Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

J.1010

(09/2016)

SERIE J: REDES DE CABLE Y TRANSMISIÓN DE PROGRAMAS RADIOFÓNICOS Y TELEVISIVOS, Y DE OTRAS SEÑALES MULTIMEDIA

Acceso condicional y protección – Soluciones de acceso condicional insertadas e intercambiables y de gestión digital de los derechos

Interfaz común insertada para soluciones CA/DRM intercambiables: Casos y requisitos de utilización

Recomendación UIT-T J.1010

Unión Internacional de Telecomunicaciones

Recomendación UIT-T J.1010

Interfaz común insertada para soluciones CA/DRM intercambiables: Casos y requisitos de utilización

Resumen

En la Recomendación UIT-T J.1010 se especifican casos y requisitos de utilización para soluciones CA/DRM insertadas e intercambiables, que habilitan a los equipos en las instalaciones del cliente (CPE) y son capaces de recibir contenidos de radiodifusión y de banda ancha, para descargar clientes CA/DRM en un entorno fiable. Al utilizar el servicio descargable multi-CA/DRM, los consumidores habilitados pueden consumir contenidos de radiodifusión y banda ancha controlados por DRM y/o sistemas de acceso condicional (CA), aun cuando un CPE no disponga del cliente CA/DRM relativo a contenidos requerido, mediante su descarga a partir de una fuente fiable en diversos tipos de CPE, incluidos decodificadores (STB), TV inteligentes, PC, teléfonos inteligentes y/o tabletas inteligentes.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T J.1010	2016-09-02	9	11.1002/1000/12772

Palabras clave

CA/DRM, CPE al por menor, interfaz común insertada intercambiable

* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Introducción

La protección del servicio y el contenido realizada mediante el acceso condicional (CA) y la gestión de derechos digitales (DRM) es fundamental para la rápida evolución de la radiodifusión y la banda ancha digitales, incluidos el contenido, los servicios, las redes y los equipos en los locales del cliente (CPE), a fin de proteger los modelos comerciales de los propietarios del contenido, los operadores de red y los operadores de televisión de pago. Si bien a nivel conceptual la CA se centra en los mecanismos de acceso al contenido protegido distribuido por un proveedor de servicio por una red, la DRM en un primer momento describe el tipo y alcance de los derechos de utilización de acuerdo con el contrato del abonado.

Los operadores de televisión de pago han creado plataformas de televisión digital, en las que se aplican normas para las funciones básicas, ampliadas con elementos propios. La mayoría de sistemas de CA y DRM utilizados para la radiodifusión digital clásica, la TVIP o los nuevos servicios superpuestos (OTT) captan los equipos en los locales del cliente vinculándolos a elementos de seguridad propios. Así, los equipos en los locales del cliente configurados para la red o la plataforma A no pueden utilizarse en la red o plataforma B y viceversa. De este modo el mercado de dispositivos electrónicos de consumidor (CE) para la televisión digital sigue fragmentado, pues las especificaciones no sólo varían de un país a otro, sino también de una plataforma a otra. Los módulos CA/DRM independientes son sólo una solución parcial, pues los módulos son nuevamente propios de un sistema de CA/DRM, tampoco son baratos, se utilizan principalmente para la televisión por cable o por satélite y no pueden emplearse con equipos modernos, como las tabletas, al carecer de las interfaces físicas necesarias.

Las soluciones utilizadas en la actualidad, ya se trate de hardware integrado o independiente, crean un efecto de "encierro", lo que limita gravemente la libertad de muchos ejecutantes en el mercado de contenido multimedios digital. Gracias a los avances tecnológicos existen ahora soluciones de CA/DRM de software innovadoras. Al maximizar la interoperatividad manteniendo un alto nivel de seguridad, prometen ajustarse a las demandas futuras del mercado, permiten la participación de nuevas empresas y amplían el abanico de opciones que se ofrecen al consumidor.

Va en interés de los consumidores que puedan seguir utilizando los CPE adquiridos, por ejemplo, después de un traslado o de un cambio de proveedor de servicios o, incluso, para obtener servicios de diversos portales de vídeo comerciales. Esto sólo se puede conseguir si los CPE son interoperativos en lo que a CA y DRM se refiere, gracias a una arquitectura de seguridad adecuada. La única manera de evitar que el mercado de CPE se siga fragmentando y de fomentar la competencia es garantizando que los sistemas de CA y DRM pueden intercambiarse de manera sencilla y en función del contexto.

Recomendación UIT-T J.1010

Interfaz común insertada para soluciones CA/DRM intercambiables: Casos y requisitos de utilización

1 Alcance

El objetivo de esta Recomendación es definir una serie de requisitos básicos para una interfaz común insertada intercambiable a fin de descargar los sistemas de CA/DRM necesarios en el CPE. El proceso de descarga se efectúa en un entorno fiable y permite el consumo de contenido protegido entregado por radiodifusión y/o conexiones de banda ancha con diversos tipos de terminales, de acuerdo con los derechos de contenido adquiridos por el usuario extremo. Esta Recomendación forma parte de una serie en la que se especifica el ecosistema de ECI en su totalidad.

2 Referencias

Las siguientes Recomendaciones UIT-T y demás referencias contienen disposiciones que, por referencia a las mismas en este texto, constituyen disposiciones de esta Recomendación. En la fecha de publicación, las ediciones citadas estaban en vigor. Todas las Recomendaciones y demás referencias están sujetas a revisión, por lo que se alienta a los usuarios de esta Recomendación a que consideren la posibilidad de aplicar la edición más reciente de las Recomendaciones y demás referencias que se indican a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T vigentes. La referencia a un documento en el marco de esta Recomendación no confiere al mismo, como documento autónomo, el rango de Recomendación. Para la aplicación de esta Recomendación se necesitan las siguientes referencias.

[ETSI GS ECI 001-1] ETSI GS ECI 001-1: 2014, *Interfaz común insertada (ECI) para soluciones CA/DRM intercambiables; Parte 1: Arquitectura, definiciones y visión general.*

[ETSI GS ECI 001-2] ETSI GS ECI 001-2: 2014, *Interfaz común insertada (ECI) para soluciones CA/DRM intercambiables; Parte 2: Casos y requisitos de utilización.*

3 Definiciones

3.1 Términos definidos en otros documentos

Ninguno

3.2 Términos definidos en esta Recomendación

En esta Recomendación se definen los siguientes términos:

3.2.1 Interfaz común insertada (ECI, *embedded common interface*): arquitectura y sistema que se especificarán en la "Embedded CI" del ETSI ISG, que permitirán el desarrollo y la aplicación de clientes ECI de software intercambiables en los equipos en las instalaciones del cliente (CPE, *customer premises equipment*), facilitando así la interoperatividad de los CPE en cuanto a la ECI.

3.2.2 Cliente de interfaz común insertada (Cliente ECI): cliente CA/DRM conforme con las especificaciones de "Embedded CI" previstas. Téngase en cuenta que es el módulo de software del CEP el que ofrece los medios para recibir de manera protegida el contenido distribuido por un distribuidor u operador de contenido cuyos derechos y autorizaciones ha adquirido el consumidor. También recibe las condiciones bajo las cuales el consumidor puede utilizar un derecho o

autorización, además de las claves para desencriptar los diversos mensajes y contenidos. Un cliente ECI puede llevar asociada una tarjeta inteligente.

3.2.3 Anfitrión de interfaz común integrada (ECI): sistema de hardware y software de un CPE, que abarca las funcionalidades ECI y tiene una interfaz con el cliente ECI. Téngase en cuenta que el anfitrión ECI forma parte del firmware del CPE.

3.2.4 Contenido protegido: todo tipo de medios protegidos, en particular audio/vídeo y los metadatos asociados, entregados a la aplicación cliente por medios lineales o no lineales.

3.2.5 Contenedor de software: serie de interfaces de software con el anfitrión y con el cliente, que separa estrictamente al cliente CA/DRM del anfitrión. La configuración de las interfaces permite el intercambio de clientes CA/DRM.

4 Abreviaturas y acrónimos

En esta Recomendación se utilizan las siguientes abreviaturas, siglas o acrónimos:

AES Norma de encriptación avanzada (*advanced encryption standard*)

CA Acceso condicional (*conditional access*)

CA/DRM Acceso condicional/gestión de derechos digitales (*conditional access/digital rights management*)

CE Electrónica de consumo (*consumer electronics*)

CPE Equipo en los locales del cliente (*customer premises equipment*)

CSA Algoritmo de aleatorización común (*common scrambling algorithm*)

DECE Ecosistema de contenido recreativo digital (*digital entertainment content ecosystem*)

DRM Gestión de derechos digitales (*digital rights management*)

DVB Radiodifusión de vídeo digital (*digital video broadcasting*)

ECI Interfaz común integrada (*embedded common interface*)

IP Protocolo Internet (*internet protocol*)

IPTV Televisión mediante el protocolo Internet (*TV using the internet protocol*)

OMA Acceso móvil abierto (*open mobile access*)

OTT Superpuesto (sobre la Internet abierta) (*over the top (over the open Internet)*)

PVR Grabador de vídeo personal (*personal video recorder*)

TTP Tercero fiable (*trusted third party*)

URI Información de derechos de utilización (*usage rights information*)

VM Máquina virtual (*virtual machine*)

5 Convenios

En este documento se utilizan las siguientes expresiones con el significado que se indica a continuación:

La expresión "**se requiere**" indica que el requisito es absolutamente obligatorio y debe aplicarse sin excepción si se pretende declarar la conformidad con este documento.

La expresión "**se recomienda**" indica que se trata de un requisito recomendado y que, por ende, no es absolutamente obligatorio. Su cumplimiento no es indispensable para poder declarar la conformidad.

La expresión "**se prohíbe**" indica que el requisito está terminantemente prohibido y no se permite excepción alguna si se pretende declarar la conformidad con este documento.

La expresión "**se tiene la opción de**" indica que el requisito se permite, sin que ello signifique que se recomienda. No se pretende implicar que el fabricante deba ofrecer esta opción y que el operador de red/proveedor de servicio tenga la posibilidad de activarla. Significa, más bien, que el fabricante tiene la opción de proporcionar esta función sin que ello afecte a la conformidad con la presente especificación.

En el cuerpo del presente documento y en sus anexos aparecen algunas veces verbos que expresan *obligación*, *prohibición*, *recomendación* y *posibilidad*, en cuyo caso deben interpretarse en dicho sentido. Cuando estas expresiones o términos aparecen en apéndices o en partes incluidas explícitamente a *título informativo* no deben interpretarse en su sentido normativo.

6 Requisitos para las soluciones de CA/DRM integradas intercambiables

6.1 Observaciones generales

La especificación global de los requisitos básicos de las **ECI,** que se presenta en esta Recomendación, es parte de una serie de documentos sobre la arquitectura de sistemas CA/DRM de software, integrados e intercambiables, para fines generales, que serán la solución más adecuada para superar la fragmentación del mercado y permitir la interoperatividad. A continuación se enumeran las principales ventajas de este método para la seguridad del contenido:

- Flexibilidad y adaptabilidad gracias al software.
- La intercambiabilidad ofrece una solución de futuro y permite la innovación.
- Se puede aplicar al contenido distribuido por radiodifusión y por banda ancha, incluidos los servicios OTT.
- Soporte del entorno multipantalla.
- Estimulación del mercado para los operadores de plataformas, los proveedores de redes/servicios y los consumidores, evitando el "encierro".
- Se especifica un ecosistema abierto proclive al desarrollo del mercado.

El sistema **ECI** pretende la intercambiabilidad de CA y DRM en los CPE a todos los niveles y en todos los aspectos pertinentes, al menor costo posible para los consumidores y con limitaciones mínimas para los creadores de CA o DRM a la hora de desarrollar sus productos para el mercado de la televisión de pago. Por consiguiente, la ECI tiene, entre otras, las siguientes funcionalidades:

- Un contenedor de software para el CA en función del núcleo DRM, en adelante denominado **cliente ECI** con:
  - interfaces normalizadas para todas las funcionalidades pertinentes del CPE;
  - una **máquina virtual (VM)** para su ejecución.
- Soporte de sistemas con y sin tarjeta inteligente.
- Inclusión de múltiples contenedores de software del mismo tiempo en un CPE, cada uno de ellos ejecutándose en su propia **VM**.
- Instalación del **cliente ECI** independientemente de otros software del CPE gracias a un concepto de carga seguro y normalizado.
- **Seguridad avanzada**, también denominada seguridad por plaqueta, para el soporte de la protección del contenido y evitar accesos no autorizados al contenido.
- Métodos para que el usuario descubra el **cliente ECI** que debe descargar.

- Métodos para la revocación (total o parcial) de la funcionalidad del **cliente ECI** y la funcionalidad del CPE.
- Adaptado a la radiodifusión digital clásica, la TVIP o los modernos sistemas OTT.

Aunque la ECI se asemeja a otras soluciones ya utilizadas, las diferencias son sustanciales:

1) El módulo se encuentra en el software, no en el hardware, por lo que el consumidor no tiene que incurrir en gastos adicionales para cambiar de sistema de CA o DRM.
2) Se pueden ejecutar varios **clientes ECI** en paralelo en un único CPE sin elevar excesivamente el costo.
3) Esos clientes pueden ejecutarse simultáneamente en un solo dispositivo.

Así resulta mucho más fácil intercambiar un componente de CA o DRM, permitiendo al usuario extremo cambiar de operador u obtener en su CPE servicios de diversos operadores sin tener que invertir en el cambio de módulo.

Esta norma está compuesta por una serie de especificaciones formada por una norma global sobre usos y requisitos que se combina con las siguientes especificaciones:

Parte 1: Arquitectura, definiciones y exposición general [ETSI GS ECI 001-1]

Parte 2: Usos y requisitos [ETSI GS ECI 001-2]

Parte 3: Contenedor, cargador, interfaces y revocación de CA/DRM [b-ETSI GS ECI 001-3]

Parte 4: La máquina virtual (VM) [b-ETSI GS ECI 001-4]

Parte 5: El sistema de seguridad avanzada [b-ETSI GS ECI 001-5]

Parte 6: Entorno fiable [b-ETSI GS ECI 001-6]

Parte 7: Requisitos ampliados [b-ETSI GS ECI 001-7]

que, juntas, describen una solución que permite la sustitución de los **clientes ECI** en cualquier momento simplemente mediante la descarga de los **clientes ECI** que solicita el usuario extremo. Los **clientes ECI** se instalan en un contenedor de software normalizado en el CPE gracias a un cargador independiente, con algoritmos de seguridad y claves independientes para proteger a los **clientes ECI** contra los ataques de integridad y sustitución, con independencia de todos los demás software del CPE. Las interfaces entre el contenedor y el CPE son genéricas y se describen en GS ECI 001-3 [b-ETSI GS ECI 001-3], lo que permite al **cliente ECI** interactuar con las diversas funciones del CPE y otras funciones exteriores.

Los **clientes ECI** se ejecutan en una máquina virtual definida en GS ECI 001-4 [b-ETSI GS ECI 001-4].

En GS ECI 001-5 [b-ETSI GS ECI 001-5] se especifica un mecanismo de seguridad avanzada para proteger la clave al contenido durante su tránsito hacia la entidad de desencriptación del contenido del procesador del CPE.

En esta Recomendación se contemplan los usos y requisitos como base para la implantación de sistemas de CA/DRM interoperativos en el CPE.

La especificación de la **ECI** sólo se aplica a la recepción y posterior procesamiento del contenido controlado por un sistema de acceso condicional y/o de gestión de derechos digitales y que el proveedor de servicios ha aleatorizado. No entra dentro del alcance de esta Recomendación el contenido no controlado por un sistema de acceso condicional y/o de DRM.

La especificación global de la **ECI** está destinada a utilizarse dentro de un marco contractual (acuerdo de licencia), de acuerdo a normas de cumplimiento y robustez y siguiendo un proceso de certificación conveniente (véase la Nota) bajo el control de una **Autoridad fiable**, GS ECI 001-6 [b-ETSI GS ECI 001-6].

La seguridad de extremo a extremo de un sistema de CA/DRM conforme a la ECI no está sujeta únicamente a especificaciones técnicas. La tecnología ECI es sólo un elemento del ecosistema de ECI, GS ECI 001-1 [ETSI GS ECI 001-1], que ha de crear la Autoridad fiable, habida cuenta también del marco jurídico, de la certificación de dispositivos y de otros asuntos. A continuación se indican los requisitos basados en los usos expuestos en el Anexo A.

6.2 Requisitos genéricos

[R 01] La **Embedded CI** será aplicable a todos los servicios de radiodifusión, banda ancha e híbridos (combinación de radiodifusión y banda ancha), que entreguen contenido protegido mediante cualquier tipo de red de acceso conveniente a cualquier tipo de dispositivo conveniente.

[R 02] La **Embedded CI** definirá un **contenedor de software** para el software núcleo de la ECI y las funcionalidades de software CA/DRM estrechamente relacionadas, claramente separado del resto de software del CPE.

[R 03] La **Embedded CI** ofrecerá una seguridad avanzada comparable a la disponible en los más modernos sistemas de CA/DRM.

[R 04] La **Embedded CI** permitirá diseñar implementaciones de sistemas de CA/DRM seguras, que puedan utilizarse y mantenerse durante un largo periodo de tiempo, en cualquier caso durante un mínimo de 5 años.

6.3 Requisitos de versatilidad

[R 05] La **Embedded CI** soportará la implementación de más de un cliente CA/DRM en los CPE que ofrezcan la posibilidad de procesar simultáneamente al menos dos eventos de **contenido protegido** diferentes.

[R 06] La arquitectura permitirá que clientes ECI diferentes en un CPE puedan reconocerse, establecer una relación de confianza y transferirse mutuamente contenido y las **URI** asociadas a él.

[R 07] La arquitectura permitirá que los **clientes ECI** puedan establecer relaciones de confianza con el **anfitrión ECI** al que están conectados y puedan transferir de manera segura **URI** al **anfitrión ECI**.

[R 08] La **Embedded CI** garantizará el cumplimiento de los requisitos jurídicos y reglamentarios, por ejemplo en lo que respecta a la protección de datos privados y la protección de menores.

[R 09] La **Embedded CI** soportará la exportación de **contenido protegido** legalmente adquirido a otros terminales (incluidos los dispositivos terminales móviles) dentro de un dominio residencial o una red residencial, lo que implica que la arquitectura ofrecerá las interfaces necesarias para que un cliente ECI en un CPE pueda hablar con otro cliente ECI del mismo dispositivo. Esto sólo será posible respetando los derechos de utilización expedidos por los propietarios de los contenidos correspondientes.

[R 10] Un cliente ECI podrá implementarse de manera que pueda exportar **contenido protegido** a un dispositivo no ECI. Esto sólo será posible respetando los derechos de utilización expedidos por los propietarios de los contenidos correspondientes.

6.4 Requisitos de orden práctico

[R 11] La **Embedded CI** ofrecerá API para la implantación de interfaces de usuario de excelente usabilidad y fácil manejo para el usuario.

[R 12] La **Embedded CI** no añadirá un retardo notable en comparación con las soluciones de CA/DRM comparables aun cuando los dos canales (servicios) implicados utilicen sistemas de CA/DRM diferentes. Téngase en cuenta que no se supone que el sistema de CA/DRM haya de intercambiarse durante un cambio de canal (servicio) ordinario.

[R 13] Ninguna actividad de la ECI (por ejemplo, funcionamiento normal, descarga de un **cliente ECI**) deberá **afectar** notablemente el rendimiento y la experiencia del usuario.

6.5 Requisitos relacionados con el intercambio de cliente ECI

[R 14] La **Embedded CI** permitirá cambiar a un nuevo proveedor de servicios sin necesitar el consentimiento del fabricante de CA/DRM, el fabricante del dispositivo, la plataforma o el operador de servicio.

[R 15] En caso de intercambio de cliente ECI, se reducirá al mínimo la interrupción del servicio.

[R 16] Tras el intercambio de un **cliente ECI** será posible consumir **contenido protegido** (por ejemplo, contenido PVR aleatorizado) legalmente adquirido antes del intercambio sin necesidad de que el usuario deba realizar maniobras complejas.

[R 17] La **Embedded CI** no restringirá indebidamente las posibilidades de los fabricantes de CA/DRM para crear distintos **clientes ECI** interoperativos/intercambiables, en función de los requisitos del mercado.

6.6 Requisitos relacionados con la seguridad del sistema ECI

[R 18] Se podrá descargar, instalar e intercambiar de manera segura **clientes ECI** en un CPE; y será posible hacerlo de manera normalizada. La descarga e instalación de **clientes ECI** sólo se efectuará de manera normalizada.

[R 19] El CPE contará con un **contenedor de software** que ofrecerá una capa de abstracción unificada a cualquier cliente ECI. Téngase en cuenta que la capa de abstracción unificada es lo que una máquina virtual ofrecería al cliente ECI.

[R 20] Los **clientes ECI** y el sistema **anfitrión** podrán aseverar y probar su fiabilidad en cualquier momento.

[R 21] La **Embedded CI** soportará el desarrollo y la implantación de una **autoridad fiable**.

[R 22] La **Embedded CI** no dependerá de un hardware (componente) específico o de la presencia de un sistema operativo concreto. Por norma general, este requisito no prohíbe funciones de seguridad avanzada, siempre y cuando su especificación esté públicamente disponible y esas funciones se ajusten a las arquitecturas de seguridad actuales de los fabricantes de plaquetas CPE pertinentes. Téngase en cuenta que los sistemas de seguridad avanzada especificados en documentos públicos no se consideran hardware específico.

[R 23] El sistema **Embedded CI** permitirá la migración de los sistemas de CA/DRM compatibles con DVB/ETSI existentes a este nuevo sistema **Embedded CI**. Esto implica que un operador puede utilizar su sistema de CA/DRM existente en los dispositivos heredados y en los nuevos dispositivos conformes a ECI que ejecuten un cliente ECI compatible con el sistema de CA/DRM existente.

[R 24] La **Embedded CI** preverá la futura compatibilidad con versiones anteriores de futuras **ECI** e implementaciones de ECI. Será posible que las actuales implementaciones de ECI puedan manejar derechos de utilización introducidos por futuras extensiones de las capacidades de los CPE o los clientes ECI.

[R 25] La **Embedded CI** soportará implementaciones de sistema con y sin tarjetas inteligentes como dispositivo de seguridad y ofrecerá los recursos necesarios para ambas soluciones.

[R 26] La **Embedded CI** ofrecerá las funcionalidades necesarias para todos los niveles de seguridad del contenido necesarios para las diversas aplicaciones del sistema de CA/DRM. Será aplicable a los grandes mercados a toda la gama de productos de pago, desde los más baratos a los productos con recargo.

[R 27] Cuando se intercambie un cliente ECI, la **Embedded CI** no exigirá la sustitución de componente de hardware alguno. Sin embargo, de acuerdo con este requisito, el intercambio de la tarjeta inteligente de sistemas de CA/DRM con tarjeta inteligente no se considerará, por lo general, como la sustitución de un componente de hardware.

[R 28] La **Embedded CI** no necesitará muchos más recursos (potencia de procesamiento, memoria, etc.) del dispositivo CPE que los que necesitan los sistemas de CA/DRM integrados comparables ya disponibles, y la implantación de la arquitectura de sistema no supondrá un costo notablemente superior/adicional.

[R 29] La **Embedded CI** soportará, como mínimo, los sistemas de aleatorización DVB CSA y de norma de encriptación avanzada por AES, y el anfitrión soportará, como mínimo, los trenes de transporte MPEG (ISO/CEI 13818-1 [b-UIT-T H.222.0]) e ISOBMFF (ISO/CEI 14496-12 [b-ISO/CEI 14496-12:2012], incluida la Enmienda 3 y conforme a la señalización definida en el esquema de encriptación común definido en el fichero ISO/CEI 23001-7 [b-ISO/CEI 23001-7:2011], pero quizá con un algoritmo de encriptación diferente). Téngase en cuenta que el soporte de este requisito será compatible con la DRM empleada hoy en día por los ecosistemas de contenido recreativo digital (DECE) y ofrecerá un formato normalizado para otras DRM a fin de lograr su soporte por la **Embedded CI**.

[R 30] La **Embedded CI** soportará una amplia gama de derechos de utilización ofreciendo las funcionalidades convenientes de la interfaz entre el contenedor ECI y el anfitrión.

[R 31] La **Embedded CI** podrá describir derechos y capacidades de utilización a un cliente ECI o desde un cliente ECI a otro.

[R 32] La **Embedded CI** ofrecerá un canal de comunicación seguro entre clientes ECI del mismo dispositivo o de dispositivos distintos.

Anexo A

Hipótesis de uso

(Este Anexo forma parte integrante de la presente Recomendación)

El número de usos previstos en el Anexo A no es exhaustivo.

A.1 Hipótesis de uso 1

En el entorno comercial de la televisión digital puede haber varias razones que motiven el intercambio de sistemas de CA/DRM en el CPE.

- Un proveedor de contenido de medios digital puede decidir cambiar el sistema de CA/DRM en el CPE para sus clientes por los siguientes motivos:
  - Diferentes razones técnicas o comerciales, como la necesidad de aumentar las funcionalidades de CA/DRM, aumentar el nivel de seguridad o de rendimiento del sistema en caso de que el sistema vigente haya sido víctima de pirateo masivo.
  - Adquisición de nuevos clientes en una determinada red, utilizada para acceder a los servicios de la competencia.
- Un operador de plataforma puede decidir cambiar el sistema de CA/DRM en el CPE en su plataforma por los siguientes motivos:
  - Diferentes razones técnicas o comerciales, como la necesidad de aumentar las funcionalidades de CA/DRM, aumentar el nivel de seguridad o de rendimiento del sistema en caso de que el sistema vigente haya sido víctima de pirateo masivo.
  - Armonización de tecnologías tras la adquisición de una red.
- Un fabricante de CA/DRM adquiere un nuevo cliente, que opera una plataforma en la que la competencia ya ha implantado su sistema de CA; o un fabricante de CA/DRM adquiere otro fabricante de CA/DRM y desea armonizar las tecnologías de seguridad.
- Un usuario extremo adquiere un CPE en una tienda y lo conecta a la red del proveedor de red de acceso A. Uno o más proveedores de servicio ofrecen sus servicios por esa red. El usuario extremo puede optar por cualquiera de esos servicios y descargar su sistema de CA/DRM, si está registrado (incluida la autentificación y la autorización) ante el proveedor de servicios en cuestión.

  Pasado cierto tiempo, el mismo usuario extremo decide conectarse a la red del proveedor de red de acceso B y conecta su CPE a esa red. Si el CPE soporta las tecnologías de recepción necesarias (por ejemplo, DVB-C/C2, -S/S2, -T/T2, Ethernet, xDSL), uno o más proveedores de servicio ofrecen sus servicios por esa red. El usuario extremo puede optar por cualquiera de esos servicios e intercambiar convenientemente los sistemas de CA/DRM si está registrado (incluida la autentificación y la autorización) ante el proveedor de servicios en cuestión.
- Un fabricante de CPE desea introducir en el mercado al por menor CPE que soporten la televisión gratuita y la televisión de pago. Los CPE pueden, no obstante, adaptarse para utilizarse en determinados servicios de televisión de pago mediante una actualización del software con el consentimiento del usuario extremo.

A.2 Hipótesis de uso 2

Hoy en día, si se ha de cambiar (por cualquier motivo) el sistema de CA instalado en un CPE que utiliza una plataforma de CA operativa, hay cuatro entidades involucradas:

- El vendedor de CA actual.

- El operador de la plataforma o el proveedor de contenido de medios digital.
- El fabricante del CPE.
- El nuevo vendedor de CA.

El vendedor de CA actual debe facilitar al nuevo vendedor tanto la información técnica para acceder a la instalación del CPE, como la licencia para utilizar ciertos componentes de hardware, protocolos o software implantados en ese CPE. En cualquier caso, el nuevo vendedor de CA debe adaptar su sistema de CA a las funcionalidades, limitaciones de hardware/software y protocolos disponibles en el CPE en cuestión. Los fabricantes de CPE deben integrar el nuevo sistema de CA en el software de los distintos CPE instalados. En el caso más desfavorable, el cambio de sistema de CA/DRM puede no ser siquiera una opción técnica/comercial viable. Esta situación ha de cambiar para lograr la interoperatividad.

Dado que los módulos de seguridad propios forman hoy en día parte integrante de la mayoría de sistemas de CA modernos, casi siempre los CPE se fabrican para un sistema de CA en concreto, lo que puede limitar el nivel de seguridad que pueda ofrecer el nuevo sistema de CA en el CPE ya instalado. Es necesario que esto deje de ser así para que toda mejora de seguridad sea completamente transferible.

A.3 Hipótesis de uso 3

El sistema ECI soportará aplicaciones de sólo consumo, incluida la entrega de **contenido protegido** a dispositivos secundarios. Hay dos hipótesis pertinentes para el soporte de aplicaciones de dispositivos secundarios:

- Aplicación centralizada: el CPE de tipo pasarela conforme con ECI entrega información sobre derechos de utilización (URI) y contenido encriptado al dispositivo secundario.
- Aplicación descentralizada: el CPE de tipo pasarela conforme con ECI sólo entrega UIR al dispositivo secundario y éste deriva el contenido encriptado de la red. Téngase en cuenta que el sistema ECI no tiene requisitos con respecto a la implementación de un cliente DRM en el dispositivo secundario. A fin de entregar contenido protegido desde una pasarela a un dispositivo secundario sólo hace falta que los dos clientes DRM puedan comunicar de manera segura entre ellos y que el propietario del contenido soporte el sistema de DRM utilizado.

A.4 Hipótesis de uso 4 (caso relacionado con un tercero fiable (TTP))

Hoy en día los ID exclusivos o certificados necesarios están integrados por el fabricante en el CPE y están definidos por el proveedor del sistema de CA/DRM. Esta solución no conviene a la interoperatividad, pues es poco probable que los fabricantes deseen divulgar los mecanismos de acceso a sus ID exclusivos o certificados. Por ejemplo, el consorcio CI plus ha demostrado que es posible transferir el tratamiento seguro de los certificados a un "tercero fiable". Para la interoperatividad de los sistemas de CA/DRM se necesitará una solución semejante.

Bibliografía

[b-ITU-T H.222.0] Recomendación UIT-T H.222.0 (2006) | ISO/IEC 13818-1 (2007), *Tecnología de la información - Codificación genérica de imágenes en movimiento e información de audio asociada: Sistemas.*

[b-ETSI GS ECI 001-3] ETSI GS ECI 001-3, *Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 3: The CA/DRM Container: Loader, Interfaces, Revocation*.

[b-ETSI GS ECI 001-4] ETSI GS ECI 001-4, *Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 4: The Virtual Machine.*

[b-ETSI GS ECI 001-5] ETSI GS ECI 001-5, *Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 5: The Advanced Security System.*

[b-ETSI GS ECI 001-6] ETSI GS ECI 001-6, *Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 6: The Trust Environment.*

[b-ETSI GS ECI 001-7] ETSI GS ECI 001-7, *Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 7: Use cases and Requirements, extended Requirements.*

[b-ETSI ISG ECI] ETSI ISG ECI White Paper-v1_20 (2014), *Industry Specification Group on Embedded Common Interface for exchangeable CA/DRM solutions.*

[b-ISO/CEI 14496-12] ISO/CEI 14496-12:2012, *Information Technology - Coding of Audio-Visual Objects - Part 12: ISO Base Media file format.*

[b-ISO/CEI 23001-7] ISO/CEI 23001-7:2011, *Information technology - MPEG systems technologies - Part 7: Common encryption in ISO base media file format files.*

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios de tarificación y contabilidad y cuestiones económicas y políticas de las telecomunicaciones/TIC internacionales
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	**Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia**
Serie K	Protección contra las interferencias
Serie L	Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de la transmisión telefónica, instalaciones telefónicas y redes de líneas locales
Serie Q	Conmutación y señalización, y mediciones y pruebas asociadas
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	Redes de datos, comunicaciones de sistemas abiertos y seguridad
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet, redes de próxima generación, Internet de las cosas y ciudades inteligentes
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2017