Universidad Central “Marta Abreu” de Las Villas

Facultad de Ingeniería Eléctrica

Departamento de Telecomunicaciones y Electrónica

TRABAJO DE DIPLOMA

Propuestas de arquitectura(s) de un Sistema de Acceso Condicional para la DTT en Cuba.

Autor: Marcos Antonio Sotolongo Yanes.

Tutor (a): MSc. Irina Siles Siles.

Santa Clara

2017

"Año 59 de la Revolución"

Universidad Central “Marta Abreu” de Las Villas

Facultad de Ingeniería Eléctrica

Departamento de Telecomunicaciones y Electrónica.

TRABAJO DE DIPLOMA

Propuestas de arquitectura(s) de un Sistema de Acceso Condicional para la DTT en Cuba.

Autor: Marcos Antonio Sotolongo Yanes.

antonios@uclv.cu

Tutor (a): MSc. Irina Siles Siles.

MSc, Asistente, Departamento de Telecomunicaciones y Electrónica, Facultad de Ingeniería Eléctrica,

irinass@uclv.edu.cu

Santa Clara

2017

"Año 59 de la Revolución"

Hago constar que el presente trabajo de diploma fue realizado en la Universidad Central "Marta Abreu" de Las Villas como parte de la culminación de estudios de la especialidad de Ingeniería en Telecomunicaciones y Electrónica, autorizando a que el mismo sea utilizado por la Institución, para los fines que estime conveniente, tanto de forma parcial como total y que además no podrá ser presentado en eventos, ni publicados sin autorización de la Universidad.

_____

Firma del Autor

Los abajo firmantes certificamos que el presente trabajo ha sido realizado según acuerdo de la dirección de nuestro centro y el mismo cumple con los requisitos que debe tener un trabajo de esta envergadura referido a la temática señalada.

_____ _____

Firma del Tutor

Firma del Jefe de Departamento donde se defiende el trabajo

_____

Firma del Responsable de Información Científico-Técnica

PENSAMIENTO

"No es necesario hacer cosas extraordinarias para conseguir resultados extraordinarios"

Warren Buffet

DEDICATORIA

A mis padres y abuelos por su esfuerzo y apoyo incondicional a lo largo de toda mi vida, por guiarme por el camino correcto, por creer en mí y ser mi fuente de inspiración para realizar este sueño.

A mi hermano por su preocupación y dedicación.

A mi novia por estar siempre a mi lado y apoyarme en todo momento.

AGRADECIMIENTOS

A mis padres y abuelos, por todo lo que han hecho y sacrificado por mí.

A mi hermano por su ayuda incondicional en todo momento.

A mi novia, por su ayuda en la realización de este trabajo y a su familia por el apoyo brindado.

A mi tío Jesús, por su ayuda y preocupación en estos últimos tiempos.

A mi tutora Irina, porque sin su ayuda incondicional no hubiera sido posible la realización de este trabajo.

A mis profesores, por sus enseñanzas.

A todos aquellos que de una forma u otra hicieron posibles la realización de este trabajo.

A todos Gracias.

TAREA TÉCNICA

1. Estudio de las características de los esquemas de los Sistemas de Acceso Condicional (CAS).
2. Caracterización de las arquitecturas típicas para CAS según las vías de difusión de la televisión.
3. Análisis y proposición de arquitectura(s) en función del contexto nacional.

Firma del Autor

Firma del Tutor

RESUMEN

El avance de la televisión digital ha impuesto retos a los desarrolladores, en cuanto a transmisión, recepción y calidad de la señal. La televisión de pago hoy en nuestros días ha tenido gran auge debido a la diversidad en sus propuestas televisivas gracias a la implementación de los Sistemas de Acceso Condicional.

Se hace imprescindible la inserción de nuevos servicios que resulten atractivos en contenidos. Esta investigación toma en consideración el hecho de que actualmente en Cuba no se vislumbran muchos estudios puntuales sobre el tema, debido a que todos los servicios son gratuitos (abiertos); solamente se avizoran incipientes proyecciones por algunas entidades sobre posibles políticas de inserción de este nuevo servicio.

El presente trabajo estará por tanto, enfocado en proponer esquemas de acceso condicional que tomen en consideración las condiciones actuales del contexto nacional y además que tengan en cuenta el despliegue de toda una infraestructura DTT. Los esquemas propuestos como resultado de la investigación estarán basados principalmente en una arquitectura MICAS (Sistema de Acceso Condicional Integrado Móvil).

ÍNDICE

INTRODUCCIÓN

Durante las últimas décadas la humanidad ha desarrollado tecnologías enfocadas al mejoramiento de la transmisión de información a través del aprovechamiento del espectro radioléctrico para la mayoría de los servicios de telecomunicaciones.

Si se toma como ejemplo el surgimiento de la televisión digital, se observa como se produce un mejor rendimiento en cuanto a ancho de banda consumido, calidad de la imagen y flexibilidad en los contenidos emitidos, siendo posible mezclar un número determinado de canales de video, audio y datos en un mismo servicio. Fue este precisamente el momento de transición del formato analógico al digital; son muchos los países que estan atravesando este cambio tecnológico importante.

Cifras de la ITU (del inglés, International Telecomunications Union) muestran que, a escala mundial, la tasa de penetración de la TV digital superó el 70 por ciento en 2015. En el mundo desarrollado, se calcula que el 81 por ciento de los hogares con televisión reciben una señal digital (The Daily Television, 2015). Esto se debe en gran medida a la televisión por suscripción (o pago), la cual es posible gracias al mecanismo de acceso condicional. Este sistema permite el control, por parte del operador, de los permisos de un subscriptor a acceder a TV, radio o datos que se emiten por su plataforma. El mismo está integrado tanto en las cabeceras como en los decodificadores, algunos se basan en tarjetas con chip y otros en códigos de *software* que generalmente se cambian cada mes para evitar los ataques de los *hackers.*

Fue en Estados Unidos en 1983 donde se implementó el primer Sistema de Acceso condicional, VIDEOCYPHER el que después transpusieron los europeos a su sistema de codificación de TV analógico D-MAC (de inglés, Multiplexed Analoge Component) con el nombre de EUROCRYPT(Coutrot and Michon, 1989).

Más adelante, en 1993 se fundó el Digital Video Broadcasting (DVB) y este desarrolló las especificaciones del Sistema de Acceso Condicional para la televisión de pago mediante satélite, cable e infraestructuras terrestres. La televisión digital propició la aparición de una serie de servicios adicionales, como por ejemplo el Pay-per-View (PPV).

Tomando en consideración los desafíos en tiempos de convergencia de tecnologías y servicios, en la literatura se constata un incremento porcentual que circunda niveles de alrededor de un 52% y un aproximado de 84 millones de suscriptores para América Latina con respecto a la penetración de la tv de pago en los hogares (Martínez, 2015). Las curvas analizadas muestran que desde el 2008 hasta la fecha se ha experimentado un incremento vertiginoso de los servicios DTH (Direct To Home) por sobre los de cable para dicho servicio. Todos los esfuerzos han estado encausados a lograr una diversificación de las posibilidades de consumo de contenidos audiovisuales enfrentando el desafío venidero de ofrecer soluciones innovadoras que amplíen la oferta de contenidos y dispositivos.

A inicios del año 2013 Cuba comenzó a desplegar los servicios de Televisión Digital Terrestre (DTT, del inglés Digital Terrestrial Television) empleando el estándar DTMB definido en la norma GB 20600-2006. Actualmente cerca del 60% del territorio nacional cuenta ya con cobertura de la señal digital y son muchos los avances que se han alcanzado posibilitando una mejor calidad de sonido e imagen, así como, una imagen en alta definición, servicios de *databroadcasting*, Guía Electrónica de Programas, etc.(Oscar, 2017).

A raíz del cúmulo de inversiones e investigaciones necesarias para la creación y funcionamiento de transmisión de señales de televisión digital, a tono con las aspiraciones y expectativas de los usuarios nacionales y en relación con el desarrollo de la ETI (Electrónica, Telecomunicaciones e Informática), se hace imprescindible la inserción de nuevos servicios que resulten atractivos en contenidos (deportes, películas, etc.) para los usuarios.

Surge así la necesidad de implementar un Sistema de Acceso Condicional (CAS, del inglés Conditional Access System) el cual tiene como objetivo limitar la recepción de determinados servicios únicamente a los usuarios autorizados por el proveedor del servicio así como, gestionar de manera sencilla las autorizaciones de cada usuario, de forma individual o colectiva. El CAS permitirá que solo los usuarios autorizados, provistos del adecuado receptor, puedan tener acceso a determinados servicios.

Actualmente en Cuba no se vislumbran estudios puntuales sobre el tema, debido a que todos los servicios son gratuitos (abiertos); solamente se avizoran incipientes proyecciones por entidades (RadioCuba o Centros de investigaciones como las universidades) sobre posibles políticas de inserción de este nuevo servicio. Sin embargo con la implementación de este sistema se pueden beneficiar no solo los usuarios sino también el país debido a los ingresos que puede brindar.

Tomando en consideración lo expuesto anteriormente se plantea la siguiente situación problemática:

- ¿Cómo realizar una propuesta para un escenario de CAS en el contexto nacional de ambientes de DTT?

Para dar respuesta a la pregunta científica planteada anteriormente, la presente tesis se propone como Objetivo General:

- Analizar esquema (s) de CAS tomando en consideración la infraestructura desplegada en el país para el servicio de televisión digital.

Como solución al Objetivo General planteado con anterioridad se enuncian los Objetivos Específicos siguientes:

- Estudiar las características de los Sistemas de Acceso Condicional.
- Caracterizar las arquitecturas típicas para CAS según las vías de difusión de la televisión.
- Analizar y proponer arquitectura(s) en función del contexto nacional.

De los objetivos se generan las siguientes interrogantes científicas a las cuales se les dan respuesta en el desarrollo de la investigación:

- ¿Cuáles son las características de los CAS?
- ¿Qué características poseen las arquitecturas CAS en cuanto a vías de difusión de televisión?
- ¿Cómo implementar estas arquitecturas en función del contexto nacional?

Con la realización de este trabajo se espera contribuir al desarrollo de la televisión digital mediante la proposición de arquitectura(s) para la DTT, en esquemas CAS en función de la infraestructura nacional y que sirva como base para su implementación en el futuro.

Con la ejecución del proyecto se dan soluciones a problemáticas modernas vinculadas con las propuestas televisivas y así crear nuevos servicios que cumplan con las expectativas del televidente en cuanto a diversidad de programas y calidad de los mismos.

El informe consta de tres capítulos que conforman el cuerpo de la tesis.

- En el capítulo 1 se aborda sobre los principios básicos, características y arquitecturas de los sistemas de acceso condicional, orientados principalmente a los estándares adoptados para televisión digital. Se enfatiza sobre el mecanismo de cifrado/descifrado de los servicios, así como en los algoritmos utilizados para su encriptación. Se analiza además la interoperabilidad de estos sistemas.
- El capítulo 2 está encausado en describir tanto las arquitecturas de los CAS como la interactividad (canal de retorno) que se produce en las diferentes redes de difusión de la televisión. Para una mejor comprensión se partirá de la elaboración de un diagrama de flujo en el cual se plasmará la metodología utilizada para arribar a un esquema CAS que se adecue a las condiciones actuales.
- En el capítulo 3 se toman en consideración el despliegue y desarrollo de la televisión digital ya instaurada en Cuba, así como las diferentes tecnologías de acceso existente, se proponen arquitecturas de CAS basadas en la imbricación de tecnologías de radiodifusión de tv y tecnologías para la transmisión de datos en redes móviles celulares, se explican consecuentemente las posibles variantes en cuanto a varios criterios en las mismas.
- Por último, en las Conclusiones se ve cómo han sido cumplidos todos los objetivos presentados. Finalmente se dejan especificadas algunas Recomendaciones para futuros proyectos.

CAPÍTULO 1. CARACTERÍSTICAS GENERALES DE LOS SISTEMAS DE ACCESO CONDICIONAL.

En el presente capítulo, se aborda sobre los principios básicos, características y arquitecturas de los sistemas de acceso condicional, orientados principalmente a los estándares adoptados para televisión digital. Se enfatiza sobre el mecanismo de cifrado/descifrado de los servicios, así como en los algoritmos utilizados para su encriptación. Se analiza además la interoperabilidad de estos sistemas.

1.1 Sistema de acceso condicional: surgimiento y evolución.

A menudo, la mayoría de los proveedores de contenidos de audiovisuales emiten contenidos de pago o de acceso condicional, que no desean que sean vistos por todos los usuarios. Esta política, crea brechas entre los usuarios finales pues aparecen las llamadas “tv abiertas” y las "tv cerradas” las unas y las otras impugnadas por las grandes cadenas televisivas y la necesidad de crear un modelo de negocios.

En consecuencia, los servicios de acceso condicional en lo referido a señales audiovisuales, se podrían definir exactamente entonces 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”. (Luis, 2012).

Fue en Estados Unidos en 1983 donde se implementó el primer sistema de Acceso Condicional, el VIDEOCYPHER. Luego fue adaptado por los europeos a su sistema TV analógico D-MAC (Multiplexado de componentes analógicos) con el nombre de EUROCRYPT (Coutrot and Michon, 1989). Más adelante, en 1993 se fundó el Digital Video

Broadcasting (DVB) y este desarrolló las especificaciones del Sistema de Acceso Condicional para la televisión de pago vía satélites, entre otros.

La llegada de la televisión digital propició la aparición de una serie de servicios adicionales, tal es el caso de Pay-per-View (PPV), Video on Demand (VoD) entre otros. Estos servicios favorecieron a un incremento en las propuestas televisivas las cuales trajeron consigo un aumento de suscriptores en las redes de televisión.

En la figura 1.1 se muestra un gráfico de barras en donde se puede observar cómo ha sido y será la evolución y la penetración de la televisión por suscripción (o pago) a partir del 2014 y hasta el 2020. Nótese como se experimenta un incremento para los servicios de satélite e IPTV para los años venideros.

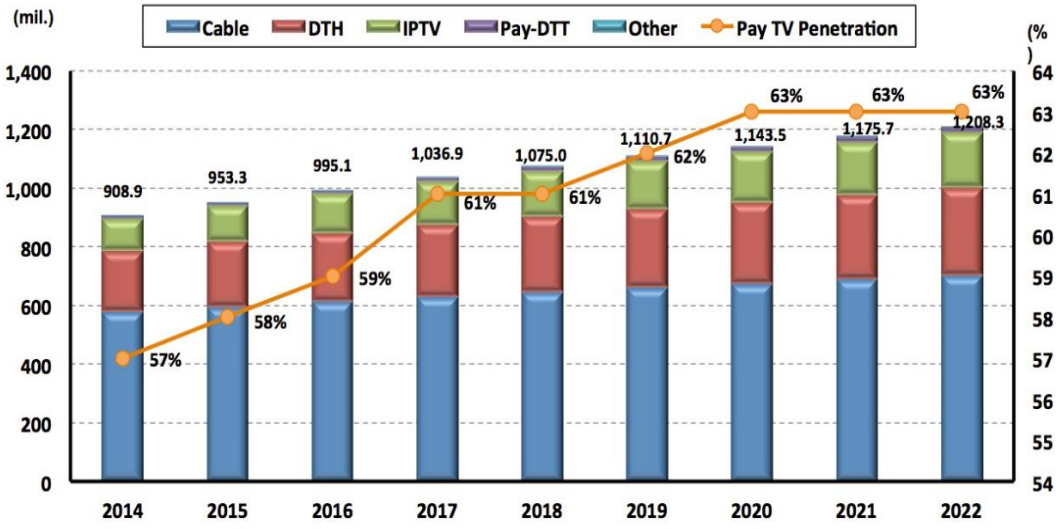

Figura 1.1 Evolución de la televisión por suscripción en el mundo. Fuente (Beaumont, 2015).

1.1.1 Requisitos que deben cumplir los CAS.

Para una correcta implementación de los CAS es necesario tener en cuenta lo recomendado en UIT-R BT. 810 por (ITU-R, 1992) y en ITU-R BT.1852-1 (ITU-T, 2016) en donde son citados requisitos que son ineludibles para su correcto funcionamiento, por listar algunos:

- ***Modos de Acceso:***
  - Disponibilidad de período (suscripción del servicio) – la autorización va desde un instante de inicio a un instante final.

- Elemento de programa o servicio (adquisición de un evento) – la disponibilidad se refiere a un elemento de servicio específico, se utilice o no en su totalidad.
- Tasa de servicio (basada en testigo) – la tasa o utilización del crédito es proporcional a la duración de la utilización y/o el valor del servicio implicado;
- Emisión libre – el servicio está protegido pero se proporciona el acceso de manera gratuita.

❖ ***Calidad:*** Los procesos de aleatorización y des aleatorización no deben alterar perceptiblemente la calidad de las señales recibidas de imagen, sonido y datos.

❖ ***Manera de evitar la degradación del servicio:*** Existen dos tipos de deterioros significativos; el deterioro del servicio finalmente disponible debido al proceso de codificación/ descodificación y la degradación debida a la adquisición deficiente o insegura de los datos de control de acceso.

❖ ***Interacción con el proceso digital:*** Hay que señalar que los procesos de aleatorización pueden limitar seriamente la posibilidad de realizar nuevos procesos, incluyendo la reducción de la velocidad binaria.

❖ ***Protección de contenido extremo a extremo:*** Está orientada a la protección del contenido (programas u otros) y al acceso (control o datos) desde el origen al destino. Una vez oculta permanece así en todos los pasos intermedios del sistema de distribución hasta su llegada al receptor.

1.2 Consideraciones técnicas.

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. En la figura 1.2 se observa cómo se realiza dicho proceso; en el epígrafe 1.3.1 se hace una descripción más detallada del mismo.

Estos sistemas interactúan con la cabecera de TV digital y siempre que ambos sistemas cumplan con la norma o estándar a emplear, el multiplexor será quién codifique los contenidos y envíe al sistema de acceso condicional la clave de cifrado.

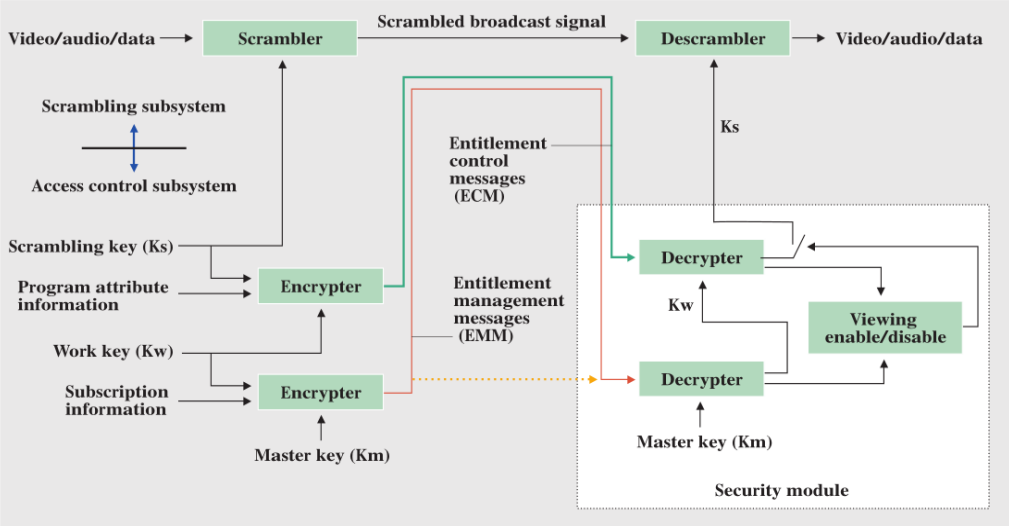

Figura 1.2 Configuración de un sistema de acceso condicional. Fuente (山田, 2001).

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 impregnados (con tarjeta inteligente o chip ensamblado) y ser genéricamente de los siguientes tipos:

- ***Sistemas basados en la Interfaz Común del DVB (DVB-CI):*** En este tipo, el sistema de acceso condicional reside en un Módulo Interfaz Común (CAM, del inglés Conditional Access Module) 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.(Européenne, 1996).
- ***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 (ISO, 2017). El decodificador traslada la información que proviene del operador a la tarjeta, este requiere de una ranura para interfaz ISO 7816 en donde se insertará y de la integración de un módulo software en el decodificador para realizar las funciones antes citadas.

- ***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.

1.3 Sistemas de cifrado.

De acuerdo a la recomendación (ITU-T, 2016) la utilización de un algoritmo de aleatorización común implica una desaleatorización común para todos los receptores, basada en un algoritmo de aleatorización normalizado, independientemente del medio de distribución utilizado; ello permite unos equipos flexibles y de coste inferior y seguiría posibilitando la competencia a través de implementaciones específicas al proveedor del servicio. La utilización de un algoritmo de aleatorización privado supone que el proceso de desaleatorización debe llevarse a cabo en los receptores que implementen únicamente un algoritmo específico.

Hay dos categorías principales de la criptografía en función del tipo de claves de seguridad utilizadas para cifrar / descifrar los datos. Estas dos categorías son: técnicas de cifrado simétricas y asimétricas.

Sistemas de cifrado simétricos:

Su nombre se debe a que dicha clave es usada tanto para el cifrado como para el descifrado. Esto quiere decir que la información se divide en "bloques", que pueden cifrarse independientemente o, para mejorar la seguridad, teniendo en cuenta información del bloque anterior. Actualmente suele emplearse un tamaño de bloque de 64 o 128 bits comúnmente.

Las características principales de estos cifradores pueden resumirse en los siguientes puntos:

- Cada símbolo o elemento del mensaje se cifra de manera dependiente de los adyacentes.
- Independientemente de la posición relativa del bloque dentro del mensaje, cada bloque se cifra con el mismo algoritmo y la misma clave.
- Si dos mensajes iguales se cifran con la misma clave, los resultados son también iguales.

La gran mayoría de cifradores simétricos siguen el llamado “esquema de Feistel": el mensaje se divide en bloques, cada uno de los cuales se cifra por separado mediante técnicas de sustitución y transposición, además de otras operaciones lineales sencillas de adición y multiplicación, durante un número de ciclos llamados “vueltas”. Para descifrar se realiza el proceso inverso, interviniendo en ambas etapas la clave simétrica.

La seguridad en clave simétrica reside en la propia clave secreta, y por tanto el principal problema es la distribución de esta clave a los distintos usuarios para cifrar y descifrar la información. (Dolores, 2016).

La misión del emisor y receptor es mantener la clave en secreto. Si cae en manos equivocadas ya no se puede considerar que la comunicación es segura y se debería generar una nueva clave. Para superar estas desventajas que presentaba el sistema de criptografía de clave privada se desarrolló en 1976 el sistema de criptografía asimétrica o de clave pública.

Sistemas de cifrado asimétrica:

En este tipo de cifrados cada comunicante tiene dos claves, una de ellas públicas y la otra privada o secreta. Para enviar un mensaje, el remitente usa la clave pública del destinatario para cifrar el mensaje. Una vez que lo ha cifrado, solamente con la clave privada del destinatario se puede descifrar, ni siquiera el que ha cifrado el mensaje puede volver a descifrarlo. Por ello, se puede dar a conocer perfectamente la clave pública para que todo aquel que se quiera comunicar con el destinatario lo pueda hacer. (Gutiérrez, 2013).

Si el propietario usa su clave privada para cifrar el mensaje, cualquiera puede descifrarlo utilizando su clave pública. En este caso se consigue por tanto la identificación y

autentificación del remitente, ya que se sabe que sólo pudo haber sido él quien empleó su clave privada. (Amieva, 2015).

La clave privada queda siempre en posesión de su dueño mientras que la clave pública se pone en conocimiento de los demás usuarios. Este último hecho no afecta a la fortaleza del criptosistema, ya que, aunque dependientes, a partir de una es computacionalmente imposible obtener la otra.

A diferencia de la clave simétrica, aquí los problemas van relacionados con el espacio que puede ocupar los datos cifrados, debido, a que aumenta el tamaño de las claves lo que traería consigo un mayor tiempo de proceso.

En la siguiente se muestran las características de los algoritmos de encriptación simétricos/asimétricos.

Tabla 1: Características principales de los algoritmos simétricos/asimétricos.

Atributos	Simétrico	Asimétrico
Velocidad	Rápida	Lenta
Uso principal	Cifrado de grandes volúmenes de datos	Intercambio de claves, Firmas digital
Claves	Compartidas entre emisor y receptor	Privada: sólo conocida por 1 persona. Pública: conocida por todos.
Intercambio de claves	Difícil de intercambiar por un canal inseguro	La clave pública se comparte por cualquier canal. La privada nunca se comparte
Longitud de claves	56 bits (vulnerables) 256 bits (seguro)	1024 bits mínimo
Algoritmos	DES, 3DES, Blowfish, IDEA, AES	Diffie-Hellman, RSA, DSA, ElGamal
Servicios de seguridad	Confidencialidad, Integridad Autenticación	Confidencialidad, Integridad Autenticación, No repudio

Ventajas	Pese a no ser del todo seguros, cuentan con la ventaja de la simplicidad y la rapidez.	Aporta una mayor seguridad en las comunicaciones.
Desventajas	La distribución de las claves y la dificultad de almacenar y proteger muchas claves diferentes.	La lentitud de los algoritmos de clave pública.

Debido a las deficiencias presentadas tanto por los algoritmos de encriptación simétricos como por los asimétricos se hace imprescindible crear un mecanismo que tome en consideración los aspectos positivos de ambos, surgiendo así el cifrado híbrido.

Sistemas de cifrado híbrido:

Según (Amieva, 2015), la criptografía híbrida soluciona los problemas de privacidad que podría suponer el uso del cifrado simétrico y el tiempo de procesado del uso del cifrado asimétrico, de esta forma se combinan ambas para su uso (Ver figura 1.3).

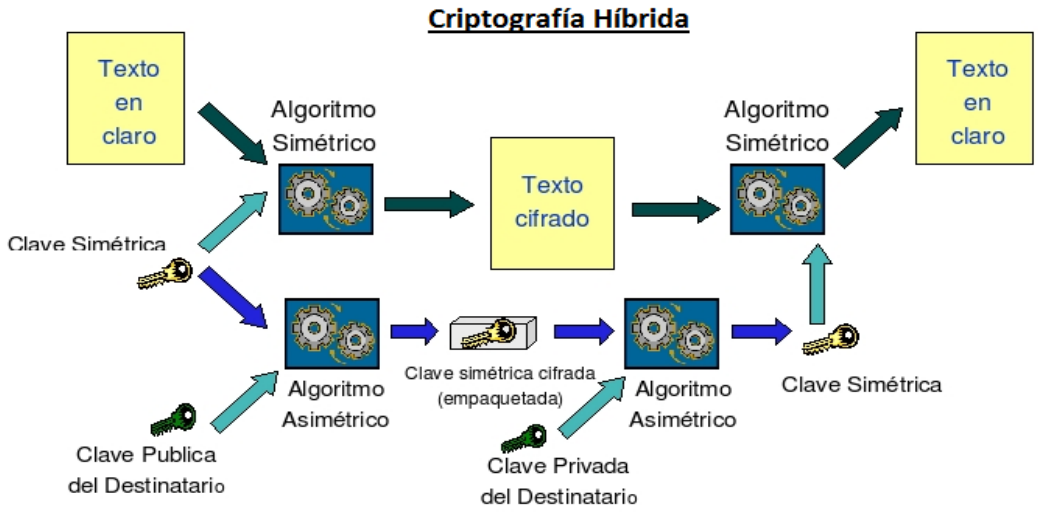

Figura 1.3 Esquema básico del cifrado híbrido. Fuente (Moreno, 2015).

Por ejemplo, si se desea mandar un mensaje, este se cifra con una clave simétrica, conocida en este proceso como la clave de sesión. Después, se cifra con la clave pública del receptor la clave de sesión. Cuando el receptor reciba el mensaje, primero descifrará con su clave

privada la clave de sesión. Una vez posee la clave de sesión ya puede acceder al contenido del mensaje.

1.3.1 Cifrado y descifrado del contenido.

Las especificaciones del CAS definen su estructura, sin embargo, los algoritmos de cifrado son propios y privados de cada proveedor y se desconocen en muchos de los casos.

A la hora de cifrar el contenido existen tres elementos en torno a los cuales gira todo el proceso:

- La palabra de control (CW, del inglés Control Word).
- La clave de servicio (SK, del inglés Service Key).
- La clave de usuario (MK, del inglés Master Key).

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 y/o programa virtual tiene una clave diferente, mediante la cual se pueden cifrar los servicios individualmente y dar acceso a unos y a otros no. Esta clave 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 asegurar 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 Mensajes de Control de Autorización (ECM, del inglés Entitlement Control Messages) y los Mensajes de Gestión de Autorización (EMM, del inglés Entitlement Management Messages). En conjunto estos mensajes tiene la capacidad de controlar el acceso al contenido de los usuarios individuales o grupos de usuarios. El ECM es el encargado de transmitir la CW necesaria para descodificar la señal en el STB de una manera segura. La

CW se coloca en un mensaje ECM que se cifra de forma propietaria y luego se inserta en el Flujo de Transporte (Ver figura 1.4).

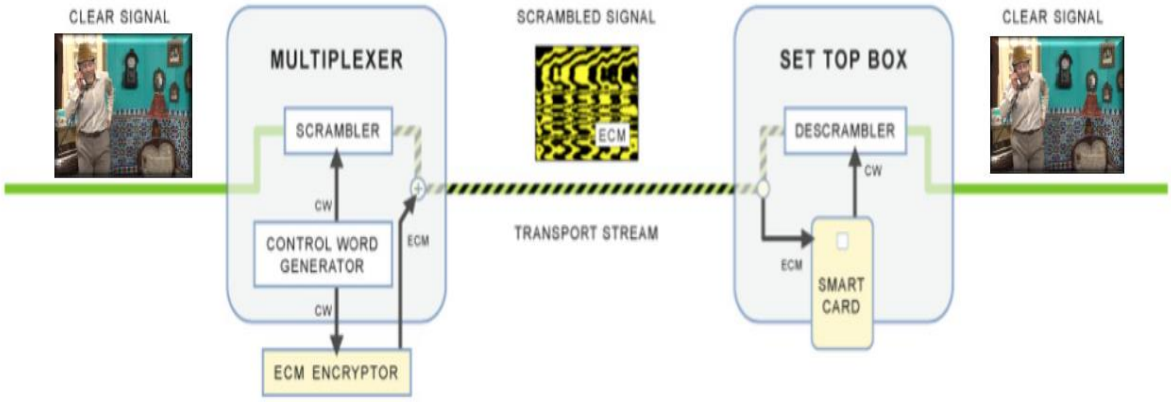

Figura 1.4 Proceso de cifrado en los mensajes ECM. Fuente (Bridge Technologies, 2010).

Cuando a un receptor le llega un "CA *messages*", se lo pasa al CAS. 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.

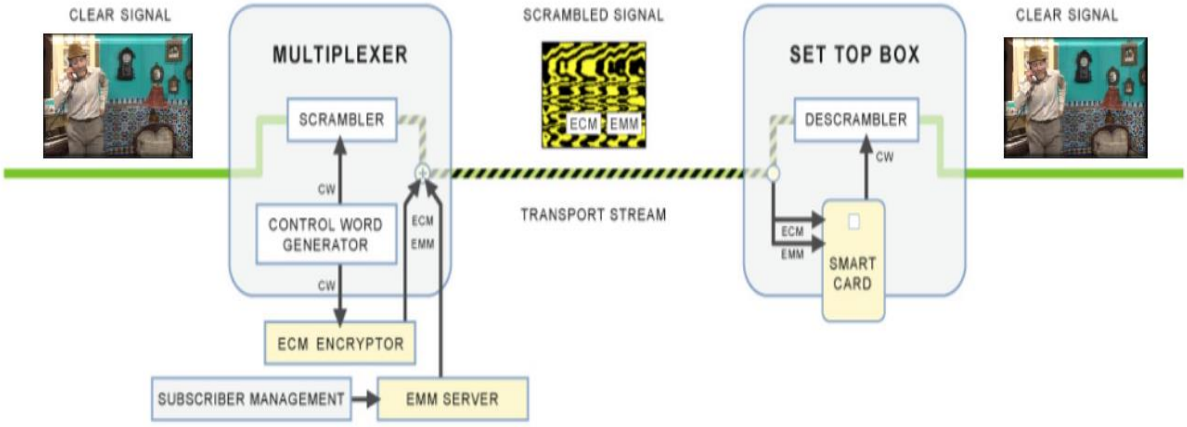

Figura 1.5 Proceso de cifrado en los mensajes EMM. Fuente (Bridge Technologies, 2010).

1.4 Verificación de la tabla de acceso condicional.

La tabla de acceso condicional (CAT, del inglés, Conditional Access Table) debe de estar presente si al menos un programa del múltiplex es de acceso condicional.

Se transporta por los paquetes con PID=0x0001 según (ITU-T, 1994), proporciona detalles de los sistemas de cifrado empleados, así como los valores de los PID de los paquetes de transporte que contienen la información del control de acceso condicional.

Los datos para el acceso condicional se envían en forma de EMM. En estos "EMM" se especifican los niveles de autorización o los servicios a que pueden acceder determinados decodificadores, y pueden ir dirigidos a decodificadores individuales o a grupos de ellos.

Estas comprobaciones solo requieren que la tabla CAT se transmita cuando hay PID codificados presentes en el flujo de transporte y que el *checksum* CRC de la tabla sea correcto. El equipo de monitoreo también debe comprobar que la tabla CAT contiene EMMs para todos los sistemas de acceso condicional utilizados para cifrar las señales. Sin embargo, no hay controles que requieran que la tabla CAT contenga información útil. En la figura 1.6 se muestra como se refleja la tabla CAT en el Flujo de Transporte (TS, del inglés Transport Stream).

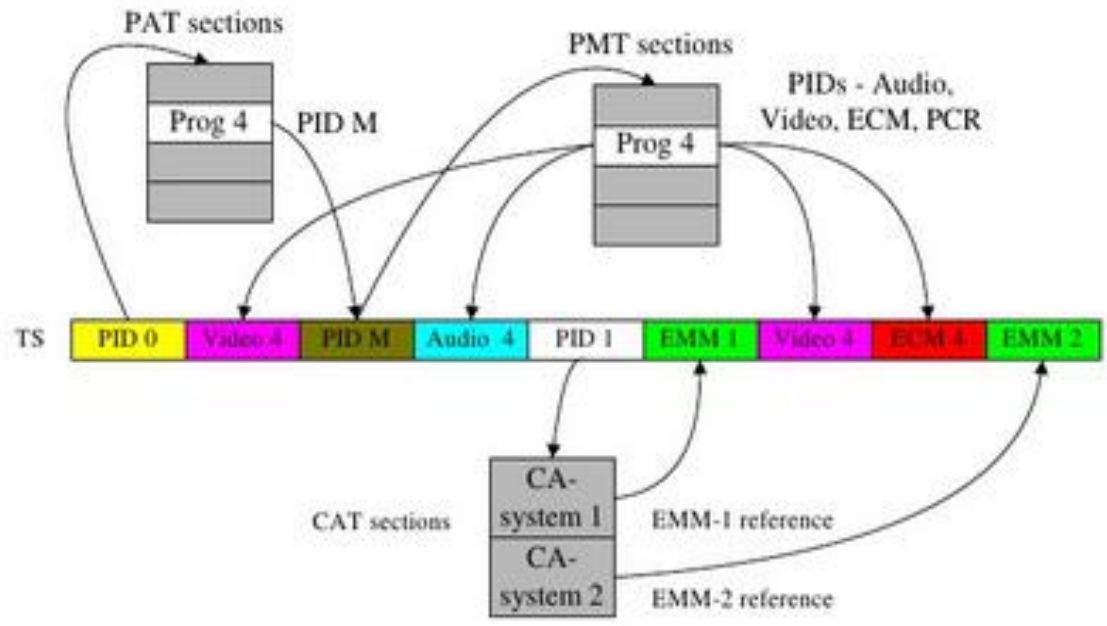

Figura 1.6 Representación de la tabla CAT dentro del TS. Fuente (Navarro, 2012).

Servicios seleccionados de la misma transmisión TS.

Si se seleccionan dos o más servicios del mismo TS de difusión y existen PID que son comunes entre varios servicios, los paquetes TS que coinciden con los PID comunes se duplicarán en el TS local generado para dichos servicios.

Por ejemplo en (ETSI, 2014), para la selección de una determinada PID en la figura 1.7 se muestra un diagrama de secuencia en donde el CICAM puede usar la APDU PID_select_req () para actualizar la lista PID seleccionada.

A continuación se describen los pasos para la autorización:

1. El anfitrión selecciona un nuevo servicio. El video_pid0x1000 y el audio_pid0x1001 están codificados y por lo tanto incluidos en el *ca_pmtas elementary_PID* y seleccionados por el anfitrión. El PID del servicio PMT es 0x0500 y es seleccionado por el anfitrión. El PMT contiene dos *ca_descriptores* que coinciden con el *ca_system_idof* del CICAM. Los PIDs correspondientes (0x0800, 0x0801) son seleccionados por el anfitrión. La lista predeterminada de PID seleccionados es entonces {0x0011, 0x0012, 0x0500, 0x0800, 0x0801, 0x1000, 0x1001}.
2. El CICAM determina que no necesita que el anfitrión filtre el SDT PID, EIT PID, PMT PID y el ECM PID 0x0801.
3. El CICAM también necesita que el CAT PID sea incluido en la lista PID seleccionada. El CICAM envía entonces una APDU PID_select_req () incluyendo el PID ECM restante (0x0800) y el PID CAT (0x0001). El host responde positivamente y la nueva lista de PID seleccionados es entonces {0x0001, 0x0800, 0x1000, 0x1001}.
4. El CICAM recibe el primer CAT, lo analiza y determina el PID EMM requerido (0x1200).
5. El CICAM entonces envía una APDU PID_select_req () incluyendo el PID (0x0800) ECM restante, el PID CAT (0x0001) y el PID EMM (0x1200). El host responde positivamente y la nueva lista de PID seleccionados es entonces {0x0001, 0x0800, 0x1000, 0x1001, 0x1200}.

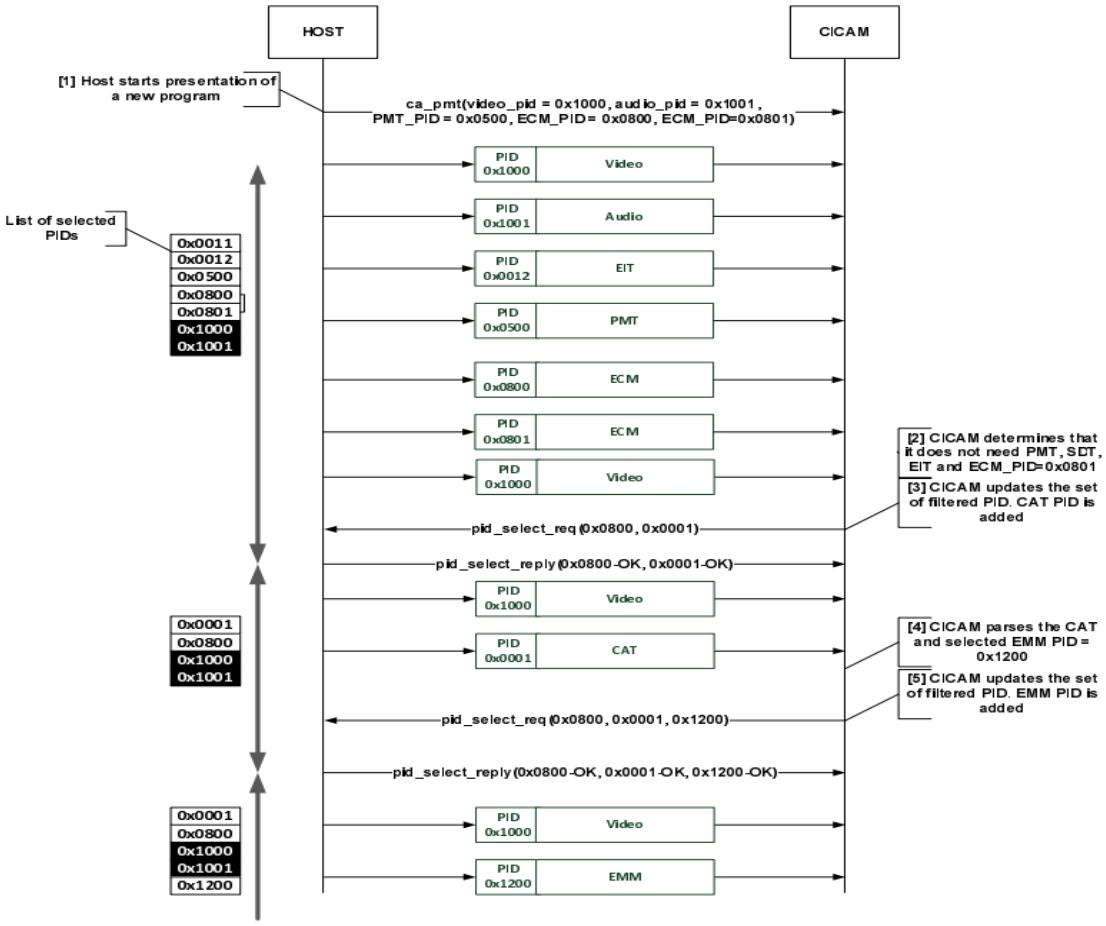

Figura 1.7 Ejemplo de selección PID diagrama de secuencia. Fuente (ETSI, 2014).

1.5 Interoperabilidad de los Sistemas de Acceso Condicional.

El proyecto DVB ha respaldado dos estándares diferenciados para los Sistemas de Acceso Condicional. El nombre de estos dos estándares es: SimulCrypt (ETSI, 2002a) y MultiCrypt (Européenne, 1996). Estos dos estándares son completamente válidos para ser usados tanto en las transmisiones vía satélite, cable o terrestres.

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 se encargara de 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.

1.5.1 SimulCrypt.

SimulCrypt es un sistema que facilita el uso de diversos sistemas de acceso condicional en paralelo aplicados sobre los programas de un mismo multiplex.

Desde el punto de vista del emisor, un múltiplex que transporta 2 programas (figura 1.8), cuyos programas están codificados con la misma CW y que ésta viaja encriptada a través de 2 mecanismos de acceso condicional. Cada sistema encripta la CW por su propio esquema de propietario y los datos resultantes se inserta en el flujo de señal a transmitir. El SimulCrypt proporciona una manera flexible para ofrecer diferentes productos a los abonados por el simple cambio del flujo de datos de acceso condicional. El Sincronizador SimulCrypt es un elemento esencial en este escenario ya que es el encargado de intercalar los mensajes ECM de cada uno de los CAS para que el abonado pueda obtener las palabras de control dentro del cripto-período.

En la figura 1.8, los componentes relativos a SimulCrypt aparecen en color cyan: los generadores de mensajes EMM de cada CAS, la información de sistema (SI) para cada uno de los CAS y la generación de mensajes ECM. La inserción en el TS de los mensajes ECM está controlada por el Sincronizador SimulCrypt (SCS, del inglés SymulCrypt Synchronizer).

En el TS 101 197 (ETSI, 2002a), se define una arquitectura de cabecera de red que permite efectuar un sistema que envía información de CA de varios proveedores en un mismo flujo de transporte. Dicho diagrama es el siguiente:

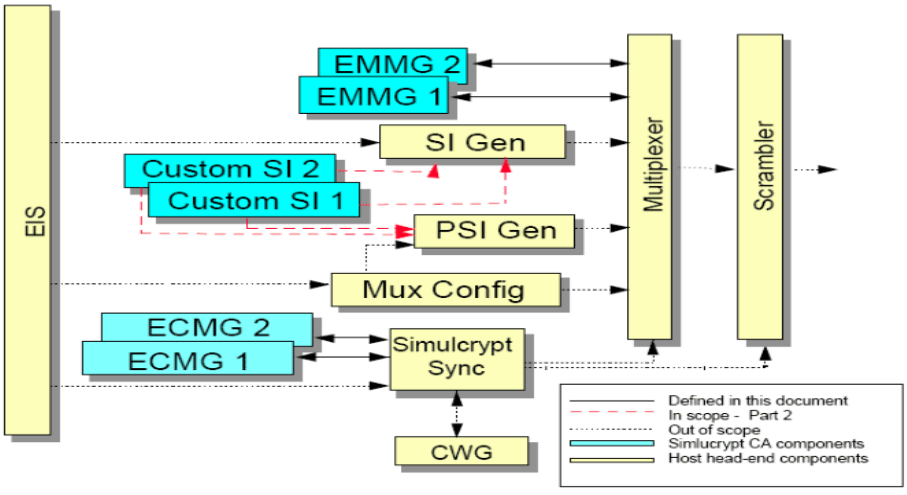

Figura:1.8 Esquema Simulcrypt Head-End (TS 101 197). Fuente (ETSI, 2002a).

1.5.2 **MultiCrypt**.

MultiCrypt es un sistema que permite que un mismo receptor funcione con múltiples CAS mediante un Interfaz Común (CI) definido en la especificación EN50221 (Européenne, 1996). Cada módulo tiene un subsistema de CA, que es administrado por el STB. Este funcionamiento posibilita la competencia entre proveedores de CAS y operadores de televisión de pago. El interfaz común es un interfaz estandarizado para conectar al receptor un módulo extraíble, generalmente un módulo denominado PCMCIA (Ver Anexo 1). El módulo PCMCIA implementa las funciones específicas para un CAS particular como se muestra en la figura 1.9. Para poder visualizar un programa codificado por un CAS que no esté instalado en el receptor, el usuario deberá intercambiar los módulos manualmente. Esto permite que varios proveedores de servicio co-existen en el receptor y les permitan actualizar su subsistema de CA con mayor comodidad. Existen algunos receptores que permiten tener varias PCMCIA al mismo tiempo y de este modo el usuario se ahorra el tener que irlas cambiando.

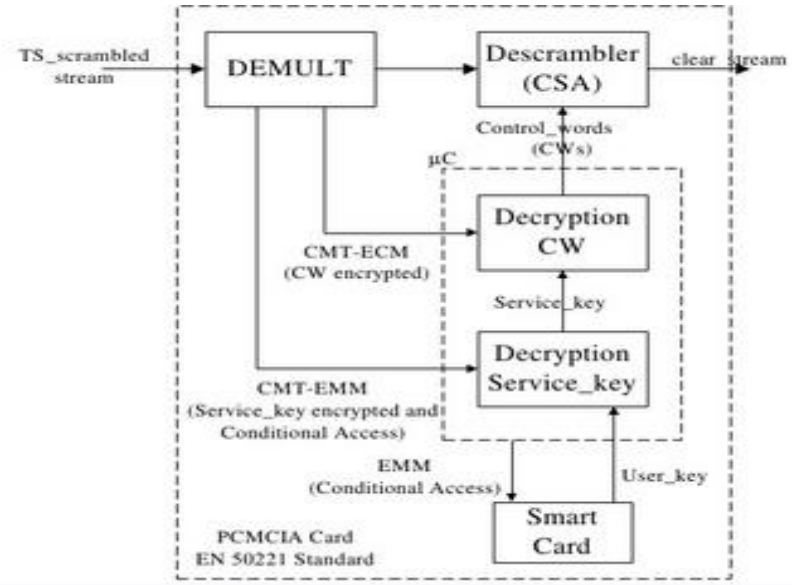

Figura 1.9 Proceso de descodificación, en módulo PCMCIA. Fuente (Navarro, 2012).

La mayoría de los grandes proveedores de contenidos audiovisuales de pago no ofrecen STBs con módulo multicrypt por diversas razones:

- Facilitan el cambio de proveedor, ya que únicamente cambiando el módulo CAM podrían contratar los servicios de otro proveedor.
- A pesar de que el coste del STB sería más económico, en conjunto con el módulo CAM supondría un precio más elevado.

Por estas razones, el uso de STB junto con módulos CAM se concentra en círculos muy reducidos habitualmente relacionados con la escena clandestina (usuarios avanzados, desarrolladores, hackers, piratas, etc.).

1.5.3 Comparación SimulCrypt vs MultiCrypt.

Con SimulCrypt se requieren acuerdos comerciales entre diferentes proveedores de servicio para conseguir la interoperabilidad entre diferentes CAS. Esto crea una barrera a las nuevas compañías que pretenden entrar en el mercado de la televisión de pago. Otra desventaja de SimulCrypt es el incremento en el uso del ancho de banda, ya que los mensajes CA se multiplicarán, por lo que se creará un problema de escalabilidad. Por otro lado, la seguridad de todo el sistema SimulCrypt será igual de fuerte que el más débil de los CAS. La ventaja principal de SimulCrypt es que no hay un costo extra para los usuarios finales.

Mientras que MultiCrypt permite que un mismo fabricante de equipos puede fabricar el mismo receptor base para diferentes sistemas CA, al que se le puede añadir una o varias interfaces diferentes al módulo de CA. El usuario podrá contratar servicios de diferentes proveedores manteniendo un único receptor solamente añadiendo los módulos de CA correspondientes. La utilización de diferentes sistemas de CA para sus contenidos trae consigo una fuerte seguridad ante ataques piratas. La principal desventaja que presentan estos sistemas es referente al costo extra para los usuarios finales, puesto que los equipos requeridos serían más caros y se requieren módulos extras.

1.6 Alternativas de televisión por suscripción.

La televisión de pago supone un acercamiento diferente al negocio televisivo, puesto que su modelo no se basa en la publicidad directa, como ocurre en la televisión en abierto, sino en el atractivo de los contenidos suministrados (películas, eventos deportivos, canales temáticos, servicios interactivos, etc.) son para aquellos usuarios que puedan pagarlos. La supervisión

de los sistemas de acceso condicional está siendo utilizada actualmente por un gran número de operadores, transmitiendo la televisión digital a través de diferentes vías de difusión.

1.6.1 Televisión vía Satélites.

El servicio de televisión por suscripción vía satélite, también conocido como televisión satelital por suscripción, opera a partir de un Sistema Directo al Hogar (DTH, del inglés Direct-to-Home) destinado a la distribución de señales de televisión por radiodifusión directamente al público desde satélites geoestacionarios.

Para garantizar la protección de los contenidos distribuidos por las señales satelitales, los servicios DTH emplean CAS con el fin de restringir el acceso solo al personar autorizado. Para la adquisición de dichos contenidos es necesario la presencia de un decodificador o STB y una tarjeta inteligente oficial del prestador de servicio DTH (Hernández, 2011). Las tarjetas inteligentes se emplean para gestionar y almacenar los derechos para descifrar contenidos en función del paquete de servicio o programas adquiridos por suscriptor.

1.6.2 Televisión vía red IP: IPTV.

En los últimos años muchas definiciones de lo que es IPTV han aparecido, pero la mayoría de ellas se desvían de lo que realmente es y terminan definiendo tecnologías diferentes.

Una definición oficial aprobada por la Unión Internacional de Telecomunicación es:

"IPTV es la denominación para los servicios multimedia de distribución de señales de televisión, video, audio, texto, gráficos y datos sobre redes basadas en el protocolo de internet (o IP por sus siglas en inglés Internet Protocol) que proveen el nivel requerido de calidad de servicio o calidad de experiencia, seguridad, interactividad y contabilidad".(Puentes Fernández and Barrera Vargas, 2013).

El proceso de transmisión sobre IP puede comenzar desde un servidor donde este almacenado el video, desde una transmisión en vivo o puede ser una señal satelital. Para convertir la señal de la fuente en datos digitales, debe pasar por un codificador, luego estos datos digitales son encapsulados en paquetes IP. Antes de ser encriptada; luego, es transmitida para llegar a un STB para que pueda ser interpretada por el televisor o una PC.

Los CAS implementados en *hardware* (Ver Anexo II) para IPTV suelen almacenar sus credenciales de acceso en *smart-cards* proporcionadas por el distribuidor de IPTV(Andreja,

2011). La conexión empleada en la transmisión del *stream* multimedia suele hacerse con UDP para aprovechar lo máximo posible el ancho de banda disponible. La contrapartida es que no se tiene la seguridad de que todos los paquetes lleguen a su destino o en orden, pero esto es una prioridad menor cuando de comunicaciones audiovisuales se trata: la pérdida de unos pocos bytes no afecta en gran medida a la reproducción. Los ECMs suelen viajar multiplexados con el *stream*, por lo que, al no haber garantía de que lleguen a su destino, es necesario enviar cada ECM repetidas veces a lo largo del tiempo. A diferencia de éstos, los EMMs viajan separados del flujo, normalmente en conexiones TCP punto a punto. Sin embargo, una de las principales limitaciones de esta arquitectura se basa en la necesidad de sustituir el *hardware* cuando se encuentra un fallo de seguridad serio en el sistema, lo cual puede suponer un desembolso de dinero muy importante para el proveedor.

Sin embargo el CAS por *software* permite una mayor flexibilidad del código, que lo capacita para realizar tareas más complejas que las que pueden llevar a cabo los sistemas basados únicamente en circuitería. Ante un fallo de seguridad en el sistema se puede actualizar un programa sin necesidad de sustituir dispositivos. Soportan cifrados fuertes (el *software* correrá en una máquina más potente que un STB tradicional) tal es el caso del CSA. Utilizan certificados digitales para la autenticación del cliente lo cual permite una mayor seguridad.(O'Driscoll, 2008).

1.6.3 Televisión vía Cable.

Los sistemas de televisión de pago por cable en sus principios se basaron en una serie de medidas simples. El más común de éstos era un filtro basado en el canal, que consistía en detener efectivamente el canal que se recibe por los que no se habían suscrito. A medida que el número de canales de televisión en estas redes de cable creció, el enfoque basado en filtro se hizo cada vez poco práctico. En la actualidad la red Híbrida de Fibra y Coaxial (HFC, del inglés Hybrid Fibre Coaxial), es una red poderosa de banda ancha que puede tener una capacidad del ancho de banda de 1 GHz (Muñoz, 2011). Esto ayuda a las grandes compañías operadoras de cables, en cubrir grandes distancias de cierta región geográfica ya que puede transportar sus datos por fibra óptica y luego la pasan a cableado coaxial, les permite al cliente tener una experiencia memorable no solo de cable sino también de internet y voz**.** Para garantizar la protección de los contenidos distribuidos por cable, la red HFC utiliza el sistema

CAS con el fin de restringir el acceso solo al personar autorizado. Para la adquisición de dichos contenidos es necesario la presencia de un decodificador o STB que se suministra al usuario, dispone de un módulo de acceso condicionado en donde utiliza una tarjeta inteligente para gestionar y almacenar los derechos para descifrar contenidos en función del paquete de servicio o programas adquiridos por suscriptor.(Pluas et al., 2015).

1.6.4 Televisión vía Terrestre.

El modelo de televisión digital terrestre consiste en enviar señales digitales de televisión mediante transmisores de televisión digital usando como medio de transmisión ondas hertzianas. Es una tecnología que permite la difusión de señales con una optimización del uso del espectro radioeléctrico, mejora la calidad de la señal de audio y de video, permite la interactividad e incrementa la oferta de programación. La adopción de modelos de acceso condicional para TDT con una mayor penetración se encuentran los países de Europa. En la mayor parte de los casos el acceso condicional se presenta mediante un modelo de suscripción por tarjeta prepago (Castillejo, 2014).

1.7 Conclusiones del capítulo.

En este capítulo se realizó una revisión sobre las principales características y requisitos que deben cumplir los CAS para llegar a una mejor comprensión sobre el mismo. Se pudo ver de forma general el proceso de encriptación/desencriptación de la señal. Se mostró una caracterización de los tipos de cifrado, donde se pudo apreciar que para realizar el proceso de cifrado de la señal la recomendación es utilizar el cifrado híbrido debido a que este radica las deficiencias de los anteriores.

CAPÍTULO 2. ARQUITECTURAS DE LOS CAS EN LAS REDES DE DIFUSIÓN DE TELEVISIÓN.

El presente capítulo está encausado en describir tanto las arquitecturas de los CAS como la interactividad (canal de retorno) que se produce en las diferentes redes de difusión de la televisión. Para una mejor comprensión se partirá de la elaboración de un diagrama de flujo en el cual se plasmará la metodología utilizada para arribar a un esquema CAS que se adecue a las condiciones actuales.

2.1 Descripción de la metodología utilizada.

La metodología utilizada en el proyecto de investigación está basada en un diagrama conceptual en el cual se explica los pasos que se tuvieron en cuenta en el desarrollo de la investigación. Dicho diagrama esta desglosado por niveles donde en un primer momento se realiza el análisis y comprensión de las arquitecturas CAS en las redes de radiodifusión. Aquí haremos alusión a las características que presentan estas arquitecturas en cuanto a transmisión/recepción del contenido y la tecnología utilizada para la interactividad (canal de retorno). Después de haber visto y analizado estas variantes se hará una propuesta acorde a la infraestructura desplegada en el país.

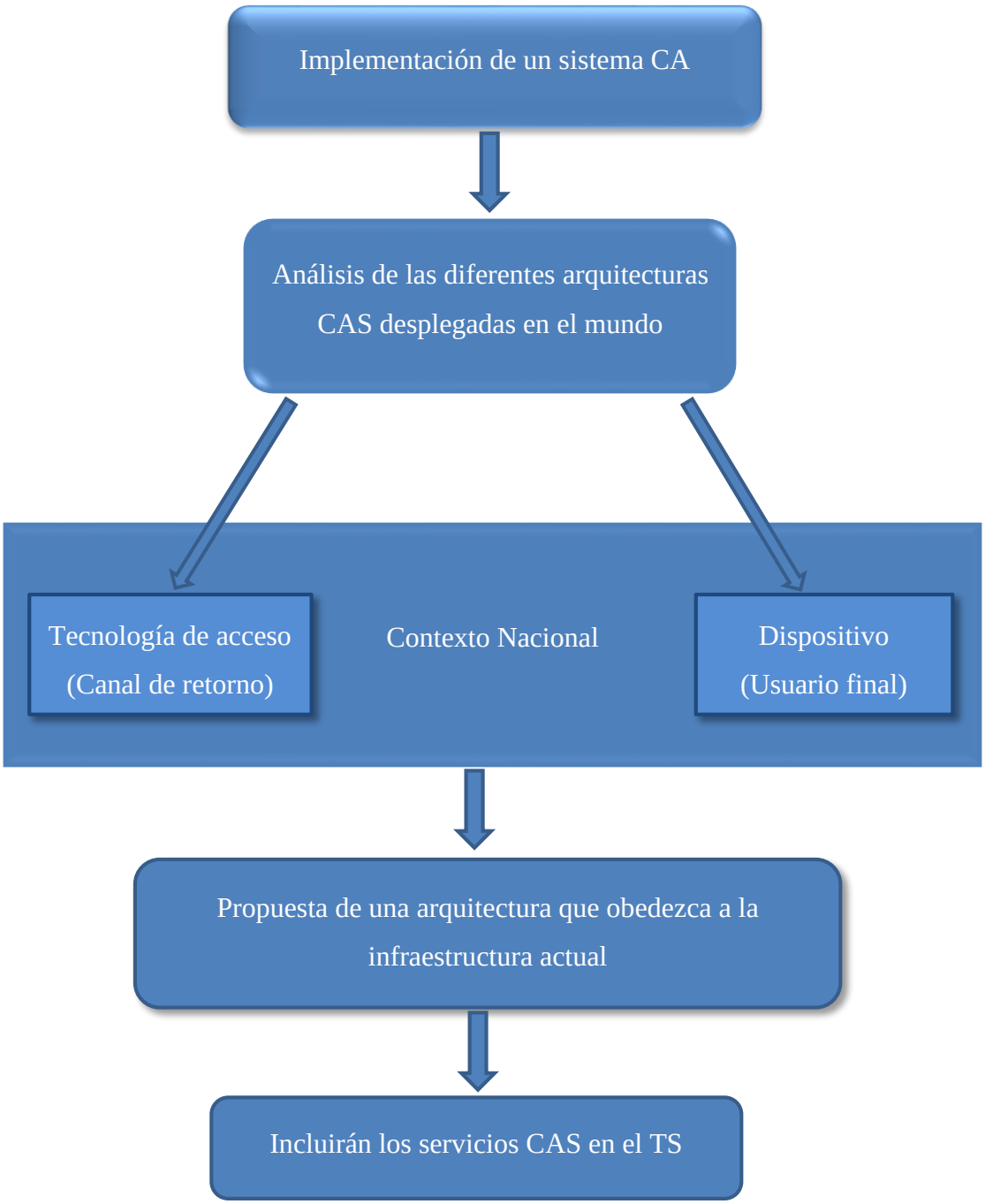

Figura 2.1 Diagrama de flujo. Fuente (Elaboración propia).

2.2 Televisión por suscripción, arquitecturas.

La televisión por suscripción es aquella en la que la señal, independientemente de la tecnología de transmisión utilizada, está destinada a ser recibida únicamente por personas

autorizadas para la recepción. La televisión por suscripción es un servicio de telecomunicaciones que ofrece programación dirigida a una parte del público en general, que consiste en la teledifusión y recepción de señales de audio y vídeo en forma simultánea. En la figura 2.2 se muestra el esquema general de transmisión de la señal por los medios de difusión Cable/Terrestre/Satélite.

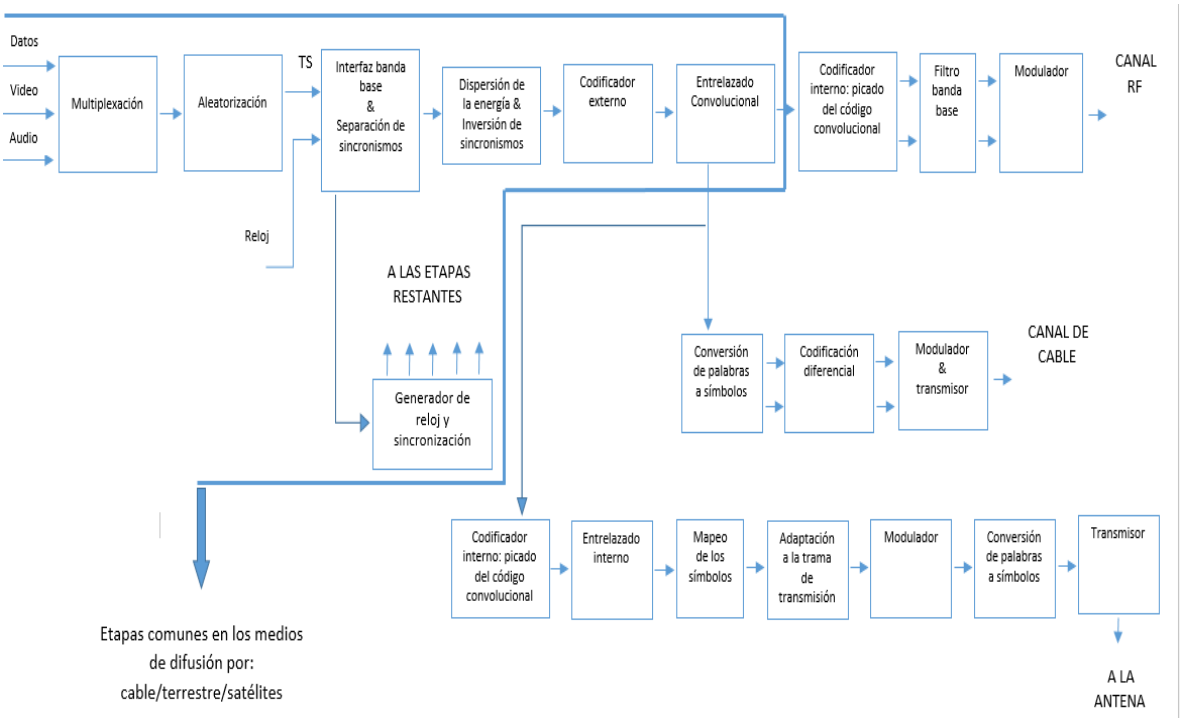

Figura 2.2 Esquema de transmisión de señal por los medios de difusión. Fuente (Elaboración propia apoyado en (Martínez et al., 2010)).

2.2.1 Suscripción vía Satélite.

En la figura 2.3 se describe el proceso de recepción de contenidos protegidos por los CAS. Cuando un suscriptor desea ver una señal específica, el STB recibe un ECM del proveedor de DTH y se lo envía a la tarjeta inteligente. La tarjeta inteligente descifra el ECM empleando la llave de trasmisión que esté vigente en ese momento y luego busca en su base de datos los derechos asignados al ECM para ver la señal en cuestión (determina si el suscriptor ha adquirido los derechos para ver la señal específica). Si los derechos coinciden, la tarjeta inteligente envía la CW al STB. La CW debe ser nuevamente encriptada para proteger la comunicación entre la tarjeta inteligente y el STB. Este proceso de protección de la señal satelital se denomina emparejamiento o *pairing*.

Figura 2.3 Funcionamiento de un sistema de televisión satelital por suscripción. Fuente (Hernández, 2011).

2.2.2 Suscripción vía IP o IPTV.

Este modelo utiliza como medio de transmisión de las señales conexiones de banda ancha sobre el protocolo IP (Saavedra Abarca, 2009). IPTV se ha desarrollado basándose en el video-streaming. Este sistema consiste en que la reproducción de los videos o películas no requieren de una descarga previa por parte del usuario, sino que el servidor entrega los datos de forma continua, sincronizada y en tiempo real (al mismo tiempo que se envía, se está visualizando el video con su audio).(Ibarra Tobar, 2015).

En la figura 2.4 se muestra el funcionamiento básico de un CAS para la televisión IPTV. En primer lugar, el cliente busca un servidor de claves y, una vez encontrado, hace una petición (pasos 1 y 2). En respuesta, el servidor desafía al cliente a que demuestre su identidad (paso 3). En el paso 4 el cliente envía su certificado, que es verificado por el servidor. Finalmente éste responde con la/s clave/s, convenientemente protegida/s bajo una conexión cifrada.

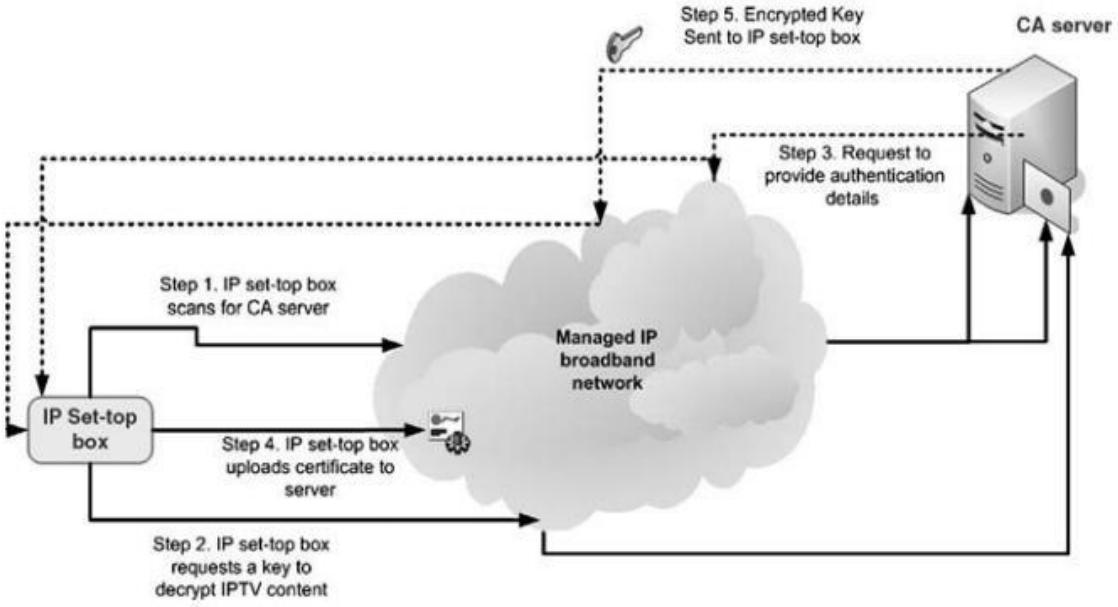

Figura 2.4 CAS básico para a autenticación del cliente. Fuente (O'Driscoll, 2008).

2.2.3 Suscripción por Cable.

Las plataformas de televisión por cable utilizan una única tecnología de codificación común normalizada. Sin embargo, para entregar la palabra de control a los clientes de forma segura se utilizan diferentes soluciones propietarias unas de estas es la que se observa en la figura 2.5.

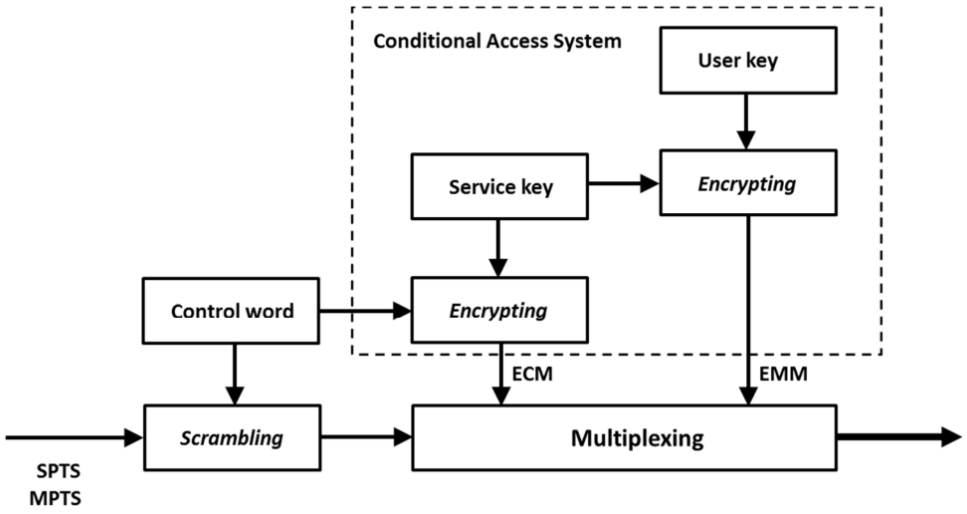

Figura 2.5 Sistema CAS para tv por cable. Fuente (TNO, 2014).

Para proporcionar el servicio de televisión digital, cada cliente necesita una clave de usuario única. Esta clave de usuario se implementa en hardware en una tarjeta inteligente con un código de identificación impreso en el exterior. Los proveedores de cable tienen la información del proveedor de las tarjetas inteligentes necesarias para asociar las claves del usuario y la palabra de control con los códigos de identificación de la tarjeta, los proveedores de cable pueden proporcionar canales digitales o paquetes de canales de televisión a cada cliente sobre una base individual.

En la figura 2.6 se muestra de forma general la estructura de una red HFC en la cual se observa el tránsito de la señal hasta llegar al cliente, la razón de transmisión por parte de los proveedores de cable varian en dependencia de las ofertas que se brinden.

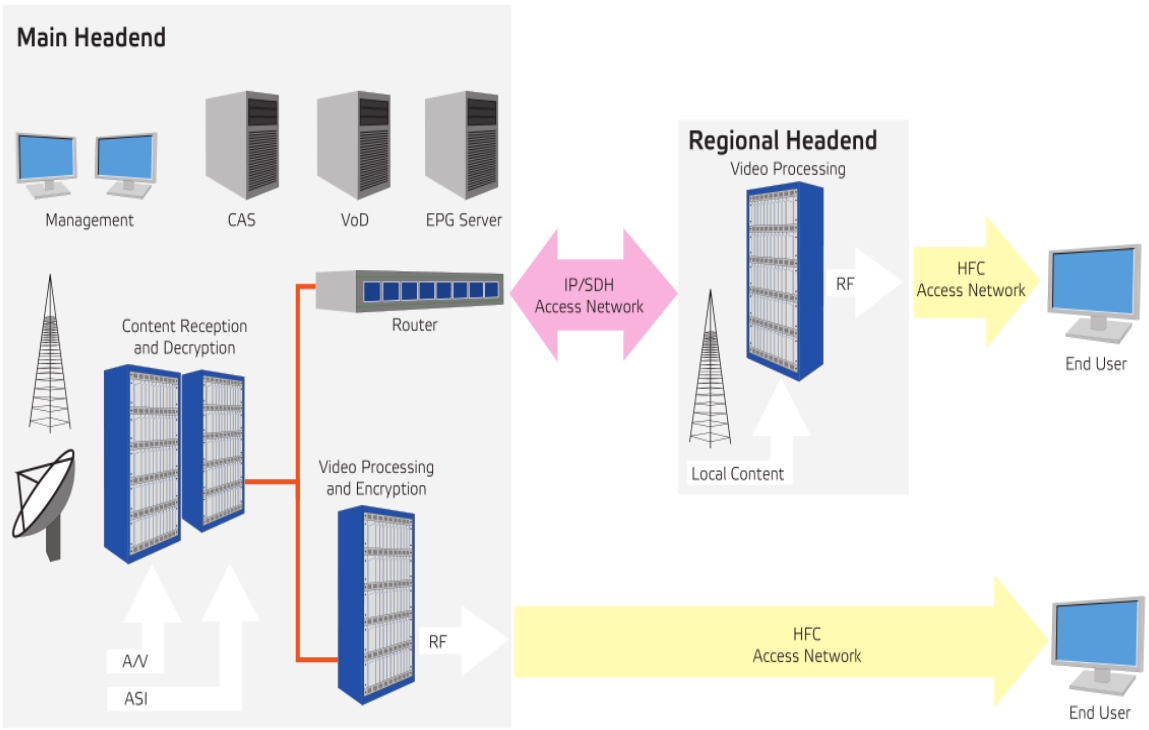

Figura 2.6 Arquitectura genérica de televisión por cable. Fuente (TNO, 2014).

2.2.4 Suscripción por difusión Terrestre.

En la figura 2.7 se muestra el proceso de transmisión/recepción de contenidos protegidos en radiodifusión en donde el suscriptor tiene acceso si realiza el pago el cual debe incluir todas las formas de transacción posibles incluyendo (efectivo, débitos directos y

tarjetas créditos, etc.). Dicho pago se realiza con el Sistema de Gestión de Suscriptor (SMS) quien se encarga de transmitir al Sistema de Gestión de Suscriptor (SAS) la verificación de que el suscriptor ha realizado el pago y tiene derechos a los servicios correspondientes.

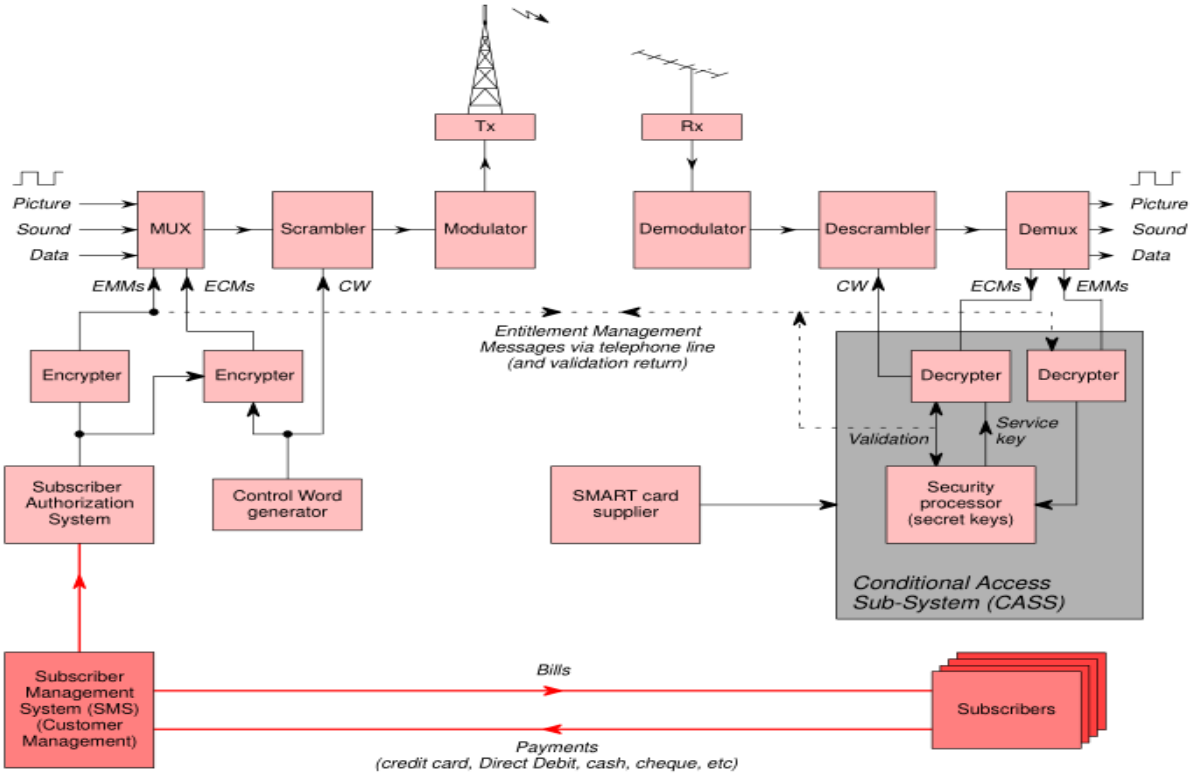

Figura 2.7 Arquitectura de pago para TDT. Fuente (Rix et al., 2002).

2.3 Interactividad en las redes de Televisión.

La interactividad entre un proveedor de servicios y los espectadores en la red, es establecida, a través de un canal de retorno para el sistema de transmisión. La evolución de la tecnología de comunicación ha influido en la manera en que un usuario final puede comunicarse con las redes intermedias que se conectan a los proveedores de servicio (Ibarra Tobar, 2015). Actualmente, la televisión interactiva ofrece servicios tales como:

- Videotelefonía por TV.
- Videoconferencia por TV.
- Descargar video bajo demanda por PC y STB.
- Grabación de video personal.
- Video Bajo Demanda.

- Transmisión de audio, bajo demanda.
- Mercadeo y Publicidad.
- Servicios de Voz y Texto.
- Mosaico/Picture in Picture (PIP).
- Televisión Interactiva.
- Acceso a correo electrónico y web (T-mail & Web Access).
- Juego en línea.
- Pago por Visión (PPV).
- Guía Electrónica de Programas (EPG).

Según el nivel de complejidad de la capacidad de interacción y transmisión, el canal de retorno desde el usuario al proveedor de servicios podría ser de un solo sentido, camino banda estrecha (o ruta estrecha) / banda ancha bidireccional.

El despliegue de un canal de interacción se divide en dos niveles:

- Primero el diseño de nivel superior que es independiente de la red y se ocupa de las diversas aplicaciones que interactúan con los usuarios.
- En segundo lugar, el diseño de nivel inferior que es dependiente de la red y proporciona el canal físico para los propósitos de interacción.

Las siguientes secciones explicarán el diseño de la red dependiente de las vías de transmisión de televisión.

2.3.1 Canal retorno vía Satelites.

En sus principios, el alcance de la utilización de sistemas satelitales para el canal de interacción se limitaba principalmente al entorno de negocio a negocio. Sin embargo, con el crecimiento del mercado, esta se ha extendido al entorno doméstico. En la especificación (ETSI, 2003) la interactividad se logra a través de los satélites geoestacionarios de redes interactivas y Canales de Retorno por Terminales Satelitales (RCST, del inglés Return Channels for Satellite Terminals). Los principales bloques funcionales que componen dicha red son los siguientes.

- *Alimentador*: Transmite la señal hacia delante (señal de enlace ascendente), transportar la señal de datos de usuario o el tiempo de control. Se necesita la

información de temporización para el funcionamiento de la red interactiva vía satélite y sincronización entre el enlace ascendente y enlace descendente.

- *Centro de Control de Red (NCC)*: Provee monitoreo y funciones de control (MCF). Genera las señales de control y temporización para la operación de la red interactiva de satélite para ser transmitida por la estación (s) del alimentador.
- *El tráfico de puerta de enlace*: Se recibe señales de retorno RCST y proporciona la contabilidad, servicios interactivos o conexión con los proveedores de servicios.

La sincronización entre RCST y la red interactiva de satélite se maneja a través de la Red de Referencia de Reloj (NCR, del inglés Clock Reference Network). El NCR es recuperado por RCST de TS MPEG-2 con un Identificador de Programa Específico (PID, del inglés Specific Program Identifier). El RCST reconstruye el reloj de referencia de la NCR recibido y compensa la portadora de frecuencia.

En el enlace directo los RCSTs se deben identificar de forma única mediante dirección MAC física y dirección lógica. La dirección MAC es un valor de 48 bits compatible con el estándar IEEE 802.3 que se almacena en una memoria no volátil que corresponde a un identificador físico único RCST. La dirección lógica consiste en dos campos; el ID de grupo y el ID de entrada. El ID de grupo de 8-bit corresponde a un grupo que se conecta a RCSTs. El ID de entrada de 16-bit identifica de forma exclusiva el RCST dentro de un ID de grupo.

La figura 2.8 muestra un modelo de RCS. La transmisión de descargar (SAT FW) y la transmisión de canal de retorno de enlace ascendente (SAT RT) se pueden proporcionar por dos satélites separados o simplemente un satélite, que se utiliza tanto para (abajo / arriba).

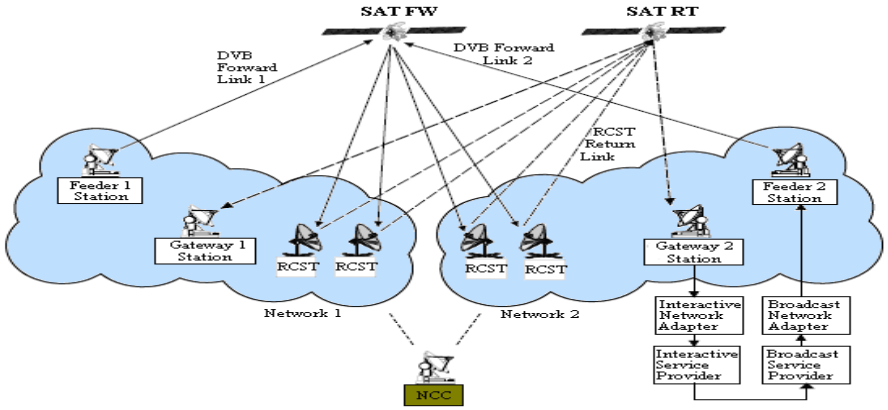

Figura 2.8 Un modelo de referencia para la red de satélite interactiva. Fuente (ETSI, 2003).

2.3.2 Canal de retorno vía IP.

La red IP ofrece interactividad en servicios específicos de televisión, servicios de programación interactiva y servicios interactivos. En la IPTV ambas difundidas por el modo de multidifusión y los canales de retorno ascendente son implementados a través de protocolos de Internet en las diferentes tecnologías de acceso (CI, 2016). Dichas tecnología se identifican en la figura 2.9.

El tráfico de IPTV puede ser protegido de otros tráficos de datos, para garantizar un nivel adecuado de QoS. El último enlace o "enlace de última milla", que llega hasta el hogar, encargado de distribuir los datos, voz y video, puede ser realizado empleando distintas tecnologías físicas (FTTx, xDSL, WLAN, WIMAX, etc.). Finalmente, los STB, u otros dispositivos multimedia se encargan de decodificar la información, y presentarla al usuario. (Morales Figueroa, 2010).

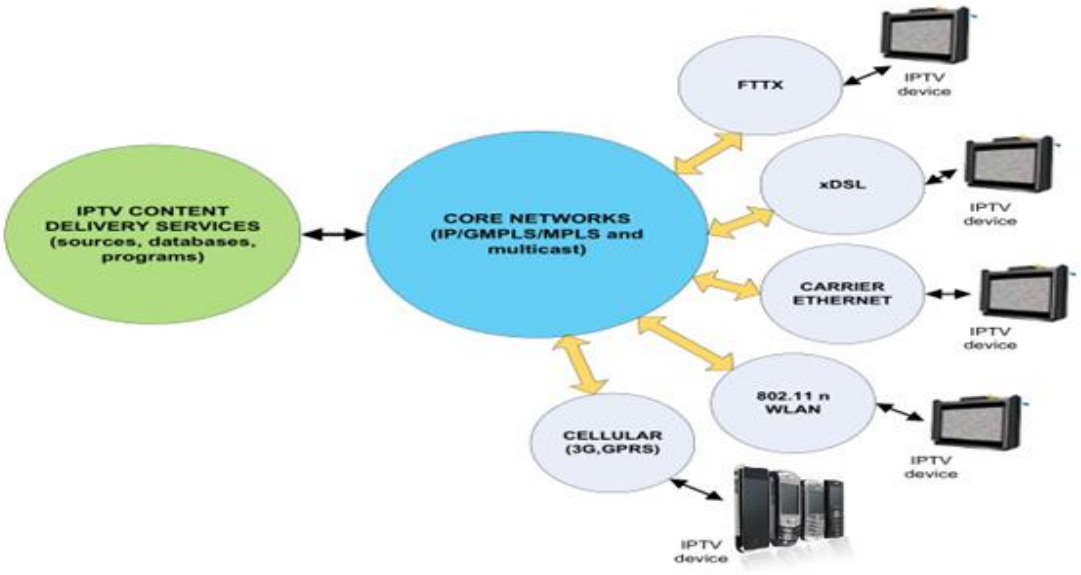

Figura 2.9 Arquitectura genérica de IPTV. Fuente (Morales Figueroa, 2010)

2.3.3 Canal de retorno vía Cable.

La televisión por cable (CATV) soporta un camino bidireccional entre un terminal de usuario y el proveedor de servicio. El camino interactivo de televisión por cable se compone de un camino de interacción hacia adelante (descendente) y un camino de interacción de regreso (ascendente). El camino descendente se utiliza para enviar la sincronización y la información

del Adaptador de Interfaz de Red (INA, del inglés Network Interface Adapter), en la cabecera de todas las Unidades de Interfaz de Red (NIU, del inglés Network Interface Units). Esto le permite a las NIUs adaptarse a la red y enviar la información sincronizada ascendente (ETSI, 2001).

Un mecanismo de control de acceso debe ser aplicado en CATV para gestionar los múltiples accesos a un cable coaxial compartido. El Acceso Múltiple por División de Tiempo (TDMA, del inglés Time Division Multiple Access), es una técnica que se utiliza para dividir la transmisión en sentido ascendente en ranuras de tiempo, que puede ser utilizado por diferentes usuarios finales. Un canal descendente se utiliza para sincronizar hasta 8 canales ascendente. Un contador en el INA se envía periódicamente a las NIUs, por lo que todas las NIUs trabajan con el mismo reloj. Esto da la oportunidad al INA para asignar intervalos de tiempo a diferentes usuarios. Los modos de acceso adoptado para este sistema pueden estar basado en contención o acceso sin contención, que varían en el nivel de congestión con los otros usuarios.

Con el fin de sincronizar y proporcionar información a todas las unidades, se definen dos alternativas: dentro de banda (IB) y fuera de banda (OOB) de señalización descendente, aunque un decodificador no necesita soportar ambos sistemas.

En la señalización OOB, es un camino de interacción hacia adelante y está reservado para los datos interactivos e información de control. En este caso, la presencia de este camino es obligatorio, además es posible enviar información descendente de velocidad de bits superior a través de un receptor de un canal de cable.

En el caso de la señalización de IB, el trayecto de información de camino hacia adelante está incrustado en el TS MPEG-2 de un canal de cable. Sin embargo, no es obligatorio incluir la información de camino hacia adelante en todos los canales de cable. Ambos sistemas pueden proporcionar la misma calidad de servicio (QoS). Sin embargo, la arquitectura general del sistema será diferente entre las redes que están utilizando IB y OOB. Ambos sistemas pueden existir en la misma red, si se le asignan diferentes frecuencias a cada sistema.

El INA puede establecer una comunicación de unidifusión a un usuario en particular utilizando direcciones en los STB. Además, tener la dirección de cada set-top box, en sentido ascendente la información puede ser diferente a la INA. Para el canal interactivo OOB

descendente, se pueden utilizar una velocidad de datos de 1,544 Mbps o 3.088 Mbps. No hay limitación para los canales IB descendente, sin embargo, la velocidad de datos será el múltiplo de 8 Kbps. En la figura 2.10 se presenta un modelo de referencia para un sistema interactivo en TV por cable (CATV).

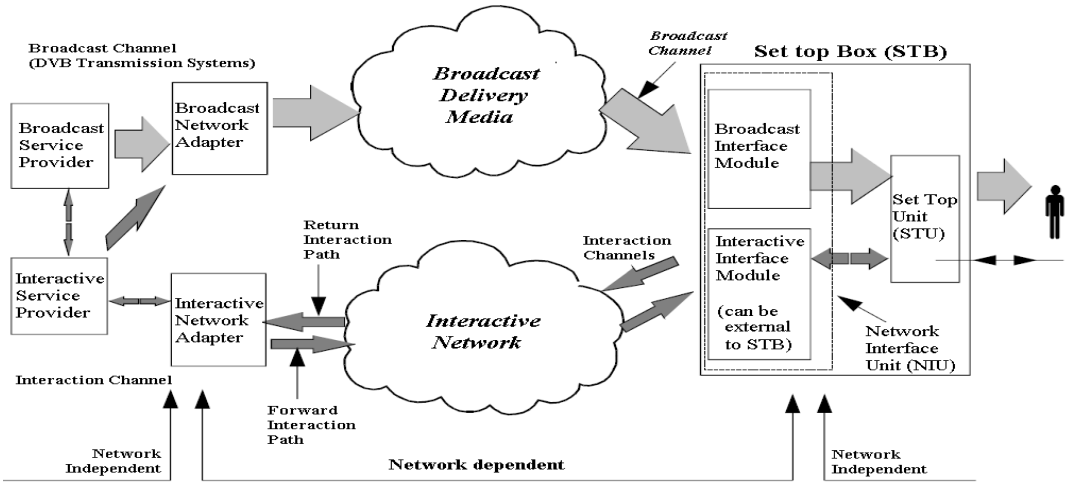

Figura 2.10 El diagrama funcional CATV interactivo. Fuente (ETSI, 2001).

2.3.4 Canal de retorno vía Terrestre.

El canal de retorno para el sistema terrestre RCT es capaz de proporcionar interactividad utilizando la infraestructura existente para la televisión digital terrestre. Conecta los Terminales Terrestres del Canal de Retorno (RCTT, del inglés Return Channel Terrestrial Terminals) a un INA.

El camino de interacción hacia adelante está integrado en el canal de radiodifusión. Como resultado, la red interactiva terrestre consiste en dos capas físicas unidireccionales. La dirección descendente está compuesta por la emisión más el camino de interacción hacia adelante y la dirección ascendente es la ruta de interacción de retorno.

En la dirección descendente se asigna un PID específico a los mensajes de señalización para los servicios interactivos. Los datos de aplicación y los mensajes de señalización a la inversa se encapsulan en el Modo de Transferencia Asíncrona (ATM, del inglés Asynchronous Transfer Mode), las celdas que se correlaciona con las ráfagas físicas de un sistema de

transmisión de VHF / UHF. Ofrece un canal inalámbrico de interacción para la televisión digital terrestre interactiva incluso en las congestionadas bandas de UHF / VHF.

Como se evidencia en la figura 2.11, la transmisión en sentido descendente desde la estación base INA proporciona información de sincronización y de gestión para todos los RCTTs. Esta información es utilizada por los RCTTs con el fin de acceso al canal ascendente y transmitir de forma sincronizada a la estación base. Una única antena en la estación remota es suficiente para recibir la difusión, reenviar los canales de interacción y enviar la información sobre el canal de interacción hacia atrás. El sistema de Multiplexación por División de Frecuencias Ortogonales (OFDM, del inglés Orthogonal Frequency-Division Multiple Access) puede gestionar rentablemente los espectros UHF / VHF.

Por lo tanto, el costo de implementación del RCT es considerablemente más baja que cualquier sistema rival como el PSTN o GSM. Además, las redes terrestres y RCT puede proporcionar servicios sin cables para la recepción del contenido en los hogares. Esto se traduce en enormes ahorros para proveedores de servicios, ya que pueden lanzar nuevos servicios y generar más ingresos con cambios mínimos en la configuración de la prestación de servicios.

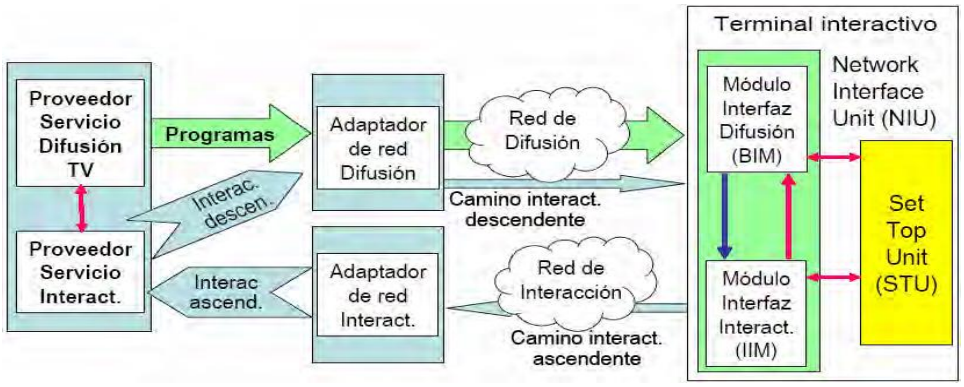

Figura 2.11 El diagrama funcional, TDT interactivo. Fuente (Cáceres, 2011).

2.3.5 Canal de retorno en red GSM.

El Sistema Global para Comunicaciones Móviles (GSM, del inglés Global System for Mobile), es una infraestructura que puede proporcionar canal de interacción para sistemas de radiodifusión (ETSI, 2002). Proporciona una bi-comunicación inalámbrica bidireccional

entre el equipo de cabecera y el extremo del receptor. La red GSM puede ser total o parcial de la red de interacción. Se puede conectar a otra red (es decir PSTN, ISDN) para llegar al proveedor de servicios.

En el lado receptor, el decodificador estará equipado con un Módulo de Interfaz Interactivo (IIM, del inglés Interactive Interface Module) para acceder a la red GSM. La interfaz entre el STB y la red GSM debe cumplir con las Funciones de Adaptación de Terminal (TAF, del inglés Terminal Adaptation Functions) para estaciones móviles y para servicios que utilizan capacidades de portadoras asíncronas (Alkan and Shafer, 2013; Rasanen, 2001). También para proporcionar el conjunto de canal de interacción la interfaz entre la red GSM y la red externa, deberá cumplir con los requisitos generales y los requisitos de interoperabilidad entre la red GSM y la ISDN o PSTN o cualquier otra especificación de interconexión GSM (Aggelou and Tafazolli, 2001; Fjortoft and Colban, 2003). Dependiendo de la red externa, la estación móvil debe estar configurada para soportar las capacidades de portadoras. Cuando sea posible, es preferible implementar GSM-ISDN, que proporciona un enlace digital de extremo a extremo entre el IIM es decir, STB y el INA (el proveedor de servicios) con tiempos de establecimiento de conexión más bajos.

Las interfaces físicas varían dependiendo de la forma en que la estación móvil GSM es conectado a la unidad decodificadora. La estación móvil puede estar integrada con el STB como un módulo interno o externo. La estación móvil externo debe apoyar los requisitos de la interfaz entre el decodificador como un Equipo de Terminal de Datos (DTE, del inglés Data Terminal Equipment) y la estación móvil como Equipo de Comunicación de Datos (DCE, del inglés Data Communication Equipment), (ETSI, 1995) y de la misma manera para la interfaz de módem (Européenne, 1996). La estación móvil interna (integrada) deberá satisfacer las mismas necesidades que el MS (del inglés, Mobile Station) externos con la excepción de proporcionar el conector de interfaz de 9 pines.

Los nuevos servicios de datos se están haciendo disponibles con la evolución de GSM hacia las comunicaciones móviles y, en particular, el Servicio de Radio Paquete General (GPRS, del inglés Radio Service General Package) ofrece un canal de interacción adecuado para el escenario con un modelo de referencia similar mostrado en la figura 2.12.

En términos de costos de implementación y despliegue, el GSM es más asequible y rentable (sobre todo para los países en desarrollo) en comparación con las tecnologías mencionadas anteriormente. Las características como la movilidad y las marcas de itinerancia, esta tecnología se destaca entre el resto.

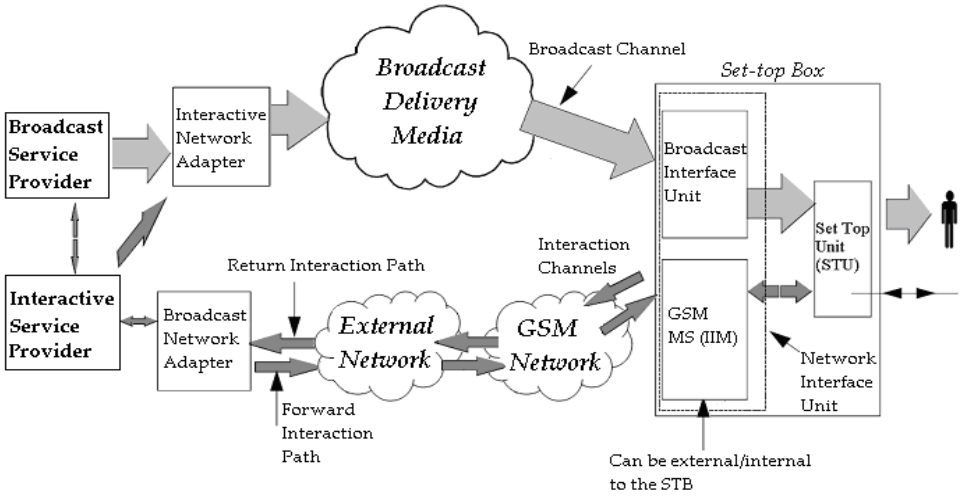

Figura 2.12 Arquitectura del sistema GSM cuando se utiliza como un canal de interacción. Fuente (ETSI, 2002).

2.4 Comparación entre las diferentes vías de trasmisión de televisión.

En la siguiente tabla podemos observar la divergencia existente entre los distintos medios de difusión.

Tabla 2.2 Características principales de los medios de comunicación en función del CAS.

Características	TDT	Satélite	Cable	ADSL
Instalación	Instalación fácil y rápida, recepción por antena convencional. Necesita un TV con descodificador incorporado o externo (STB).	Requiere la instalación de una antena parabólica. Necesita decodificador.	Requiere de cable. Necesita decodificador o modem.	Requiere conexión ADSL con proveedor que ofrezca TV. Necesita decodificador o modem.

Suscripción	No requiere suscripción pero si se podría tener.	Requiere servicio de suscripción.	Requiere servicio de suscripción.	Requiere servicio de suscripción.
Ancho de banda	Medio	Muy alto	Alto	Alto
Cobertura	Nacional regional y local; posibilidad de desconexiones territoriales	Continental y nacional	Nacional, regional y local	Nacional, regional y local
Canal de retorno	Canal telefónico, o celular	Canal telefónico	Conexión coaxial	Canal ADSL
Portabilidad	Permite recepción portátil y móvil	No permite	No permite	No permite
Otras características	Óptima calidad en condiciones precarias de recepción	Acceso a canales extranjeros	Posibilidad de servicios adicionales de telefonía e internet.	No requiere instalación exterior

2.5 Conclusiones del capítulo.

En este capítulo se analizó el funcionamiento del CA en las arquitecturas de las diferentes vías de transmisión de la televisión. Se constata que la variante de CA más usada es mediante la tarjeta inteligente (*Smart card*) debido a las ventajas que son proporcionadas por las mismas con respecto a la diversidad de proveedores de servicios que se pueden utilizar a través del CAM.

Después de haber visto la interactividad (canal de retorno) en las redes de difusión se observa que las más idónea a emplear es mediante la red GSM debido a sus características (facilidades, menor costo de implementación) que poseen las mismas.

El estudio y análisis de las características principales de las misma forjara e incidirá en alternativas a analizar en el capítulo venidero

CAPÍTULO 3. PROPUESTAS DE ARQUITECTURAS CAS EN CUBA.

En el presente capítulo, tomando en consideración el despliegue y desarrollo de la televisión digital ya instaurada en Cuba, así como las diferentes tecnologías de acceso existente, se proponen arquitecturas de CAS basadas en la imbricación de tecnologías de radiodifusión de tv y tecnologías para la transmisión de datos en redes móviles celulares se explican consecuentemente las posibles variantes en cuanto a varios criterios en las mismas.

3.1 Desarrollo de las TIC en Cuba, actualidad.

Como parte de la política integral para el perfeccionamiento de la informatización de la sociedad en el país, se plantea que el objetivo general está encaminado en lograr que las tecnologías de la Informatización y las Comunicaciones se conviertan en un sector de desarrollo estratégico de la nación, fortaleciendo una economía basada en el conocimiento, que se exprese en aportes significativos a las exportaciones y a la economía nacional, facilitando el amplio acceso a los contenidos y servicios digitales por los ciudadanos.

Está concebido además, priorizar y potenciar la infraestructura de telecomunicaciones que soporten el desarrollo de canales de pago con especial énfasis en la banca telefónica y móvil, la pasarela de cobros y pagos y los terminales de puntos de venta. Esta política estará encausada en algunos proyectos y sistemas básicos encargados de garantizar interoperabilidad con plataformas de gobierno, resultados con mayor inmediatez e impacto tanto en la gestión interna como en la población. Por lo que se definen dos líneas de trabajo, la primera es orientada a la creación de la infraestructura tecnológica y la segunda a la generación de servicios y contenidos digitales (MIC, 2017). Dichas líneas son desglosadas en la siguiente figura 3.1.

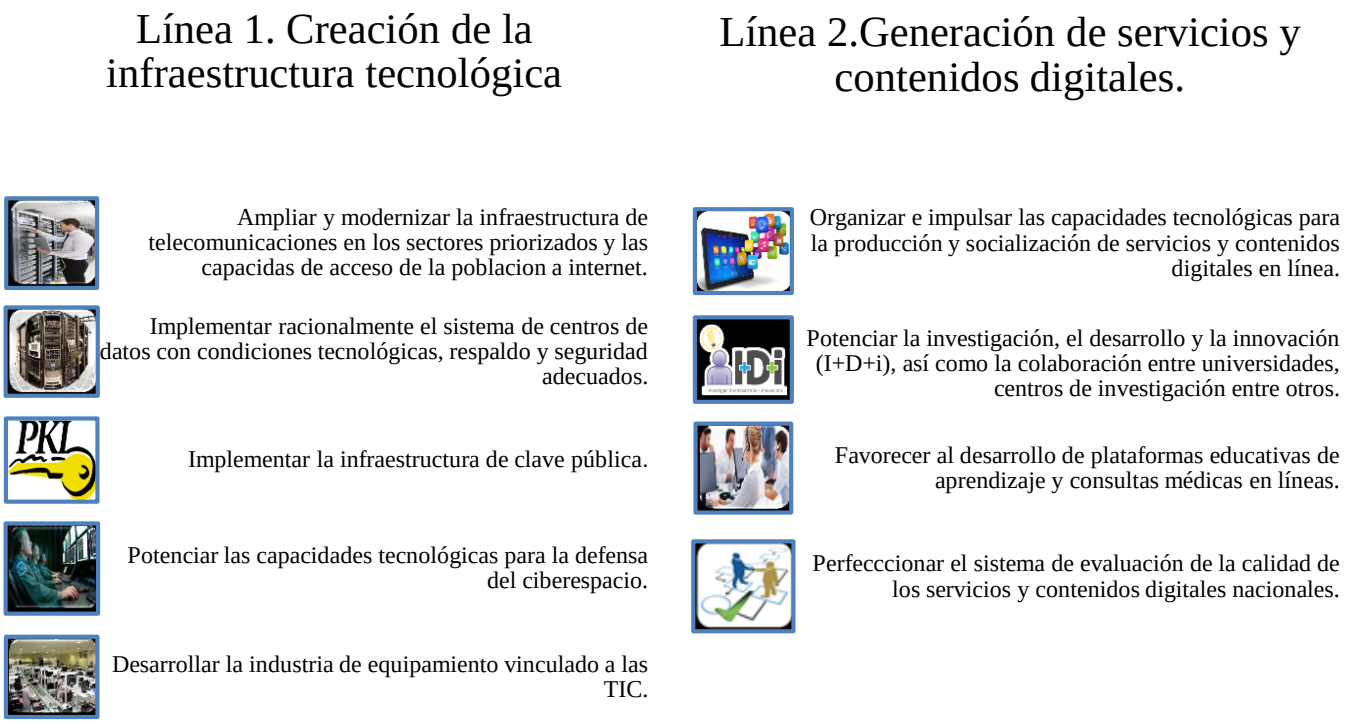

Figura 3.1 Líneas de trabajo definidas por las TIC. Fuente (Elaboración propia).

A inicios del año 2013 Cuba comenzó a desplegar los servicios de Televisión Digital Terrestre (TDT), empleando el estándar DTMB, hasta la fecha ha ocurrido un despliegue de 83 transmisores de ellos (76 de definición estándar y 7 de alta definición) a lo largo del país, dando una cobertura de servicio que se aproxima al 60% del territorio nacional. Para que los usuarios pudieran disfrutar de este servicio se hizo indispensable la obtención de cajas descodificadoras. Este dispositivo es el encargado de recibir y procesar la señal digital, para posteriormente visualizar la información y permitir que el usuario interactúe con esta (Oscar, 2017).

Hasta el 11 de noviembre del 2016 se han comercializado 1.2 millones de dispositivos receptores (cajas descodificadores y televisores híbridos) y de acuerdo al censo de población y vivienda existen una totalidad de 3.5 millones televisores en los hogares cubanos. Del total de cajas decodificadoras comercializadas en el 2016, el 80% son de alta definición y la totalidad de los televisores híbridos LED son de alta definición. A raíz de esto se estima que un tercio de los hogares tiene acceso a los 8 canales virtuales SD, 2 canales virtuales HD y

las nueves emisoras de radio que se transmiten por esta vía; además se incluyen los servicios de *databroadcasting* y la Guía Electrónica de Programas. Las figuras 3.2 y 3.3 muestran el despliegue a lo largo del territorio nacional de los transmisores SD y HD.

Figura 3.2 Cobertura actual del servicio de televisión digital en SD inicios 2017. Fuente (Oscar, 2017).

Figura 3.3 Cobertura actual del servicio de televisión en HD inicios 2017.Fuente (Oscar, 2017).

El Centro de Estudios de Población y Desarrollo (Cepde)**,** prevé que en el 2015 la cantidad de hogares crecerá en casi 302000 en los próximos 15 años, es decir aproximadamente de 3,9 millones de hogares se pasará a 4,2 millones, lo cual significaría un aumento de poco más de 20000 por año (Labacena Romero, 2017). A raíz de este estudio y tomando en consideración

que la población actual en Cuba es de 11422961 habitantes, se estima que el promedio de personas por hogares sea de 2,93385 habitantes, es decir un aproximado de 3 personas por hogar.

Actualmente en nuestro país hay alrededor de 600 salas de navegación de ETECSA disponibles en Joven Club de Computación y Electrónica, locales de Etecsa y algunos hoteles. Para el acceso inalámbrico como parte de la estrategia de informatización se encuentran desplegados pot todo el país, poco más de 360 sitios públicos con la tecnología 802.11 en parques, hoteles y determinadas zonas públicas. La figura 3.4 ilustra por provincias la cantidad de sitios inalámbricos. Por otra parte el proyecto "Acceso Internet en los hogares" se plantea para el 2016 lograr la prueba piloto del Casco Histórico mediante tecnología de acceso por fibra óptica FTTx y la utilización de la tecnología ADSL, para migrar los accesos conmutados existentes. Se constata que el despligue y uso de tecnologías satelitales y basadas en cables en el territorio nacional está realmente muy circunscrito para los destinos turísticos.

Figura 3.4 Puntos Wifi en Cuba. Fuente (MIC, 2017).

En la figura 3.5 se evidencia como ha ido en aumento la telefonía celular en Cuba desde el 2003 hasta el 10 de mayo del 2017. Nótese que del 2014 hasta 2015 fue donde hubo el incremento más significativo de más de 920240 la causa fundamental de este aumento se

debe a las promociones de venta de las líneas. Hasta el 10 de mayo del 2017 ETECSA ha vendido un aproximado de 4220000 líneas celulares en todo el país lo que da como promedio de acuerdo a las estadísticas que al menos exista un teléfono celular por hogar. Esta situación incide directamente en las propuestas de arquitectura que se propone, ya que es de vital importancia la presencia del teléfono celular, pues mediante el mismo se completa el proceso de interactividad requerido para el CAS.

Figura 3.5 Evolución de las líneas móviles en Cuba hasta el 10 de mayo del 2017. Fuente (Figueredo Reinaldo and Domínguez, 2017)

3.2 Modelo del sistema CA integrado a la red GSM.

La red GSM es una red popular y segura que ha sido reconocida como un canal potencial de retorno en los sistemas de radiodifusión. Cada abonado GSM tiene un teléfono móvil que funciona con una tarjeta SIM (del inglés, Subscriber Identity Module). La tarjeta SIM que está vinculada al suscriptor proporciona una plataforma segura, programable y de acceso remoto. Si el operador móvil concede el permiso, puede utilizarse para almacenar e implementar mecanismos de acceso condicional. Por lo tanto, puede considerarse como una alternativa a la tecnología de tarjetas inteligentes.

Adicionalmente, la incorporación de tecnologías móviles puede también expandir las características de movilidad en los sistemas de radiodifusión, significa que el suscriptor ya no necesita estar en casa en las cercanías del STB preseleccionado para disfrutar de sus derechos. Cada teléfono móvil puede ser identificado por su IMEI (del inglés, International

Mobile System Equipment Identity) y su ubicación puede ser reconocida por la LAI (del inglés, Location Area Identity) almacenada en la tarjeta SIM. Su decodificador se puede identificar por su originalidad utilizando un número de identidad único asignado por su fabricante. Vale la pena mencionar que el número de identificación del decodificador y las direcciones únicas (o de grupo) de la tarjeta inteligente ya son utilizadas por los proveedores de servicios para la autenticación y el control de acceso.

La solución que se propone necesita un decodificador con conectividad inalámbrica (es decir, GSM/GPRS o Wi-Fi) y una clase de API (del inglés, Application Programming Interface) para manejar funciones de seguridad, así como suscripción. Las APIs requeridas pueden ser descargadas o actualizadas por el Proveedor Servicio (SP, del inglés, Service Provider) a través de cualquier enlace de comunicación disponible (es decir, medio de radiodifusión). Las APIs instaladas en el decodificador proporcionan un asistente para la presentación de solicitudes en la selección de un determinado servicio favorito y el teléfono móvil de la lista, por ejemplo, dispositivos Bluetooth cercanos descubiertos por el decodificador. El decodificador firma la solicitud con su número de identificación y la envía a través de un enlace inalámbrico (es decir, Bluetooth o Wi-Fi) al dispositivo seleccionado (es decir, teléfono móvil). La solicitud se puede volver a firmar digitalmente en la tarjeta SIM utilizando la firma (es decir, usando su número IMSI o una clave privada proporcionada por SP) y luego se envían al CASS utilizando protocolos de transporte tales como el Servicio de Mensajes Cortos (SMS, del inglés Short Message Service) o Protocolo de Aplicaciones Inalámbricas (WAP, del inglés Wireless Application Protocol). Una vez que el mensaje se recibe en la cabecera, se valida el remitente, el decodificador y la solicitud de suscripción. Si el proceso de validación tiene éxito, las credenciales necesarias se transferirán al decodificador a través de la red de radiodifusión o de la red GSM utilizando el teléfono móvil como un dispositivo intermediario entre SP y STB.

El escenario anteriormente descrito se puede tipificar mediante la siguiente figura; en la misma de muestra los entes involucrados en una “convencional” arquitectura del Sistema de Acceso Condicional Integrado Móvil (MICAS, de inglés Mobile Integrated Conditional Access System) en los sistemas de TV de-pago.

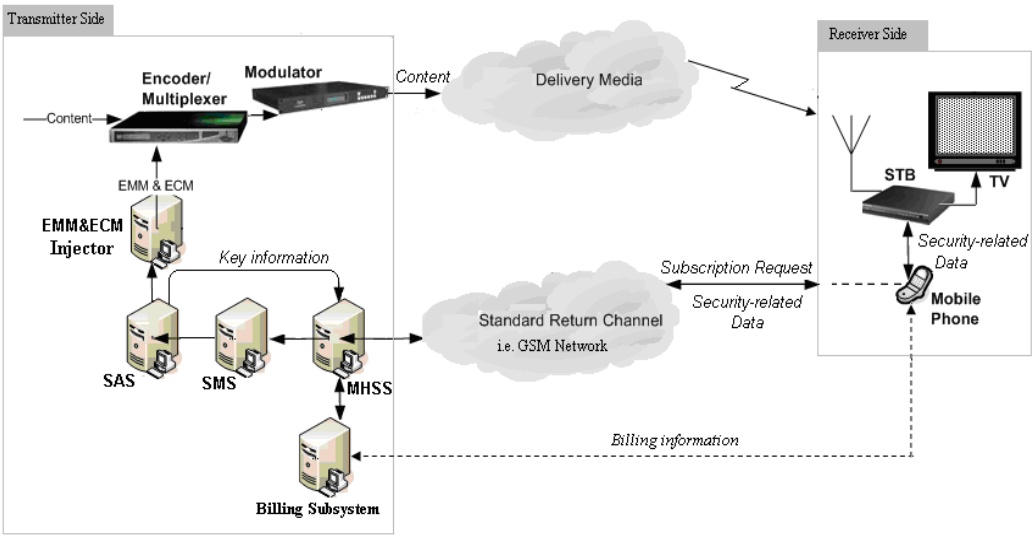

Figura 3.6 Modelo de referencia del sistema CA integrado a la red GSM. Fuente (Shirazi et al., 2010).

3.2.1 Diseño del sistema de acceso condicional integrado móvil.

El MICAS introduce una nueva aplicación móvil en los sistemas de acceso condicional. Es compatible con varias arquitecturas de seguridad y modelos de flujo de datos relacionados con la distribución de los derechos y acceso a información clave para los espectadores. Además, incorpora características de movilidad al sistema tradicional de televisión de pago, como los servicios " *Follow me*". Tales características de movilidad requieren subsistemas de implementación como el Subsistema de Manejo de Mensajes (MHSS, del inglés, Message Handling Subsystem) que operan en el transmisor desplegando algunas API en el receptor (es decir, decodificadores o teléfono móvil). El MHSS se ocupará de las solicitudes de los abonados y establece un subsistema de control de acceso seguro monitoreando de forma proactiva el comportamiento de los usuarios finales y actualizando los mecanismos de seguridad. Las API utilizadas en el extremo receptor proporcionan diversas funcionalidades con interfaces de usuario adecuadas que permiten a los espectadores navegar a través de servicios disponibles, pago por visión y "*Follow me*".

3.2.2 Arquitectura del sistema.

En la vista interna del MICAS, el proveedor de servicios interactúa con el espectador utilizando el teléfono móvil del espectador a través de la red GSM/GPRS. En el extremo receptor, el espectador (abonado) también establece una conexión entre su teléfono móvil y decodificador, por ejemplo, a través de un canal vía (Wi-Fi o Bluetooth). Durante el curso de

interacción, el espectador puede realizar un pedido para un servicio o cambiar sus preferencias para personalizar los servicios. En la cabecera, MHSS se ocupa de todas las interacciones y procesos de instalación CASS en el campo. Codifica / descodifica mensajes salientes / entrantes y verifica la identidad del visor al recibir la solicitud de suscripción a través de una base de datos local o central. También actualiza las cuentas del cliente por ejemplo con respecto a la información de personalización (Shirazi et al., 2010).

El MHSS envía las solicitudes de suscripción verificadas con éxito al Subsistema de Gestión de Suscriptor (SMSS, del inglés Subscriber Management Subsystem). Las consultas SMSS generan o actualizan la cuenta del espectador basada en la solicitud de suscripción, instruye al Sistema de Autorización del Suscriptor (SAS, del inglés, Subscriber Authorization Subsytem) a decidir sobre los mecanismos de CA y le ordena al subsistema de facturación que prosiga las transacciones financieras. Si se autorizan los pagos, el SAS comienza a responder a la instrucción de CA. El SAS puede reenviar la información de la clave&derechos como el Objeto de Seguridad al MHSS o como el mensaje CA al Multiplexor en dependencia de la arquitectura de seguridad implementada y descrita más adelante.

Las funcionalidades SMSS y SAS definidas/implementadas en los esquemas MICAS con sus contrapartes han de ser definidas en el sistema DTV, excepto para la interfaz con SMSS. La figura 3.7 describe la relación interna y el flujo de datos entre los subsistemas de la MICAS.

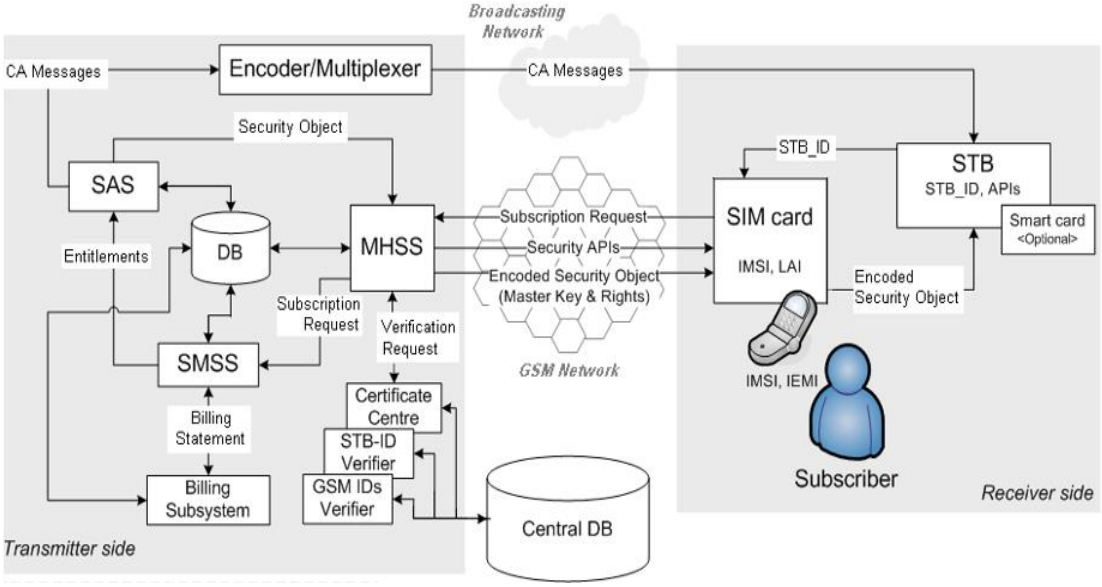

Figura 3.7 Arquitectura general de MICAS. Fuente (Shirazi et al., 2008).

3.3 APIs utilizadas en MICAS.

Las APIs que deben desarrollarse e instalarse para facilitar el sistema de control de acceso y las comunicaciones a través del MICAS son las siguientes:

- El controlador de solicitud de suscripción es un *MIDLet* (programa desarrollado en Java) que se ejecuta en el teléfono móvil que proporciona al suscriptor una interfaz para seleccionar el proveedor de servicios de una lista predefinida de proveedores de servicios y genera y envía una solicitud de suscripción al proveedor de servicios. El protocolo de transmisión entre el teléfono móvil y el proveedor de servicios, por ejemplo en la tecnología GSM, puede ser el SMS o el WAP.

- La autenticación mutua es la comunicación con MHSS para realizar un proceso de autenticación mutua entre el abonado y el proveedor de servicios. Puede ser implementado como una subfunción del controlador de solicitud de abonado descrito anteriormente.
- El controlador de acceso condicional es un *applet* (aplicación pequeña) instalada en la SIM con acceso a dominios privilegiados. Se descarga a la tarjeta SIM a través del MHSS y realiza algoritmos y comunicaciones sensibles a la seguridad. Sus funcionalidades pueden variar en cada propuesta.

- El dominio de comunicación es una aplicación instalada en el STB. Interconecta el STB con el exterior a través del canal de interacción (es decir, GSM/GPRS). Contiene una serie de APIs instaladas por el fabricante de STB para acceder a los dominios privilegiados y realizar algoritmos relacionados con la seguridad. Se comunica con el controlador de acceso condicional para preparar un canal de comunicación seguro en el proceso de vinculación. Proporciona el controlador de acceso condicional con la identidad del STB que debe ser obtenible únicamente para el usuario privilegiado del dominio de comunicación mediante derechos especiales.

El controlador de acceso condicional genera un mensaje que contiene la Identidad Internacional del Abonado a un Móvil (IMSI, del inglés International Mobile **S**ubscriber Identity), la Identidad Internacional de Equipo Móvil (IMEI, del inglés International Mobile Station Equipment Identity), el número de identidad de STB (STB ID) proporcionado por el dominio de comunicación. A continuación, envía el mensaje al MHSS para verificar si el suscriptor y el STB son válidos conformes a los estándares.

El MHSS identifica al suscriptor y su equipo usando el IMSI y el IMEI y verifica si son válidos y únicos en el sistema. Por razones de seguridad, el controlador de acceso condicional puede verificar el número y el origen al contactar al operador de la red móvil para determinar los números IMSI e IMEI. El STB_ID indica el tipo de STB, que se utiliza para autenticar los STB. Los STB pueden registrarse con el proveedor de servicios o con una agencia especial para asegurar que cumplen con las normas de protección de servicios y contenido e implementar especificaciones estándar. El MHSS transfiere la clave maestra y el derecho del suscriptor (objetos de seguridad) al controlador de acceso condicional en la tarjeta SIM.

El "paso de inicialización" es un procedimiento realizado en todas las arquitecturas de seguridad presentadas. Se refiere a la secuencia de emparejamiento incurrida entre el teléfono móvil y el decodificador, la presentación de la solicitud de suscripción a través del teléfono móvil del abonado, la autorización de la solicitud, la identificación del abonado, la validación del decodificador y finalmente el envío e instalación de *applets* de seguridad en un dominio (s) seguro (s) en la tarjeta SIM del suscriptor. Los diagramas de flujo de datos posibles y el modelo de procesamiento que contiene el decodificador, el teléfono móvil (tarjeta SIM) y el proveedor de servicios se presentan en las siguientes secciones de arquitecturas de seguridad.

3.3.1 Decodificación de EMM y ECM en STB utilizando objetos de seguridad entregados a través del teléfono móvil.

Este modelo es una implementación de un simple sistema de acceso condicional jerárquico de 3 niveles en el que se utiliza la clave maestra (o de usuario) (definida como MK) para descifrar el EMM. El EMM descifrado proporcionará la clave de servicio (definida como SK) que se utiliza para descodificar el mensaje de ECM y extraer la palabra de control (definida como CW) para descodificar el contenido.

En el modelo conceptual, el generador/gestor de CA entrega los objetos de seguridad MICAS (MKs y derechos del espectador) al agente CA móvil a través de la red GSM. Los mensajes CA (es decir, EMM y ECM) también se transmiten inalámbricamente al decodificador/STB. El agente de CA en el teléfono móvil transfiere completamente las credenciales al agente de CA en el STB a través del canal seguro establecido por el agente de comunicación. En el STB, el agente de CA invoca los algoritmos de seguridad subyacentes para descifrar el EMM y extraer la SK para descifrar la ECM. Los derechos del suscriptor se contrastan con los

derechos asociados al contenido (tal como se insertan en el ECM). Si la condición se satisface, las CWs son liberadas para descodificar el contenido. En la figura 3.8 **se** muestra la interacción entre el extremo de la cabeza de línea y el extremo del receptor en esta arquitectura de seguridad donde el teléfono móvil juega un papel intermediario entre el proveedor de servicios y el decodificador.

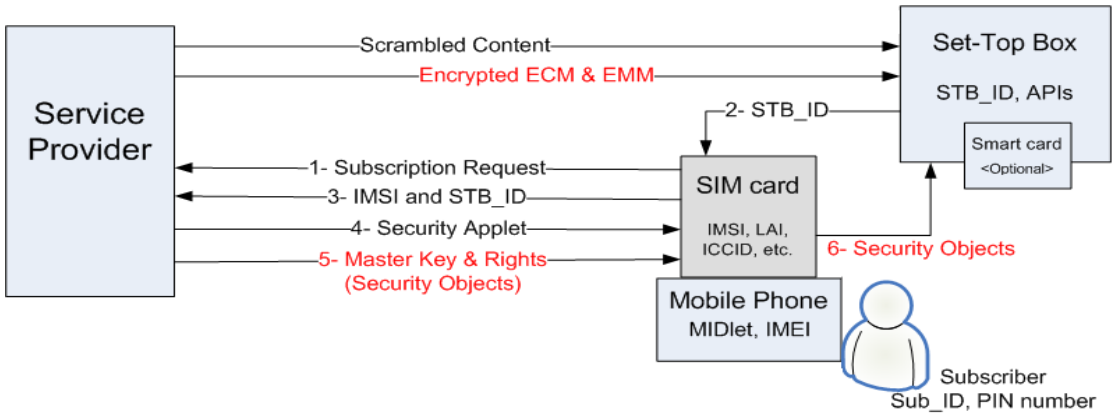

Figura 3.8 El flujo de datos de una arquitectura de seguridad jerárquica de 3 niveles donde todas las funciones de seguridad tienen lugar en STB. Fuente (Shirazi et al., 2008).

3.3.2 Decodificación de EMM en la tarjeta SIM y ECM en STB utilizando Objetos de Seguridad entregados a la tarjeta SIM.

Este esquema es otro modelo de la arquitectura anterior donde se adopta una seguridad de 3 capas y los mensajes de CA (EMM y ECM) se entregan a través del medio de difusión.

Después de haber establecido el paso de inicialización, el agente CA de la caja decodificadora envía el EMM al agente CA móvil. El agente de CA móvil descifra el EMM y extrae la SK utilizando la MK suministrada por el objeto de seguridad (MK y los derechos del suscriptor) a través del canal GSM. El agente CA móvil envía entonces la SK extraída, así como los derechos del suscriptor al agente CA de la caja descodificadora que se utilizará para el proceso de descifrado del contenido. En la figura 3.9 se muestra el diagrama de flujo de datos cuando el EMM se emite por el decodificador y se envía al teléfono móvil del abonado para su procesamiento.

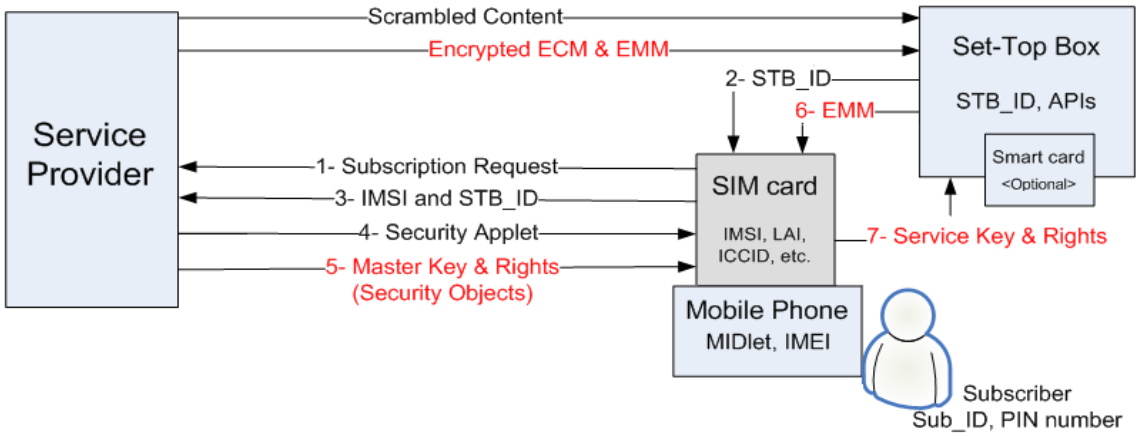

Figura 3.9 El flujo de datos de una arquitectura de seguridad jerárquica de 3 niveles en la que EMM y ECM decodificación es equilibrada entre STB y teléfono móvil. Fuente (Shirazi et al., 2008).

3.3.3 Descodificación de EMM & ECM en la tarjeta SIM utilizando objetos de seguridad entregados a la tarjeta SIM.

De forma similar, en este modelo se adopta un sistema de seguridad jerárquico clave de 3 niveles. Los mensajes de CA se transmiten a la población receptora. El procesamiento de los EMM y ECM se realiza principalmente/únicamente en el teléfono móvil del espectador.

En esta arquitectura, después del paso de inicialización, el agente CA de la caja decodificadora envía el mensaje CA (es decir, EMM y ECM) al agente CA móvil a través del enlace Bluetooth/Wifi establecido por los agentes de comunicación. El agente de CA móvil descifra el EMM y extrae la SK utilizando el conocimiento de los objetos de seguridad (MK y derechos del Suscriptor) entregados por el proveedor de servicios a través de la red GSM. La SK extraída se utiliza entonces para decodificar el ECM y extraer las CWs. El agente de CA móvil transfiere de nuevo las CW extraídas al agente CA del STB para descodificar el contenido. En la figura 3.10 se muestra el diagrama de flujo de datos donde el EMM y el ECM son entregados al teléfono móvil a través del decodificador. Los procesos de descodificación se realizan principalmente en el teléfono móvil del abonado (tarjeta SIM) y el descifrado se realiza en el decodificador.

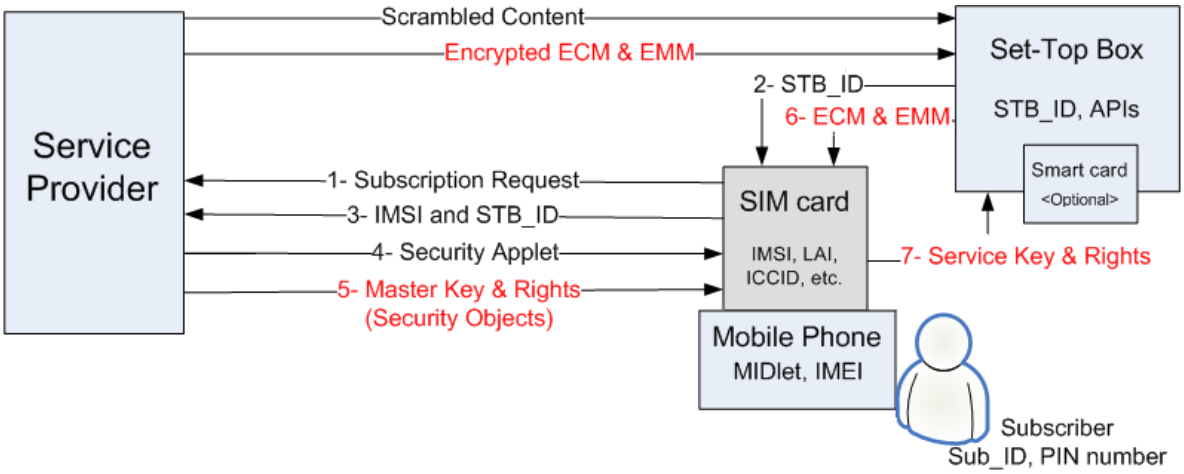

Figura 3.10. Jerarquía de 3 niveles en la que la decodificación EMM y ECM tiene lugar en el teléfono móvil. Fuente (Shirazi et al., 2008).

Nótese que en las propuestas anteriores, los mensajes de la CA (es decir, ECM y EMM) se transmitían a los receptores. Por otro lado, la información clave se entregaba a través del canal de retorno (red GSM) para abrir el EMM cifrado. El proceso de decodificación puede tener lugar en el decodificador o en el teléfono móvil del espectador.

3.3.4 Decodificación de EMM & ECM en STB usando EMM entregado vía teléfono móvil.

En este esquema después de haber establecido el paso de inicialización, el MHSS transfiere el mensaje EMM al controlador de acceso condicional. El EMM contiene la información de la clave de servicio y los derechos del suscriptor, pero no puede estar limitado. El controlador de acceso condicional transfiere el EMM al agente de comunicación. El agente de comunicación proporciona un mensaje EMM a los algoritmos relacionados con la seguridad para descifrar el ECM (recibido del canal de difusión) y extraer las CWs para descodificar el contenido solo si el suscriptor tiene derecho al acceso del contenido.

En la figura 3.11 se muestra el diagrama de flujo de datos cuando EMM es entregado al teléfono móvil del abonado a través de la red GSM. El teléfono móvil envía entonces el mensaje al STB para descodificar el ECM y descodificar el contenido.

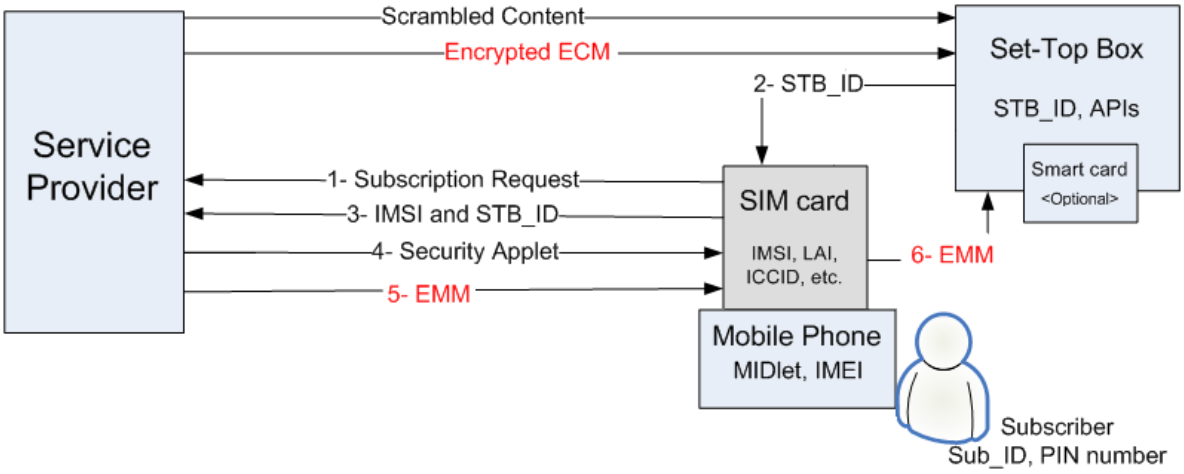

Figura 3.11 El flujo de datos de una arquitectura de seguridad jerárquica de 3 niveles en la que EMM se transfiere a través de la red móvil y todas las funciones de seguridad tienen lugar en el STB. Fuente (Shirazi et al., 2008).

3.3.5 Decodificación de EMM en la tarjeta SIM y ECM en STB utilizando EMM entregado a la tarjeta SIM.

En este modelo, la red de radiodifusión se utiliza para transferir una parte del mensaje CA (es decir, ECM) y la red GSM se utiliza para transferir otra parte del mensaje CA (es decir, EMM) al extremo receptor. El procesamiento de EMM tiene lugar en el teléfono móvil del visor y el procesamiento de ECM tiene lugar en el decodificador.

Después de la etapa de inicialización, el CA Manager en el *head-end* transfiere el EMM al agente de CA móvil. El mensaje EMM se decodifica utilizando la MK, que puede ser obtenida por el emisor de la tarjeta SIM o entregada por el proveedor de servicios a la tarjeta SIM antes de la entrega del EMM. A continuación, se extraen los derechos de la SK de los suscriptores para transferirlos del agente de CA al STB. El agente CA de la caja descodificadora descifra entonces el mensaje ECM que se recibe del medio de difusión. Si el derecho del abonado coincide con el derecho del programa, se liberan las CWs para descifrar el contenido. En la figura 3.12 se muestra el diagrama de flujo de datos cuando el EMM se procesa en el teléfono móvil del abonado (tarjeta SIM) y la SK y los derechos se envían al decodificador para descodificar ECM y descifrar el contenido.

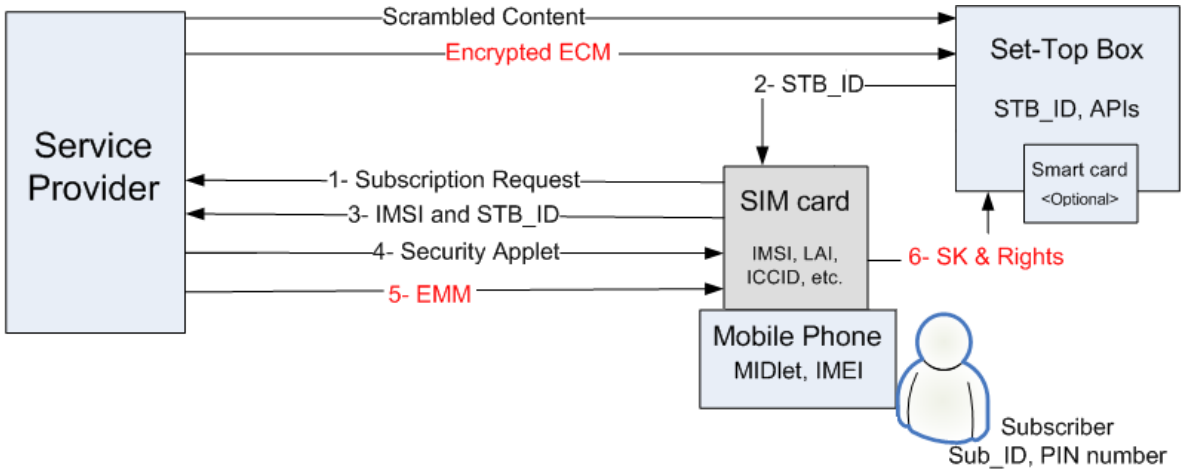

Figura 3.12. En donde el EMM se transfiere a través de redes móviles y la decodificación EMM & ECM se equilibra entre STB y teléfono móvil. Fuente (Shirazi et al., 2008).

3.3.6 Descodificación de EMM y ECM en la tarjeta SIM usando EMM entregado a la tarjeta SIM.

Similar al modelo anterior, el ECM se transmite como parte del servicio de radiodifusión y el EMM es enviado de modo *unicast* al teléfono móvil del espectador a través de la red GSM. Pero, en este modelo, el STB es un intermediario para entregar el ECM al teléfono móvil donde se procesan los mensajes CA y se extraen las CWs.

Después de la inicialización, el generador/gestor de CA transfiere el mensaje EMM al agente de CA del móvil. El agente CA del STB también transfiere el ECM al agente de CA móvil para descifrar el ECM utilizando el conocimiento de la SK transportada con el EMM y extraer la CW si los derechos del abonado coinciden con el derecho del programa insertado en el mensaje ECM. El agente CA móvil pasa las CWs al agente CA de la caja descodificadora para descodificar el contenido. En la figura 3.13 se muestra el diagrama de flujo de datos donde se transfieren tantos los EMM y ECM al teléfono móvil del espectador, respectivamente desde las redes GSM y de radiodifusión, utilizando el decodificador como dispositivo intermedio.

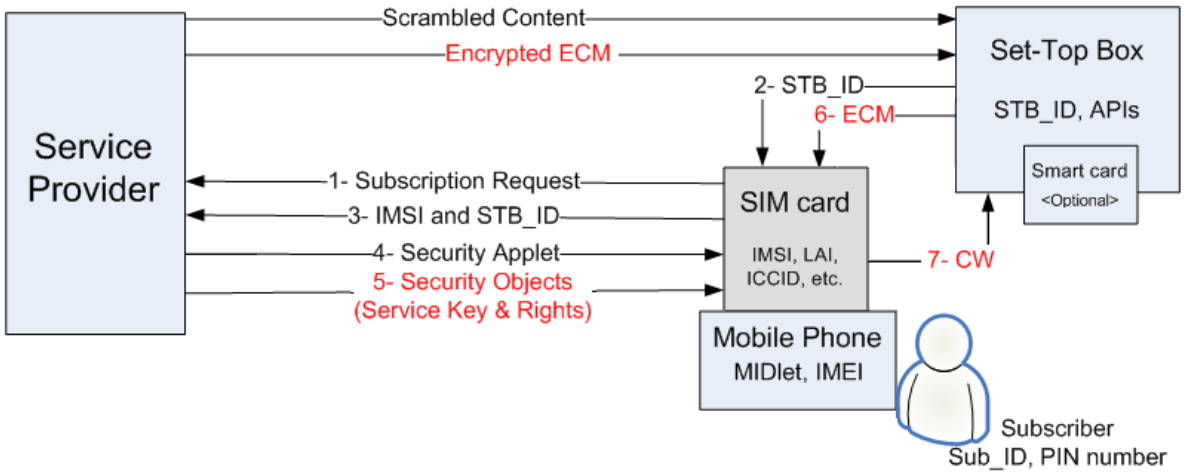

Figura 3.13. Flujo de datos de una arquitectura de seguridad jerárquica de 3 niveles en la que el EMM se transfiere a través de la red móvil y la decodificación EMM & ECM tiene lugar en el teléfono móvil. Fuente (Shirazi et al., 2008).

3.3.7 Descodificación de ECM en STB utilizando los objetos de seguridad entregados vía teléfono móvil.

Este modelo representa una arquitectura en la que se utiliza un sistema jerárquico de seguridad de dos niveles. Como la información de la clave es de unidifusión con el extremo receptor, la MK utilizada para descifrar el mensaje EMM puede ser eliminada de la jerarquía de claves. Como resultado, la única clave para transferir será la SK que se utiliza para descifrar el mensaje ECM. Dependiendo del modelo de procesamiento, la arquitectura de seguridad puede variar de la siguiente manera.

Después de la etapa de inicialización, el administrador CA transfiere la SK y los objetos de seguridad al agente de CA móvil. El agente de CA móvil entonces transfiere los objetos de seguridad al agente de CA del decodificador. La SK y los derechos del suscriptor pueden ser utilizados por el agente de CA del decodificador o por cualquier algoritmo de seguridad incorporado en el decodificador para descifrar el mensaje del ECM. Las CWs son liberadas para descodificar el contenido solo si los derechos del suscriptor coinciden con los derechos de acceso del contenido.

La figura 3.14 presenta el diagrama de flujo de datos en el que la SK y los derechos del espectador desde el lado GSM y el mensaje ECM desde el lado del medio de radiodifusión

son entregados al decodificador. El móvil desempeña un papel intermediario y todo el proceso de acceso condicional está alojado en el decodificador.

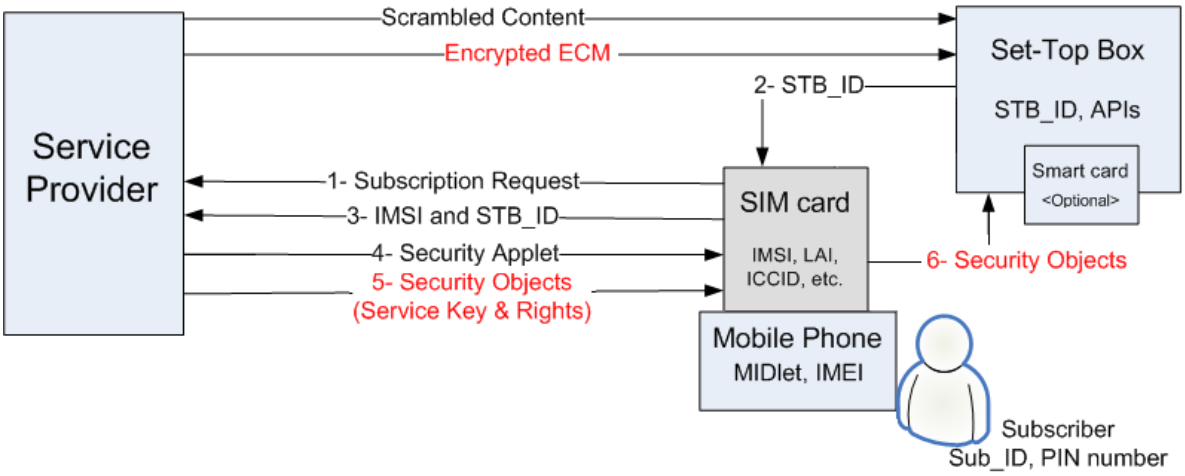

Figura 3.14. El flujo de datos de una arquitectura jerárquica de seguridad de 2 niveles en la que todas las funciones de seguridad tienen lugar en el STB. Fuente (Shirazi et al., 2008).

3.3.8 Decodificación de ECM en la tarjeta SIM utilizando los Objetos de Seguridad entregados a la tarjeta SIM.

Este modelo es otro tipo de sistema de seguridad jerárquico clave de 2 niveles. En este modelo, todo el procesamiento de CA se lleva a cabo en el teléfono móvil y las CWs extraídas son entregadas al decodificador para el proceso de descifrado.

Después de haber establecido el paso de inicialización, el MHSS transfiere la clave de servicio y los derechos del suscriptor (objetos de seguridad) al controlador de acceso condicional. El agente de comunicación transfiere el ECM al agente de CA para descifrar el ECM usando la clave de servicio y extraer las CWs si el derecho del suscriptor coincide con los criterios establecidos para el contenido. El controlador de acceso condicional envía las CW al agente de comunicación que se va a utilizar para descodificar el contenido.

La figura 3.15 muestra el diagrama de flujo de datos cuando los objetos de seguridad (clave de servicio y derechos) y mensajes ECM se envían al teléfono móvil del abonado respectivamente desde la red GSM y el STB. El proceso de descodificación tiene lugar en el teléfono móvil del abonado y las CWs extraídas se entregan al STB para el proceso de descodificación.

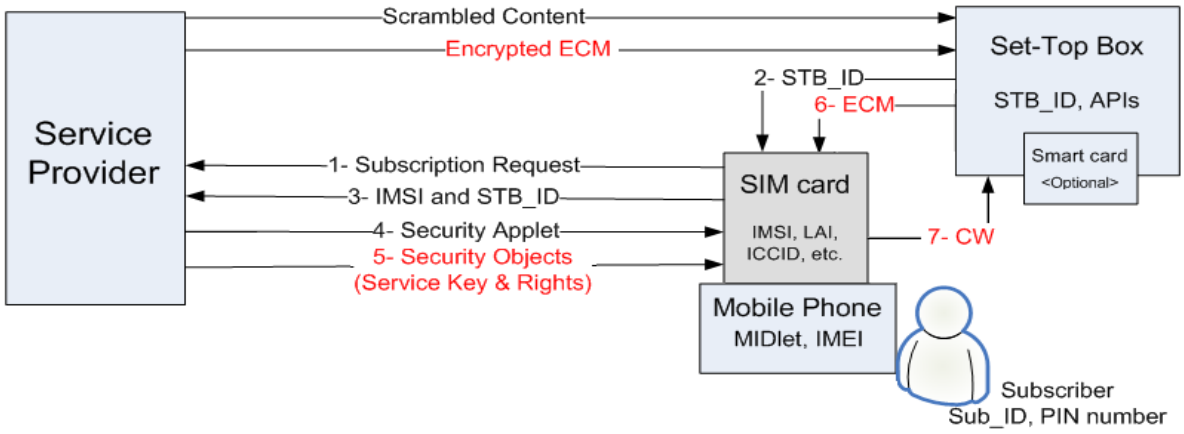

Figura 3.15. El flujo de datos de una arquitectura jerárquica de seguridad de dos niveles en la que se realiza la descodificación ECM en el teléfono móvil. Fuente (Shirazi et al., 2008).

3.4 Conclusiones del capítulo.

En este capítulo se analizaron varias arquitecturas de alto nivel de seguridad MICAS para posibles consideraciones en aplicaciones de la televisión de pago la cual permitiría establecer la interoperabilidad entre varios sistemas de CA en un futuro.

El sistema propuesto proporciona una plataforma dinámica que ofrece interoperabilidad entre los futuros proveedores de servicios. Además, mejora la seguridad general del sistema mediante la interacción con el receptor de cabecera y la descarga de nuevos mecanismos de seguridad. Es notorio destacar que las funciones de revocar las claves comprometidas y supervisar el comportamiento contractual de los abonados se realizan de forma automática y rentable a través del canal de interacción GSM (o sus homólogos evolutivos como UMTS, 3G, etc.).

El MHSS aparece como una nueva entidad en el sistema de radiodifusión para operar desde el lado del transmisor y manejar la comunicación entre el proveedor de servicios y el suscriptor a través de la red. Interactúa con el suscriptor a través del teléfono móvil y realiza la solicitud de suscripción del suscriptor al Subsistema de Gestión de Suscriptores (SMS) y al Subsistemas Autenticación de Suscriptores (SAS) para autorizar los derechos correspondientes.

Los sistemas de acceso condicional de forma global mejoran el concepto de atención personalizada para los televidentes en las tradicionales redes de radiodifusión y proporciona al suscriptor acceso activo a sus derechos/servicios reservados.

La elección de cualquiera de las arquitecturas descritas estará condicionada por:

- Costo de implementación de los decodificadores.
- Complejidad de la propuesta.
- Mecanismos de seguridad de la propuesta.
- Capacidad de procesamiento en el dispositivo.
- Interfaz de comunicación entre el dispositivo móvil y el STB.
- Latencia de los mensajes entregados por la red GSM

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

En este trabajo se realizó un estudio del sistema CAS el cual culmina con la propuesta de una arquitectura basada en la infraestructura actual del país. Teniendo en cuenta todo el desarrollo de la tesis se puede arribar a las siguientes conclusiones:

1. A lo largo de la evolución de la encriptación del contenido se han desarrollado algoritmos y técnicas de cifrado que se han enfocado en ser cada vez más seguros, resultando el cifrado híbrido la técnica de mayor seguridad y rapidez en cuanto a (codificación / descodificación) del contenido.
2. Los mecanismos de acceso condicional rompen la relación rígida entre el televidente y STB debido a la propia naturaleza y prestaciones de los CAS; situación muy necesaria en la actualidad por las demandas que ya vienen haciendo los usuarios.
3. Después de haber analizado las arquitecturas de los medios de difusión en ambientes CAS se opta por la TDT ya que resulta la más conveniente, debido a que se cuenta con la infraestructura ya desarrollada lo cual resultaría un menor costo económico al país.
4. Vislumbra la red GSM como ideal para ser el medio por donde se realice la interacción proveedor / cliente (canal de retorno) por las ventajas que este brinda en cuanto a fácil acceso por parte de cliente y economía.
5. Las arquitecturas que se analizan y proponen son basadas todas en MICAS, la cual utiliza la plataforma móvil para completar el sistema de TV-de pago. La utilización

de la tecnología móvil en el sistema de televisión de pago puede mejorar la interactividad, la seguridad y, potencialmente, reducir los costos operativos.

Recomendaciones

Con los resultados obtenidos el tema abordado no queda agotado, por lo cual se sugieren como posibles líneas de trabajo futuro, las siguientes:

1. Profundizar más sobre las caracteristicas que presenta la arquitectura MICAS haciendo énfasis en su seguridad.
2. Que la investigación sirva como pilar para proximas investigaciones acerca del tema.

REFERENCIAS BIBLIOGRÁFICAS

Aggelou, G.N., Tafazolli, R., 2001. On the relaying capability of next-generation GSM cellular networks. IEEE Pers. Commun. 8, 40–47.

Alkan, E., Shafer, S.K., 2013. Home network frequency conditioning device and method. Google Patents.

Amieva, E., 2015. Criptografía: simétrica, asimétrica e híbrida. Eneko Amieva.

Andreja, S.B., 2011. Tehnološke karakteristike digitalnog standarda DVB-H za difuzni video-prenos kod prenosivih ure\d jaja. Vojnoteh. Glas. 59.

Asghar, M.N., Fleury, M., Makki, S., 2016. Interoperable conditional access with video selective encryption for portable devices. Multimed. Tools Appl. 1–14. doi:10.1007/s11042-016-3725-3

Beaumont, F., 2015. Global pay-TV market to exceed one billion by 2017 [WWW Document]. TVBEurope. URL http://www.tvbeurope.com/global-pay-tv-market-exceed-one-billion-2017/ (accessed 5.8.17).

Bridge Technologies, 2010. Monitoring Conditional Access Systems.

Cáceres, L.A., 2011. Redes de Computadoras. Obtenido de http://electronicahz. webcindario. com/pdf/manual_redes_v2.

Castillejo, Á.G., 2014. Régimen jurídico y mercado de la televisión de pago en España. Editorial UOC.

CI, S.G.C.I., 2016. Digital Video Broadcasting (DVB); Second Generation Common Interface (CI); Part 1: Implementation Using the Universal Serial Bus (USB).

Coutrot, F., Michon, V., 1989. A single conditional access system for satellite-cable and terrestrial TV. IEEE Trans. Consum. Electron. 35, 464–468.

Dolores, M., 2016. Tipos de criptografía: criptografía simétrica, criptografía asimétrica y criptografía hibrida. Tipos Criptografía.

ETSI, 2014. ETSI TS 103 205 V1.1.1 (2014-03). Digit. Video Broadcast. DVB Ext. CI Plus™ Specif.

ETSI, 2003. 301 790 V1. 3.1 (2003-03). Digit. Video Broadcast. DVB.

ETSI, 2002a. TS 101 197 - V1.2.1 - Digital Video Broadcasting (DVB); DVB SimulCrypt; Head-end architecture and synchronization.

ETSI, 2002b. 301 195 V1.1.1 (1999-02). Digit. Video Broadcast. DVB Interact. Channel Glob. Syst. Mob. Commun. GSM.

ETSI, 2001. 200 800 v. 1.3. 1. Digital Video Broadcasting: Interaction Channel for Cable TV Distribution Systems (CATV). ETSI.

ETSI, 1995. 300 586 ,v2, 1995-07. GSM 0706 Eur. Digit. Cell. Telecommun. Syst. Phase 2 Use V Ser. Data Termin. Equip. - Data Circuit Termin. Equip. DTE - DCE Interface Mob. Stn. MS Mob. Termin. MT Config.

Européenne, N., 1996. Common Interface Specification for Conditional Access and other Digital Video Broadcasting Decoder Applications.

Figueredo Reinaldo, O., Domínguez, E., 2017. ETECSA tiene la palabra (+ Infografías y Video) [WWW Document]. Cubadebate. URL http://www.cubadebate.cu/especiales/2017/05/11/etecsa-tiene-la-palabra-infografia-y-video/ (accessed 5.31.17).

Fjortoft, J., Colban, E.A., 2003. Method for improving service level selection in a communication network system. Google Patents.

Gutiérrez, P., 2013. Tipos de criptografía: simétrica, asimétrica e hibrida [WWW Document]. Genbeta Dev. URL https://www.genbetadev.com/seguridad-informatica/tipos-de-criptografia-simetrica-asimetrica-e-hibrida (accessed 6.15.17).

Hernández, J., 2011. Todo en Televisión FTA: Televisión Digital por Satélite. Sistema de acceso condicional. Como funcional, diagnostico y errores. Todo En Telev. FTA.

Ibarra Tobar, O.D., 2015. IPTV TV sobre IP [WWW Document]. URL https://www.slideshare.net/oscardanielibarra/iptv-tv-sobre-ip (accessed 6.2.17).

ISO, 2017. ISO 7816-4 (ISO7816 part 4 section 5) Smart card standard, Basic Organizations [WWW Document]. URL http://www.cardwerk.com/smartcards/smartcard_standard_ISO7816-4_5_basic_organizations.aspx (accessed 6.15.17).

ITU-R, 1992. Rec. UIT-R BT.810. Sist. Radiodifusión Acceso Condicional.

ITU-T, 2016. Recommendation ITU-R BT.1852-1. Cond.-Access Syst. Digit. Broadcast.

ITU-T, 1994. Rec. H. 222.0, ISO/IEC 13818 1, 1994. Inf. Technol. Coding Mov. Pict. Assoc. Audio Part 1.

Labacena Romero, Y., 2017. Hombre o mujer: ¿quién mandará en las casas cubanas en 2030? - Cuba - Juventud Rebelde - Diario de la juventud cubana [WWW Document]. URL http://www.juventudrebelde.cu/cuba/2017-04-14/hombre-o-mujer-quien-mandara-en-las-casas-cubanas-en-2030/ (accessed 5.10.17).

Luis, J., 2012. Servicios de satelite y television digital: Acceso condicional. Serv. Satelite Telev. Digit.

Martínez, J., 2015. En Latinoamérica, la TV paga creció un 17 por ciento en 2014 [WWW Document]. URL http://www.adlatina.com/medios/en-latinoam%C3%A9rica-la-tv-paga-creci%C3%B3-un-17-por-ciento-en-2014 (accessed 5.10.17).

Martínez, J.M., Proyecto, D.V.B., Series, D.V.B., 2010. Distribución y Recepción de Señales de Televisión Digital Visión general de DVB.

MIC, 2017. Proceso de Informatización de la sociedad cubana.

Morales Figueroa, A.A., 2010. Diseño de la red para interactividad en televisión digital terrestre e IPTV en el campus ESPE Sangolquí.

Moreno, B., 2015. La criptografía: CRIPTOGRAFÍA HÍBRIDA. La criptografía.

Muñoz, M., 2011. TELEVISION CATV: Redes de acceso de banda ancha (HFC). Telev. CATV.

Navarro, A., 2012. intro_dgital_TV [WWW Document]. URL https://www.slideshare.net/chetanrao2012/introdgitaltv (accessed 5.16.17).

O'Driscoll, G., 2008. Next Generation IPTV Services and Technologies. John Wiley & Sons.

Oscar, F.R., 2017. La televisión que viene: Novedades de la TV digital (+ Fotos, Video e Infografía) [WWW Document]. Cubadebate. URL http://www.cubadebate.cu/especiales/2017/02/09/la-television-que-viene-novedades-de-la-tv-digital-fotos-video-e-infografia/ (accessed 3.28.17).

Pluas, V., Arturo, E., Arias Vera, A.J., 2015. Análisis Comparativo de las Tecnologías utilizadas para Distribución de Señales DTH.

Puentes Fernández, J.H., Barrera Vargas, C.A., 2013. Parámetros técnicos y normativos para la implementación de Iptv sobre las redes Dvb-c e internet en Ipv6 con QoS.

Rasanen, J., 2001. Method and an arrangement for setting up a data call, and an adapter equipment. Google Patents.

Reyes, P. por I.F., 2016. TV de PAGA: Mercado Latinoamericano al 4T-2015.

Rix, S.P.A., Glasspool, A., Davies, D.W., 2002. Method for providing a secure communication between two devices and application of this method. Google Patents.

Saavedra Abarca, E.V., 2009. Estudio de factibilidad para la implementación de un laboratorio de televisión digital interactiva para la ESPE (B.S. thesis). SANGOLQUÍ/ESPE/2009.

Shirazi, H., Cosmas, J., Cutts, D., 2010. A Cooperative Cellular and Broadcast Conditional Access System for Pay-TV Systems. IEEE Trans. Broadcast. 56, 44–57. doi:10.1109/TBC.2009.2036956

Shirazi, H., Cosmas, J., Cutts, D., Birch, N., Daly, P., 2008. Security architectures in mobile integrated pay-TV conditional access system, in: Telecommunications Network Strategy and Planning Symposium, 2008. Networks 2008. The 13th International. IEEE, pp. 1–6.

The Daily Television, 2015. Penetración de TV digital alcanza a casi el 70% a nivel mundial en 2014 [WWW Document]. Dly. Telev. URL http://www.thedailytelevision.com/articulo/research/penetracion-de-tv-digital-alcanza-casi-el-70-nivel-mundial-en-2014 (accessed 4.13.17).

TNO, 2014. Third-Party Service Providers Options for Selling Cable Services and Cable Access.

山田宰, 2001. ディジタル放送の技術とサービス.

GLOSARIO

API: Interfaz de Programación de Aplicaciones (del inglés, *Application Programming Interface*)

ATM: Modo de Transferencia Asíncrona (ATM, del inglés *Asynchronous Transfer Mode*)

CAM: Módulo de Acceso Condicional (del inglés, *Conditional Access Module*)

CAS: Sistema de Acceso Condicional (del inglés, *Conditional Access Service*)

CP Crypto Period.

CSA: Algoritmo de Aleatorización Común (del inglés, *Common Scrambling Algorithm*)

DCE: Equipo de Comunicación de Datos (DCE, del inglés *Data Communication Equipment*)

DTE: Equipo de Terminal de Datos (DTE, del inglés *Data Terminal Equipment*)

ECM: Mensajes de Control de Autorización (del inglés, *Entitlement Control Messages*)

ECMG: Generador de Mensajes de Control de Autorización (del inglés, *Entitlement Control Message Generator*)

EMM: Mensajes de Gestión de Autorización (del inglés, *Entitlement management Messages*)

EMMG: Generador de Mensajes de Gestión de Autorización (del inglés, *Entitlement Management Message Generator*)

ESI: Planificador de información del evento (del inglés, *Event Information Scheduler*)

GPRS: Servicio de Radio Paquete General (GPRS, del inglés *Radio Service General Package*)

GSM: Sistema global para comunicaciones móviles (del inglés, *Global System for Mobile Communications*)

GSM: Sistema Global para Comunicaciones Móviles (GSM, del inglés *Global System for Mobile*)

IMEI: Identidad Internacional de Equipo Móvil (IMEI, del inglés *International Mobile Station Equipment Identity*)

IMSI: Identidad Internacional del Abonado a un Móvil (IMSI, del inglés *International Mobile **S**ubscriber Identity*)

INA: Adaptador de Interfaz de Red (INA, del inglés *Network Interface Adapter*)

ISO: Organización Internacional de Estandarización (del inglés *International Organization for Standardization*)

ITU: Unión Internacional de Telecomunicaciones (del inglés *International Telecommunication Union*)

LAI: Identificador de Área Local (del inglés, *Location Area Identity*)

NCR: Red de Referencia de Reloj (NCR, del inglés, *Clock Reference Network*)

NIU: Unidades de Interfaz de Red (NIU, del inglés *Network Interface Units*)

PDG: Generador de Datos Privados (del inglés, *Private Data Generator*)

PID: Identificador de Programa Específico (PID, del inglés *Specific Program Identifier*)

RCST: Canales de Retorno por Terminales Satelitales (RCST, del inglés *Return Channels for Satellite Terminals*)

RCTT: Terminales Terrestres del Canal de Retorno (RCTT, del inglés *Return Channel Terrestrial Terminals*)

SCS: Sincronizador SimulCrypt (del inglés, *SymulCrypt Synchronizer*)

SIG: Generador de información de servicio personalizado (del inglés, *Custom Service Information Generator*)

SMS: Sistema de Gestión de Suscriptores (del inglés, *Subscriber Management System*)

STB Set Top Box

TDMA: Acceso Múltiple por División de Tiempo (TDMA, del inglés *Time Division Multiple Access*)

ANEXOS

Anexo I Módulo CAM usado en los STB.

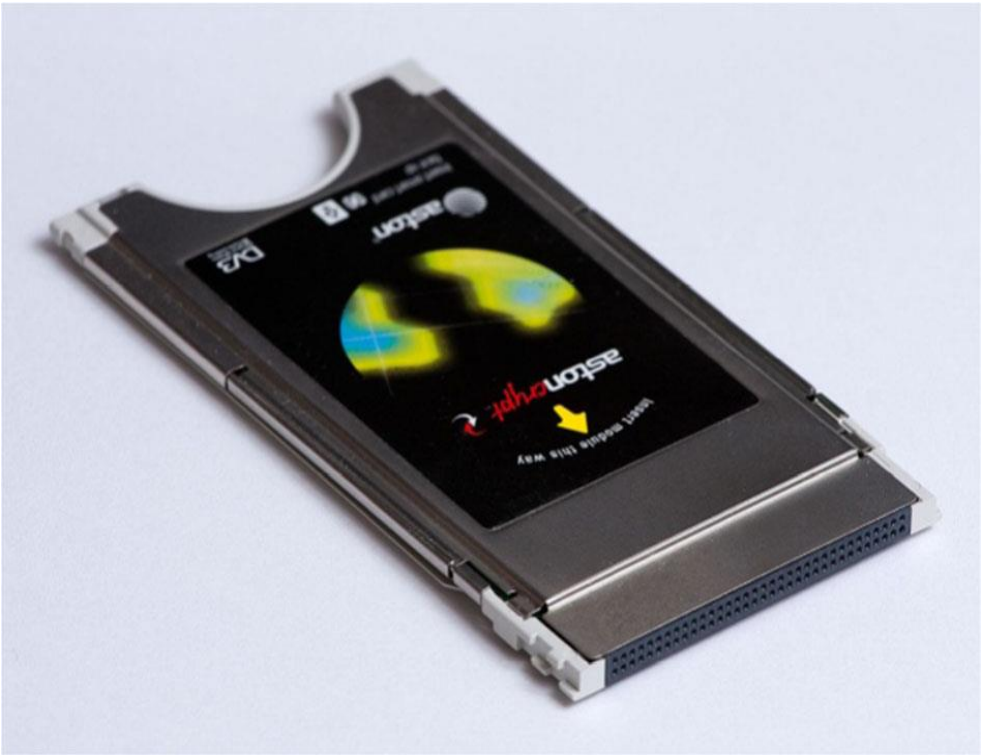

Figura 1. Módulo CAM usado en los STB. Fuente (Asghar et al., 2016).

Anexo II CAS básico para IPTV mediante hardware.

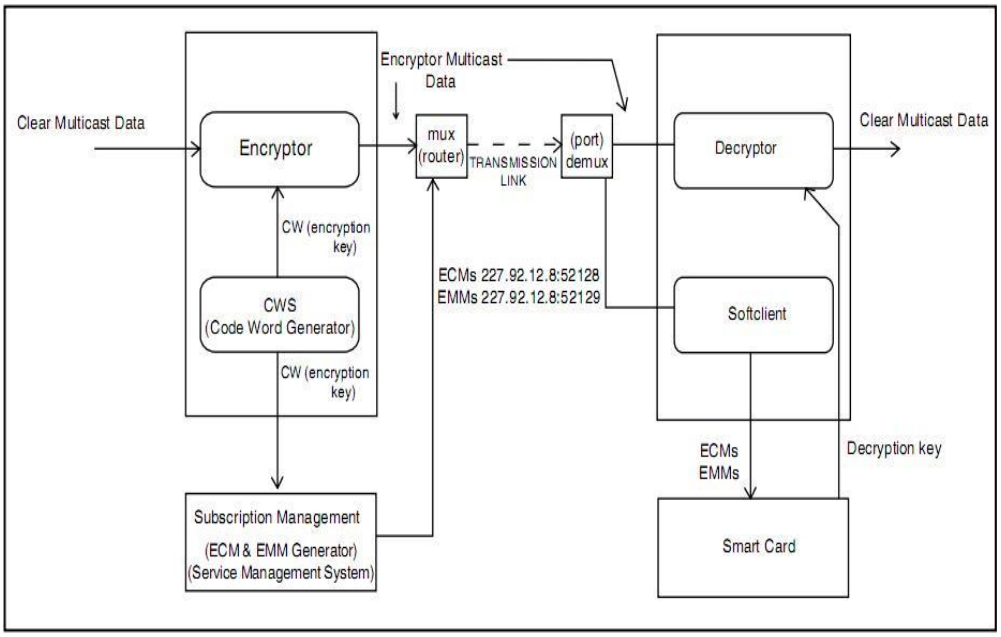

Figura 2. CAS básico para IPTV mediante hardware. Fuente (Andreja, 2011).