Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

J.1015.1

(04/2020)

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 integrada (ECI) para soluciones CA/DRM intercambiables:

El sistema de seguridad avanzada – Bloque de escalera de claves: Autentificación de la información de reglas de utilización de palabra de control y datos conexos 1

Recomendación UIT-T J.1015.1

Unión Internacional de Telecomunicaciones

Recomendación UIT-T J.1015.1

Interfaz común integrada (ECI) para soluciones CA/DRM intercambiables: El sistema de seguridad avanzada – Bloque de escalera de claves: Autentificación de la información de reglas de utilización de palabra de control y datos conexos 1

Resumen

La Recomendación UIT-T J.1015.1 forma parte de un conjunto de publicaciones que abarca el bloque de escalera de claves del sistema de seguridad avanzada para la interfaz común integrada a los efectos de la especificación de soluciones intercambiables de acceso condicional/gestión de derechos digitales (CA/DRM).

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T J.1015.1	2020-04-23	9	11.1002/1000/13837

Palabras clave

AC, acceso condicional, DRM, gestión de derechos digitales, intercambio.

* 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

El objetivo de esta Recomendación[1] es facilitar la interoperabilidad y la competencia en los servicios de comunicaciones electrónicas y, en particular, en el mercado de los dispositivos de radiodifusión y audiovisuales. Sin embargo, existen otras tecnologías disponibles que también pueden resultar adecuadas y beneficiosas, en función de las circunstancias de los Estados Miembros.

Los proveedores de contenido encriptan su contenido digital y utilizan un **sistema de protección de contenido**[2] para protegerlo contra el acceso no autorizado. Los consumidores emplean un **receptor de contenido** para acceder al contenido protegido. Para ello, el **receptor de contenido** está dotado con un chip que ejecuta una o más operaciones de desencriptación del contenido. Se utiliza un protocolo de establecimiento de clave criptográfica para asegurar el transporte de las claves de desencriptación del contenido del **sistema de protección del contenido** al chip. En la presente Recomendación, los pasos del protocolo que se ejecutan en el chip se denominan escalera de claves.

La escalera de claves y el protocolo también pueden utilizarse para asegurar el transporte de las claves de encriptación del contenido al chip. Esas claves se utilizan cuando el contenido se vuelve a encriptar en el chip. El chip puede ejecutar una o más operaciones de encriptación para tal fin. La grabación de vídeos personales y la exportación de contenido protegido a un **sistema de protección de contenido** diferente son ejemplos típicos de reencriptación del contenido. En esta Recomendación, las claves de desencriptación del contenido y las claves de encriptación del contenido se denominan **palabras de control (CW)**.

En esta Recomendación también se especifica un mecanismo de autenticación, que está estrechamente relacionado con la escalera de claves y puede utilizarse para la autenticación de entidades; es decir, este mecanismo puede utilizarse para autentificar el chip.

La escalera de claves y el mecanismo de autenticación especificados en esta Recomendación son independientes tanto del **sistema de protección del contenido** como del **proveedor de contenido,** lo que permite al **proveedor de contenido** utilizar cualquier **sistema de protección del contenido** conforme; y al consumidor utilizar el **receptor de contenido** para acceder al contenido de cualquier **proveedor de contenido** que utilice un **sistema de protección del contenido** conforme.

Una **autoridad de certificación** gestiona el certificado de clave pública de cada chip en los mecanismos especificados en este documento. Concretamente, la **autoridad de certificación** distribuye esos certificados y la información de revocación de certificado a los **proveedores de contenido** que desean utilizar la escalera de claves y/o el mecanismo de autenticación. A continuación, los **proveedores de contenido** alimentan sus **sistemas de protección del contenido** con esos certificados e información de revocación de certificados. Como se detalla en la cláusula 7 de [UIT-T J.1015]; el conocimiento de la clave pública del certificado de un chip permite al **sistema de protección del contenido** generar mensajes de entrada adecuados para la escalera de claves y el mecanismo de autenticación del chip.

---

1 En el Apéndice II se indican varios aspectos susceptibles de mejora.

2 La letra negrita en el texto de esta Recomendación indica términos con definiciones específicas para el contexto de la interfaz común integrada que pueden diferir del uso común.

Recomendación UIT-T J.1015.1

Interfaz común integrada (ECI) para soluciones CA/DRM intercambiables: El sistema de seguridad avanzada – Bloque de escalera de claves: Autentificación de la información de reglas de utilización de palabra de control y datos conexos 1

1 Alcance

En la presente Recomendación se especifica el bloque de escalera de claves para su utilización en un chip de **receptor de contenido**. El bloque de escalera de claves está formado por una escalera de claves para asegurar el transporte de las **palabras de control** (CW) al chip y un mecanismo de autenticación. En esta Recomendación se especifican también los aspectos de la personalización de un chip conforme.

La presente Recomendación está destinada a los fabricantes de chips.

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. En esta Recomendación, la referencia a un documento autónomo no le otorga, como documento independiente, el rango de Recomendación.

[UIT-T J.1015] Recomendación UIT-T J.1015 (2020), *Interfaz común integrada (ECI) para soluciones CA/DRM intercambiables: El sistema de seguridad avanzada – Bloque de escalera de claves*

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 autoridad de certificación: Parte que se encarga de gestionar los certificados de clave pública en un **ecosistema ECI** (interfaz común integrada). Todas las demás partes del sistema confían en la autoridad de certificación para realizar las operaciones relacionadas con los certificados.

3.2.2 ID de chip: Número no secreto que se utiliza para identificar un chip.

3.2.3 sistema de protección del contenido: Sistema de un **ecosistema ECI** que emplea técnicas criptográficas para gestionar el acceso a los contenidos y servicios. Con frecuencia este término es equivalente a sistema de protección del servicio. Los sistemas de este tipo suelen ser sistemas de acceso condicional (CA) o sistemas de gestión de derechos digitales (DRM).

3.2.4 proveedor de contenido: Parte que distribuye contenido digital a un **receptor de contenido** en un **ecosistema ECI**.

3.2.5 receptor de contenido: Dispositivo que se emplea para acceder a contenido digital dentro de un **ecosistema ECI**. El **receptor de contenido** contiene un chip con el **desaleatorizador de contenido**.

3.2.6 desaleatorizador de contenido: Componente del chip de un **ecosistema ECI** capaz de desencriptar el contenido. El desaleatorizador de contenido también puede ser capaz de encriptar el contenido (para volver a encriptarlo). En esta Recomendación la encriptación/desencriptación del contenido utiliza un **esquema de encriptación simétrico**. En el caso del contenido MPEG-2, la encriptación y desencriptación del contenido se denominan también aleatorización y desaleatorización, respectivamente.

3.2.7 palabra de control: Clave secreta utilizada para encriptar y desencriptar el contenido dentro de un **ecosistema ECI**. En los sistemas de gestión de derechos digitales, la palabra de control suele denominarse clave de contenido.

3.2.8 función hash criptográfica: Función criptográfica sin claves en un ecosistema de ECI que acepta como entrada datos de tamaño arbitrario, denominado mensaje, y genera un bloque de datos de salida de tamaño fijo, denominado resumen del mensaje. En esta Recomendación se supone que la función hash criptográfica tiene la propiedad de comportarse como una función aleatoria y es resistente a la segunda imagen previa.

3.2.9 esquema de firma digital: Esquema criptográfico asimétrico con claves que se utiliza para proteger la autenticidad de los datos en un **ecosistema ECI**. Consiste en un algoritmo de generación de claves, una operación de generación de firmas y una operación de verificación de firmas. Las claves se generan por pares (clave secreta/privada, clave pública). Los datos se firman utilizando una clave secreta/privada y la correspondiente clave pública se utiliza para verificar la firma. El **esquema de firma digital** especificado en la presente Recomendación se utiliza para proteger la autenticidad de los mensajes definidos en [b-ROEL]; cabe señalar que en la presente Recomendación no se utiliza este esquema para proporcionar el no repudio o la autenticación del origen.

3.2.10 ecosistema ECI: Una operación comercial que consiste en una autoridad de confianza y varias plataformas y un equipo conforme a ECI instalado en locales del cliente en el terreno.

4 Abreviaturas y acrónimos

En esta Recomendación se utilizan las siguientes abreviaturas y acrónimos:

AD1 Datos Asociados 1 (*associated data 1*)

AK Clave de autenticación (*authentication key*)

CA Acceso condicional (*conditional access*)

CW Palabra de control (*control word*)

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

ECI Interfaz común integrada (*embedded common interface*)

ID Identidad (*IDentity*)

LK Clave de enlace (*link key*)

SHA Algoritmo hash seguro (*secure hash algorithm*)

SPK Clave pública del emisor (*sender public key*)

SSK Clave secreta/privada del emisor (*sender secret/private key*)

T Etiqueta (*Tag*)

URI Información de reglas de utilización (*usage rules information*)

5 Convenios

En la presente Recomendación, cuando un término va en negrita indica que tiene un significado específico en el contexto de la interfaz común integrada y que puede ser diferente de la utilización habitual de ese término.

6 Autentificación de la información sobre las reglas de utilización de la palabra de control y datos asociados 1

En lo que respecta a los detalles de especificación en la cláusula 7 de [UIT-T J.1015], se especifican varias entradas al bloque de escalera de claves, entre las que cabe destacar: CW-URI, AD1, τ_b, SPK-URI, SPK, LK encriptada, ID de chip firmado, etc. Algunas de estas entradas, como la LK y el ID de chip, se transmiten encriptadas y se aplican con un esquema de firma digital. Por otra parte, CW-URI, AD1, τ_b, SPK-URI y SPK se transmiten sin que se les apliquen esquemas criptográficos. La autenticación de estas entradas se basa en la autentificación implícita; en caso de que se proporcione un valor no auténtico para cualquiera de las entradas de la escalera de claves, el cálculo dará un valor inválido de CW y el contenido no se podrá desaleatorizar debidamente.

Un emisor puede enviar SPK, SPK-URI y τ_b sin aplicar esquemas criptográficos habida cuenta de las características de las entradas. Concretamente, es posible verificar τ_b siguiendo rutinas de verificación de Datos Asociados, por lo que ya no se les aplica un esquema de autenticación.

En caso necesario, los proveedores de servicios pueden introducir un método adicional de autentificación explícita para las entradas CW-URI y AD1 del bloque de la escalera de claves. Esa funcionalidad podría mejorar la conveniencia para los usuarios, y aportar ventajas operativas para los proveedores de servicios.

En esta Recomendación se especifica la aplicación de un esquema de autenticación a CW-URI y AD1 cuando son entradas para el bloque de escalera de claves. Para ello se puede aplicar un esquema de firma digital que ya se utiliza para ID de chip || E(SPK, LK) con SSK. Los operadores de servicio pueden optar por autentificar CW-URI, AD1 o ambas al mismo tiempo.

Si los operadores de servicio quieren proteger CW-URI y/o AD1, se deberá utilizar el esquema especificado en esta Recomendación.

Véase la Figura 1.

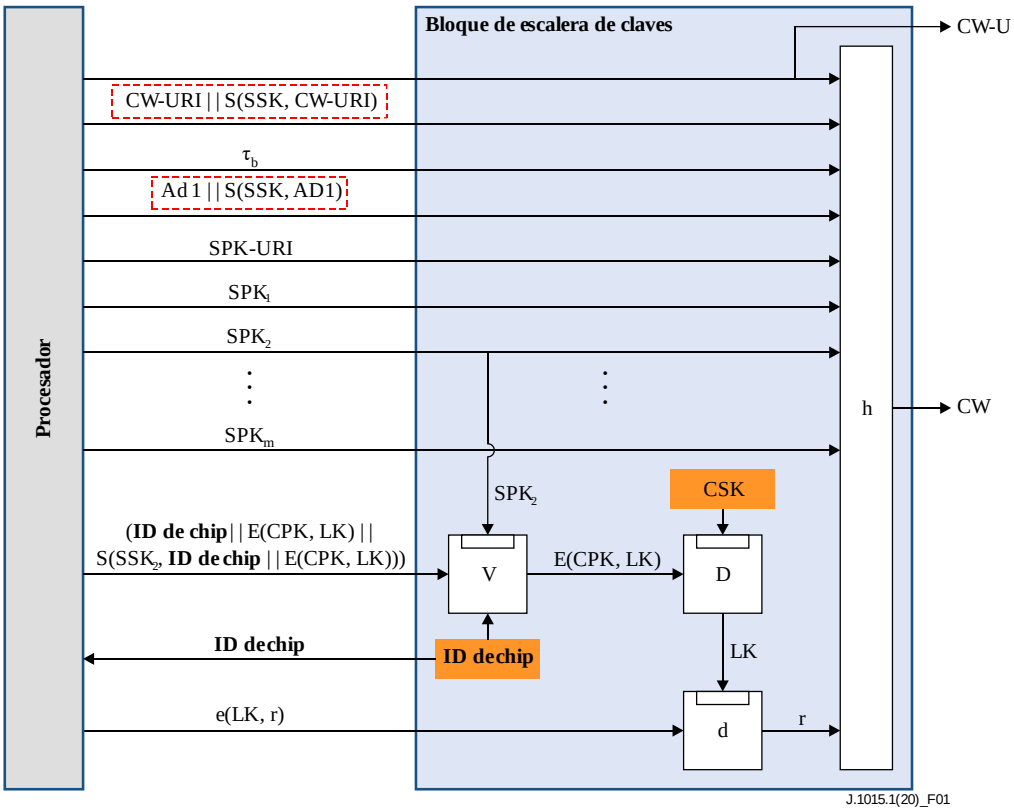

Figura A.1 – Autenticación de la información sobre las reglas de utilización de la palabra de control y datos asociados

6.1 Autenticación de la información sobre las reglas de utilización de la palabra de control

Calcular CW-URI ||firma (emisor)

1) Firmar la cadena de bits CW-URI utilizando la SSK_i. La firma está denotada por S(SSK_i, CW-URI).

2) Añadir esta firma a la cadena de bits CW-URI.

Extraer CW-URI (bloque de escalera de claves)

1) Comprobar la longitud de los datos de entrada. Si la longitud de la CW-URI es de 64 bits, el bloque de escalera de claves ejecutará el proceso normal definido en la cláusula 7.3.1 de [UIT-T J.1015] y abortará el proceso de autenticación de la CW-URI. En caso contrario, es decir, si la longitud es superior a 64 bits, aplicar el proceso de autenticación de la CW-URI y pasar a la etapa siguiente.

2) Comprobar si la SPK-URI y la regla de utilización, definida en la cláusula 7.3.2 de [UIT-T J.1015], permiten que V utilice SPK_i para verificar la firma. De no ser así, el bloque de escalera de claves abortará el cálculo.

3) Utilizar la (CW-URI ||firma) recibida y la SPK_i para verificar la firma. Si la firma no es válida, el bloque de escalera de claves abortará el cálculo.

4) Extraer la CW-URI.

6.2 Autenticación de datos asociados 1

Calcular AD1 ||firma (emisor)

1) Firmar la cadena de bits AD1 utilizando SPK_i. La firma se denota mediante S(SPK_i, AD1).

2) Añadir esta firma a la cadena de bits AD1.

Extraer datos asociados 1 (bloque de escalera de claves)

1) Comprobar la longitud de los datos de entrada. Si la longitud de AD1 es de 256 bits, el bloque de escalera de claves ejecutará el proceso normal definido en la cláusula 7.3.1 de [UIT-T J.1015] y abortará el proceso de autenticación de AD1. En caso contrario, es decir, si la longitud es superior a 256 bits, aplicar el proceso de autenticación de AD1 y pasar a la etapa siguiente.
2) Comprobar si la SPK-URI y la regla de utilización, definida en la cláusula 7.3.2 de [UIT-T J.1015], permiten que V utilice SPK_i para verificar la firma. De no ser así, el bloque de escalera de claves abortará el cálculo.
3) Utilizar la (AD1 ||firma) recibida y la SPK_i para verificar la firma. Si la firma no es válida, el bloque de escalera de claves abortará el cálculo.
4) Extraer AD1.

Apéndice I

Aspectos que se han de mejorar

(Este Apéndice no forma parte integrante de la presente Recomendación.)

Se ha llegado a la conclusión de que es necesario mejorar y validar la presente Recomendación para que cumpla los requisitos estipulados en [UIT-T J.1010] y que [UIT-T J.1010] debe actualizarse para incorporar los requisitos de la especificación de protección mejorada del contenido (ECP) de MovieLabs [b ECP]. Las Recomendaciones [b-UIT-T J.1011], [UIT-T J.1012], [b-UIT-T J.1013], [b-UIT-T J.1014], [b-UIT-T J.1015] y [b-UIT-T J.1015.1] deben actualizarse en el futuro para incorporar esas modificaciones de la [UIT-T J.1010].

Varios Estados Miembros de la UIT y otras partes interesadas de diversas industrias –incluidos fabricantes de dispositivos y componentes electrónicos, los propietarios y titulares de contenido protegido por derecho de autor, proveedores de servicios de televisión por satélite (OTT) y de televisión por cable, y los proveedores de soluciones de sistemas de acceso condicional (CAS) y de gestión de derechos digitales (DRM)– de todo el mundo han expresado su preocupación por el hecho de que la interfaz común integrada (ECI) no satisface plenamente los requisitos de la ECP ni los requisitos más amplios de protección del contenido de la industria.

Más concretamente, sus preocupaciones se plantearon en las contribuciones a la reunión de la Comisión de Estudio 9 (CE 9) del UIT-T (16 a 23 de abril de 2020). En las contribuciones de Israel, Australia, el Miembro de Sector del UIT-T Samsung, y los Asociados de la CE 9, Sky Group y MovieLabs, se propuso la introducción de diversas modificaciones en las Recomendaciones sobre ECI, pero no se llegó a un acuerdo al respecto. Estas modificaciones se consignaron en [b-SG9 Report 17 Ann.1].

Las propuestas tienen por objeto:

1) simplificar el sistema ECI reduciendo su alcance;
2) eliminar el DRM;
3) eliminar la recodificación del contenido;
4) eliminar la gestión de software;
5) añadir API para el almacenamiento seguro y las operaciones criptográficas;
6) permitir escalas de claves específicas para cada proveedor;
7) utilizar los requisitos de la norma UIT-T J.1207 TEE;
8) incluir la implementación de la TEE para la VM;
9) mejorar la robustez de los algoritmos criptográficos, por ejemplo, utilizando SHA-384;
10) utilizar certificados normalizados, como los de la Recomendación UIT-T X.509;
11) reconsiderar las comunicaciones entre clientes;
12) realizar declaraciones de coordinación adicionales con el ETSI;
13) realizar revisiones adicionales por pares;
14) analizar alternativas al modelo de autoridad fiduciaria;
15) definir más detalladamente los aspectos técnicos de las normas de cumplimiento y robustez de ECI;
16) añadir requisitos de diversidad, por ejemplo, la aleatorización del espacio de direcciones;
17) añadir requisitos para verificar la integridad en tiempo de ejecución.

Estas propuestas responden a que la protección de contenidos y las amenazas de su compromiso evolucionan continuamente. La ECI fue concebida originalmente casi una década antes de que se aprobara esta Recomendación UIT-T. Los sistemas como la ECI han de evaluarse regularmente respecto del estado actual de la técnica tanto en lo relativo a las técnicas analíticas como a los requisitos de protección de la industria.

Existen otros mecanismos que permiten la interoperabilidad. En particular, en el caso de la utilización de DRM, la mayoría de los servicios de vídeo por Internet han desplegado otras soluciones que ofrecen interoperabilidad y satisfacen sus necesidades.

Es importante que haya una mayor claridad, por cuanto muchos Estados Miembros consideran que las normas de la UIT tienen gran influencia en el desarrollo de sus mercados e industrias. La lista de preocupaciones garantiza la implementación de ECI en sus mercados nacionales, lo que puede requerir comprender plenamente las repercusiones de la presente Recomendación UIT-T y velar por que se tomen en consideración dichas cuestiones cuando se examine la legislación o la reglamentación o cuando las necesidades del mercado exijan que los aparatos de televisión digital de consumo sean interoperables. También garantiza que los fabricantes de equipo tecnológico, que pueden preferir utilizar un conjunto único de requisitos u otras normas a la hora de diseñar los productos, puedan tener en cuenta estas cuestiones al desarrollar productos para diferentes mercados.

Bibliografía

[b-UIT-T J.1010] Recomendación UIT-T J.1010 (2016), *Interfaz común integrada para soluciones CA/DRM intercambiables; casos y requisitos de utilización.*

[b-UIT-T J.1011] Recomendación UIT-T J.1011 (2016), *Interfaz común integrada para soluciones CA/DRM intercambiables: El sistema de seguridad avanzada; arquitectura, definiciones y visión general*.

[b-UIT-T J.1012] Recomendación UIT-T J.1012 (2020), *Interfaz común integrada para soluciones CA/DRM intercambiables; contenedor, cargador, interfaces y revocación CA/DRM*.

[b-UIT -T J.1013] Recomendación UIT-T J.1013 (2020), *Interfaz común integrada para soluciones CA/DRM intercambiables; La máquina virtual*.

[b-UIT-T J.1014] Recomendación UIT-T J.1014 (2020), *Interfaz común integrada para soluciones CA/DRM intercambiables; Seguridad avanzada – Funcionalidades específicas ECI*.

[b-SG9 Report 17 Ann.1] Informe de la reunión de la CE 9 del UIT-T, SG9-R17-Anexo 1 (2020), Anexo 1 al Informe 17 de la reunión virtual de la CE 9 celebrada del 16 al 23 de abril de 2020.
https://www.itu.int/md/T17-SG09-R-0017/en

[b-ECP] MovieLabs Specification for Enhanced Content Protection – Version 1.2 Available at:
https://movielabs.com/ngvideo/MovieLabs_ECP_Spec_v1.2.pdf

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, 2020