MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

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

Foro Técnico de la televisión digital

Especificación de receptores de televisión digital terrestre para acceso condicional

Versión 1.1.1

Elaborado por

Subgrupo 3 del Grupo de Trabajo 7 del Foro Técnico de la televisión digital

Coordinado por
Subdirección General de Infraestructuras y Normativa Técnica

Junio de 2009

Índice

1 Introducción

En el marco del Grupo de Trabajo 7 del Foro Técnico de la Televisión Digital se ha detectado la necesidad de elaborar una serie de documentos que recojan las especificaciones mínimas que deben cumplir los receptores de televisión digital terrestre que se comercialicen en el mercado español. Para ello se ha dividido la tarea en varios subgrupos:

- Subgrupo 1: Especificación básica de receptores de televisión digital terrestre.
- Subgrupo 2: Especificación de receptores de televisión digital para alta definición.
- Subgrupo 3: Especificación de receptores de televisión digital para acceso condicional.
- Subgrupo 4: Especificación de receptores de televisión digital para aplicaciones interactivas.

Los cuatro documentos se complementan entre sí, conteniendo el primero de ellos la especificación básica que debe cumplir cualquier receptor de televisión digital terrestre que se ponga en el mercado español para garantizar plena compatibilidad con las emisiones de televisión digital terrestre y que puede complementarse con uno o varios de los documentos elaborados por los subgrupos 2, 3 y 4, dependiendo de las funcionalidades que disponga el mismo.

Este documento, elaborado por el Subgrupo 3, “Especificación de receptores de televisión digital terrestre para acceso condicional”, define los requisitos mínimos que deben cumplir los receptores para permitir el acceso a los servicios de acceso condicional que se difundan a través de la televisión digital terrestre.

2 Documentos de referencia

[1] ETSI EN 300 744 Digital Video Broadcasting (DVB); DVB Framing structure, channel coding and modulation for digital terrestrial television.

[2] ETSI EN 300 468 Digital Video Broadcasting (DVB): Digital broadcasting systems for television, sound and data services: Specification for Service Information (SI) in Digital Video Broadcasting (DVB) systems.

[3] DVB A 011 Common Scrambling Algorithm. DVB Blue Book A011.

[4] ETSI EN 50221 Common Interface for Conditional Access and other Digital Video Broadcasting Decoder Applications.

[5] ETSI ETR 289 Digital Video Broadcasting (DVB); Support for use of scrambling and Conditional Access within digital broadcasting systems.

[6] ETSI TS 101 699 Digital Video Broadcasting (DVB); Extensions to the Common Interface Specification.

[7] ETSI ETR 154 ed3 Digital Video Broadcasting (DVB); Implementation Guidelines for the use of MPEG-2 Systems, Video and Audio in Satellite Cable and Terrestrial Broadcasting Applications.

[8] ETSI ETR 211 Digital Broadcasting Systems for Television, Sound and Data Services; Guidelines on the Implementation and Usage of DVB Service Information.

[9] ETSI TS 102 201 Digital Video Broadcasting (DVB); Interfaces for DVB Integrated Receiver Decoder (DVB-IRD)

[10] ETSI TS 101 154 DVB Specification for the use of Video and Audio Coding in Broadcasting Applications based on the MPEG-2 Transport Stream.

[11] ETSI TS 101 812 Digital Video Broadcasting (DVB); Multimedia Home Platform (MHP) Specification version 1.0.3

[12] ETSI TS 102 006 Digital Video Broadcasting (DVB) Specification for SSU (System Software Update) in DVB systems.

[13] ETSI TS 102 366 DVB Digital Audio Compression (AC-3, Enhanced AC-3) Standard.

[14] ISO/IEC 7816, partes 1 a 3 Identification cards - Integrated circuit cards with contacts, Parts 1-3. ISO/IEC International Standard IS 7816.

[15] NorDig Unified NorDig Unified Requirements for Integrated Receiver Decoders for use in cable, satellite, terrestrial and IP-based networks, Version 1.0.2.

[16] Ley 32/2003 Ley general de Telecomunicaciones y Real Decreto 2296/2004 Reglamento sobre mercados de comunicaciones electrónicas, acceso a las redes y numeración.

[17] AENOR UNE 133 300 AENOR UNE 133 300 Navegación y Acceso.Información de los contenidos en las emisiones de TDT.

[18] CENELC EN 62216-1 Receptores de TV digital terrestre para sistemas DVB-T. Parte 1: Especificación del receptor básico.

[19] CENELEC R 206 001 “Guidelines for Implementations and Use of the Common Interface for DVB Decoder Applications”.

[20] ISO/IEC 13818 Information Technology – Generic coding of Moving Pictures and associated audio information.

[21] CI Plus Specification V1.2. Technical Specification. CI Plus Specification. Content Security Extensions to the common interface.

[22] PPSCVA T1 Perfil de protección para la aplicación de creación y verificación de firma electrónica Tipo 1 de INTECO.

[23]DGTVi D-Book DGTVi D-Book 1.2, rev.1, Compatible DTV receivers for the Italian market: baseline requirements.

[24] EMV 4.2 Book 1. Application Independent ICC to Terminal Interface Requirements.

3 Abreviaturas

CAM	Módulo de Acceso Condicional (funciona a través del CI)
CAK	Núcleo de Acceso Condicional
CAS	Sistema de Acceso Condicional
CAT	Tabla de acceso condicional (Condicional Access Table)
CI	Interfaz Común
CW	Palabra de Control o palabra clave (Control Word)
DVB	Digital Video Broadcasting
ECM	Mensaje control de autorización
EMM	Mensajes de gestión de la autorización
EMV	Europay MasterCard Visa
ETSI	Instituto Europeo de Normas de Telecomunicaciones
INTECO	Instituto Nacional de Tecnologías de la Comunicación.
IRD	Receptor profesional
MMI	Interfaz Hombre Máquina (Man Machine Interface)
OTA	Descarga vía canal de ondas hertzianas (Over The Air).
PCMCIA	Personal Computer Memory Card International Association
PES	Flujo elemental de paquetes (habitualmente corresponde a un flujo de audio, vídeo o datos).
PID	Identificador de paquete (Packet ID)
PMT	Tabla de programa (Program Map Table)
S/W	Software
SAS	Sistema de gestión de derechos del abonado
SC	Tarjeta Inteligente (Smart Card)
SDT	Tabla descriptiva del Servicio (Service Description Table)
SMS	Sistema de gestión de abonados
SSU	Sistema de actualización de software (System Software Update)
STB	Receptor doméstico (Set Top Box)
TID	Identificador de tabla (Table ID)
TS	Trama de Transporte
UER	Unión Europea de Radiodifusión
USB	Universal Serial Bus

4 Marco regulatorio de los sistemas de acceso condicional

La Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones (en adelante LGTel) define en su Anexo II, Definiciones, Sistema de Acceso Condicional como:

"toda medida técnica o mecanismo técnico que condicione el acceso en forma inteligible a un servicio protegido de radiodifusión sonora o televisiva al pago de una cuota u otra forma de autorización individual previa".

La definición recogida en la LGTel es perfectamente aplicable en el entorno heredado del mundo de la difusión convencional, como es el caso de la televisión digital: se refiere a un mecanismo de protección del servicio para entregar contenido televisivo de pago a un receptor.

Además, la citada Ley indica que el sistema de acceso condicional está considerado como un recurso asociado a las redes de comunicaciones electrónicas y sometido, por tanto, a lo dispuesto para tales elementos:

Recursos asociados: *"aquellos sistemas, dispositivos u otros recursos asociados con una red de comunicaciones electrónicas o con un servicio de comunicaciones electrónicas que permitan o apoyen la prestación de servicios a través de dicha red o servicio; incluyen los sistemas de acceso condicional y las guías electrónicas de programas"*.

El artículo 24, condiciones relativas a los sistemas de acceso condicional, del Real Decreto 2296/2004, de 10 de diciembre, por el que se aprueba el Reglamento sobre mercados de comunicaciones electrónicas, acceso a las redes y numeración establece que en relación con los sistemas y servicios de acceso condicional empleados en el acceso a servicios de radiodifusión y televisión digitales, con independencia de cuál sea el medio de transmisión utilizado, deberán cumplirse una serie de condiciones.

"Artículo 24. Condiciones relativas a los sistemas de acceso condicional.

1. En relación con los sistemas y servicios de acceso condicional empleados en el acceso a servicios de radiodifusión y televisión digitales, con independencia de cuál sea el medio de transmisión utilizado, deberán cumplirse las siguientes condiciones:

a) Todo sistema de acceso condicional que se emplee deberá contar con la capacidad técnica necesaria para efectuar, con buena relación coste-eficacia, un transcontrol que permita a los operadores de la red la posibilidad de control completo de los servicios de difusión que empleen el sistema de acceso condicional en la totalidad de su red, así como en ámbitos inferiores al de cobertura de ésta, en particular y cuando sea pertinente, en el ámbito local o regional.

b) Los operadores y proveedores de los servicios de acceso condicional deberán ofrecer a los proveedores de servicios de televisión y radiodifusión digitales, en condiciones equitativas, razonables y no discriminatorias, medios técnicos que permitan a estos últimos habilitar la recepción de sus servicios por usuarios de los descodificadores gestionados por aquellos.

c) Los proveedores de servicios de acceso condicional deberán llevar una contabilidad financiera separada en lo que se refiere a su actividad de suministro de dichos servicios.

d) Los titulares de los derechos de propiedad industrial relativos a los sistemas y productos de acceso condicional concederán las licencias a los fabricantes de equipos de consumo teniendo en cuenta los condicionantes técnicos y de mercado, en condiciones equitativas, razonables y no discriminatorias, sin subordinarse a condiciones que prohíban, disuadan o desalienten la inclusión en el mismo producto de:

> *1.º Una interfaz común que permita la conexión con otros sistemas de acceso condicional, o bien*
>
> *2.º Medios específicos de otro sistema de acceso condicional, siempre que el beneficiario de la licencia respete condiciones razonables y apropiadas que garanticen, por lo que a él se refiere, la seguridad de las transacciones de los operadores de sistemas de acceso condicional.*

2. La Comisión del Mercado de las Telecomunicaciones podrá revisar periódicamente la conveniencia de mantener la imposición de las condiciones relacionadas en el apartado anterior o decidir su supresión o modificación, para lo que deberá efectuar un análisis de mercado, de conformidad con lo establecido en el artículo 3.

Si como consecuencia del citado análisis la Comisión del Mercado de las Telecomunicaciones determina que el mercado de servicios de acceso condicional se desarrolla en un entorno de competencia efectiva, podrá decidir la modificación o supresión de las obligaciones anteriores, e informará de ello a todas las partes interesadas con una antelación mínima de dos meses a su efectividad, siempre que dicha modificación o supresión no incida negativamente en las perspectivas de competencia efectiva en los mercados al por menor de servicios de televisión y radiodifusión digital o en los de sistemas de acceso condicional y otros recursos asociados.

En cualquier caso, no podrá determinar la modificación o supresión de estas condiciones cuando ello pudiera incidir negativamente en el acceso de los usuarios finales a los servicios de radiodifusión o televisión, o a los canales o servicios de programas de radio o televisión para los que, de conformidad con el apartado 4 de la disposición adicional séptima de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, se hubieran establecido obligaciones de transmisión."

Asimismo, el punto primero de la Disposición adicional segunda del antes citado Real Decreto, interoperabilidad de los equipos de consumo utilizados para la televisión digital, establece condiciones adicionales garantes de este proceso así como de los derechos de los consumidores tales como que los equipos receptores deberán tener la capacidad de descifrar señales con arreglo al algoritmo de cifrado común europeo y deberán permitir también la visualización de las emisiones en abierto:

"1. Los equipos para la recepción de señales de televisión digital disponibles a la venta, en alquiler o en otras condiciones, y con capacidad para descifrar señales de televisión digital, deberán incluir las siguientes funciones:

a) El descifrado de señales con arreglo al algoritmo de cifrado común europeo gestionado por una organización europea de normalización reconocida, en la actualidad el Instituto Europeo de Normas de Telecomunicaciones (ETSI).

b) La visualización de señales transmitidas en abierto, a condición de que, en los casos en que el equipo se suministre en alquiler, el arrendatario se halle en situación de cumplimiento del contrato correspondiente".

Finalmente, la citada disposición adicional determina que:

"2. …Los aparatos digitales de televisión dotados de una pantalla de visualización integral de una diagonal visible superior a 30 centímetros comercializados para su venta o alquiler deberán estar provistos, al menos, de una conexión de interfaz abierta, normalizada por una organización europea de normalización reconocida o conforme con la norma adoptada por esta o con las especificaciones adoptadas por la industria, y poder transferir todos los elementos de una señal de televisión digital, incluida la información relativa a servicios interactivos y de acceso condicional".

Este último párrafo establece, por tanto, que los receptores digitales de TV que incluyan una pantalla de visualización con una diagonal superior a los 30 cm deben estar dotados de una interfaz abierta susceptible de incorporar un sistema de acceso condicional externo. Esto es lo que se ha venido en denominar Interfaz Común, si bien el marco regulatorio no establece que protocolo concreto normalizado se debe utilizar.

Como conclusión cabe destacar que el marco regulatorio vigente establece claramente una serie de obligaciones a todas las partes implicadas: proveedores de sistemas de acceso condicional, fabricantes y operadores, para facilitar el acceso por parte de los usuarios a todos los servicios de acceso condicional disponibles, con el fin de que este mercado se desarrolle en un entorno de competencia efectiva.

5 Consideraciones técnicas sobre los sistemas de acceso condicional

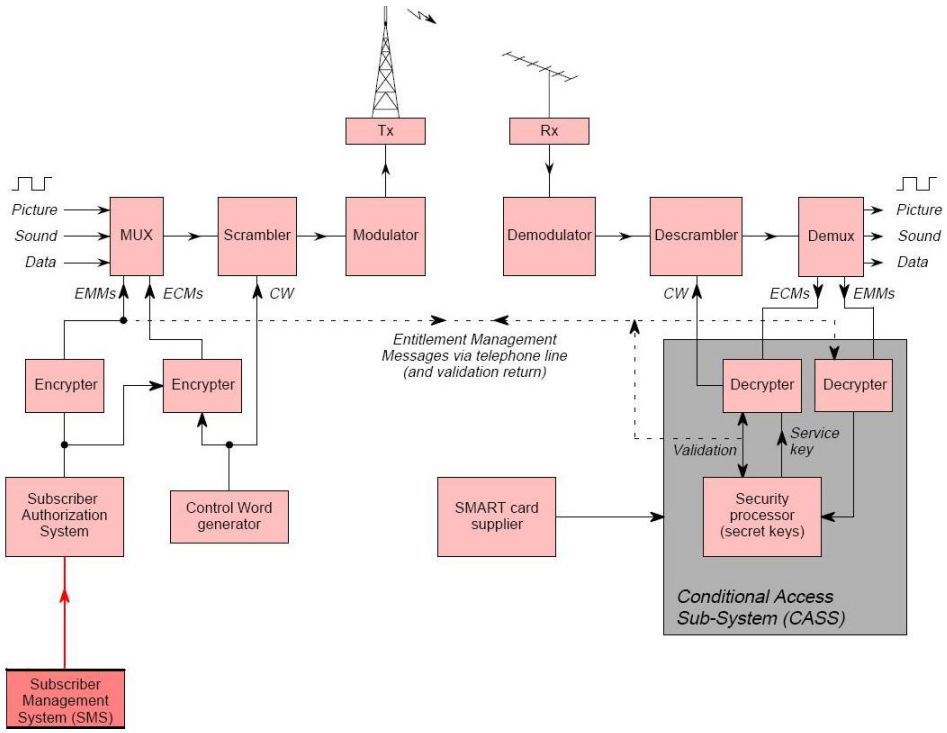
Los sistemas de acceso condicional (CAS), de acuerdo con la definición de la LGTel [16], se utilizan para ocultar los contenidos a aquellos usuarios que no disponen de los permisos adecuados y al mismo tiempo permiten ver los contenidos a aquellos usuarios que sí disponen de dichos permisos.

Un sistema de acceso condicional consta de un sistema de codificación del contenido más un sistema de cifrado de claves y derechos para prevenir una recepción no autorizada.

Los sistemas CAS pueden ser muy variados, los principales sistemas se basan en algoritmos estándares que se describen en la norma "DVB Common Scrambling Algorithm" [3]. Estos sistemas interactúan con la cabecera de TV digital y siempre que ambos sistemas cumplan con la norma DVB antes citada, el multiplexor será quién codifique los contenidos y envíe al sistema de acceso condicional la clave de encriptado.

El proceso de encriptación es complejo, se genera una palabra de control (CW) que sirve para codificar los contenidos digitales según el algoritmo utilizado y a la vez la misma CW se envía al receptor para que éste pueda desencriptar dichos contenidos si se obtienen los derechos pertinentes. En todo caso la encriptación podrá ser siempre a nivel de PES o bien a nivel de TS, pero no en ambos a la vez.

Una descripción funcional de los sistemas de Acceso Condicional se presenta a en la siguiente figura proporcionada por la UER:



Desde del punto de vista de coexistencia de sistemas, los sistemas de acceso condicional se pueden dividir en dos tipos:

- **Simulcrypt**. El mismo contenido se protege con dos sistemas de acceso condicional de forma simultánea. Normalmente el parque de receptores es diferente.

- **Multicrypt.** Que permite la implementación simultánea de varios CAS en el mismo dispositivo con el fin de proteger contenidos diferenciados.

Los sistemas de acceso condicional requieren de diversos elementos que se distribuyen entre la cabecera de TV digital y el descodificador digital. Atendiendo al grado de integración en los receptores digitales, estos sistemas pueden estar en un módulo externo o estar embebidos (con tarjeta inteligente o chip ensamblado) y ser genéricamente de los siguientes tipos:

- Sistemas basados en la Interfaz Común del DVB [4] (DVB-CI): En este tipo, el sistema de acceso condicional reside en un módulo Interfaz Común (CAM) externo (tipo la tarjeta PCMCIA de los sistemas informáticos), que se inserta en una ranura normalizada del DVB-CI en el descodificador. A su vez, la Interfaz Común puede disponer de una tarjeta chip externa para almacenar parte del sistema de acceso condicional o tenerlo todo integrado en el módulo CAM.
- Sistemas basados en una tarjeta inteligente: En este tipo de sistemas la seguridad está repartida entre un S/W residente y una tarjeta inteligente extraíble. La parte esencial del sistema de acceso condicional reside, por razones de seguridad, en una tarjeta inteligente del tipo ISO7816 [14]. El descodificador

traslada la información que proviene del operador a la tarjeta, y sigue las órdenes que provienen de la misma. El descodificador requiere de una ranura para interfaz ISO7816 en donde se inserta la tarjeta y de la integración de un módulo software en el descodificador para realizar las funciones antes indicadas. La parte de S/W residente en el receptor es actualizable vía las propias emisiones del canal de televisión.

- Sistemas basados en un chip, en los que el sistema de acceso condicional o parte de él está integrado en el chip, el cual, a su vez, debe ser integrado en el hardware del descodificador. No se requieren de elementos externos al descodificador. Todas las actualizaciones y gestión del sistema se realiza vía las propias emisiones del canal de televisión. Se debe tener en cuenta que los sistemas basados en chips también pueden estar alojados en las tarjetas CAM's.
- Sistemas basados en tarjeta inteligente virtual, en los que el STB tiene conectividad IP, disponiendo de un canal dedicado, permanente y seguro (mediante protocolos IP adecuados), entre el terminal y la red interactiva. Este canal permite realizar una función equivalente a la de la tarjeta inteligente, pero donde las operaciones de obtención de derechos se realizan en la red, en un servidor especial que provee el proveedor de la solución CAS.

Existen diferentes alternativas para la configuración de sistemas de Acceso Condicional desde un punto de vista del terminal. En todo caso se debe entender que los equipos son muy sensibles a las diferentes modalidades por lo que se debe minimizar las implicaciones en ellos:

- **Sistema Residente**. Sistema integrado y activado desde el inicio de la fabricación del terminal.

- **Sistema Descargado vía OTA**. Posteriormente a su salida al mercado y siempre que se hayan llegado a los acuerdos pertinentes entre los proveedores de CAS y los fabricantes de terminales se podrá realizar una descarga del CAK.

- **Sistema Durmiente**. En otros casos los fabricantes de terminales y proveedores de CAS llegan a un acuerdo para que los equipos lleven implantado un determinado sistema de acceso condicional, pero que no se active hasta que no reciba la instrucción por el aire.

6 Especificación técnica de receptores para acceso condicional

Esta especificación aplica a receptores TDT que dispongan de capacidad para el acceso a contenidos de pago distribuidos por la red de televisión digital terrestre, no siendo de aplicación para receptores TDT que adicionalmente a la recepción de contenidos TDT en abierto permitan acceder a contenidos de pago de otras plataformas.

Los sistemas de acceso condicional pueden estar o bien integrados en el receptor o bien en un Módulo de Acceso Condicional (CAM) que se inserte en una ranura de Interfaz Común (CI) y deben, en cualquier caso, cumplir con lo dispuesto en el artículo 24 del Real Decreto 2296/2004, de 10 de diciembre, sobre condiciones relativas a los sistemas de acceso condicional.

6.1 Requisitos mínimos generales.

Estos requisitos aplican tanto a los receptores con CAS embebido como a los módulos CAM. A ambos se les denominará genéricamente **dispositivos de Acceso Condicional** (CA).

Los dispositivos de acceso condicional deben:

- Contener un *descrambler* implementando el algoritmo DVB-CSA (Common Scrambling Algorithm) según se especifica en DVB A011 [3] y en ETSI ETR 289 [5].
- Implementar la recepción de ECMs y EMMs de acuerdo con la norma ETSI ETR 289 [5]. Así mismo deberá ser capaz de recibir por lo menos dos flujos de ECMs y un flujo de EMMs.

  Las ECMs deberán poder ser filtradas según:

  - PID
  - TID

  Las EMMs deberán poder ser filtradas según:

  - PID
  - TID
  - Campo de direccionamiento en la tabla (Específico del CAS)

  Éste último es específico de cada sistema de acceso condicional y se describe como parte de la interfaz de aplicación de la SC. El receptor deberá ser capaz de filtrar según tres combinaciones de TID y campo de direccionamiento simultáneamente.
- Soportar los tres tipos de acceso condicional definidos: residente, descargado y durmiente.
- Presentar en pantalla información sobre los datos de del servicio: Suscripción, PPV, derechos y otros.
- Permitir la actualización del núcleo del CAS a versiones posteriores con mejoras respecto a la actual. (Ver apartado 6.4)
- Permitir actualizar el software/firmware con otro sistema de acceso condicional CAS adicional. (Ver apartado 6.4)
- Implementar el bloqueo de menús.

- Soportar los modelos de negocio básicos: Suscripción y PPV.
- Soportar las funcionalidades de protección anticopia.
- El proceso de búsqueda y almacenamiento de canales será independiente del estado de encriptación de los canales.
- Para proporcionar soporte a un mercado horizontal a la vez que una plataforma abierta en donde cualquier fabricante pueda suministrar receptores con soporte a servicios de televisión de pago, el acceso condicional en el receptor no obligará a la utilización de una plataforma de receptor específica, en lo que al fabricante de chip decodificador se refiere con el fin de fomentar un marco de competencia; sin embargo cada proveedor de CAS podrá especificar, de forma no exclusiva para otros CAS, sus propios requisitos de seguridad al receptor para garantizar la seguridad en la protección del servicio extremo a extremo y evitar brechas. Dichos requisitos deben permitir la integración y posible coexistencia de otros CAS, según se dispone en el punto d) del Art. 24 del Real Decreto 2296/2004

De forma opcional el receptor podrá:

- Presentar un interfaz con el usuario donde se informe de los eventos encriptados.
- Soportar otros modelos de negocio como iPPV, PPT, NVOD, etc.
- Utilizar un control de contenidos tipo DRM o marcas de agua, si el receptor es de tipo PVR o con posibilidad de grabación.

6.2 Receptores con CAS embebido.

Los receptores con CAS embebido, tanto basados en tarjeta inteligente como en chip, serán capaces de albergar y trabajar con al menos 3 sistemas de acceso condicional, que pueden encontrase activos o durmientes o bien descargados por el aire. Esta solución implica que la memoria del receptor deberá estar adecuadamente dimensionada para el almacenamiento de los tres sistemas de Acceso Condicional.

6.2.1 Requisitos mínimos

Además de todos los requisitos mínimos de carácter general especificados en el apartado 6.1, los receptores con CAS embebido, de forma obligatoria, deben disponer de al menos un interfaz para tarjeta inteligente con las características que se recogen en el apartado 6.5.

Se considerará altamente recomendable que el receptor disponga:

- De al menos un interfaz común CI para servicios de acceso condicional con las características recogidas en el apartado 6.3.1.
- De dos o más interfaces de tarjeta inteligente con las características que se recogen en el apartado 6.5.

Asimismo de forma opcional el receptor podrá utilizar tarjetas SC síncronas.

6.3 Receptores con CI

La inclusión de un interfaz común (CI) es una solución alternativa a la integración de varios CAS en el receptor. El receptor debe emitir el TS encriptado hacia la CAM y recibe de vuelta el TS ya desencriptado. Así el conjunto de almacenado y entrega de

claves, así como de desencriptado, se encuentran ambos en la CAM y no en el terminal receptor.

Cada sistema de AC se implementa en una tarjeta (CAM) que se conecta al receptor a través del módulo CI.

Los módulos CAM serán capaces de albergar y trabajar con al menos 3 sistemas de acceso condicional, que pueden encontrase activos o durmientes o bien descargados por el aire. Esta solución implica que la memoria de la CAM deberá estar adecuadamente dimensionada para el almacenamiento de los tres sistemas de Acceso Condicional.

6.3.1 Requisitos mínimos

Los receptores que implementen esta solución deberán disponer de al menos una ranura de interfaz común CI que cumpla con la especificación EN 50221 [4] (más las extensiones definidas en TS 101 699 [6] y las directrices de implementación [19]). Excepto los recursos "*low speed communications*" y "*low level MMI*" que son opcionales.

El receptor deberá cumplir como mínimo los siguientes requisitos en cuanto al interfaz DVB-CI Versión 1 (al receptor se le denomina host en lo que sigue):

- El host debe soportar el interfaz MMI High Level como se especifica en EN 50221 [4].
- El host incluye un menú dedicado a y definido por el CAM dentro del menú principal.
- El host debe soportar pop-ups MMI.
- Los siguientes requisitos aplican a los menús y pop-ups del CAM:
    - Se deben mostrar en pantallas al menos 5 líneas simultáneamente.
    - En caso de pop-ups o menús de más de 5 líneas, se debe soportar scrolling.
    - Se deben poder mostrar al menos 50 caracteres en cada línea.
- Los pop-ups MMI deben tener el control de las teclas del control remoto hasta que el usuario sale del MMI.
- El MMI debe soportar las siguientes teclas del control remoto:
    - Teclas numéricas.
    - Flechas Arriba, Abajo, Izquierda, Derecha.
    - Tecla OK.
    - Teclas Atrás / Salir (Back/Exit).
- Si una tecla de control remoto de sistema (P+, P-, Menu, List, …) es presionada por el usuario mientras se está mostrando un pop-up del CAM en pantalla, el host cerrará el pop-up y realizará la tarea de sistema asociada.

- Durante el proceso de búsqueda automática de canales, todos los canales encontrados serán almacenados en el receptor independientemente del estado de encriptación del canal.
- El host permanece en la última frecuencia sintonizada después de entrar en el menú principal.
- Los pop-ups MMI tienen el control de las teclas de control remoto.

Para evitar problemas de interoperabilidad entre módulos CAM y receptores, se aplicarán los mecanismos de resolución de problemas de interoperabilidad documentados en el DGTVi D-Book [23], Anexo G.

6.3.2 Características del módulo CAM

Además de todos los requisitos mínimos de carácter general especificados en los apartados 6.1 y 6.3, el módulo CAM debe:

- Disponer de al menos un interfaz para tarjeta inteligente con las características que se recogen en el apartado 6.5.
- Contener o bien el dispositivo de seguridad de acceso condicional embebido o bien una interfaz para conectar una tarjeta SC:
  - Módulo CAM con CAS embebido: El módulo CAM contendrá todos los elementos y funciones necesarias para el funcionamiento del sistema de acceso condicional.
  - Módulo CAM con lector de tarjeta SC: El módulo CAM ofrecerá las funciones especificas de la interfaz común, según se describe en la norma ETSI EN 50221 y las funciones adicionales para la interfaz de tarjeta SC especificadas por el proveedor del sistema de acceso condicional.

6.3.3 Evolución a CI+

De forma opcional:

- Se tendrá en cuenta la inclusión del estándar CI+ una vez esté terminado el estándar como tal. Actualmente se está en fase de finalización de la versión 1.2 por el consorcio CI+. Por el momento no es un estándar ETSI. Dicha implantación aplica tanto a los receptores como a los módulos CAM.

NOTA: En caso de que el equipo receptor esté habilitado para la Alta Definición deberán tenerse en cuenta las especificaciones elaboradas por el Subgrupo de Trabajo 2: *"Especificaciones de receptores de televisión digital terrestre para alta definición"*.

6.4 Procedimientos para la actualización de software CAS

Para permitir una solución abierta en caso de que diferentes radiodifusores elijan diferentes accesos condicionales y para garantizar el correcto funcionamiento del acceso condicional en el dispositivo de acceso condicional, éste deberá:

- Ser capaz de reemplazar el sistema de acceso condicional a través de una descarga segura de un nuevo software/firmware realizada a través del aire vía OTA. Esto supone una implicación del fabricante del dispositivo de acceso condicional y del proveedor del Sistema de Acceso Condicional.

- Disponer de un sistema de actualización del SW CAS que no dependa del middleware incluido en el dispositivo de acceso condicional, a no ser que exista alguna dependencia conocida del middleware con el CAS.
- Evitar la interferencia entre los distintos CAS y permitir la actualización de cada uno de ellos de forma independiente.

NOTA: En cualquier caso para la actualización del software CAS será necesaria la coordinación entre los fabricantes de dispositivos de acceso condicional y proveedores de CAS, radiodifusores y operadores de red. Dicha coordinación se aplica en menor medida a fabricantes de receptores que dispongan de CI y no tengan CAS embebido.

De forma opcional podrá:

- Reemplazar el software / firmware a través de una interfaz local.
- Soportar la actualización del CAS a través de la conexión Ethernet.

6.4.1 Actualización del CAS vía radio (OTA)

Los dispositivos de acceso condicional deberán poder recibir nuevas versiones de software/firmware del sistema de acceso condicional mediante descargas seguras por el aire, cumpliendo con:

- La norma ETSI TS 102 006 que describe las actualizaciones el software y en su versión de perfil simple.

6.4.2 Actualización del CAS vía interfaz local

Los dispositivos de acceso condicional deberán poder modificar su software/firmware a través de una interfaz local de forma segura de forma que incorpore mecanismos de seguridad o bien en el protocolo de comunicaciones o bien en el contenido a actualizar.

- Lo realizarán mediante una conexión por puerto local, a través de:
  - Conexión por interfaz serie (RS-232, USB)
  - Conexión por interfaz común en el caso de CAMs.
  - Actualización en el arranque del equipo (Bootloader)
- Debe ser posible actualizar cada uno de los CAS que coexistan en el receptor de forma independiente.

6.5 Tarjetas inteligentes SC

El interfaz de tarjeta inteligente con el que deberán estar dotados todos los dispositivos CA debe:

- Soportar el uso de tarjetas SC externas que tengan como finalidad permitir el acceso a uno o varios sistemas de acceso condicional.
- Permitir la utilización de tarjetas SC asíncronas, contemplándose las siguientes excepciones:
  - No es necesario soportar Vpp
  - No es necesario implementar el pinout de AFNOR

- El rango de Vcc será de 5V +/-5%
- Icc max será de 65mA

6.5.1 Lector de Tarjetas SC

El lector de SC dispondrá de una interfaz hardware/firmware para desencriptar los contenidos protegidos con acceso condicional.

- Dicho interfaz cumplirá con el estándar ISO 7816 partes 1 a 3 [14].
- Este interfaz deberá ser accesible desde el exterior.

Opcionalmente el lector de tarjetas SC podrá:

- Cumplir la especificación de tarjetas inteligentes para tarjetas financieras EMV L1.
- Soportar el uso de DNI-e según la guía PPSCVA T1 de INTECO [22].

6.5.2 Tarjetas inteligentes

Las tarjetas deberán:

- Permitir el filtrado de flujos de EMMs, ECMs e interfaces de programa como se especifica más adelante para servicios de acceso condicional.
- Soportar la posibilidad de utilizar el protocolo de intercambio de datos T=0 y deberá ser posible incluir soporte para utilizar el protocolo de intercambio de datos T=1 mediante una ampliación del software.

6.5.3 Tarjeta virtual

Opcionalmente para terminales con canal de retorno por banda ancha a través de un interfaz IP los receptores podrán disponer de una solución CAS con un perfil basado en tarjeta virtual, de este modo:

- Disponer de este canal IP como sustituto de la tarjeta inteligente SC. El canal IP actuará de forma equivalente a las tarjetas inteligentes pero donde la obtención de los derechos se realiza en la red en un servidor especial que provee el propio proveedor de la solución CAS.

6.5.4 Receptores con CAS basado en un chip

Aunque el lector de tarjetas inteligentes (SC) sea obligatorio esto no impedirá:

- la utilización de otras soluciones existentes, como la utilización de chips de seguridad embebidos en el receptor.
- que cualquier otra solución tecnológica futura pueda ser considerada si resulta práctica y asegura una solución abierta.

6.6 Interfaz de nivel de aplicación para servicios de acceso condicional

La interfaz de nivel de aplicación para acceso condicional es específica de cada sistema de acceso condicional, pero deberá ser compatible con el middleware externo adoptado.

- El sistema de acceso condicional no deberá determinar el middleware del receptor, ya sea nativo o externo.

6.7 Información de servicio

El receptor debe:

- Ser capaz de interpretar el CA_descriptor en las tablas PMT y CAT de acuerdo con lo definido en la norma ETSI ETR 289 [5].
- El envío de información propietaria propia del sistema de acceso condicional como tablas, descriptores, etc. deberá así mismo cumplir con el estándar de señalización de DVB que es la norma ETSI EN 300 468 [2].
- Soportar la tabla CAT de acuerdo a la especificación ISO/IEC 13818 [20].
- Soportar el CA_identifier_Descriptor en la tabla SDT de acuerdo con la especificación ETSI EN 300 468 [2].

6.8 Interoperabilidad

Los receptores deberán asegurar una compatibilidad con los diferentes sistemas de acceso condicional que puedan estar presentes en el mercado nacional, sea cual sea la naturaleza de su implementación, bien a través de tarjetas módulos CAM o chips, siempre y cuando se cumplan las condiciones de integración negociadas entre el fabricante del receptor y el proveedor de acceso condicional.

Se debe también asegurar la implementación sencilla de los sistemas de acceso condicional que se adopten, en el parque actual de receptores integrados (iDTV's).