XVII SIMPOSIO DE INGENIERÍA ELÉCTRICA (SIE-2017)

Título
Propuestas de arquitecturas de un sistema de CAS para DTT en Cuba basado en MICAS

Title
Proposals for architectures of a CAS system for DTT in Cuba based on MICAS

MSc Ing. Irina Siles Siles[1], Marcos Antonio Sotolongo Yanes[2]

1- Irina Siles Siles. UCLV, Cuba. E-mail: irinass@uclv.edu.cu

2- Marcos Antonio Sotolongo Yanes. UCLV, Cuba. E-mail: antonios@uclv.cu.

Resumen: Tomando en consideración los desafíos en tiempos de convergencia de tecnologías y servicios, en la literatura se constata un incremento porcentual con respecto a la penetración de la tv de pago en los hogares. Con la llegada de la televisión digital, los sistemas de acceso condicional difieren del analógico en la manera de fusionar la señal; este sistema permite el control, por parte del operador, de los permisos de un subscriptor para acceder a TV, radio o datos que se emiten por su plataforma. 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. 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 Televisión Digital Terrestre (DTT). Los esquemas propuestos como resultado de la

investigación estarán basados principalmente en una arquitectura MICAS (Sistema de Acceso Condicional Integrado Móvil).

Palabras Clave: Acceso condicional; DTT; MICAS.

Abstract: *Taking into account the challenges in times of convergence of technologies and services, the literature shows a percentage increase with respect to the penetration of pay TV in households. With the advent of digital television, conditional access systems differ from analog in the way of fusing the signal; this system allows the control, by the operator, of the permissions of a subscriber to access TV, radio or data that are transmitted by its platform. Following the accumulation of investments and research necessary for the creation and operation of digital television signal transmission, in line with the aspirations and expectations of national users and in relation to the development of the ETI (Electronics, Telecommunications and Information Technology) it is essential the insertion of new services that are attractive in content. This research takes in consideration the fact that in Cuba there are not many studies on the subject, since all services are free (open); only incipient projections by some entities on possible policies of insertion of this new service are perceived. The present work will therefore be focused on proposing conditional access schemes that take into account the current conditions of the national context and take into account the deployment of an entire TDT (Digital Terrestrial Television) infrastructure. The schemes proposed as a result of the research will be based mainly on a MICAS (Integrated Mobile Conditional Access System) architecture.*

Keywords: *Conditional Access; DTT; MICAS.*

1. 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. Cifras de la UIT 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.*

A inicios del año 2013 Cuba comenzó a desplegar los servicios de DTT empleando el estándar DTMB. 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, 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 CAS el cual tienen como objetivo limitar la recepción de determinados servicios únicamente a los usuarios autorizados por el proveedor de servicio. 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 realizar una propuesta para un escenario de CAS en el contexto nacional de ambientes de TDT que tomen en consideración las condiciones actuales.

1 Funcionamiento de los CAS.

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 se observa cómo se realiza dicho proceso.

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 (KS, del inglés Service Key).

- La clave de usuario (KM, del inglés, Master Key).

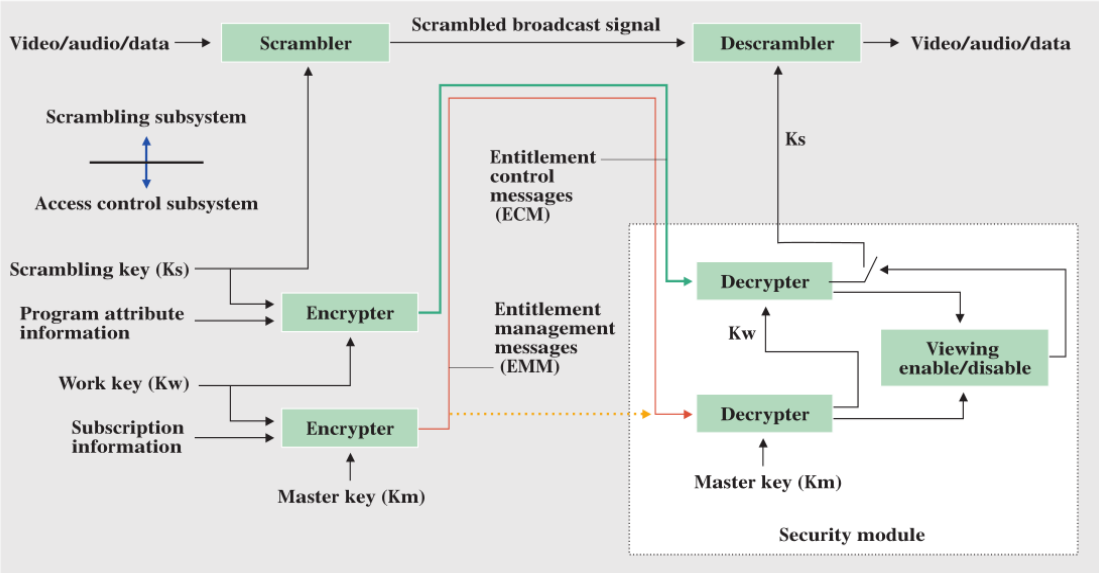

Figura 1 Configuración de un sistema de acceso condicional. Fuente (山田, 2001).

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. Si es un EMM el receptor comprueba si va dirigido a ese receptor, y si lo es, usará su clave de usuario para descifrar la clave de servicio. A partir de entonces esa clave de servicio se utiliza para descifrar los ECMs que lleguen destinados para ese servicio y así recuperar la palabra de control. Una vez obtenida la palabra de control, puede empezar a descifrar el contenido. Con el objetivo de generar los EMMs de manera adecuada, el sistema de CA necesita saber qué usuarios están autorizados a ver los diferentes eventos o servicios. El Sistema de Gestión de Suscriptores (del inglés, Subscriber Management System, SMS) se utiliza para establecer que canales puede ver un usuario. Se trata de una gran base de datos de todos los usuarios conectado al sistema de facturación y al sistema de acceso condicional. El SMS controla el sistema de CA decidiendo que EMMs se deben generar y así permitir que cada usuario vea solo los contenidos a los que tiene acceso.

2. Metodología.

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 está desglosado por niveles donde en un primer momento se realiza el análisis y comprensión de las arquitecturas CAS en las redes de radiodifusión en cuanto a tecnología de acceso y dispositivo de conexión para posteriormente arribar a una propuesta que se adecue a las condiciones actuales (arquitectura) en el país.

En cuba está concebido, 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).

Tras haber hecho un estudio sobre las arquitecturas de las redes de difusión de la televisión con CA se llega a la conclusión que la más idónea es DTT debido a que en la actualidad es la red vigente y por la cual se está brindando dicho servicio. La variante que se propone es la red MICAS en donde se integra sistema CA con la red GSM.

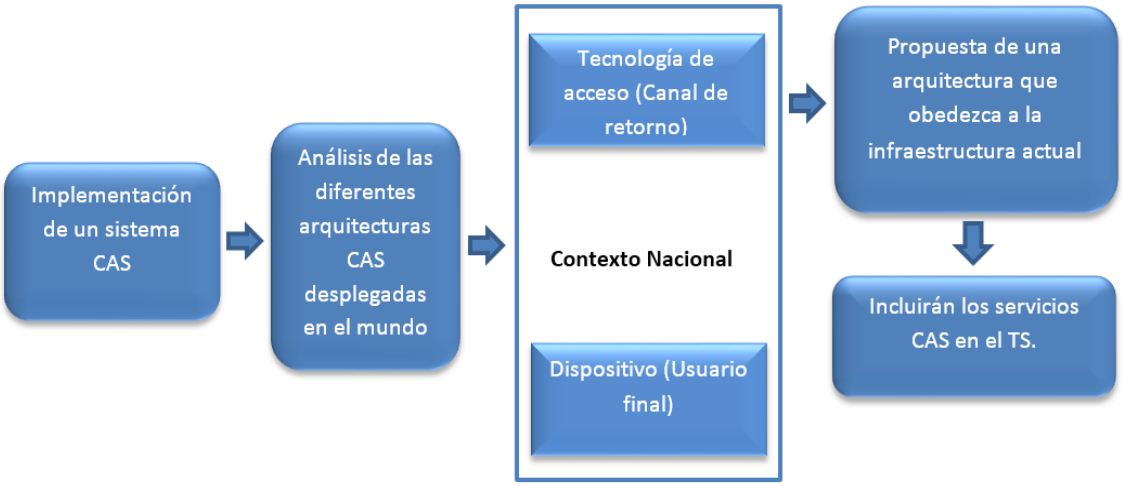

Figura 2. Diagrama de flujo. Fuente (Elaboración propia).

A inicios del año 2013 Cuba comenzó a desplegar los servicios DTT, 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. 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.

En Cuba se experimentó un aumento de la telefonía celular 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.

3. 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. Además, 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. Su teléfono móvil puede ser identificado por su IMEI (del inglés, *International Mobile System Equipment Identity*) y su ubicación puede ser reconocida por 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 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 de 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 su 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 mensaje corto servicio (SMS) o protocolo de aplicaciones inalámbricas (WAP). 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.

La figura 3 Muestra la arquitectura del sistema de acceso condicional integrado móvil (MICAS) en los sistemas de TV-Pago.

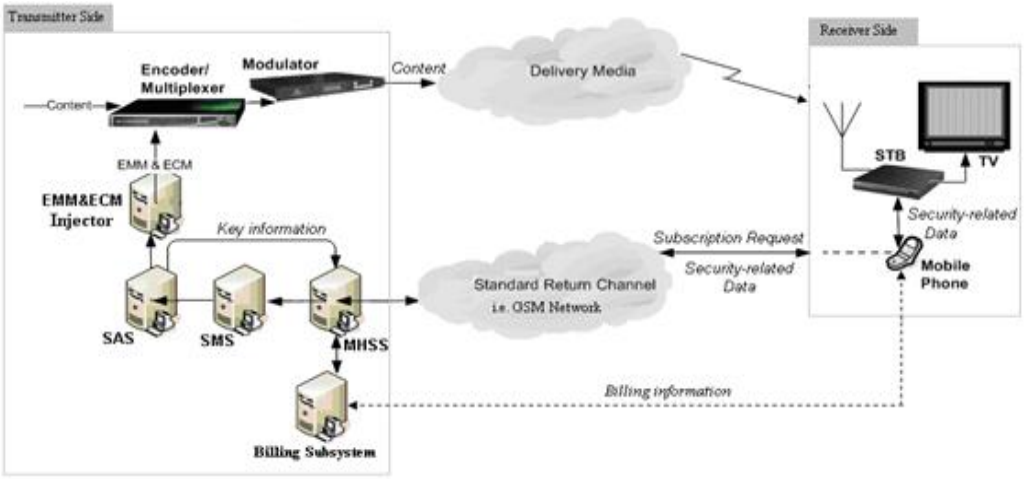

Figura 3 Modelo de referencia del sistema CA integrado a la red GSM. Fuente (Shirazi et al., 2010).

3.1 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. 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, el Subsistema de Manejo

de Mensajes (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. El MHSS envía las solicitudes de suscripción verificadas con éxito al subsistema de gestión de suscriptor (SMSS). Las consultas SMSS generan o actualizan la cuenta del espectador basada en la solicitud de suscripción, instruye al 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 dependiendo de la arquitectura de seguridad, descrito más adelante. Las funcionalidades SMSS y SAS definidas en la superposición MICAS con sus contrapartes definidas en el sistema DVB, excepto para la interfaz con SMSS. La figura 3 describe la relación interna y el flujo de datos entre los subsistemas de la MICAS.

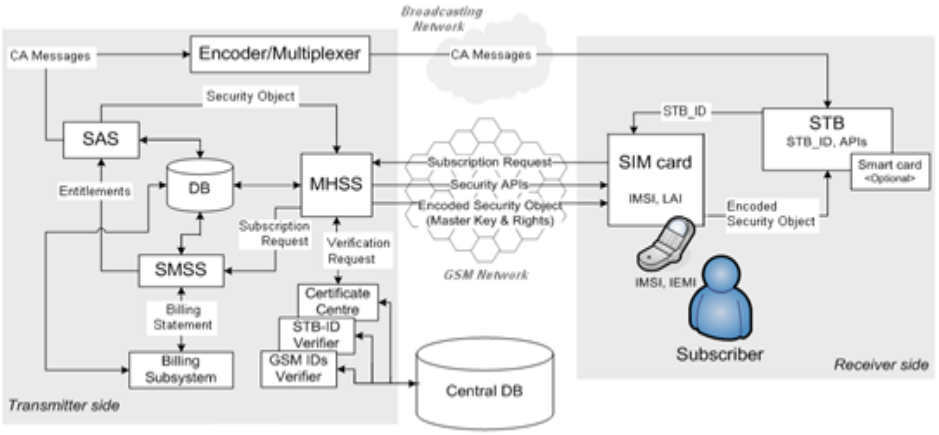

Figura 3. Arquitectura general de MICAS. Fuente (Shirazi et al., 2008).

3.2 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 servicio de mensajes cortos (SMS) o el Protocolo de aplicaciones inalámbrica (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 SIM con acceso a dominios privilegiados. Se descarga a la tarjeta SIM por 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). 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 el número de identificación de abonado internacional (del inglés, International Mobile **S**ubscriber Identity, IMSI), el número de equipo móvil internacional (IMEI), 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 IMSI e 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 el operador de la red móvil para determinar los números IMSI e IMEI. STB_ID indica el tipo de STB, que se utiliza para autenticar el 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 & 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 4 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.

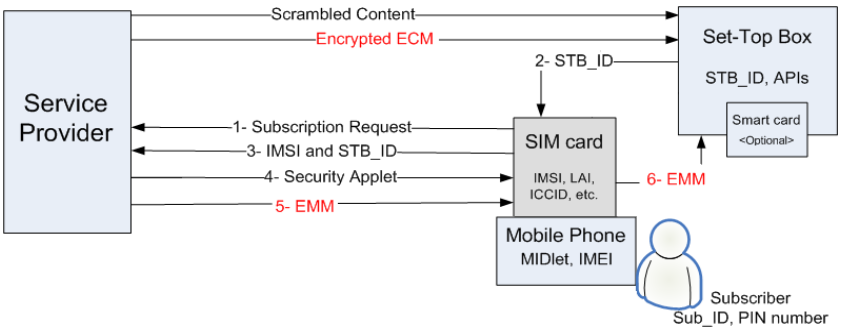

Figura 5 El flujo de datos de una arquitectura de seguridad jerárquica de 3 niveles en la que EMM se transfiere a través de la red móvil y todas las funciones de seguridad tienen lugar en el STB. Fuente (Shirazi et al., 2008).

3.3.2 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 6 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.

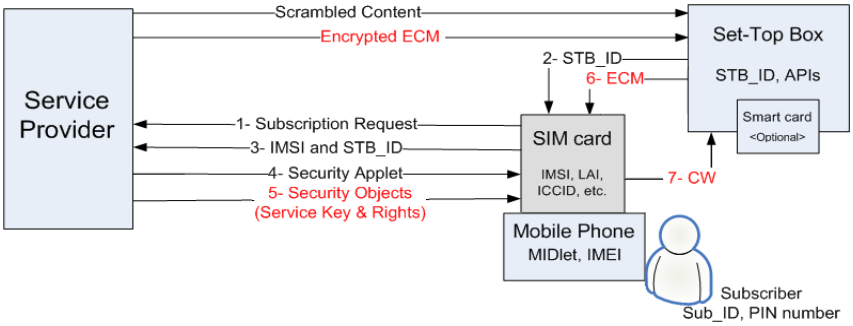

Figura 6. Flujo de datos de una arquitectura de seguridad jerárquica de 3 niveles en la que el EMM se transfiere a través de la red móvil y la decodificación EMM & ECM tiene lugar en el teléfono móvil. Fuente (Shirazi et al., 2008).

3.3.3 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 7 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.

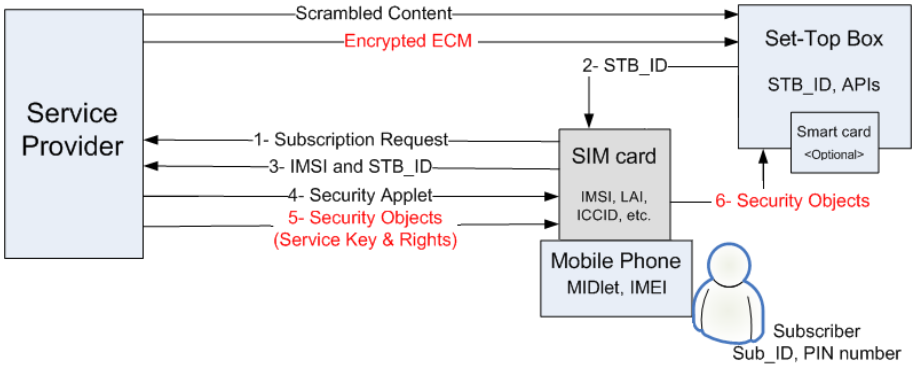

Figura 7. El flujo de datos de una arquitectura jerárquica de seguridad de 2 niveles en la que todas las funciones de seguridad tienen lugar en el STB. Fuente (Shirazi et al., 2008).

3.3.3 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 8 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.

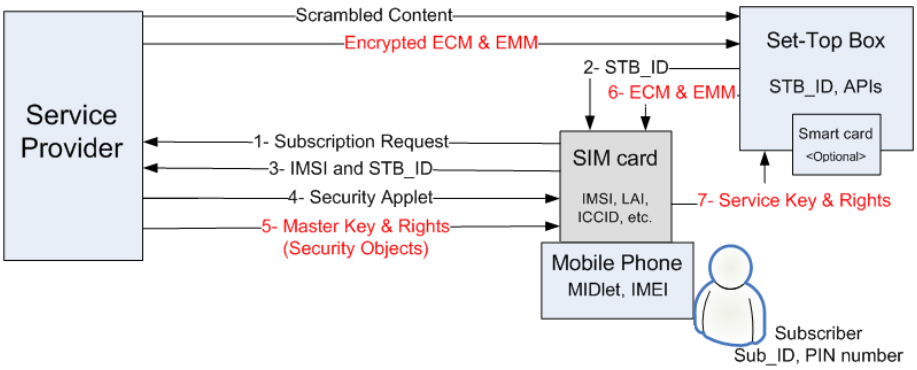

Figura 8. Jerarquía de 3 niveles en la que la decodificación EMM y ECM tiene lugar en el teléfono móvil. Fuente (Shirazi et al., 2008).

4. Conclusiones.

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

5. Referencias bibliográficas.

Oscar, F.R., 2017. La televisión que viene: Novedades de la TV digital [WWWDocument].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).

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

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).

山田宰, 2001. ディジタル放送の技術とサービス.