dicha cabecera es el siguiente:




Fuente: TS 101 197 ([5])

Como se puede observar hay dos tipos de componentes: los de cabecera de red y los de CA Simulcrytp. Los componentes de cabecera de red son aquellos que deben de existir necesariamente para poder implementar el sistema Simulcrypt. Los componentes de CA Simulcrypt son aquellos que debe tener cada proveedor que quiera introducir su información de CA en el sistema.

Todas las flechas que podemos ver en la última figura son conexiones y flujos de datos. Las que nos interesan para implementar un sistema de CA Simulcrypt son aquellas que interconectan los elementos de CA Simulcrypt que son propiedad del proveedor de contenidos, con los elementos de la cabecera de red propiedad del operador de red.

En la TS 101 197 ([5]) solamente se definen y especifican las interfaces que conectan los componentes de CA con los componentes de la cabecera de red, quedando fuera de ella las interfaces que conectan entre ellos los componentes exclusivos de la cabecera de red. Hay que resaltar que únicamente quedan

definidas las interfaces y la manera de comunicarse entre los diferentes módulos, no la manera de implementar cada módulo concreto.

A continuación se pasa a explicar cada uno de los módulos por separado.

EIS: "Event Information Scheduler"

El EIS es la unidad encargada de manejar la información programada, las configuraciones y la información específica de CA que se requiere para el completo funcionamiento del sistema. Es la base de datos general para todo el sistema de cabecera de red. Una de sus misiones es la de proveer a los ECMGs a través del SCS la información que necesiten para generar los ECMs.

SCS: "Symulcrypt Synchronizer"

El SCS tiene varias misiones:

- Establecer conexiones TCP con los ECMGs y fijar un canal por conexión.
- Fijar los flujos necesarios dentro de los canales y asignar los valores ECM_stream_ID.
- Obtener las CWs ("Control Words") de los CWGs.
- Proporcionar las CWs a los ECMGs pertinentes en los flujos pertinentes, así como cualquier información específica de CA.
- Obtener los ECMs de los ECMGs.
- Sincronizar cada ECMs con su CP ("Crypto Period"), asociados en función de los parámetros del canal.
- Introducir estos ECMs en el multiplexor y solicitar su repetición en función de los parámetros del canal.
- Proveer la CW al cifrador para usarla en su CP específico.

ECMG: "Entitlement Control Message Generator"

El ECMG recibe las CWs en un mensaje CW provisional así como los criterios de acceso y responde con un mensaje ECM o un mensaje de error. El ECMG no repite periódicamente los mensajes ECM.

EMMG: "Entitlement Management Message Generator"

Este componente, proporcionado por el proveedor de CA, debe tener una interfaz directa con el multiplexor. El EMMG debe de iniciar las conexiones con el multiplexor.

PDG: "Private Data Generator"

Este componente se muestra en la arquitectura de DVB Simulcrytp para subrayar el hecho de que la interfaz del EMMG al multiplexor se puede usar para transmitir los EMMs e información privada relacionada al CA. El PDG inicia las conexiones con el multiplexor.

SIG: "Custom Service Information Generator"

Este componente es el responsable de generar información privada de SI. Tiene interfaz con el generador de SI y con el generador de PSI.

MUX Config: "Multiplexer configuration"

Este componente es el encargado de configurar el multiplexor y de proveer un enlace al generador de PSI para construir y adjuntar la PSI.

Generador de SI

Este componente es el responsable de generar la información de SI del sistema, definida en la EN 300 468 ([7]). Toma su información principal del EIS y la información suplementaria la toma de los servidores SI proporcionados por los proveedores de CA.

Generador de PSI

Este componente es el responsable de generar la PSI del sistema, como se define en la ISO/IEC 13818-1 ([2]). El servidor PSI toma su información principal del MUX Config y la información suplementaria la obtiene de los servidores de SI proporcionados por los proveedores de CA.

MUX: "Multiplexer"

El papel de este componente de la cabecera de red es la de realizar la multiplexación en el tiempo de la información que le llega, obteniéndose a su salida un flujo de transporte MPEG-2. La información de entrada pueden ser paquetes de transporte, secciones MPEG o datos sin tratar.

El multiplexor debe comunicarse con el SCS, y debe de aceptar conexiones de los EMMGs.

SCR: "Scrambler"

El SCR es el cifrador. Se encarga de cifrar la información que deba ser cifrada con la clave pertinente.

CWG: "Control Word Generator"

El CWG se encarga de generar las palabras de control con las que se van a cifrar los datos. Se debe poder comunicar con el SCS.

**Comunicación entre módulos: mensaje genérico**

En todas las interfaces, la estructura de los mensajes debe de ser la siguiente:

```
generic_message
{
   protocol_version 1 bytes
   message_type 2 bytes
   message_length 2 bytes
   for (i=0; i < n; i++)
   {
      parameter_type 2 bytes
      parameter_length 2 bytes
      parameter_value <parameter_length> bytes
   }
}
```

Cada uno de los campos indica lo siguiente:

**protocol_version:** Campo de 8 bits que identifica la versión del protocolo. Su valor debe ser 0x01.

**message_type:** Campo de 16 bits que identifica el tipo de mensaje. Los mensajes no conocidos deben de ser ignorados por la entidad receptora.

**message_length:** Campo de 16 bits que indica el número de bytes en el mensaje inmediatamente después de este campo.

**parameter_type:** Campo de 16 bits que indica el tipo del siguiente parámetro. Los parámetros con valores desconocidos deben de ser ignorados por la entidad receptora.

**parameter_length:** Campo de 16 bits que indica el número de bytes del campo parameter_value que viene a continuación.

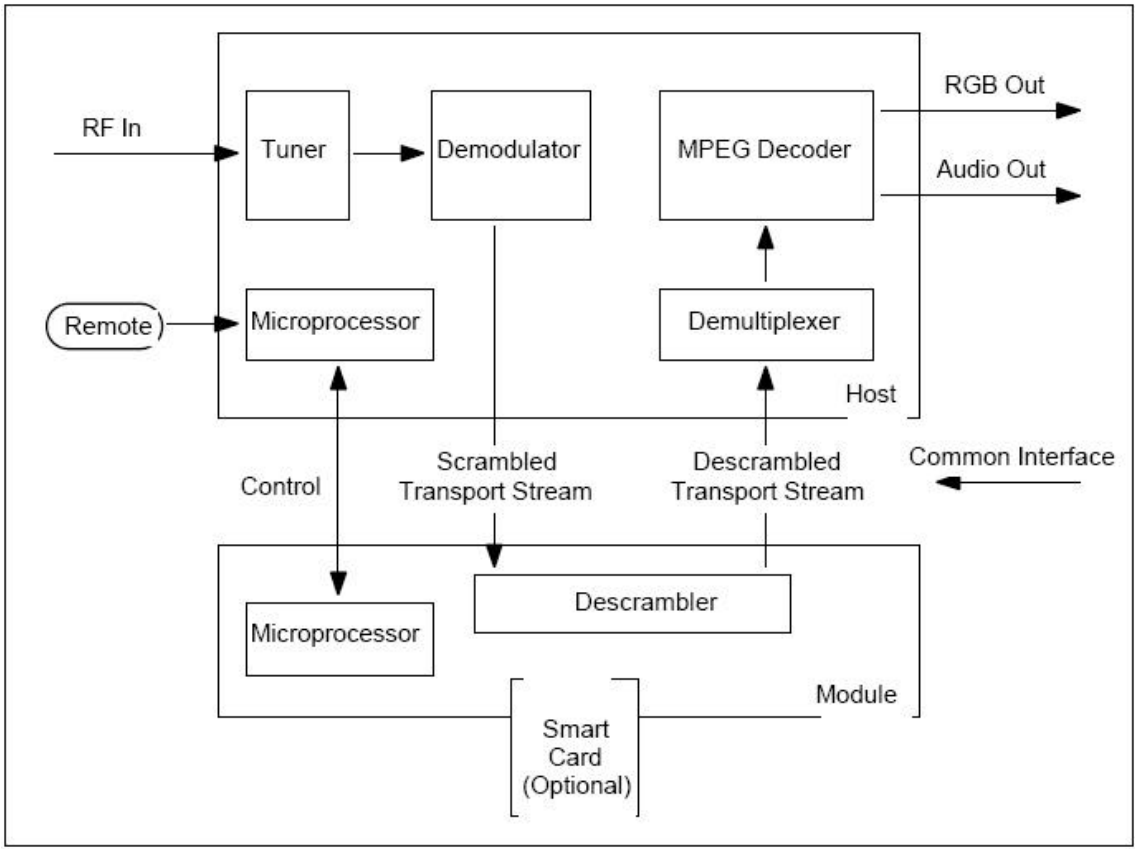
**parameter_value:** Campo de longitud variable que indica el valor real del parámetro. Su sintaxis depende del tipo de parámetro al que nos estemos refiriendo.

## 4.2 Multicrypt

Multicrypt, en la especificación EN50221 ([6]), define un interfaz común y estandarizado entre un receptor-descodificador y un módulo de acceso condicional, encargado de hacer las funciones propias de descifrado de la información. Las ventajas que ofrece este sistema son varias:

- Un mismo fabricante de equipos puede fabricar el mismo receptor base para diferentes sistemas de CA, al que se le puede añadir a través de una o varias interfaces diferentes módulos de CA.
- Un usuario puede contratar servicios de diferentes proveedores y mantener un único receptor, al cual solamente tiene que añadir los módulos de CA correspondientes.
- Un proveedor puede utilizar diferentes sistemas de CA para sus contenidos, incrementando su seguridad frente a ataques pirata.

El decodificador tiene la siguiente estructura:




Fuente: EN 50221 ([6])

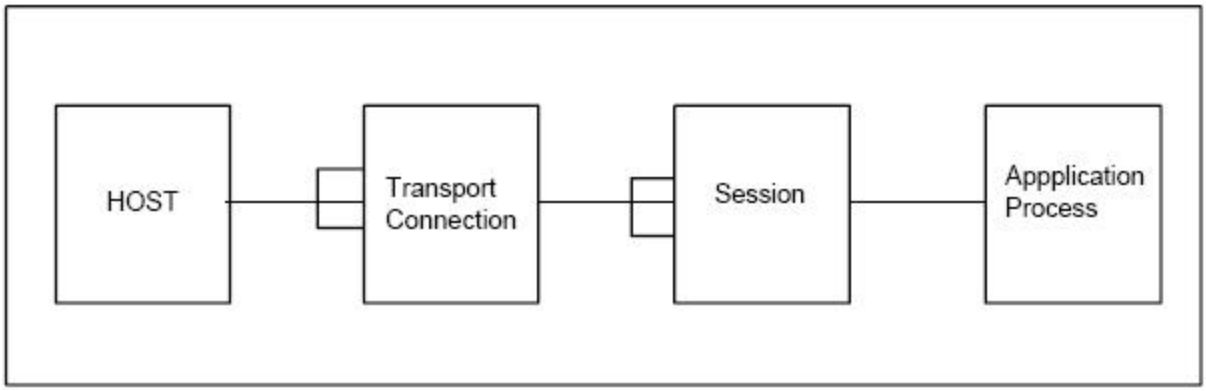
El decodificador incluye las funciones necesarias para recibir video, audio y datos codificados en MPEG-2.

Hay que incluir dos interfaces entre ambos módulos. La primera es la interfaz del flujo de transporte MPEG-2. La segunda, denominada interfaz de control, transporta órdenes entre el receptor y el módulo de CA.

La especificación EN50221 ([6]) está descrita en capas para permitir en el futuro variaciones de implementación. Las capas de aplicación y de sesión se definen para todas las aplicaciones que utilicen la interfaz común. La capa de transporte y la de enlace dependerán de la capa física que se use en una implementación concreta. La capa física se define en la EN50221 ([6]) e incluye una especificación completa del módulo.

La división por capas en la especificación permite gran flexibilidad en el uso de la interfaz. A parte del CA, se pueden implementar un gran número de aplicaciones diferentes. También permite el uso de múltiples sistemas de CA en el mismo receptor.

A continuación se muestra una representación de la división por capas de la interfaz de control. Es posible que el receptor deba abrir conexiones de transporte con más de un módulo, que puede estar conectado al receptor de manera directa o indirecta. Cada conexión se mantiene mientras el módulo esté conectado, y cada módulo debe gestionar diferentes sesiones con el receptor.




Fuente: EN50221 ([6])

## Arquitectura

La interfaz común se divide en dos componentes: la interfaz del flujo de transporte y la interfaz de control. Ambas están estructuradas en capas para hacer el proceso de diseño y de implementación más sencillo. Las capas superiores son comunes a todas las implementaciones, pero es posible realizar implementaciones alternativas de las capas bajas. La especificación EN50221 ([6]) incluye una basada en el estándar PC Card, pero también se indica que es posible que en futuras versiones se incluyan más.

### Interfaz de flujo de transporte

La interfaz de flujo de transporte lleva paquetes en ambas direcciones. Si el módulo da acceso a algún servicio del flujo de transporte y esos servicios han sido seleccionados por el receptor, entonces esos paquetes que llevan dichos servicios vuelven del módulo externo al receptor descifrados, y el resto de paquetes no se modifican. Podemos ver a continuación la división por capas de la interfaz de flujo de transporte:

| Upper Layers |
|---|
| Transport Layer |
| PC Card Link Layer |
| PC Card Physical Layer |

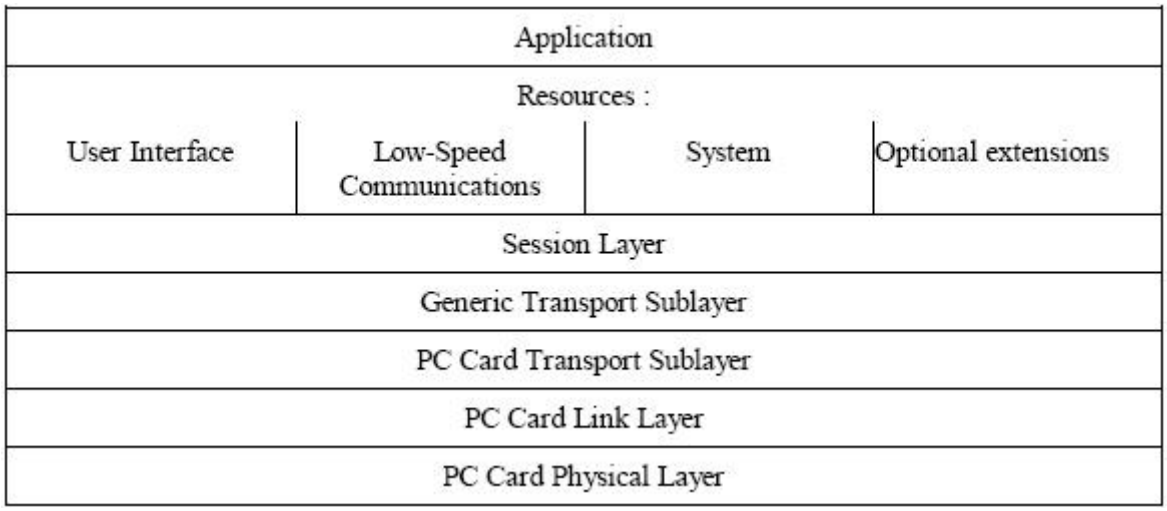
Fuente: EN50221 ([6])

La capa de transporte y las capas superiores están definidas en la especificación de MPEG-2, ISO/IEC 13818-1 ([2]).

### Interfaz de control

La interfaz de control lleva todas las comunicaciones entre las aplicaciones que se están ejecutando en el módulo externo y el receptor. Los protocolos de comunicación en esta interfaz están definidos en diferentes capas con el objetivo de proveer las funcionalidades necesarias. Estas funcionalidades son la capacidad de

soportar múltiples módulos externos en el receptor, la capacidad soportar combinaciones complejas de transacciones entre el módulo y el receptor y un conjunto extensible de primitivas funcionales que permiten al receptor proveer recursos al módulo. La división por capas se muestra en la siguiente figura:




Fuente: EN50221 ([6])

Las capas de sesión, recursos y de aplicación son comunes a todas las implementaciones físicas. La implementación de PC Card de la EN50221 ([6]) tiene su propia capa física y de enlace, así como su propia subcapa de transporte. Es posible que futuras implementaciones físicas difieran en estas capas.

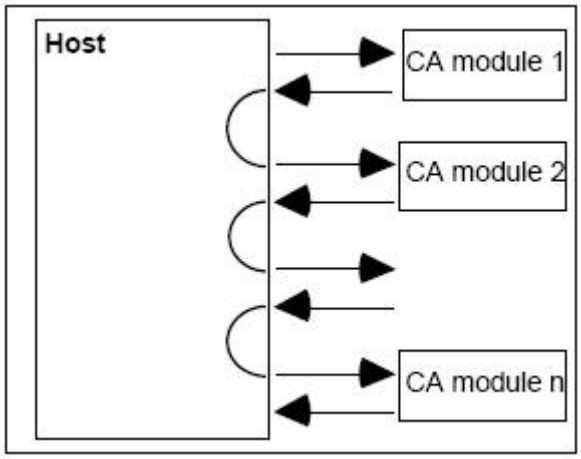
La capa de aplicación se ha diseñado para ser independiente de la sintaxis de una aplicación específica. Esta estrategia permite implementar de manera sencilla módulos que realizan otras tareas además de las relacionadas con las de acceso condicional.

Módulos múltiples

La capa de aplicación no impone un límite en el número de módulos que se pueden conectar al receptor al mismo tiempo. Sin embargo, el diseño concreto del receptor y las capas físicas sí que lo harán.

La especificación de la capa física debe permitir que haya varios módulos conectados a la vez al receptor, a pesar de que el diseño del receptor permita únicamente una conexión. Idealmente la capa física no debería imponer un límite en el número de módulos que se pueden conectar, pero en realidad hay un límite impuesto, que no debe ser menor a 15 módulos.

Cuando se puede conectar más de un módulo, la interfaz de flujo de transporte debe pasar a través de cada módulo, atravesándolos todos tal y como se muestra a continuación:




Fuente: EN50221 ([6])

El receptor debe de mantener simultáneamente y de manera separada interfaces de control con cada módulo, de tal manera que las transacciones entre receptor y módulo se puedan tratar de manera independiente para cada módulo. Cuando se desconecta un módulo la conexión de la capa de transporte de la interfaz de control de los otros módulos no se debe interrumpir o terminar.

Si hay varios módulos conectados al receptor, éste debe ser capaz de seleccionar el módulo o módulos encargados de descifrar los servicios seleccionados.

# 5 Estudio de prestaciones y características de sistemas de acceso condicional

## 5.1 Revisión de sistemas

A continuación se presentan los sistemas más relevantes a nivel mundial que están en uso. A excepción de los sistemas abiertos es muy difícil conseguir información detallada de los sistemas privados. De estos últimos solo se dispone de lo que se puede encontrar en sus páginas web. Normalmente no es información detallada ni técnica. Se trata de información que describe las prestaciones que ofrece y las innovaciones que aporta frente a otros sistemas.

### 5.1.1 ISMA Crypt

ISMA Crypt es el nombre no oficial del sistema de cifrado "ISMA Encryption and Authentication", desarrollado por ISMA ("Internet Streaming Media Alliance").

El documento público ([8]) que se puede descargar de la página web de ISMA ([9]) define el cifrado del contenido, los servicios de autentificación de mensajes, un formato de carga RTP y un formato de contenido precifrado para ISMA 1.0, ISMA 2.0 y cualquier contenido que se pueda almacenar como un flujo elemental en un archivo ISO.

La estructura que ofrece ISMA Crypt es extensible a nuevas maneras de codificación de datos, se puede actualizar a nuevas transformaciones de cifrado y se puede aplicar a numerosos sistemas de seguridad y de gestión. ISMA Crypt define una forma de cifrar por defecto flujos de datos y de autenticación de mensajes.

### 5.1.2 Viaccess

Viaccess es un miembro del grupo France Telecom, y ha desarrollado soluciones de acceso condicional para televisión, Internet y telefonía móvil ([10]).

Para televisión digital ofrece tres soluciones diferentes: TV On, GD On, OD On, orientadas a difusores de diferentes tamaños.

TV On es una solución sencilla para difusores pequeños. Es una solución que permite hasta un máximo de 10 canales y 50.000 usuarios. No existe una base de datos de usuarios: los contenidos son de prepago, y los usuarios adquieren tarjetas inteligentes para ver los contenidos. La integración en la cabecera de red es rápida y sencilla con costes bajos. Solo se necesita un servidor para cifrar e insertar el contenido en el flujo. Las aplicaciones de Viaccess se ejecutan en un sistema operativo Linux y son compatibles con DVB Simulcrypt.

La solución de GD On ofrece un sistema de acceso condicional para operadores mayores. Permite tener entre 50.000 y 2.000.000 de usuarios, servicios multicanal y canales a la carta. La integración en la cabecera de red es rápida, sencilla y de bajo coste. Existe una base de datos de clientes, gestionada por el sistema de Viaccess que se actualiza con cada tarjeta inteligente nueva. Este sistema utiliza un sistema operativo Linux, bases de datos Oracle y es compatible con DVB Simulcrypt.

OD On permite tener también un número de clientes que va desde los 50.000 a los 2.000.000. Ofrece servicios multicanal, canales a la carta y Pay-per-view. De modo opcional permite tener servicios de video-on-demand. El contenido se protege para entrega y para redistribución. Esta solución ofrece gran flexibilidad en la contratación de canales, PPV y VoD.

Algunos usuarios de este sistema son NTV Plus, Poverkhnost, CanalSat, algunos canales de Viacom y Turner Europe.

### 5.1.3 Betacrypt

Betacrypt es un sistema de acceso condicional de la antigua compañía Betaresearch, que ahora es Comvenient, y que ofrece diferentes soluciones para televisión digital ([11]).

Ofrece dos sistemas de cifrado: el Basicrypt, que ofrece un cifrado sencillo y con una opción con canal de re torno (Basicrypt R), y Betacrypt 2, que ofrece un cifrado complejo y también una opción con canal de retorno (Betacrytp 2 R).

El sistema Basicrypt ofrece un sistema de CA escalable a millones de usuarios con o sin canal de retorno de bajo coste sin necesidad de tarjeta inteligente, ofreciendo gran flexibilidad al proveedor, sea grande o pequeño. Es compatible con el estándar DVB, por lo que se puede implementar en todas las STBs compatibles con DVB, tarjetas PC-TV e interfaz común.

El sistema Betacrypt es un sistema más complejo y a la vez seguro que el Basicrypt. Está realizado en el marco de DVB, por lo que es compatible con todos los equipos que implementan este interfaz. Algunas de sus características técnicas son la utilización de claves de 128 bits, diversificación de claves, tarjetas inteligentes multisector, repetición de ataques preventivos, PPV y control paterno.

Algunos usuarios de este sistema son canales emitidos por satélite en Brasil y en Latinoamérica, y algunos canales emitidos por satélites Astra como el MTV o los de Premiere.

### 5.1.4 Nagravision

El sistema de CA Nagravisión, también conocido como Nagra, es un sistema de la empresa Nagravisión, que es una división y propiedad de la Kudelsky Group, con más de 71 millones de usuarios finales y más de 100 operadores que lo utilizan. Nagravisión es ahora la propietaria del sistema de CA Mediaguard ([12]).

Inicialmente se puede contratar un servicio básico como cifrado y descifrado de contenidos, PPV y subscripciones, pero se pueden ir ampliando los productos con servicios bajo demanda como DVR, Push-VOD, mensajería, t-commerce, t-banking y t-voting. Permite a los usuarios acceder a contenidos vía pay-per-view, impulse-pay-per-view, juegos, email, t-comercio y otros servicios interactivos. Nagravision también ofrece un sistema de SMS completamente integrado con su sistema de CA que permite gestionar todas las subscripciones.

El sistema Nagra es compatible con DVB. Existen más de 100 fabricantes de STBs y más de 10 fabricantes de cabeceras de red que implementan la tecnología de Nagravisión.

Algunos usuarios de este sistema son la plataforma Multicanal, TV Cabo, Abertis Telecom, RTVE y Digital Plus.

### 5.1.5 Irdeto

Irdeto ofrece un sistema de acceso condicional para difusores con audiencias de cualquier tamaño. Su sistema de acceso condicional y control es independiente de la plataforma de transmisión, pudiendo utilizarse para redes satelitales, terrestres o de cable. En abril de 2006 adquirió las actividades de CA de Philips, junto a su sistema Cryptoworks. En la actualidad el sistema Irdeto posee más de 300 clientes por todo el mundo ([13]).

A parte de ofrecer un sistema de CA, Irdeto tiene diferentes socios que le permite ofrecer soluciones extremo a extremo que incluyen todos los equipos necesarios para montar el sistema. Ofrece dos sistemas base a los que se les pueden añadir servicios: uno para pequeñas y medianas empresas y otro para grandes operadores.

El sistema Irdeto ofrece módulos adicionales para implementar soluciones pay-per-view, contratación de servicios a través del mando a distancia o por prepago, video-on-demand, un decodificador dual para visualizar los contenidos en dos televisiones y un codificador de video personal para guardar cifrados los contenidos que el usuario desee.

Una de las estrategias por las que apuesta Irdeto para aumentar la seguridad de los contenidos es la del continuo desarrollo de tarjetas inteligentes, que van sacando al mercado, dificultando los ataques piratas.

Algunos usuarios del sistema Irdeto son TV Banco do Brasil, DT Com, Auxtar, Foxtel y Optus Aurora.

### 5.1.6 Conax CAS7

El sistema Conax CAS7, desarrollado por la compañía Conax ofrece protección de contenidos para difusión en todo tipo de redes. Está construido sobre la fuerte plataforma tecnológica Conax ([14]).

El núcleo del sistema incluye los componentes necesarios para la TV estándar de pago y soporta un modo de suscripciones que permite a los usuarios acceso a uno o varios servicios por un periodo fijo de tiempo. Conax ofrece dos soluciones diferentes: Conax CAS7 Core y Conax CAS7 Extended.

Conax CAS7 Core permite a los operadores de TV digital empezar ofreciendo un servicio de televisión de pago básico. Permite ofrecer canales de TV o paquetes de canales de TV por con una subscripción por un periodo fijo de tiempo. Conax CAS7 Extended permite añadir diferentes servicios a Conax Core. Estos incluyen el envío de mensajes entre STBs, la contratación de eventos o de películas en near-video-on-demand, la compra de contenidos a través de SMSs, la compra de contenidos a través de tarjetas de prepago y otros servicios más relacionados.

Para ayudar a sus clientes en las operaciones diarias, Conax ofrece un acuerdo de operación en donde se responsabiliza del establecimiento, mantenimiento y operación del sistema de CA del cliente.

Algunas compañías que utilizan este sistema operadores nórdicos tales como Canal Digital y NRK, y otros latinoamericanos como ZAP y CDF.

### 5.1.7 BISS

BISS es un sistema de acceso condicional creado por la EBU-EUR (Unión Europea de Radiodifusión) y un grupo de difusores satelitales de Europa. Este sistema se considera como uno de los menos seguros ya que no utiliza ECMs para distribuir la información de decodificación.
El BISS es el acrónimo en inglés de Basic Interoperable Scrambling System o lo que es lo mismo en español, sistema básico de codificación interoperable. Es un sistema abierto que podemos encontrar en la página web de la EBU ([15]).

A diferencia de otros sistemas de acceso condicional más populares, BISS se usa para proteger ciertas transmisiones ocasionales de canales únicos de televisión por lo que no es utilizado por las plataformas. La gran ventaja de este sistema es que un receptor cualquiera que implemente BISS puede recibir una señal codificada en BISS (si se conocen las claves) independientemente del fabricante de los equipos, del operador de red… etc. Otra gran ventaja de este sistema es su menor coste frente a otros sistemas de CA.

Algunos usuarios de este sistema son emisoras de radio por satélite en países árabes y algunos canales de TV por satélite en Marruecos.

### 5.1.8 Dreamcrypt

El sistema de acceso condicional Dreamcrypt es un sistema abierto desarrollado por Dream Multimedia TV para funcionar exclusivamente con DVB. Existe un documento en su página web ([16]) especificando cómo implementarlo. A diferencia de otros sistemas comerciales de CA, Dreamcrypt solo especifica como implementar el receptor, dejando libertad en el manejo de la gestión de subscripciones.

Está diseñado para implementar receptores domésticos. El algoritmo de cifrado que utiliza, el TEA ("Tiny Encryption Algorithm") es también público. La especificación explica cómo implementar el receptor, pero no habla de la cabecera de red. Deja libertad a la entidad que haga uso de él para gestionar el acceso a los contenidos, pudiendo dar diferentes servicios cifrados a unos usuarios y a otros. Tampoco habla de cómo gestionar las subscripciones, dejando que el operador elija los canales que quiera para solicitar acceso a los contenidos. Esto implica que el operador tiene flexibilidad para ofrecer servicios por un periodo de tiempo fijado, servicios Pay-per-view etc.

Dreamcrypt no es un sistema muy usado. Lo utilizan algunos canales de cine adulto, como por ejemplo InXtc distribuido por T-Systems.

### 5.1.9 Codico CAS 5000

Codico CAS 5000 es un sistema de acceso condicional desarrollado por la empresa Scopus destinado a pequeñas y medianas empresas distribuidoras ([17]).

La empresa Scopus vende sus propios equipos necesarios para la transmisión y para la recepción de los contenidos. También dispone del módulo Codicrypt, que es un módulo de acceso condicional que se puede conectar a una STB que disponga de interfaz común, ampliando por tanto el número de receptores en los que se puede descifrar la información.

Tiene ofertas multicanal, contratación de eventos programados y subscripciones fijas por periodos de tiempo, permitiendo manejar de manera dinámica las subscripciones y autorizaciones. El algoritmo de cifrado que utiliza es propio y la estructura de su sistema de CA se basa en la de DVB con palabras de control, ECMs y EMMs.

Algunos de sus usuarios son SkyCast, America y algunos canales emitidos por T-Systems.

### 5.1.10 PowerVu

PowerVu es un sistema de acceso condicional desarrollado por la empresa Scientific Atlanta, de Cisco ([18]). Es un sistema profesional. Sus usuarios son compañías profesionales de cable o de satélite que usan sus servicios y equipos para redistribuir la señal. No es para uso doméstico.

PowerVu posee decodificadores que decodifican la señal proveniente de ciertos satélites para su redistribución. Estos decodificadores también se pueden usar como receptores de satélite FTA ("free-to-air") si se configuran adecuadamente. PowerVu se considera un sistema muy seguro y nunca ha sido comprometido ya que usa un complicado sistema que autoriza a cada receptor PowerVu y tiene un seguimiento de cada uno en cuanto a su uso y pertenencia. Solo los equipos de Scientific Atlanta pueden implementar PowerVu.

Algunas de las compañías que lo usan son Abertis Telecom, Bloomberg Television, Discovery Channel, AFRTS y American Forces Network. También lo usan compañías de cable para evitar que usuarios no autorizados vean sus contenidos.

Abertis Telecom emplea este sistema de acceso condicional para el transporte de señales dentro de su red técnica de difusión de canales terrestre en España. Esta aplicación guarda relación con el objetivo final del presente proyecto.

### 5.1.11 RAS

No se ha encontrado apenas información del sistema RAS. Es posible que se trate de un sistema profesional, ya que lo utiliza la plataforma APTN Asia y APTN Washington para proteger de manera global todos sus contenidos y no canales independientes.

### 5.1.12 Keyfly

KeyFly es un sistema de acceso condicional (CA) desarrollado por la empresa española SIDSA que es compatible con la plataforma DVB ([19]). El sistema puede integrar directamente una tarjeta en el CAM (Módulo de Acceso Condicional).

KeyFly es independiente de la cabecera de red que lo use ya que está basado en estándares públicos. Soporta una gestión distribuida de los subscriptores, permitiendo a otras organizaciones gestionar a los subscriptores. Proporciona múltiples interfaces al usuario, como Internet, SMS o centros de llamadas. También es compatible con la Interfaz Común, permitiendo utilizarlo en receptores que la tengan implementada.

KeyFly es una plataforma para televisión digital. Además de ofrecer seguridad como sistema CA, es una plataforma que permite nuevas fuentes de beneficio para la televisión de pago (pago por visión) o para los operadores en abierto. La plataforma va más allá de los sistemas de pago por suscripción tradicionales, incorporando modelos de negocio más flexibles sin necesidad de suscripciones permanentes, servicios de valor añadido a la televisión en abierto, así como nuevas formas de pago a través del teléfono móvil. KeyFly permite diferentes opciones con o sin tarjeta inteligente (smart card), CAS incrustada en un set-top box o en Common Interface CAMs, con o sin necesidad de suscripción. KeyFly soporta diferentes métodos para la gestión de derechos digitales desde los tradicionales sistemas de televisión de pago hasta la televisión en abierto con nuevos servicios de valor añadido.

KeyFly permite la compra de eventos de Pago por visión (PPV) o períodos de suscripción, que pueden ser pagados a través de SMS o Internet. Los tipos de suscripción abarcan desde las temporales a los modelos renovables donde el contenido es solicitado a través del teléfono móvil o Internet.

Algunos de sus usuarios son Al-Jazeera, TVE, Telefónica Servicios Audiovisuales y algunos canales emitidos por el Hot Bird.

### 5.1.13 Videoguard

VideoGuard es un sistema de codificación de señales audiovisuales, diseñado especialmente para los sistemas por satélite. Esta protección está desarrollada por la empresa NDS. Existen varias variantes de la protección dependiendo de las necesidades del proveedor. Este sistema de codificación es uno de los más extendidos por todo el mundo por las compañías audiovisuales ([20]).

NDS ofrece soluciones para televisión por cable, por satélite, IPTV y televisión para teléfonos móviles. La solución que NDS ofrece para la TV por satélite es VideoGuard STB. NDS no manufactura las STBs, pero existen más de 150 modelos de STBs que tienen implementado el sistema VideoGuard, y que funcionan con tarjetas inteligentes.

Permite ofrecer diferentes grupos de servicios, con diferente tarificación. También permite ofrecer eventos individuales Pay-per-view. También permite contratar eventos con el mando a distancia a través de la guía NDS, y comprar películas que se emiten en near-video-on-demand.

VideoGuard STB lo usan actualmente unas 50 plataformas en todo el mundo y tiene alrededor de 78 millones de usuarios. Algunos usuarios de VideoGuard son BSkyB, ONO, Itelsat y Cablevisión.

## 5.2 Sistemas profesionales y domésticos

La principal diferencia entre los sistemas de acceso condicional profesionales y domésticos es el entorno en el que se va a usar. Los sistemas domésticos son aquellos que posibilitan a los usuarios finales su implementación en los receptores. Pueden ser sistemas basados en tarjetas inteligentes, en módulos de acceso condicional que se conectan a través de una interfaz común o en receptores que lo llevan todo integrado. Estos sistemas son los más numerosos. Ejemplos de ellos son Videoguard, que implementa una tecnología de tarjetas inteligentes, Codico, que implementa una tecnología basada en receptores propios y de módulos de CA que se conectan a través de una interfaz común, Nagravisión o KeyFly, todos ellos de pago. Como ejemplos de sistemas abiertos están BISS o Dreamcrypt.

Los sistemas profesionales son sistemas cuyos costes, mantenimiento e instalación no pueden ser afrontados por un usuario final. Son sistemas que utilizan las plataformas de televisión para proteger sus contenidos en el proceso de distribución antes de llegar a los usuarios finales. La implementación de estos sistemas es mucho más cara. Requieren un nivel de seguridad mayor que los sistemas domésticos ya que la información que protegen es mayor. Un buen ejemplo de este tipo de sistemas es PowerVu, de la empresa Scientific Atlanta, propiedad de Cisco. Ofrece un sistema de acceso condicional para empresas profesionales y todos los equipos necesarios para su implementación.

## 5.3 Criterios de comparación

### 5.3.1 Sistemas abiertos o propietarios

Un sistema abierto es aquel en el que no hay que de disponer de licencia para su uso.
La característica principal de esos sistemas es que existe una especificación pública. Puede usarlo libremente quien quiera, sin pagar por su uso. Esos sistemas suelen ser desarrollados por organizaciones o grupos con el objetivo de conseguir interoperabilidad entre los sistemas de acceso condicional de los distintos difusores. Son conocidos públicamente, y debido a ellos apenas se utilizan, a excepción de algunos canales o difusores pequeños que prefieren no pagar por el uso de un sistema propietario. Los sistemas abiertos suelen ser domésticos, y como ejemplo tenemos BISS o Dreamcrypt.

Los sistemas propietarios, por el contrario, pertenecen a la compañía que lo ha desarrollado o comprado y su uso está sujeto a licencias y a patentes. Es necesario pagar para usarlos y depender en mayor o menor manera de la compañía que lo ha desarrollado para su implementación y mantenimiento. Son sistemas que ofrecen gran cantidad de servicios y no solo el de cifrado y descifrado de información. Algunas compañías ofrecen diferentes variantes según el tamaño de la empresa difusora o según los servicios que se puedan dar. Estos sistemas son más seguros que los abiertos, ya que se guardan altamente en secreto porque su ruptura podría implicar graves pérdidas tanto para el difusor que lo utiliza como para la compañía que lo ha desarrollado. Por este motivo cuando es muy poca la información que se publica de ellos, y en las páginas web de las compañías que lo desarrollan apenas aparecen características técnicas detalladas. Algunos ejemplos de estos sistemas son VideoGuard, KeyFly y Nagra

### 5.3.2 Precio

Otro criterio importante de comparación es el precio del sistema. Los sistemas abiertos son de libre uso y por lo tanto no hay que pagar por ellos. Por otro lado, es necesario pagar por el uso de los sistemas propietarios.

Los sistemas abiertos especifican solamente una forma de cifrar y descifrar la información, a diferencia de los sistemas propietarios, que dependiendo del que se elija, ofrecen mayor o menor cantidad de servicios además del cifrado y descifrado de la información, como por ejemplo gestión de las subscripciones, capacidad de la contratación de eventos por diferentes canales, PPV, NVoD, VOD, mantenimiento, actualizaciones…etc. También dan la garantía de que un número muy reducido de personas van a conocerlo al detalle, haciendo más complicada su ruptura mediante ataques pirata.

Algunos sistemas propietarios, como por ejemplo PowerVu, solo se pueden utilizar con sus propios equipos, lo que hace que el precio del sistema sea mayor. Estos sistemas suelen ser los de uso profesional, ya que los fabricantes de sistemas de AC condicional domésticos tienden a tener una amplia gama de equipos compatibles.

### 5.3.3 Complejidad de implementación

La implementación depende enormemente de las características técnicas de cada sistema de acceso condicional. Debido a que los sistemas propietarios no publican apenas detalles de sus sistemas no podemos saber hasta que punto es de compleja su implementación. Pero sí que podemos sacar algunas conclusiones de lo analizado hasta ahora.

Los sistemas abiertos, al ser los que menos servicios y opciones ofrecen son los más sencillos de implementar. A continuación tenemos los sistemas propietarios domésticos. Algunas empresas ofrecen diferentes soluciones según el tamaño de la empresa difusora. Cuanto más pequeña sea la empresa más sencilla será la implementación del sistema. Si por el contrario se trata de una gran difusora, la implementación de dicho sistema será más compleja. También hay empresas que ofrecen diferentes soluciones según los servicios que se quieran tener. Cuantos menos servicios haya, más sencilla será la implementación. Por el contrario, cuantos más servicios se quieran ofrecer mayor será la complejidad. Por ejemplo, sistemas de acceso condicional que ofrezcan servicios que requieren un canal de retorno son más complejos de implementar que aquellos que no los necesiten. Por último nos encontramos con los sistemas profesionales, cuya implementación es la más compleja. Son sistemas muy seguros que requieren diferentes equipos para su implementación.

# 6 PROSPECCIÓN DE DVB-CPCM

## Introducción

DVB-CPCM es un sistema para gestionar los contenidos digitales de carácter comercial en un entorno de red con múltiples dispositivos de consumo. Protege contenidos después de que hayan sido recibidos por el consumidor para asegurar que su uso se ajusta de acuerdo con los derechos fijados por el poseedor o difusor del contenido y permite gestionar las copias que de ellos se realizan. Se encarga de controlar el uso de los contenidos desde que entran en el sistema CPCM hasta que llegan al consumidor final.

Las posibles fuentes de estos contenidos son las de difusión terrestre, por satélite y por cable, servicios de Internet, datos empaquetados y servicios para móviles. Se puede utilizar CPCM para proteger audio, video, aplicaciones o datos.

En la actualidad los usuarios pueden obtener contenidos multimedia de muy diversas maneras para después consumirlos en diferentes tipos de dispositivos. Los actuales mecanismos de protección de contenidos son demasiado simples para las redes con múltiples dispositivos. CPCM amplia las nuevas necesidades que surgen a raíz de esto, permitiendo ofrecer a los proveedores de contenidos más opciones a los consumidores.

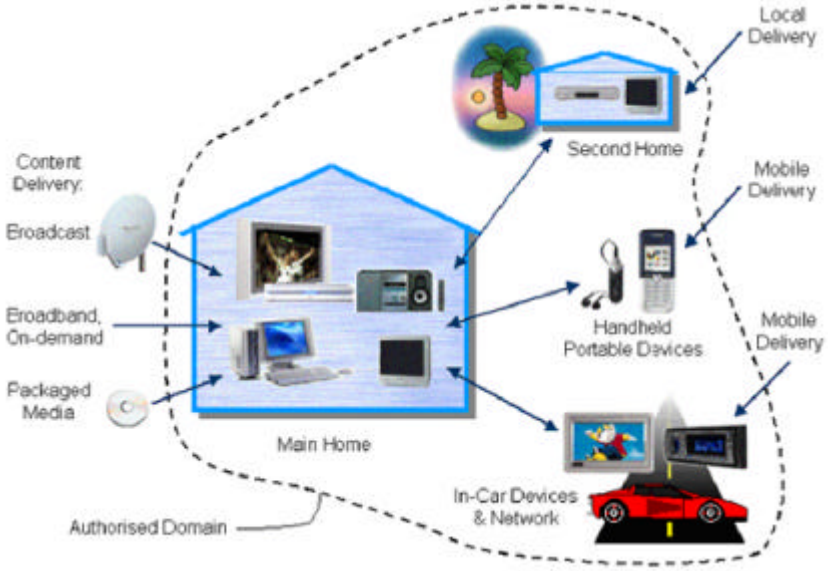
El propósito de CPCM es proporcionar un estándar abierto que permita la interoperabilidad entre dispositivos diferentes, resolviendo el problema de interconexión entre dispositivos que utilizan diferentes sistemas de protección de contenidos ([21]).

## Funcionamiento

CPCM no define unas normas para cifrar la información. Establece cómo se usan los contenidos una vez que han sido adquiridos, a diferencia de los sistemas de acceso condicional o DRM ("Digital Rights Management"), que protegen el contenido en su camino hasta el usuario.

Para ello se definen entornos locales y dominios autorizados. Un Dominio Autorizado ("Authorised Domain", AD) es un conjunto de dispositivos compatibles con CPCM controlados por los miembros de un mismo hogar. Existe una información específica para contenido denominada "Usage State Information" (USI) que describe cómo este contenido puede ser consumido, copiado o exportado en relación a su dominio autorizado y a su entorno local.

En la siguiente ilustración se muestra el entorno de CPCM y su relación con el dominio autorizado:




Fuente: DVB Fact sheet ([21])

Un contenido se puede mover por el interior del sistema CPCM, llevando siempre información bien definida sobre su uso. Todos los dispositivos deben interactuar con esta información, y actuar de manera coherente a lo que indique. Aquí entra en juego la buena fe de los fabricantes de dispositivos, que deben respetar estas normas de uso.

DVB-CPCM se basa en los siguientes elementos clave definidos en el DVB A094 ([22]):

**Modelo de Referencia ("Referente Model"):** proporciona un marco técnico y una arquitectura para el sistema DVB-CPCM.

**Información de Estado de Uso ("Usage State Informatidon", USI):** Proporciona un conjunto muy completo de información que indica el dominio autorizado de cada contenido. La USI define las normas para copiar y consumir un contenido dentro del dominio autorizado y dentro de un área geográfica así como normas para su exportación.

**Gestión del Dominio Autorizado ("Authorised Domain Management", ADM):** ADM es el mecanismo que permite que los dispositivos CPCM que pertenecen a un mismo hogar se unan al dominio autorizado DVB-CPCM.

**Herramientas de seguridad ("Security toolbox"):** Describe los algoritmos y protocolos de cifrado que se deben de usar para asegurar la interoperabilidad de implementaciones diferentes de CPCM.

**Especificaciones de sistema ("System specification"):** Describe el comportamiento global del sistema, los mensajes y los protocolos, además de cómo gestionar el contenido.

**Definiciones y terminología ("Definitions & Terms"):** Contiene abreviaciones, definiciones y terminología utilizada en DVB-CPCM.

**Instrucciones de implementación ("Implementation Guidelines"):** Describe cómo se puede utilizar CPCM en diferentes escenarios, por ejemplo en un entorno FTA ("free-to-air") o en un entorno de CA.

**Compatibilidad y Robustez ("Compliance & Robustness", C&R):** La especificación CPCM no describe un mecanismo para reforzar la C&R ya que no es función de DVB. Sin embargo, se dan una serie de indicaciones para ello.

La especificación aún no está completa. Sin embargo, está lo suficientemente avanzada como para ir realizando pruebas en paralelo con su desarrollo y así probar su viabilidad tecnológica.

# 7 BIBLIOGRAFÍA


[1] Interactive tv web: www.interactivetvweb.org

[2] ISO/IEC 13818-1: "Information technology - Generic coding of moving pictures and associated audio information: Systems"

[3] ETR 289: "Digital Video Broadcasting (DVB); Support for use of scrambling and Conditional Access (CA) within digital broadcasting systems"

[4] ETR 162: "Digital broadcasting systems for television, sound and data services; Allocation of Service Information (SI) codes for Digital Video Broadcasting (DVB) systems"

[5] TS 101 197: "Digital Video Broadcasting (DVB); DVB SimulCrypt; Head-end architecture and synchronization"

[6] EN 50221: "Common Interface Specification for Conditional Access and other Digital Video Broadcasting Decoder Applications"

[7] EN 300 468: "Digital Video Broadcasting (DVB); Specification for Service Information (SI) in DVB systems"

[8] TN01207: "Isma encryption and authentication, Version 2.0"

[9] Página web de Isma: www.isma.tv

[10] Página web de Viacces: www.viaccess.com

[11] Página web de Betacrypt: www.comvenient.com

[12] Página web de Nagravisión: www.nagravision.com

[13] Página web de Irdeto: www.irdeto.com

[14] Página web de Conax: www.conax.com

[15] Página web de la EBU-EUR: www.ebu.ch

[16] Página web de Dream Multimedia TV: www.dream-multimedia-tv.de

[17] Página web de Scopus: www.scopus.net

[18] Página web de Scientific Atlanta: www.scientificatlanta.com

[19] Página web de Sidsa: www.sidsa.es

[20] Página web de Nds: www.nds.com

[21] DVB Fact sheet - Agosto de 2007

[22] DVB A094: "Digital Video Broadcasting Content Protection & Copy Management (DVB-CPCM)"