Distribución y Recepción de Señales de Televisión Digital
Introducción al acceso condicional DVB

José M. Martínez
Escuela Politécnica Superior
Universidad Autónoma de Madrid, SPAIN

JoseM.Martinez@uam.es
tel:+34.91.497.22.58

2008-2009

Escuela Politécnica Superior
Universidad Autónoma de Madrid

Distribución y Recepción de Señales de Televisión Digital
Introducción al acceso condicional DVB

- Introducción
- DVB-CSA
- Señalización DVB para CA
- Sistemas de acceso condicional en DVB
  - Common Interface
  - La Tarjeta Inteligente
  - Multicrypt
  - Simulcrypt
  - "Transcontrol" de CA
  - Nagravision
- Referencias

Distribución y Recepción de Señales de Televisión Digital
Introducción al acceso condicional DVB

- **Introducción**
- DVB-CSA
- Señalización DVB para CA
- Sistemas de acceso condicional en DVB
  - Common Interface
  - La Tarjeta Inteligente
  - Multicrypt
  - Simulcrypt
  - "Transcontrol" de CA
  - Nagravision
- Referencias

Introducción (I)

El acceso condicional restringe el acceso de contenidos en base a los derechos de acceso: televisión de pago

- Pay-per-channel: subscripción
- Pay-per-view: compra individual (generalmente con suscripción previa)

Un sistema de acceso condicional enmascara contenidos mediante el empleo de algoritmos de encriptación basados en claves privadas.

El decodificador desencripta tras recuperar las claves privadas que son transmitidas mediante un protocolo de mensajes de control (ECM) y que complementa a un protocolo de mensajes de gestión (EMM)

Introducción (II)

Un sistema de CA tiene diversos subsistemas:
En el difusor
- Gestión de usuarios: Subscriber Management System (SMS)
- Autorización de usuarios y derechos: Subscriber Authorisation System (SAS)
  - Call Collector: recibe ordenes de compra (opcional)
  - Access Control System (ACS) - Entitlement Management System (EMS)
    Genera los Entitlement Management Message (EMM): autorizaciones, gestión de tarjeta, etc.
- Generación de palabras de control privadas: Control Word Generator (CWG)
- Information Management System (IMS)
  - Generación de claves (CW cifradas)
    Genera los Entitlement Control Message (ECM): CW, criterios de acceso, …
  - Inyección de claves en el múltiplex: EMM+ECM
    Generación de información de servicio (DVB-SI)
- Multiplex: encripta (baraja) la información a partir de las CW

En los receptores
- El demultiplexor entrega la señal encriptada y los EMM y ECM.
- El Sistema de CA genera las CW
- El "descifrador" genera a partir de las CW la señal "en abierto".

Canal interactivo
- Conecta al sistema de autorización y al sistema CA del STB para la compra de eventos (sistemas pay-per-view)

Introducción (III)

El acceso condicional en DVB está basado en:
- un sistema común de encriptación
  - Algoritmo común europeo (DVB-CSA)
    Lo *suficientemente* seguro
    Dos sistemas en cascada
  - Algoritmos de clave privada
  - Según la protección de claves y los algoritmos concretos utilizados se crean distintos proveedores de CA
    NagraX, SecaX, ViaccessX, IrdetoX, …
- Un interfaz común para desasociar el sistema CA del descodificador (STB)
  - Estándar europeo Common Interface (CI)

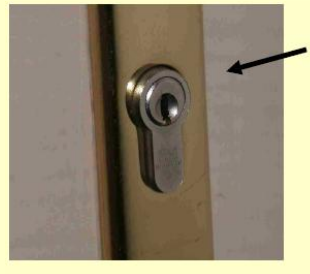
Distribución y Recepción de Señales de Televisión Digital
Introducción al acceso condicional DVB

- *Introducción*
- **DVB-CSA**
- Señalización DVB para CA
- Sistemas de acceso condicional en DVB
  - Common Interface
  - La Tarjeta Inteligente
  - Multicrypt
  - Simulcrypt
  - "Transcontrol" de CA
  - Nagravision
- Referencias

DVB-CSA (I)

CSA: Common Scrambling Algortihm

- Fundamento: sistema común con algoritmos diversos



Cilindro reemplazable de forma normalizada con una llave (CA) específica

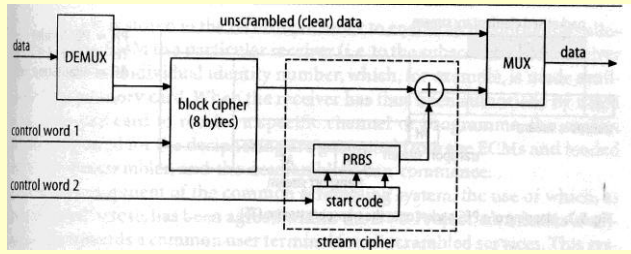
vs. un sistema de formato de llave no reemplazable

© Dionisio Oliver, Sogecable (2007)

DVB-CSA (II)

El DVB-CSA se basa en dos pasos de cifrado en cascada [ETR 289]

- Bloques de 8 bytes se “barajan”
- Los bits resultantes se vuelven a “barajar”



Se puede encriptar todo el canal o solamente parte de sus servicios

- Encriptación a nivel TS o PES
  - solamente uno de los dos niveles simultáneamente
- Las cabeceras de los paquetes TS/PES no se encriptan pues son necesarias para la sincronización del receptor
  - Se encripta la carga útil (payload)

DVB-CSA (III) (*)

En las cabeceras de los TS/PES se envían bits de control de cifrado (“barajado”-scrambling)

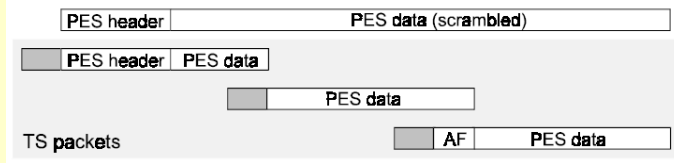
- 00: no scrambling
- 01: for future use
- 10: scrambled with even code word
- 11: scrambled with uneven code word

La clave (representación encriptada de las dos palabras código) se cambia de vez en cuando y el segundo bit 1x se usa para indicar que la clave que aplica es la renovada

DVB-CSA (IV) (*)

Existen ciertas restricciones al “mapeo” PES a TS a nivel de acceso condicional (para reducir la complejidad del receptor):

- Las cabeceras PES tienen que ser <= 184 bytes
  - Para que entre en un paquete TS
- Tras la cabecera PES, el PES se divide en segmentos de 184 bytes a mapear en paquetes TS
  - Estos paquetes TS no pueden tener “adaptation field (AF)”
- Si el último segmento PES en menor de 184 bytes, el paquete TS debe incluir un AF de la diferencia
- Si es necesario tener un AF propio, es necesario incluir un paquete TS que contenga únicamente ese AF



DVB-CSA (V)

Las dos palabras de control (clave) se encriptan de forma independiente (aunque dependiente del sistema utilizado) convirtiéndolas en ECMs (Entitlement Control Messages)

- La primera para (des)cifrado byte a byte
- La segunda para (des)cifrado bit a bit

La tabla CAT se usa para transmitir la información necesaria para el acceso condicional:

- ECMs
  - Claves cifradas
- EMMs (Entitlement Management Message)
  - Generados por el SMS individualmente para cada abonado
  - Asociado a un identificador único (tarjeta de abonado)
- Si la tarjeta y el EMM “autorizan” la visualización de un servicio
  - ECM genera las palabras clave y se las pasa al algoritmo de descifrado

Distribución y Recepción de Señales de Televisión Digital
Introducción al acceso condicional DVB

- *Introducción*
- *DVB-CSA*
- **Señalización DVB para CA**
- Sistemas de acceso condicional en DVB
  - Common Interface
  - La Tarjeta Inteligente
  - Multicrypt
  - Simulcrypt
  - "Transcontrol" de CA
  - Nagravision
- Referencias

Señalización DVB para CA (I): CAT

La CAT indica a los receptores donde se encuentran los flujos EMM (mensajes de gestión) y ECM (mensajes de control)

El CA_descriptor (descriptor_tag 0x09) identifica el PID de los paquetes que transportan esos flujos y el proveedor de los mismos

- Los EMMs se referencian con el CA_descriptor en la CAT (table_id=0x01)
- Los ECMs se referencian con el CA_descriptor en la PMT (table_id=0x02) o en el bucle de ESs
- CA_system_ID [ETR 162]

Syntax	No. of bits	Mnemonic
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**
}		
}		

Señalización DVB para CA (II): DVB-CA data

ISO/IEC 13818-1 define el transporte de datos de CA tales como ECM, EMM y futuros.

- Se transportan como secciones privadas

Si bien la estructura de datos depende de cada proveedor de CA se identifican dos tipos de mensajes (ECMs y EMM) y se dejan otros para uso futuro

```
CA_message_section(){
        table_id (0x80-0x8F)              8 bits
        section_syntax_indicator ('0')    1 bit
        DVB_reserved                      1 bit
        ISO_reserved                      2 bits
        CA_section_length                 12 bits
        for(i=0;i<N;i++){
                CA_data_byte              8 bits
        }
}
```

table_id value	Description
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

El cambio entre 0x80 y 0x81 indica un cambio de claves

Distribución y Recepción de Señales de Televisión Digital
Introducción al acceso condicional DVB

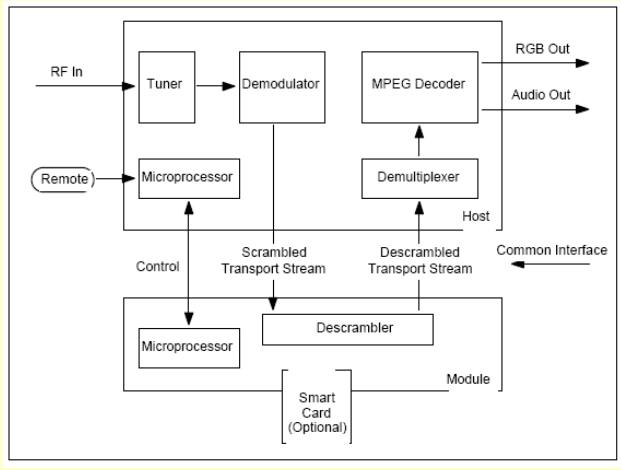
- *Introducción*
- *DVB-CSA*
- *Señalización DVB para CA*
- **Sistemas de acceso condicional en DVB**
  - **Common Interface**
  - **La Tarjeta Inteligente**
  - **Multicrypt**
  - **Simulcrypt**
  - **"Transcontrol" de CA**
  - **Nagravision**
- Referencias

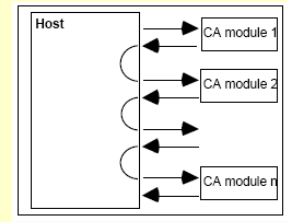
Sistemas de acceso condicional en DVB (I)

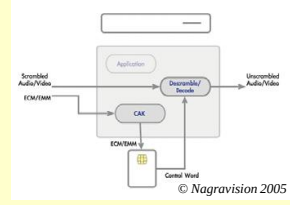
Partiendo del acuerdo de uso de DVB-CSA, los proveedores de STBs deben dar un paso adicional a nivel de estandarización:

- Sistema común de CA
  - Poco realístico desde un punto de vista comercial
- Interfaz común (CI [EN 50221]) para decodificadores con módulos CA *plug-in* intercambiables
  - El procesado de los ECMs y EMMs propios de cada proveedor se pueden integrar en dicho módulo
  - Multicrypt [EN 50221]
  - Para "disuadir" a los "piratas" el CI llega hasta el nivel de MPEG-2 TS
- Decodificador con módulo CA único y propietario
- Decodificador con módulo CA único y multi-propietario
  - Hardware común
  - Licencias multi-sistemas CAs
  - Simulcrypt [ETSI TS 101 197][ETSI TS 102 035]

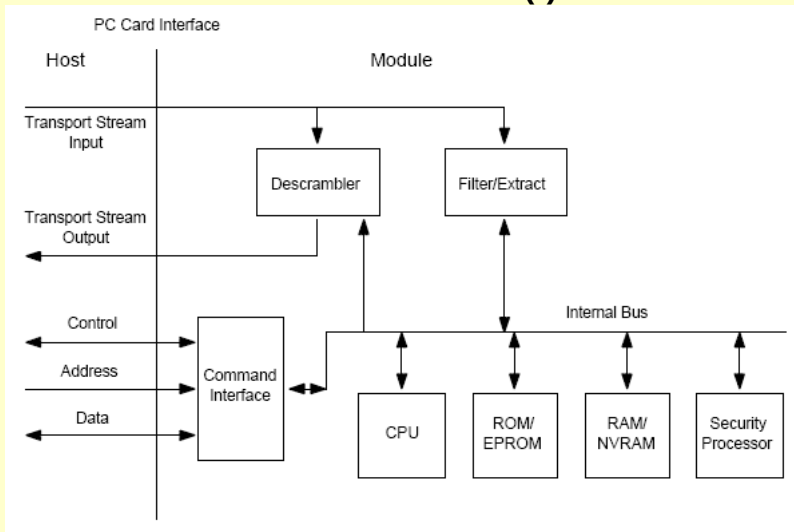
Sistemas de acceso condicional en DVB (II): Common Interface (*)







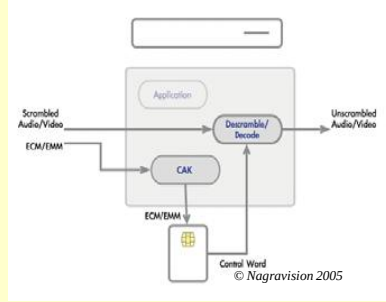
Sistemas de acceso condicional en DVB (III): Common Interface (*)



Sistemas de acceso condicional en DVB (IV): la tarjeta inteligente

La tarjeta inteligente recibe los EMMs, los desencripta y actualiza los derechos

La tarjeta inteligente recibe los ECMs y, tras comprobar los derechos, desencripta el ECM, extrae las palabras de control y las proporciona al “descifrador” para que proceda al desenmascarado



Sistemas de acceso condicional en DVB (V): Multicrypt

Se basa en la interfaz común (física y lógica) CI [EN 50221] que separa la circuitería y funcionalidades del descodificador de las del CA

Un módulo PCMCIA recibe el flujo de transporte encriptado y devuelve los programas seleccionados desencriptados

El demultiplexor envía el servicio seleccionado al módulo CA-CI quien ejecuta los programas necesarios para obtener las claves y desencriptar el servicio

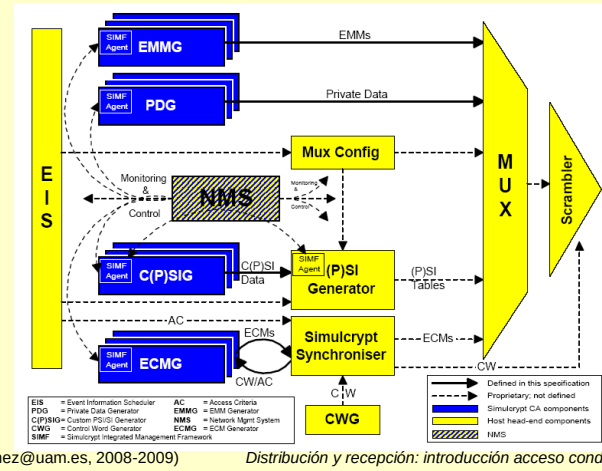
Ventajas

- Se pueden añadir nuevos sistemas sin complicaciones
- El receptor es universal, ya que el sistema CA se encuentra en la tarjeta inteligente (intercambiable)
- Compatible con Simulcrypt

Sistemas de acceso condicional en DVB (VI): Simulcrypt

Complejidad en la transmisión

- Una única clave se envía encriptada con ECMs de diferentes sistemas CA
- Se envian EMMs para cada sistema



Sistemas de acceso condicional en DVB (VII): "Transcontrol" de CA

Sistema que permite a redifusores de servicios encriptados a poner sus propios sistemas/condiciones de CA

- Redifusor cable que accede a contenidos satélite encriptados y los redifunde en nuevos "paquetes"
- [ETR 289] propone recomendaciones sencillas para asegurar sistemas de transcontrol eficientes

Sistemas de acceso condicional en DVB (VIII): Nagravision

Nagravisión, también conocido como **Nagra**, es el sistema de CA que utilizan diversas plataformas de televisión vía satélite como Digital+ (España), Premiere (Alemania), Polsat (Polonia) o Cabo TV(Portugal), entre otras muchas.

El proyecto Nagravisión ha tenido varias versiones y numerosos parches de seguridad; conocidas como Nagra 1, Nagra 2 y Nagra 3 que van superarando los "inconvenientes de la piratería", que ha dejado en evidencia a la compañía (http://www.nagravision.com) en numerosas ocasiones del pasado.

Nagravisión 1 era utilizado por Canal+ en los primeros años de emisión de la plataforma siendo remplazado en noviembre de 2005 por Nagravisión 2. Tanto los sistemas Nagravisión 1 y Nagravisión 2 tenían numerosos fallos de seguridad graves, que permitieron que los sistemas fuesen pirateados y visionados ilegalmente.

Desde diciembre de 2007 se está usando Nagravisión 3 (que por ahora sigue sin ser crakeado).

Distribución y Recepción de Señales de Televisión Digital
Introducción al acceso condicional DVB

- *Introducción*
- *DVB-CSA*
- *Señalización DVB para CA*
- *Sistemas de acceso condicional en DVB*
  - *Common Interface*
  - *La Tarjeta Inteligente*
  - *Multicrypt*
  - *Simulcrypt*
  - *"Transcontrol" de CA*
  - *Nagravision*
- **Referencias**

Referencias

- ETSI TR 289 (1996-10): Digital Video Broadcasting (DVB); Support for use of scrambling and Conditional Access (CA) within digital broadcasting systems
- ETSI TS 101 197 v1.2.1 (2002-02): Digital Video Broadcasting (DVB); DVB Simulcrypt; Head-end architecture and synchronization
- ETSI TS 102 035 v1.1.1 (2002-04): Digital Video Broadcasting (DVB); Implementation Guidelines of the DVB Simulcrypt Standard
- CENELEC EN 50221 (1997-02): Common Interface Specification for Conditional Access and other Digital Video Broadcasting Decoder Applications
- ISO/IEC IS 13818-1:2000(200-12-01): Information technology – Generic Coding of movng pictures and assocaited audio inforamtion: Systems
- ETSI TR 162 (1995-10): Digital Video Broadcasting (DVB); Allocation of Service Information (SI) codes for DVB systems
- http://www.dvb.org/
- U. Reimers, "DVB: The Familiy of International Standards for Digital Video Broadcasting", 2nd ed., Springer, 2005.
- http://www.nagravision.com/

Distribución y Recepción de Señales de Televisión Digital
Introducción al acceso condicional DVB

- *Introducción*
- *DVB-CSA*
- *Señalización DVB para CA*
- *Sistemas de acceso condicional en DVB*
  - *Common Interface*
  - *La Tarjeta Inteligente*
  - *Multicrypt*
  - *Simulcrypt*
  - *"Transcontrol" de CA*
  - *Nagravision*
- *Referencias*