Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

J.1011

(09/2016)

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

Interfaz común insertada para soluciones CA/DR intercambiables: Arquitectura, definiciones y visión general

Recomendación UIT-T J.1011

Unión Internacional de Telecomunicaciones

Recomendación UIT-T J.1011

Interfaz común insertada para soluciones CA/DRM intercambiables: Arquitectura, definiciones y visión general

Resumen

En la Recomendación UIT-T J.1011 se especifica una arquitectura para la gestión de derechos de acceso/digitales condicionales intercambiables e insertados o soluciones CA/DRM, 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 mediante gestión de derechos digitales (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.1011	2016-09-02	9	11.1002/1000/12773

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 [ha recibido/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

Página

1 Alcance 1
2 Referencias 1
3 Definiciones 1
3.1 Términos definidos en otros documentos 1
3.2 Términos definidos en esta Recomendación 1
4 Siglas y acrónimos 2
5 Convenios 3
6 Arquitectura de soluciones CA/DRM integradas e intercambiables 4
6.1 Generalidades 4
6.2 Concepto técnico del sistema ECI 6
7 Entorno de confianza 12
7.1 Flujos de trabajo operacionales necesarios 13
Apéndice I – Realización de un sistema de confianza que sea conforme una ECI 15
Bibliografía 17

Introducción

La protección de servicios y contenidos mediante acceso condicional (CA) y gestión de derechos digitales (DRM) es esencial en el ámbito en continua evolución de la radiodifusión digital y la banda ancha, que abarca contenidos, servicios, redes y equipos en las instalaciones del cliente (CPE), con el fin de proteger los modelos de negocio de los propietarios de contenidos, operadores de red y operadores de sistemas de TV de pago. Mientras que conceptualmente el acceso condicional se centra en los mecanismos de acceso a contenidos distribuidos por un proveedor de servicio sobre una red, la gestión de derechos digitales describe el tipo y alcance de los derechos de su utilización, de conformidad con el contrato del abonado.

Los operadores de televisión de pago han creado plataformas de TV digital que incorporan funciones básicas basadas en normas, que amplían con elementos privativos. La mayoría de los sistemas de CA y DRM típicamente utilizados en la radiodifusión digital, ya sea la televisión por IP (IPTV) o basada en los nuevos servicios superpuestos (OTT), establecen la asociación con el CPE mediante una vinculación que utiliza elementos de seguridad privativos. Como consecuencia, un CPE configurado para ser utilizado en la red o plataforma "A", no puede ser utilizado en la plataforma "B" o viceversa. Por tanto, el mercado de la electrónica de consumo para TV digital está aún fragmentado, ya que las especificaciones difieren no sólo entre países, sino también entre plataformas. Los módulos de CA/DRM enchufables constituyen una solución parcial: los módulos son también privativos del sistema de CA/DRM, no son baratos, se utilizan fundamentalmente para TV por cable o por satélite y no pueden utilizarse en equipos modernos, como tabletas, debido a la falta de interfaces físicos adecuados.

Las soluciones actualmente instaladas, ya sean integradas o con hardware enchufable, generan un efecto de "dependencia". Esta situación restringe de manera muy importante la libertad de muchos agentes de los mercados de contenidos multimedios digitales. Los avances tecnológicos actuales permiten soluciones de CA/DRM innovadoras basadas en software. Al maximizar la interoperabilidad y mantener un elevado nivel de seguridad, son soluciones prometedoras para satisfacer las futuras demandas del mercado, permitir nuevos enfoques de negocio y ampliar las posibilidades de elección de consumidor.

Resulta beneficioso para el consumidor poder seguir utilizando un CPE previamente adquirido, por ejemplo, tras un traslado o un cambio de proveedor de red, o incluso utilizar dispositivos para servicios de distintos portales de video comerciales. Esto sólo es posible mediante la interoperabilidad de los CPE, con independencia del CA y DRM, y con una arquitectura de seguridad adecuada. Sólo garantizando una intercambiabilidad de los sistemas CA y DRM que realice fácilmente el propio consumidor y que sea sensible al contexto, podrá evitarse una mayor fragmentación del mercado de los CPE y alentarse así la competencia.

Recomendación UIT-T J.1011

Interfaz común insertada para soluciones CA/DRM intercambiables: Arquitectura, definiciones y visión general

1 Alcance

El objeto de esta Recomendación es especificar las entidades funcionales de la arquitectura de una interfaz común intercambiable, la interfaz común integrada, que permita descargar cualquier sistema de acceso condicional/gestión de derechos digitales (CA/DRM) en un equipo de cliente (CPE). El proceso de descarga se realiza en un entorno fiable y habilita el consumo de contenidos protegidos que se distribuyen a través de sistemas de radiodifusión o de banda ancha con diversos tipos de equipos terminales en consonancia con los derechos de contenidos adquiridos por el usuario final. Esta Recomendación pertenece a una serie de Recomendaciones que especifican el ecosistema de la interfaz común integrada (ECI).

2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación.

[ETSI GS ECI 001-1] ETSI GS ECI 001-1 (2014): Interfaz común integrada (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 integrada (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 términos siguientes:

3.2.1 seguridad avanzada: función de un CPE que es conforme con ECI que ofrece funciones de seguridad mejoradas (hardware y software) para un cliente ECI. Nótese que la especificación de detalle figura en [b-ETSI GS ECI 001-5].

3.2.2 ECI (interfaz común integrada): arquitectura y sistema especificado en el ISG de ETSI *"Embedded CI"* (CI integrada), que permite la creación e instalación en equipos de cliente (CPE) de **clientes ECI** intercambiables basados en software y que, por tanto, permiten la interoperabilidad de dispositivos CPE con relación a la ECI.

3.2.3 cliente ECI (cliente de la interfaz común integrada): realización de un cliente de CA/DRM conforme con las especificaciones de la CI integrada. Nótese que es el módulo de software del CPE lo que habilita todas las formas de recepción, de manera protegida, y de control de la ejecución de las autorizaciones y derechos del consumidor sobre el contenido que distribuye un distribuidor de contenidos o un operador. También recibe las condiciones en las que el consumidor puede aplicar un derecho o una autorización y las claves para desencriptar los mensajes y contenidos.

3.2.4 cargador de cliente ECI: parte del módulo software del anfitrión ECI que permite la descarga, verificación e instalación de un nuevo software de cliente ECI en un contenedor ECI del anfitrión ECI.

3.2.5 contenedor ECI (contenedor de CI integrada): concepto abstracto que proporciona un entorno aislado compuesto por una máquina virtual y un único cliente ECI.

3.2.6 anfitrión ECI: sistema hardware y software de un CPE que dispone de funcionalidades relacionadas con la ECI y que tiene interfaces con un cliente ECI. El anfitrión ECI forma parte del firmware del CPE. El anfitrión ECI es responsable de garantizar el aislamiento de cada contenedor ECI y proporcionar la descarga autentificada de clientes ECI.

3.2.7 cargador de anfitrión ECI: modulo software que permite la descarga, verificación e instalación de un (nuevo) software de anfitrión ECI en un CPE. Nótese que en una configuración de carga en varias etapas este término hace referencia a todas las funciones de descarga críticas en términos de seguridad que participan en la descarga del anfitrión ECI.

3.2.8 autoridad de confianza (TA, *trust authority***)**: organización que rige todas las normas y regulaciones aplicables en la realización de una **ECI**. Nótese que la autoridad de confianza debe ser una entidad jurídica para poder realizar demandas legales. La autoridad de confianza debe ser imparcial para todos los agentes del ecosistema CA/DRM descargable.

3.2.9 tercera parte de confianza (TTP, *trusted third party***)**: proveedor técnico de servicio que emite un certificado y claves para fabricantes que cumplen las normas relativas a lo componentes pertinentes de un sistema ECI controlado por la autoridad de confianza (TA).

4 Siglas y acrónimos

En la presente Recomendación se utilizan las siglas y los acrónimos siguientes:

API Interfaz de programación de aplicaciones (*application programming interface*)

CA Acceso condicional (*conditional access*)

CENC Encriptación común (*common encryption*)

CI Interfaz común (*common interface*)

CPE Equipo en las instalaciones de cliente (*customer premises equipment*)

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

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

ECI Interfaz común integrada (*embedded common interface*)

HD Alta definición (*high definition*)

HTTP Protocolo de transferencia de hipertexto (*hyper text transfer protocol*)

iDTV TV digital integrada (*integrated digital TV*)

IP Protocolo de Internet (*internet protocol*)

IPTV Televisión por protocolo Internet (*internet protocol television*)

LA Acuerdo de licencia (*license agreement*)

MPEG Grupo de expertos en imágenes en movimiento (*motion picture experts group*)

OS Sistema operativo (*operating system*)

OSD Presentación en pantalla (*on screen display*)

OTT Servicio superpuesto (*over the top*)

PIN Número de identificación personal (*personal identification number*)

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

ROM Memoria de solo lectura (*read only memory*)

SI Información de servicio (*service information*)

STB Decodificador (*set-top box*)

TA Autoridad de confianza (*trust authority*)

TTP Tercera parte fiable (*trusted third party*)

TV Televisión

UI Interfaz de usuario (*user interface*)

VM Máquina virtual (*virtual machine*)

5 Convenios

En esta Recomendación:

La expresión "se requiere" indica un requisito que debe cumplirse estrictamente y del que no se permite desviación alguna si se pretende declarar la conformidad con esta Recomendación.

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

La expresión "se prohíbe" indica que indica que un requisito que debe cumplirse estrictamente y del que no se permite desviación alguna si se pretende declarar la conformidad con esta Recomendación.

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 de la presente Recomendación 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 Arquitectura de soluciones CA/DRM integradas e intercambiables

6.1 Generalidades

La arquitectura, definiciones y visión general de la ECI que recoge esta Recomendación marco forma parte de una norma que se compone de varias partes que especifica una arquitectura de sistema para sistemas de acceso condicional/gestión de derechos digitales (CA/DRM) de propósito general, basada en software, integrada e intercambiable que resulta la más adecuada para soluciones

preparadas para el futuro y para evitar la fragmentación del mercado y permitir la interoperabilidad. Los beneficios fundamentales de este enfoque para la seguridad de los contenidos son los siguientes:

– flexibilidad y escalabilidad por tratarse de una implementación en software;
– intercambiabilidad, que propicia soluciones preparadas para el futuro y estimula la innovación;
– aplicación a contenidos distribuidos mediante radiodifusión y mediante banda ancha, incluidos los servicios superpuestos (OTT);
– soporte de un entorno multipantalla;
– estimulación del mercado de los operadores de plataformas, proveedores de red/servicio y consumidores y evitar situaciones de "dependencia del proveedor";
– especificación de un ecosistema abierto que impulse el desarrollo del mercado.

El sistema ECI tiene por objetivo la intercambiabilidad de los sistemas de CA y DRM de los equipos de cliente (CPE) a todos los niveles y en todos los aspectos pertinentes, con el menor coste posible para el usuario y las mínimas restricciones al desarrollo de los productos para el mercado de la TV de pago de los suministradores de CA y DRM. El elemento fundamental de la ECI es la especificación de la interfaz entre el cliente CA/DRM basado en software y el sistema anfitrión. Por tanto, la ECI tiene, entre otras, las siguientes funcionalidades:

– Un contenedor software para el CA y para el kernel DRM respectivamente – en adelante denominado cliente ECI, con:
  • interfaces normalizadas para todas las funcionalidades pertinentes del CPE;
  • una máquina virtual estandarizada (VM) sobre la que se ejecuta.
– Soporte de sistemas sin tarjeta inteligente, así como su uso en sistemas basados en tarjetas inteligentes.
– Inclusión de varios contenedores software en un mismo CPE, donde cada contenedor se ejecuta sobre su propia instancia de VM.
– Instalación del cliente ECI con independencia de cualquier otro software de CPE mediante un concepto de cargador seguro y normalizado.
– Seguridad avanzada, también conocida como seguridad del conjunto de chips o circuitos integrados, para una protección de contenidos de última generación.
– Disposiciones que aprovechen funcionalidades de seguridad que utilizan hardware.
– Métodos para que el usuario identifique el cliente ECI adecuado que debe descargar.
– Métodos para la revocación de (o de partes de) la funcionalidad del cliente ECI y de la funcionalidad del CPE.
– Adecuación a sistemas clásicos de radiodifusión digital, IPTV y a nuevos sistemas OTT.

Aunque la ECI muestra algunas similitudes con soluciones actualmente instaladas, las diferencias son sustanciales:

1) El módulo de cliente CA/DRM se implementa en software, no en hardware. Por tanto, el consumidor no incurre en costos cuando cambia de sistema CA o DRM.
2) En un mismo CPE pueden instalarse varios clientes ECI, sin añadir costos reseñables.
3) Estos clientes pueden ejecutarse simultáneamente en un mismo dispositivo.

Como consecuencia, un componente CA o DRM puede intercambiarse mucho más fácilmente, y permitir al usuario final cambiar de operador o disponer de servicios de varios operadores en su CPE sin verse obligado a sustituir costosos módulos del mismo.

La norma completa tiene varias partes y consta de un grupo de especificaciones, incluida una especificación marco, junto con las especificaciones subyacentes:

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

– Parte 2: Casos de uso 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: Máquina virtual (VM) [b-ETSI GS ECI 001-4]

– Parte 5: Sistema de seguridad avanzado [b-ETSI GS ECI 001-5]

– Parte 6: Entorno de confianza [b-ETSI GS ECI 001-6]

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

El conjunto de las cuales describe una solución que permite sustituir clientes ECI en cualquier momento simplemente mediante la descarga de los clientes ECI requeridos por el usuario final. Los clientes ECI se instalan en un contenedor software estandarizado del CPE mediante un cargador separado, con algoritmos de seguridad y claves para la protección específicas para proteger a los clientes ECI de ataques a la integridad y de sustitución, con independencia de todo el resto del software del CPE. Las interfaces del contenedor con el CPE son genéricas y se definen en [b-ETSI GS ECI 001-3], que permiten al cliente ECI interactuar con las diversas funciones del CPE y más allá.

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

[b-ETSI GS ECI 001-5] especifica un mecanismo de Seguridad avanzada para proteger la clave de acceso al contenido durante su transmisión hasta el sistema de desencriptado del contenido que reside en el chip del procesador del CPE.

En esta Recomendación se presenta la arquitectura e información general de las especificaciones de las interfaces pertinentes para la implementación de sistemas CA/DRM interoperables en los CPE.

La especificación ECI sólo se aplica a la recepción y posterior procesamiento de contenido controlado por un sistema de acceso condicional y/o de gestión de derechos digitales y que el proveedor de servicio ha aleatorizado. Esta Recomendación no incluye el caso de contenidos no controlados por un sistema de acceso condicional y/o DRM.

La especificación de grupo de la ECI está diseñada para ser utilizada conjuntamente con un marco contractual (un acuerdo de licencia), normas de conformidad y robustez y un proceso de certificación adecuado (véase la nota), bajo el control de una autoridad de confianza [b-ETSI GS ECI 001-6]. Nótese que el marco contractual (acuerdo de licencia), las normas de conformidad y robustez y los procesos de certificación adecuados no están incluidos en los trabajos de normalización del ISG (grupo de normalización de la industria) sobre ECI.

6.2 Concepto técnico del sistema ECI

6.2.1 Consideraciones básicas

Esta Recomendación, junto con las Partes 2 a 5 y 7 de las especificaciones ([ETSI GS ECI 001-2], [b-ETSI GS ECI 001-3], [b-ETSI GS ECI 001-4], [b-ETSI GS ECI 001-5] y [b-ETSI GS ECI 001-7]), especifica una arquitectura que permite la descarga, instalación, actualización, eliminación y sustitución de clientes ECI en cualquier momento, independientemente de otros clientes ECI que se estén ejecutando en el mismo anfitrión, del software del sistema del CPE del anfitrión o de las aplicaciones que se ejecutan sobre dicho anfitrión. Un anfitrión de ECI deberá poder incluir y proporcionar un entorno de ejecución al menos a dos clientes ECI o a tantos como pueda admitir en función de sus recursos. Los clientes ECI de un anfitrión se ejecutan en paralelo,

siendo posible la desencriptación simultánea o la reencriptación de flujos de contenidos de distintos operadores.

El concepto técnico descrito en esta Recomendación y especificado en [ETSI GS ECI 001-2], [b-ETSI GS ECI 001-3], [b-ETSI GS ECI 001-4] y [b-ETSI GS ECI 001-5] es aplicable a sistemas de CA conformes con DVB Multicrypt y a DRM compatibles con encriptación común (CENC, *common encryption*).

El CPE aloja un único cargador especial para clientes ECI que incluye la funcionalidad de seguridad necesaria para proteger la integridad y autenticidad de los clientes ECI. El cargador puede ser invocado y utilizado en cualquier momento para descargar y verificar otro cliente ECI. El cargador y sus medios de seguridad conexos se especifican en [b-ETSI GS ECI 001-3].

En relación con este concepto técnico, cada clientes ECI se instala en un contenedor software separado, con su propia instancia de máquina virtual (instancia VM), especificada en [b-ETSI GS ECI 001-4]. El contenedor ECI se especifica solamente para la funcionalidad CA/DRM, tal como se recoge en [b-ETSI GS ECI 001-3]. La interfaz con el CPE, que se detalla en [b-ETSI GS ECI 001-3], permite la solicitud e intercambio de datos que necesitan las diversas funciones de CA/DRM. Estas solicitudes e intercambios de datos se realizan entre el cliente ECI y el anfitrión, entre dos clientes ECI en el mismo anfitrión o entre dos clientes ECI en distintos anfitriones.

Los dispositivos diseñados para ser utilizados en torno a la TV, se definen como dispositivos cuyo conjunto de chips tienen la capacidad de procesar flujos de trasporte MPEG-2. La norma ECI requiere que dichos conjuntos de chips implementen funcionalidades de seguridad avanzadas conformes con la misma. [b-ETSI GS ECI 001-5] especifica cómo aprovechar los mecanismos de Seguridad avanzada del conjunto de chips para proteger la clave asociada al contenido durante su transporte hasta el sistema de desencriptación de contenidos del chip del procesador de la ECI. Este concepto de Seguridad avanzada permite que todos los clientes ECI que utilicen dicho sistema funcionen simultánea e independientemente.

Los dispositivos para otros entornos, especialmente IPTV y tabletas, teléfonos inteligentes, etc., típicamente implementan más funcionalidades en el software y ofrecen comunicación IP bidireccional. Ello permite utilizar nuevos tipos de mecanismos de mejora de la seguridad. Dado que los chips utilizados en estos dispositivos incluyen hardware para varias funciones de seguridad del procesamiento, la conformidad con ECI exige la implementación de funcionalidades de seguridad y robustez dedicadas asistidas por hardware. Por tanto, la especificación [b-ETSI GS ECI 001-3] incluye métodos para que un cliente ECI obtenga los parámetros pertinentes de las capacidades y funcionalidades técnicas del anfitrión, en la medida que sean pertinentes, incluido el posible soporte de la seguridad avanzada especificada en [b-ETSI GS ECI 001-5].

Las funcionalidades de seguridad avanzada están disponibles simultáneamente para cualquier cliente ECI que esté activo en un CPE. Los clientes ECI también pueden desplegarse en plataformas con sistemas de CA para DVB o en sistemas DRM para CENC en modo simulcrypt o multicrypt, en la medida que el lado servidor de dichos sistemas sea conforme con las respectivas normas de DVC/CENC.

6.2.2 Visión general de la arquitectura

La ECI permite que los proveedores de CA/DRM implementen soluciones de acceso condicional (CA) y de gestión de derechos digitales (DRM) en el dominio de un cliente individual. En la Figura 1 se muestra una configuración de referencia soportada íntegramente por una implementación completa de ECI.

Para entornos multipantalla en el dominio de un cliente individual, los clientes ECI de ese dominio deben comunicarse entre sí y poder utilizar una red bidireccional con el proveedor, en función de la disponibilidad de cada una de las redes y las funcionalidades de apoyo en los sistemas CA/DRM y en sus clientes ECI. En [b-ETSI GS ECI 001-3] puede encontrarse más información al respecto.

Un cliente ECI puede implementarse de tal forma que también pueda funcionar como pasarela para clientes que no sean conformes con ECI. En [b-ETSI GS ECI 001-5 se especifican los mecanismos para la retrocompatibilidad de futuras implementaciones. Los protocolos e implementaciones específicas de los clientes privativos quedan fueran del alcance de estas especificaciones de ECI.

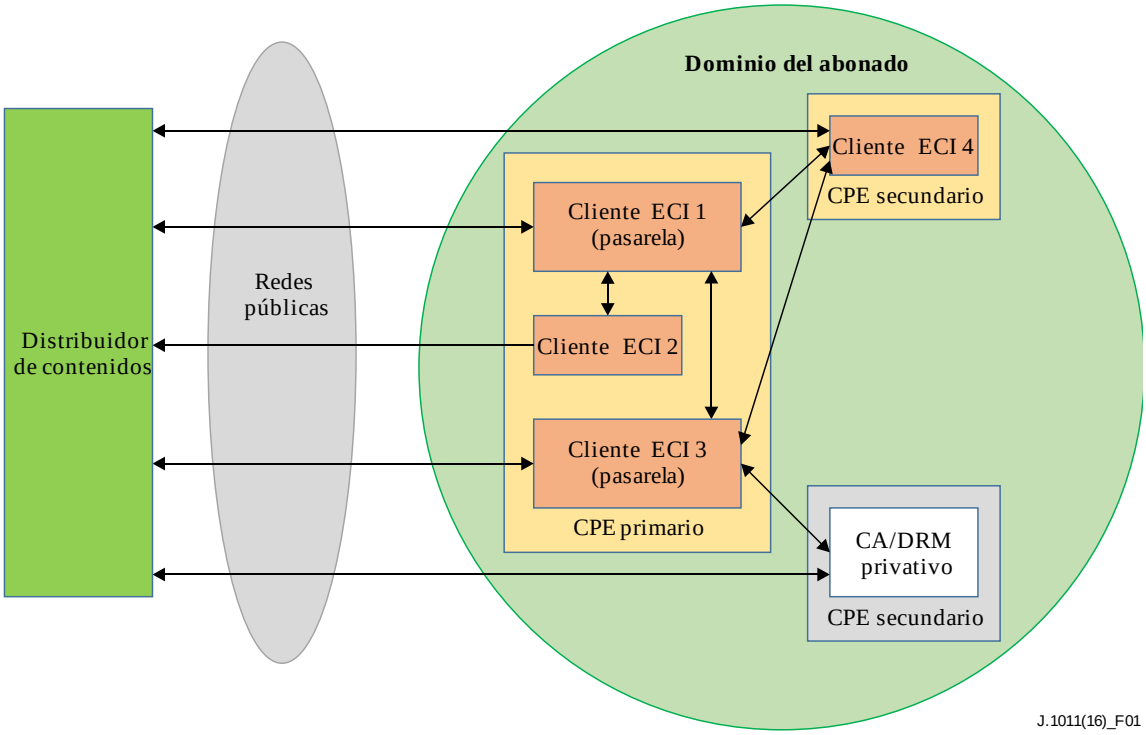


Figura 1 – Clientes ECI en un dominio de un único cliente

La especificación ECI define, entre otras, la interfaz entre el contenedor ECI y el anfitrión ECI. En la Figura 2 se muestra un diagrama de bloques de un CPE con contenedores ECI y las restantes funciones en el anfitrión ECI con las que se comunican o pueden comunicarse los contenedores ECI. Algunas de dichas funciones son facultativas. Durante la instalación de un cliente ECI y durante el arranque de un cliente ECI, el anfitrión especifica las funciones que puede poner a disposición del cliente ECI.

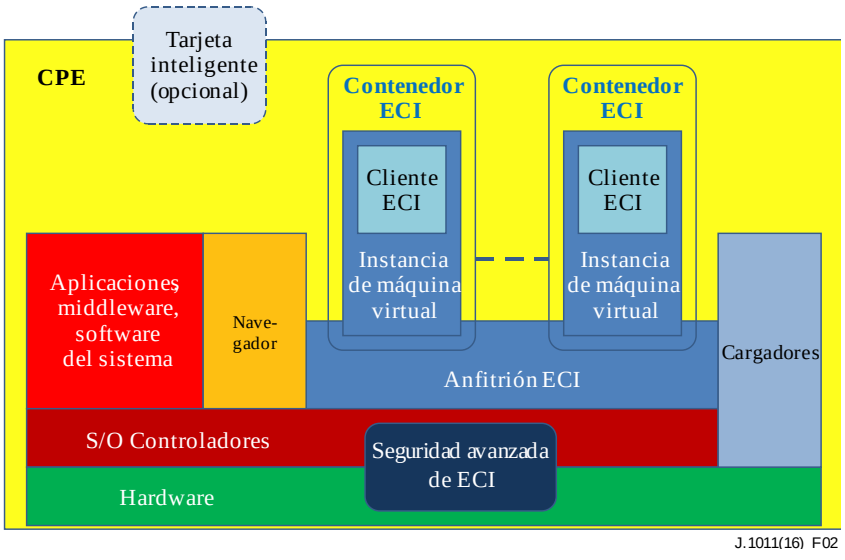


Figura 2 – Diagrama de bloques de un CPE con clientes ECI integrados, cada uno en su contenedor ECI y con su instancia de máquina virtual

En primer lugar, el concepto se basa en un concepto de cargador jerárquico (véase la Figura 3) que consta de un cargador basado en chips, el cargador de software del sistema y el cargador de cliente ECI.

El cargador del anfitrión ECI se encarga de cargar el software del mismo. Ello incluye, además de otros elementos, la máquina virtual, el acceso a componentes de seguridad avanzada y el cargador del cliente ECI. Un anfitrión ECI puede cargar varios clientes ECI en distintas instancias de máquina virtual, que funcionan independientemente y están aisladas unas de otras.

Cuando se carga un cliente ECI en el sistema, se crea una instancia de máquina virtual en la que se carga el cliente ECI. Esta instancia de VM actúa como mecanismo de asilamiento (*sandbox*) entre el cliente ECI y el anfitrión. La interfaz entre el cliente ECI y la instancia de VM es la interfaz fundamental que actualmente se está desarrollando en la especificación de grupo (GS) del ETSI. La interfaz especifica además el flujo de información/protocolo entre múltiples instancias de cliente ECI y hacia otras funcionalidades del CPE, como la seguridad avanzada, la pantalla, etc. Nótese que los restantes clientes ECI no tienen que estar necesariamente en el mismo anfitrión ECI. Esta interfaz y protocolo de comunicación se especifica en [b-ETSI GS ECI 001-3].

El anfitrión ECI depende de la implementación del fabricante. El anfitrión ECI tiene interfaces con el sistema operativo y con la capa de control y proporciona todas las funcionalidades definidas en la especificación de la interfaz de cliente ECI. La ECI no especifica el anfitrión ECI, pero debe ser certificado por la autoridad de confianza a fin de garantizar la conformidad con la especificación de la interfaz del cliente ECI.

6.2.3 Funcionalidades obligatorias de dispositivos conformes con la ECI

La ECI es aplicable a una gama de escenarios de uso (véase la Figura 1). Por tanto, debe de contemplar una amplia gama de dispositivos, que incluyen iDTVs, STBs, grabadoras de vídeo personales (PVR), IPTV, tabletas, teléfonos inteligentes, etc. Los dispositivos tienen capacidades muy diversas y la ECI ofrece un marco de seguridad armonizado. La ECI diferencia entre dispositivos en torno a la TV y dispositivos de otros entornos, entre otros, dispositivos IPTV y tabletas.

Los dispositivos entorno a la TV son dispositivos cuyo conjunto de chips incluye la capacidad de procesamiento de flujos de trasporte MPEG-2. ECI requiere que dichos conjuntos de chips implementen funcionalidades de seguridad avanzadas conformes con ECI (véase 6.2.1 anterior). Los CPE entorno a la TV y conformes con ECI incluirán las funciones recogidas en las especificaciones [b-ETSI GS ECI 001-3], [b-ETSI GS ECI 001-4] y [b-ETSI GS ECI 001-5].

Los dispositivos adaptados a otros entornos, especialmente IPTV, computadoras y tabletas típicamente implementan más funcionalidades en software y se conectan a un canal de comunicaciones IP bidireccional. Ello permite disponer de distintos tipos de mecanismos de seguridad. Puesto que el conjunto de chips utilizados en esos dispositivos incluye hardware para diversas funciones de procesamiento de seguridad, la ECI requiere que los conjuntos de chips implementen funcionalidades de seguridad y robustez basadas en hardware. Las [b-ETSI GS ECI 001-3], [b-ETSI GS ECI 001-4] y [b-ETSI GS ECI 001-5] especifican los mecanismos necesarios para aprovechar dichas funcionalidades.

6.2.4 Interfaces necesarias entre el anfitrión ECI y el cliente ECI

El contenedor ECI es un concepto técnico que combina la VM con el cliente ECI para aislar y proteger a la VM y a la ECI del resto del CPE. La máquina virtual es una funcionalidad del anfitrión ECI. Al cargar un cliente ECI, el anfitrión ECI crea una instancia de máquina virtual. La máquina virtual proporciona las interfaces necesarias con el cliente ECI y las conecta con el anfitrión ECI. La especificación ECI define la interfaz entre la VM y el cliente ECI; véase en la Figura 2 una arquitectura de alto nivel sobre un dispositivo conforme con ECI. La interfaz

proporciona algunas interfaces de programación de aplicaciones (API) y también establece un canal de comunicación seguro.

Se señalan a continuación interfaces software que son importantes:

– Interfaz para la información sobre capacidades del anfitrión ECI al cliente ECI y viceversa.
– Interfaz para el procesado de señales de entrada y de salida del CPE.
– Interfaz con el bloque de hardware/controladores de seguridad avanzada.
– Interfaz con funcionalidades de cargador.
– Interfaz para la interacción con el usuario.
– Interfaz con la funcionalidad de encriptación y desencriptación.
– Interfaz con el lector opcional de tarjetas inteligentes.
– Interfaz con funcionalidades de seguridad específicas, como huellas digitales y marca de agua.
– Interfaz con el almacenamiento local.

La máquina virtual proporciona todas las interfaces del cliente ECI.

Además, también existen protocolos de comunicación sobre las interfaces para comunicación segura. En particular, se especifica un protocolo para la comunicación establecida entre clientes ECI, que puede ser interno o externo.

El CPE puede conectarse a cualquier tipo de red y a varias redes de forma simultánea, de forma unidireccional y bidireccional. No siempre tiene que estar conectado a una red (por ejemplo cuando se trata de contenido descargado o almacenado).

6.2.5 Funcionalidad mínima de la interfaz de usuario y de visualización

El contenedor ECI debe disponer de funciones mínimas de interfaz de usuario (UI) y de visualización en pantalla (OSD) para las comunicaciones con el usuario, tal como se especifica en [b-ETSI GS ECI 001-3]. Se utiliza para mostrar los mensajes al usuario que los ha generado o al que han sido enviados utilizando el sistema de CA/DRM. También se utiliza para permitir que el usuario introduzca información, como un número de identificación personal (PIN). En [b-ETSI GS ECI 001-3] puede encontrarse más información.

El usuario interactúa localmente con el sistema de CA/DRM a través del cliente ECI.

6.2.6 Máquina virtual

El cliente ECI se ejecuta sobre una máquina virtual (VM) normalizada. Este componente se especifica en [b-ETSI GS ECI 001-4]. Cada cliente ECI tendrá su propia instancia de la VM. La instancia de la VM proporciona un entorno seguro para a la ejecución del kernel del acceso condicional o las aplicaciones cliente de Gestión de Derechos Digitales. La VM proporciona APIs a través de las que puede accederse a recursos del entorno del anfitrión ECI de forma normalizada.

6.2.7 Capacidades de seguridad avanzada

La ECI define las funcionalidades de seguridad mínimas necesarias para crear un sistema seguro de protección de contenidos. La ECI requiere mejoras basadas en elementos hardware. En el caso de dispositivos en torno a la TV, ello se logra mediante funciones de seguridad avanzada específicas para TV. Especifica lo que en los sistemas basados en chips (SoC, "*Systems on Chip*") normalmente se denomina "*Key Ladder Block*"(bloque de escalera de claves). Una tarea esencial de la capacidad de seguridad avanzada en proteger las claves de protección de contenidos durante su transporte desde el cliente ECI hasta el sistema de desencriptación de contenidos del CPE o durante la transferencia de contenidos protegidos desde un cliente ECI a otro cliente ECI (véase la Figura 1). El sistema de seguridad avanzada, tal como se especifica en [b-ETSI GS ECI 001-5], soporta varios

flujos de palabras de control simultáneos y varios clientes ECI que simultáneamente solicitan sus servicios. Además, la capacidad de seguridad avanzada juega un papel fundamental en la verificación de la descarga del software del anfitrión y de los clientes ECI.

Los dispositivos para otros entornos, especialmente IPTV, computadoras y tabletas implementan, típicamente, más funcionalidades en software y se conectan a una comunicación IP bidireccional. La ECI especifica los mismos conceptos y mecanismos de seguridad avanzada, pero lo integra de forma diferente en las arquitecturas de seguridad de los dispositivos [b-ETSI GS ECI 001-3], [b-ETSI GS ECI 001-4] y [b-ETSI GS ECI 001-5].

La disponibilidad de la seguridad avanzada en el CPE se comunica al cliente ECI durante su fase de instalación y puesta en funcionamiento.

6.2.8 Realeatorización

El contenido protegido que recibe un CPE conforme con ECI puede no ser consumido inmediatamente. Las funcionalidades siguientes están disponibles en los dispositivos conformes con ECI:

– Almacenamiento local:
  - bajo el control del CPE;
  - bajo el control del cliente CA o DRM.

– Pasarela:
  - entrega de un elemento de contenido protegido a un dispositivo externo bajo el control de un cliente DRM;
  - entrega de un elemento de contenido protegido a otro cliente ECI que está dentro del mismo CPE o se ejecuta en otro CPE conforme con ECI.

Para soportar estas funcionalidades, el dispositivo conforme con ECI puede volver a aleatorizar el contenido. El sistema ECI no especifica los mecanismos de transporte ni las funcionalidades DRM disponibles para almacenar o entregar contenido protegido a otros dispositivos. En [b-ETSI GS ECI 001-5] se definen las interfaces necesarias entre el anfitrión ECI y el cliente ECI.

6.2.9 Funcionalidades del cargador de ECI

Un CPE conforme con ECI dispondrá de funcionalidades de cargador, permitiendo la carga e instalación, así como la integridad y la protección frente a un intento de sustitución de los módulos de software pertinentes del ECI.

Inicialmente, el cargador integrado en el chip carga el cargador de software del sistema. Este cargador integrado garantiza que sólo pueda instalarse y ponerse en funcionamiento un cargador certificado de software del sistema. El cargador de software del sistema incluye el cargador del anfitrión ECI y, por tanto, debe estar firmado por la autoridad de confianza. El cargador de software del sistema puede incluir cargadores de otro software del sistema no relacionado con las funcionalidades ECI y sin relación con los elementos de seguridad del sistema. El software del anfitrión ECI incluye el cargador del cliente ECI que, bajo demanda, puede cargar el cliente ECI.

Durante la instalación en su contenedor ECI, así como durante su puesta en funcionamiento, el cliente ECI es informado por el anfitrión ECI de sus capacidades, tales como grabación, disco duro, lector inteligente de tarjetas, lector de huellas digitales y marca de agua, y de las redes, así como la conformidad con la especificación marco (esta Recomendación) y con [b-ETSI GS ECI 001-3], [b-ETSI GS ECI 001-4] y [b-ETSI GS ECI 001-5] y posiblemente [b-ETSI GS ECI 001-6].

El cargador ECI con las capacidades de seguridad conexas se especifica en [b-ETSI GS ECI 001-3].

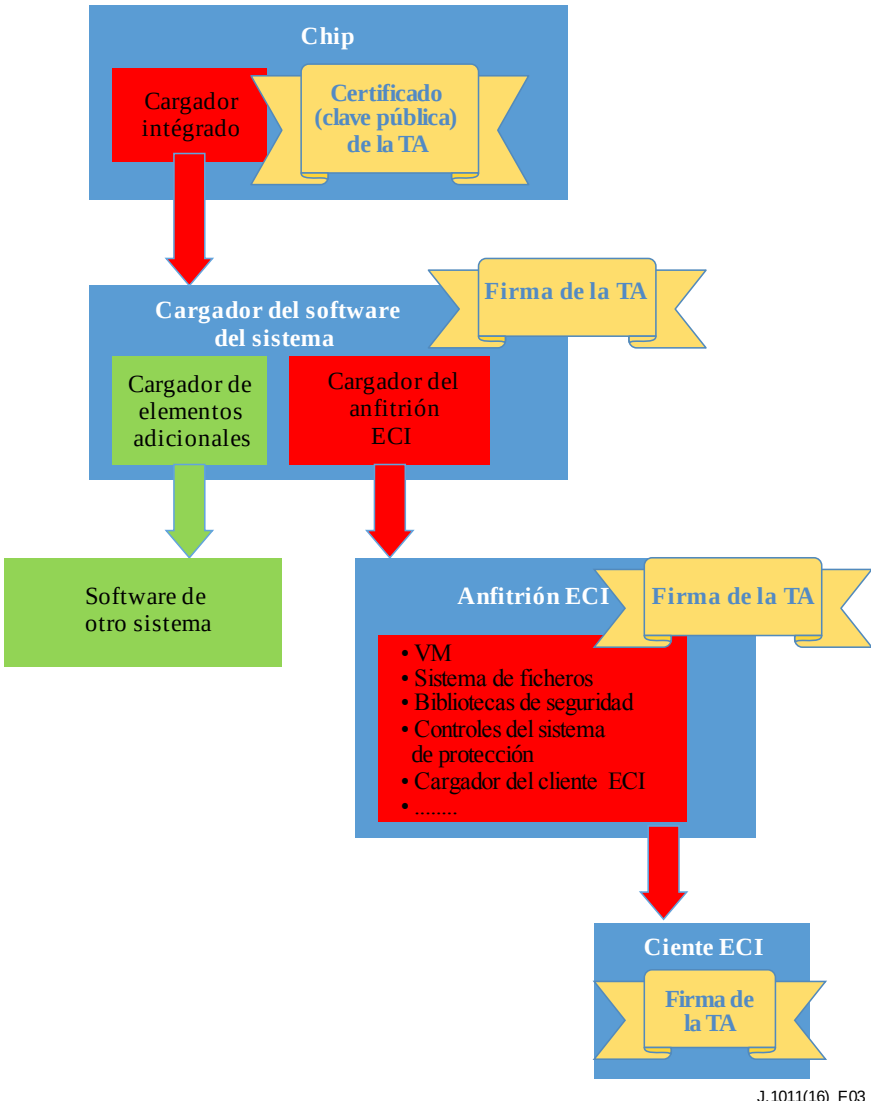


Figura 3 – Concepto jerárquico del cargador

6.2.10 Revocación

La autoridad de confianza puede decidir poner un CPE, un conjunto CPE, un tipo de CPE o todos los CPE de un fabricante en una lista negra. El proveedor de contenidos o el operador puede revocar de su punto de distribución del servicio el CPE o los CPE afectados. Los métodos utilizados permiten a otros operadores y distribuidores de contenidos seguir utilizando dichos CPE en sus servicios si así lo desean.

La revocación puede bloquear todos los servicios, o un subconjunto de ellos, del operador o del proveedor de contenidos al equipo o equipos CPE afectados. Esto forma parte de la funcionalidad del CA o DRM pertinentes y queda fuera del alcance de esta Recomendación.

El proceso de revocación se especifica en [b-ETSI GS ECI 001-3].

7 Entorno de confianza

Para poder establecer un sistema basado en una interfaz común integrada, debe crearse un entorno de confianza. La información detallada acerca del entorno de confianza queda fuera del alcance de las especificaciones ECI. Sin embargo, los principios que se especifican en [b-ETSI GS ECI 001-6] son esenciales para entender plenamente cómo funciona la ECI.

La autoridad de confianza (TA) es una organización que rige las normas y la regulación para la implementación de la arquitectura ECI. La autoridad de confianza debe ser una entidad jurídica para

poder ejercer demandas legales. La autoridad de confianza debe ser imparcial para todos los agentes del ecosistema CA/DRM descargable. Ello incluye a:

– fabricantes de CPE;
– fabricantes de CA/DRM (cliente ECI);
– fabricantes de chips, cuyos componentes incluyen claves y certificados de procesador seguro intercambiables, necesarios para la interacción entre el anfitrión y un sistema que sea conforme a CA/DRM;
– operadores de plataformas; el operador de plataforma es la parte que controla todos los elementos necesarios de un sistema CA/DRM. Los operadores de plataforma pueden ser proveedores de servicio u operadores de red;
– proveedores de aplicaciones, si procede.

La tercera parte de confianza (TTP, *Trusted Third Party*) es un proveedor de servicio técnico que emite certificados y claves para fabricantes cuyos productos son conformes con los componentes de un sistema ECI. La autoridad de confianza (TA) garantiza la confianza en dichas claves y certificados y mantiene la raíz de confianza.

La autoridad de confianza y la tercera parte de confianza constituyen la base de la cadena de confianza y, por tanto, participan en todo el proceso, desde la producción (chips y CPE), pasando por las operaciones (descarga y activación de un cliente ECI seguro), hasta las medidas de control (por ejemplo, revocación).

Como entidad jurídica, la autoridad de confianza garantiza el funcionamiento del entorno de confianza a través de un marco contractual conocido como Acuerdo de licencia, bajo el cual las diversas partes involucradas asumen sus responsabilidades y obligaciones. En virtud del Acuerdo de licencia, la autoridad de confianza/tercera parte de confianza generan y emiten pares de claves, certificados, credenciales de prueba e ID de operadores, etc.

Una TA establece un vínculo de confianza entre todos los participantes del mercado. No puede existir otra TA que establezca la confianza "por segunda vez" para el mismo entorno. Sin embargo, puede haber múltiples TA, por ejemplo, por país o región, segmentos o ecosistemas.

Si existen varias TA en paralelo, es prerrequisito necesario la confianza mutua entre la TA A y la TA B para que los dispositivos registrados en la TA A puedan ser utilizados en el dominio de la TA B.

7.1 Flujos de trabajo operacionales necesarios

En esta cláusula se presenta una visión general de los flujos de trabajo operacionales necesarios para responder a las necesidades de los distintos partícipes del mercado a fin de poner en marcha un negocio basado en la tecnología ECI. Además, dichos flujos de trabajo se basan en los elementos técnicos esenciales necesarios para la implementación de un sistema ECI. En la Figura 4 se muestran las interacciones entre los componentes técnicos y los partícipes del mercado pertinentes.

Observación: la descripción es genérica y no pretende reflejar ninguna solución privativa existente o alguna actividad de normalización en curso.

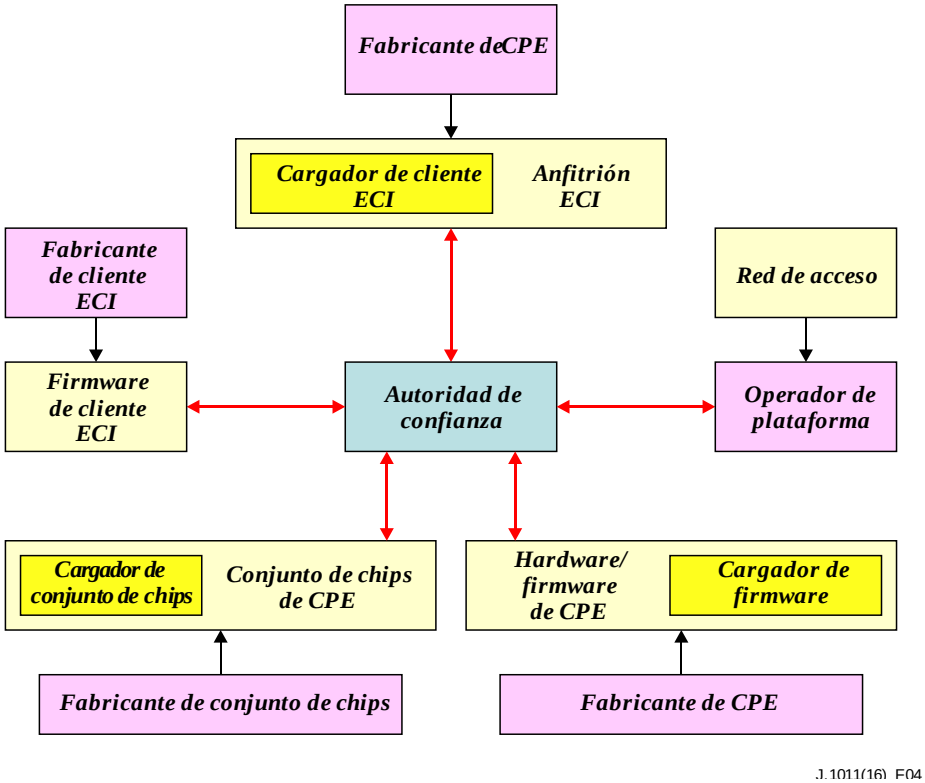


Figura 4 – Gestión de la confianza necesaria entre la autoridad de confianza (TA) y los agentes participantes en el mercado

Los aspectos operacionales y contractuales (véanse las flechas rojas en la Figura 4) del entorno de confianza son los siguientes:

1) Integridad

Significa que un partícipe del mercado puede verificar que un componente hardware o software proporcionado por otro partícipe del Mercado no ha sido modificado por una parte no autorizada y cumple las especificaciones y normas de robustez. Este requisito puede satisfacerse mediante las adecuadas credenciales y firmas y los procedimientos de prueba basados en credenciales de prueba proporcionadas por la autoridad de confianza/tercera parte de confianza.

2) Autenticidad

Autenticidad significa que cualquier componente hardware/software de un asociado contractual TA y que ha superado la necesaria verificación y pasos de certificación, puede estar vinculado al asociado contractual y, por tanto, ser distinguible de cualquier componente clonado. El sistema ECI analiza la autenticidad de cualquier hardware/software de interés.

3) Marco contractual

El marco contractual que establece la autoridad de confianza como entidad jurídica cumplirá las condiciones de conformidad y robustez y los procedimientos de certificación a fin de proporcionar el entorno necesario para el establecimiento de sistemas ECI.

4) Medidas de subsanación

En caso de que los componentes hardware o software de un sistema ECI dejen de ser conformes, la autoridad de confianza establece procedimientos para el proveedor de dicho componente dirigidos a restablecer la integridad del ecosistema en un plazo razonable.

Los componentes técnicos esenciales (cajas amarillas de la Figura 4) son:

1) Conjunto de chips del CPE

   El conjunto de chips del CPE es el componente principal del hardware del CPE que normalmente incluye sistema en chip (SoC ("*system on chip*")) debido a los requisitos impuestos a los operadores de plataformas y proveedores de contenidos. Además, normalmente el cargador de chips está incluido en los chips del CPE.

2) Hardware del CPE

   La implementación segura del conjunto de chips del CPE, la prevención de accesos no autorizados a los elementos de almacenaje (memorias flash, ROM) y la protección de las interfaces son aspectos esenciales.

3) Cargadores diversos

   El cargador de chips descarga otros cargadores adicionales en función de la configuración hardware/software del CPE.

4) Firmware del CPE

   El firmware del CPE está sujeto a interacciones con el cliente ECI y con todas las interfaces hardware pertinentes del CPE. Las especificaciones detalladas, una adecuada conformidad y las reglas de robustez garantizan la seguridad.

5) Cliente ECI

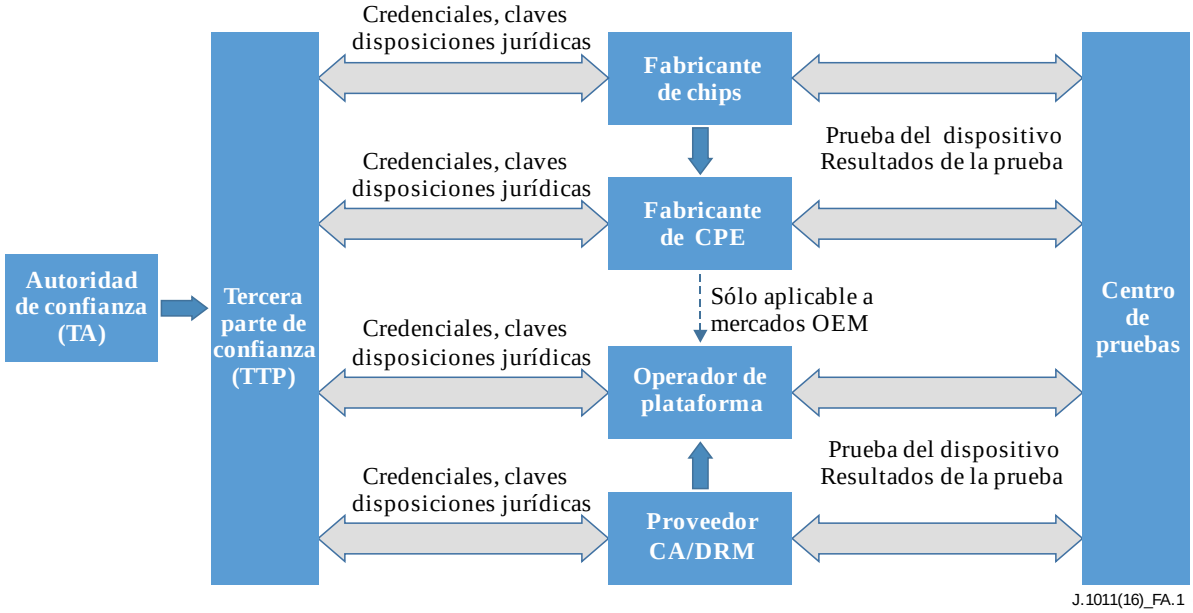
   El cliente ECI extrae toda la información de los CA y DRM que entregan los elementos frontales del CPE y realiza los ajustes necesarios en el CPE (desaleatorizador, interfaces), que obviamente precisa una interacción estrecha y segura con el firmware del CPE.

Apéndice I

Realización de un sistema de confianza que sea conforme una ECI

(El presente apéndice no forma parte integrante de esta Recomendación.)

En este Apéndice I se presenta una visión general de los flujos de trabajo operacionales necesarios que responden a las necesidades de distintos partícipes del mercado para implementar un negocio basado en la tecnología ECI. La Figura I.1 muestra una visión global del flujo de trabajo general. Además, dichos flujos de trabajo se basan en los elementos técnicos esenciales necesarios para la implementación de un sistema ECI. La Figura 4 de la cláusula 7.1 muestra esas interacciones entre los componentes técnicos y los partícipes pertinentes del mercado.



NOTA – La tercera parte de confianza (TTP) y el centro de prueba son asociados contractuales de la autoridad de confianza (TA) para los procesos de certificación y emisión de claves.

Figura I.1 – Visión general del flujo de trabajo

Marco jurídico/contractual

La gestión de la confianza en la seguridad sólo puede realizarse en un marco jurídico y contractual claramente definido, en el que el acuerdo de licencia (LA) sea el elemento fundamental. La autoridad de confianza proporciona un acuerdo de licencia a todo aquél que desee implementar la especificación o las especificaciones, ya sea fabricante del CPE, vendedor de sistemas CA/DRM, fabricante de chips, proveedores de otras tecnologías, operadores de plataformas, etc.

Por tanto, el acuerdo de licencia es el instrumento esencial para que la autoridad de confianza cree, mantenga y ponga a disposición del mercado horizontal un método seguro pero de fácil uso para recibir y poner en funcionamiento todas las claves necesarias y otros recursos e información relativos a la seguridad cuando los CPE se conectan a los proveedores seleccionados que se ajustan a las normas de utilización pertinentes. Igualmente, el marco del acuerdo de licencia permite a la autoridad de confianza tomar la medida de revocación que sea necesaria de todo el material de seguridad cuando el proveedor desconecta a un consumidor, en la medida que sea técnica y económicamente posible.

El acuerdo de licencia permite la aplicación coordinada y consistente de todos los restantes elementos del marco contractual como la especificación técnica, reglas de conformidad y robustez, obligaciones y responsabilidades, prueba y certificación, orientaciones para la implementación, etc.

La Figura I.2 muestra los componentes del acuerdo de licencia.

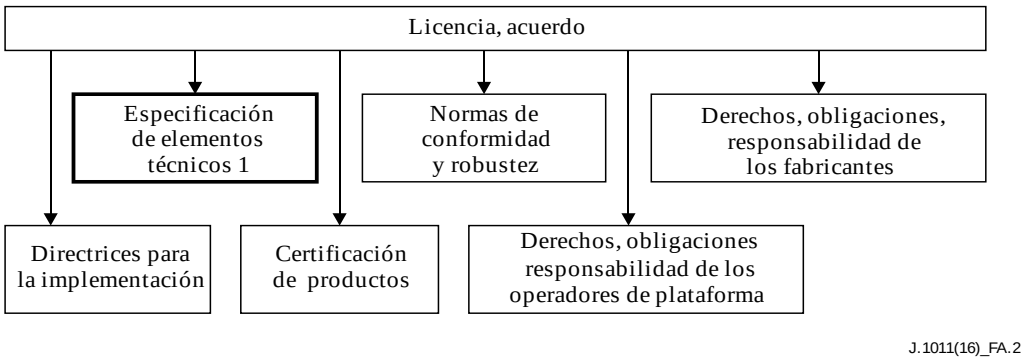


Figura I.2 – Componentes del acuerdo de licencia

Estas especificaciones serán desarrolladas como especificaciones de grupo por el Grupo de Normalización de la Industria sobre ECI del ETSI (ETSI ISG ECI).

Bibliografía

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

[b-CENELEC EN 50221] CENELEC EN 50221 (1997), *Common Interface Specification for Conditional Access and other Digital Video Broadcasting Decoder Applications.*

[b-CI Plus Specification] CI Plus Specification (V1.3.1) (2011), *Content Security Extensions to the Common Interface*.

[b-ETSI EN 300 468] ETSI EN 300 468 V1.13.1 (2012), *Digital Video Broadcasting (DVB); Specification for Service Information (SI) in DVB systems*.

[b-ETSI ISG ECI] ETSI ISG ECI White Paper (2014), *Industry Specification Group on Embedded Common Interface for exchangeable CA/DRM solutions*. www.etsi.org/deliver/etsi.../ECI/.../gs_ECI00101v010101p.pdf

[b-ETSI TS 101 699] ETSI TS 101 699 V1.1.1 (1999), *Digital Video Broadcasting (DVB); Extensions to the Common Interface Specification*. http://webstore.ansi.org/RecordDetail.aspx?sku=ETSI+TS+101+699-v1.1.1-1999-11

[b-ETSI TS 103 162] ETSI TS 103 162 V1.1.1 (2010), *Access, Terminals, Transmission and Multiplexing (ATTM); Integrated Broadband Cable and Television Networks; K-LAD Functional Specification*.

[b-ETSI TS 103 205] ETSI TS 103 205 V1.1.1 (2014), *Digital Video Broadcasting (DVB); Extensions to the CI PlusTM Specification*.

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, 2018