Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

J.1015

(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

Recomendación UIT-T J.1015

Unión Internacional de Telecomunicaciones

Recomendación UIT-T J.1015

Interfaz común integrada (ECI) para soluciones CA/DRM intercambiables; El sistema de seguridad avanzada – Bloque de escalera de claves

Resumen

La presente Recomendación 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).

Esta Recomendación del UIT-T es una transposición de la norma [b-ETSI GS ECI 001-5-2], y es el resultado de la colaboración entre la CE 9 del UIT-T y el ISG ECI del ETSI.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T J.1015	2020-04-23	9	11.1002/1000/13576

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 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/.

© UIT 2020

Reservados todos los derechos. Ninguna parte de esta publicación puede reproducirse por ningún procedimiento sin previa autorización escrita por parte de la UIT.

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 Abreviaturas y acrónimos 3
5 Convenios 4
6 ID de chip y par de claves maestras del chip 4
7 Escalera de claves 5
7.1 Generalidades 5
7.2 Cálculos de la escalera de claves 7
7.3 Información de reglas de utilización 8
7.4 Capas de claves adicionales 10
7.5 Datos Asociados 2 11
8 Mecanismo de autenticación 12
8.1 Generalidades 12
8.2 Cálculos del mecanismo de autenticación 13
9 Primitivas de conversión de datos 14
9.1 BS2OSP 14
9.2 OS2BSP 14
9.3 I2BSP 15
10 Operaciones criptográficas 15
10.1 Esquema de encriptación simétrica 15
10.2 Esquema de encriptación con clave pública 15
10.3 Esquema de firma digital 16
10.4 Función h 16
10.5 Algoritmo de código de autenticación de mensaje 17
Apéndice I – Aspectos que se han de mejorar 18
Bibliografía 20

Introducción

Esta Recomendación del UIT-T[1] es una transposición de la norma [b-ETSI GS ECI 001-5-2], y es el resultado de la colaboración entre la CE 9 del UIT-T y el ISG ECI del ETSI.

El objetivo de esta Recomendación 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, en la que se especifica una escalera de claves para el protocolo de establecimiento de claves definido en [b-ROEL].

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**.

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; 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 I 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

Interfaz común integrada (ECI) para soluciones CA/DRM intercambiables; El sistema de seguridad avanzada – Bloque de escalera de claves

1 Alcance

En el presente documento 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** 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.

[IETF RFC 8017] IETF RFC 8017 (2016), *PKCS #1: RSA Cryptography Specifications Version 2.2.*

[ISO/IEC 9797-1] ISO/IEC 9797-1 (2011), *Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher.*

[NIST FIPS 180-4] NIST FIPS PUB 180-4 (2015), *Secure Hash Standard (SHS).*

[NIST FIPS 197] NIST FIPS PUB 197 (2001), *Specification for the Advanced Encryption Standard (AES).*

[NIST SP 800-107] NIST SP 800-107 Revision 1 (2012), *Recommendation for Applications Using Approved Hash Algorithms.*

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 señalr 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.

3.2.11 algoritmo de código de autenticación de mensajes: Algoritmo criptográfico simétrico con claves que se utiliza para proteger la autenticidad de los datos en un **ecosistema ECI**. El **algoritmo de código de autenticación de mensajes** acepta como entrada un mensaje y una clave secreta, y genera un bloque de datos de salida denominado MAC. El **algoritmo de código de autenticación de mensajes** especificado en la presente Recomendación se utiliza para vincular criptográficamente un mensaje de texto cifrado con sus correspondientes datos; obsérvese que en la presente Recomendación el algoritmo no se utiliza para proporcionar autenticación de origen.

3.2.12 plan de encriptación con claves públicas: Esquema criptográfico asimétrico con claves que se utiliza para proteger la confidencialidad de los datos en un **ecosistema ECI**. El **esquema de encriptación con clave pública** consiste en un **algoritmo de generación de claves**, una operación de encriptación y una operación de desencriptación. Las claves se generan por pares (clave pública, clave secreta/privada). Los datos se cifran utilizando una clave pública y los datos se recuperan del texto cifrado utilizando la correspondiente clave secreta/privada.

3.2.13 plan de encriptación simétrico: Esquema criptográfico simétrico clave que se utiliza para proteger la confidencialidad de los datos en un **ecosistema ECI**. Un **esquema de encriptación simétrico** consiste en un algoritmo de generación de claves, una operación de encriptación y una

operación de desencriptación. Las operaciones de encriptación y desencriptación de un **esquema de encriptación simétrico** utilizan la misma clave secreta que la entrada.

4 Abreviaturas y acrónimos

En esta Recomendación se utilizan las siguientes abreviaturas y acrónimos:

AES Norma de encriptación avanzada (*Advanced Encryption Standard)*

AD1 Datos Asociados 1 (*associated data 1*)

AD2 Datos Asociados 2 (*associated data 2*)

AK Clave de autenticación (*authentication key*)

CA Acceso condicional (*conditional access*)

CID Identificador de empresa (*company identifier*)

CISSA Algoritmo de aleatorización de TVIP común orientado al software (*common IPTV software-oriented scrambling algorithm*)

CPU Unidad central de procesamiento (*central processing unit*)

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

CPK Clave pública de chip (*chipset public key*)

CSK Clave secreta/privada de chip (*chipset secret/private key*)

CW Palabra de control (*control word*)

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

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

ECB Libro de códigos electrónicos (*electronic code book*)

ECI Interfaz común integrada (*embedded common interface*)

ECP Protección de contenido mejorada (*enhanced content protection*)

ID Identidad (*IDentity*)

LK Clave de enlace (*link key*)

MAC Código de autenticación de mensaje (*message authentication code*)

MK Clave MAC (*MAC key*)

OUI Identificador único de organización (*organizationally unique identifier)*

RSA Rivest Shamir Adleman

SHA Algoritmo hash seguro (*secure hash algorithm*)

SIM Mensaje de entrada firmado (*signed input message*)

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 ID de chip y par de claves maestras del chip

En esta cláusula se especifican los aspectos de la personalización de un chip conforme. Todo chip conforme tiene asociado un identrificador (ID) formado por una cadena de bits y que se denomina **ID de chip**, y un par de claves maestras del chip.

A cada chip conforme se le atribuirá un **ID de chip** de 64 bits exclusivo a nivel mundial. Si los bits del **ID de chip** se numeran de 0 a 63 de izquierda a derecha y si el i-ésimo bit ($0 \leq i \leq 63$) se denomina b_i, entonces (b_0, b_1, b_2, b_3) contendrá un ID de autoridad de registro. Cada valor del ID de autoridad de registro se asociará, como máximo, con una autoridad de registro. El **ID de chip** contendrá también un ID de fabricante de chip. El valor del ID de autoridad de registro y del ID de fabricante de chip del **ID de chip** de un chip conforme identificará unívocamente al fabricante que ha fabricado el chip. Además, la autoridad de registro identificada por el valor de (b_0, b_1, b_2, b_3) administrará la asignación de los identificadores de fabricante de chip que pueden utilizarse con combinación con este valor.

Si (b_0, b_1, b_2, b_3) = (0, 0, 0, 0), la Autoridad de Registro del IEEE (https://standards.ieee.org/faqs/regauth.html) será la autoridad de registro y se utilizarán el OUI de 24 bits o el CID de 24 bits para identificar a los fabricantes de chips. Además, si (b_0, b_1, b_2, b_3) = (0, 0, 0, 0), (b_4, b_5, … b_{27}) contendrá el OUI/CID, siendo b_4 el bit más significativo del octeto 0 del OUI/CID (véase también [b-IEEE-OUI]) y siendo b_{27} el bit menos significativo del octeto 2 del OUI/CID.

Todos los demás valores del ID de la autoridad de registro están reservados para usos ulteriores.

El par de claves maestras del chip se asocia con un esquema de encriptación de clave pública y consiste en una clave secreta/privada de chip (CSK) y una clave pública de chip (CPK). Como se detalla en las cláusulas 7 y 8 siguientes, (CSK, CPK) es el par de claves maestras tanto de la escalera de claves como del mecanismo de autenticación. El **esquema de encriptación de clave pública** y las representaciones de CSK y CPK se especifican en la cláusula 10.2.

Un chip conforme debe generar su propio par de claves (CSK, CPK) para impedir que se revele a cualquier otra parte del sistema el valor de la CSK. Así, sólo se ha de distribuir el **ID de chip** al chip durante su personalización y la autenticidad del **ID de chip** deberá protegerse durante esta distribución. Si el chip no genera su propio par de claves, la autenticidad del trío (**ID de chip**, CSK, CPK) y la confidencialidad de la CSK deberán protegerse durante la distribución de (**ID de chip**, CSK, CPK) al chip.

El número aleatorio utilizado como entrada para el algoritmo de generación de pares de claves (CSK, CPK) deberá tener una entropía mínima de 128 bits.

Un chip conforme deberá almacenar permanentemente su trío (**ID de chip**, CSK, CPK) y aplicar medidas para proteger la confidencialidad de la CSK almacenada, así como la integridad del **ID de chip**, la CSK y la CPK almacenados.

La unidad central de procesamiento (CPU) del **receptor de contenido** deberá tener acceso a la lectura del **ID de chip** almacenado y a la clave pública del chip (CPK) almacenada. De este modo una **autoridad de certificación** puede utilizar la información exportada como entrada para crear un certificado de clave pública para el chip. Además, el **ID de chip** exportado permite a un **proveedor de contenido** identificar el chip y su certificado.

La **autoridad de certificación** mantendrá el par (**ID de chip**, CPK) de todos los chips que gestione. En la presente Recomendación no se excluye la presencia de más de una **autoridad de certificación**

en el sistema. La autenticidad del par (**ID de chip**, CPK) deberá protegerse durante su distribución a la **autoridad**(es) **de certificación** asociada(s).

7 Escalera de claves

7.1 Generalidades

En esta cláusula se presenta el diseño funcional de la escalera de claves. En esta Recomendación se denomina bloque de escalera de claves el bloque del chip que ejecuta la escalera de claves. La escalera de claves se muestra en la Figura 7-1. Como se especifica en la cláusula 6 y se muestra en la figura, el chip se personaliza con un **ID de chip** y con una clave secreta/privada de chip (CSK).

Uno de los productos del bloque de escalera de claves es la **palabra de control** (CW). La CW se utiliza para encriptar o desencriptar el contenido. Otro producto del bloque de escalera de claves es una cadena de bits compuesta de la información sobre las reglas de utilización de la palabra de control (CW-URI), que determina la URI para una CW (véase en la cláusula 7.3.1 de la especificación de la CW-URI y las reglas de utilización asociadas). La CW y la CW-URI alimentan el **desaleatorizador de contenido** (que no se muestra en la Figura 7-1).

- El bloque de escalera de claves y el **desaleatorizador de contenido** se implementarán en un único chip de silicio.
- Si el **desaleatorizador de contenido** ofrece una interfaz para un procesador en el **receptor de contenido** que permite al procesador transmitir las CW sin encriptar al **desaleatorizador de contenido** (es decir, que obvia el bloque de escalera de claves), se podrá desactivar permanentemente esta funcionalidad.
- Si la escalera de claves calcula una CW, solo el bloque de escalera de claves y el **desaleatorizador de contenido** podrán acceder a esa CW.
- La autenticidad del par (CW, CW-URI) y la confidencialidad de la CW deberán protegerse durante su distribución del bloque de escalera de claves al **desaleatorizador de contenido**.

El bloque de escalera de claves deberá tener una interfaz para un procesador del **receptor de contenido.** Por ejemplo, el procesador puede ser un procesador de seguridad o la CPU del **receptor de contenido**. Como se especifica en la cláusula 6 y se muestra en la Figura 7-1, el procesador tiene acceso de lectura al **ID de chip,** lo que permite al **proveedor de contenido** identificar el chip y obtener el correspondiente certificado de clave pública con la CPK de la **autoridad de certificación**. Es necesario conocer el valor de la CPK para calcular uno de los mensajes que alimentan la escalera de claves, como se escribe en la cláusula 7.2.

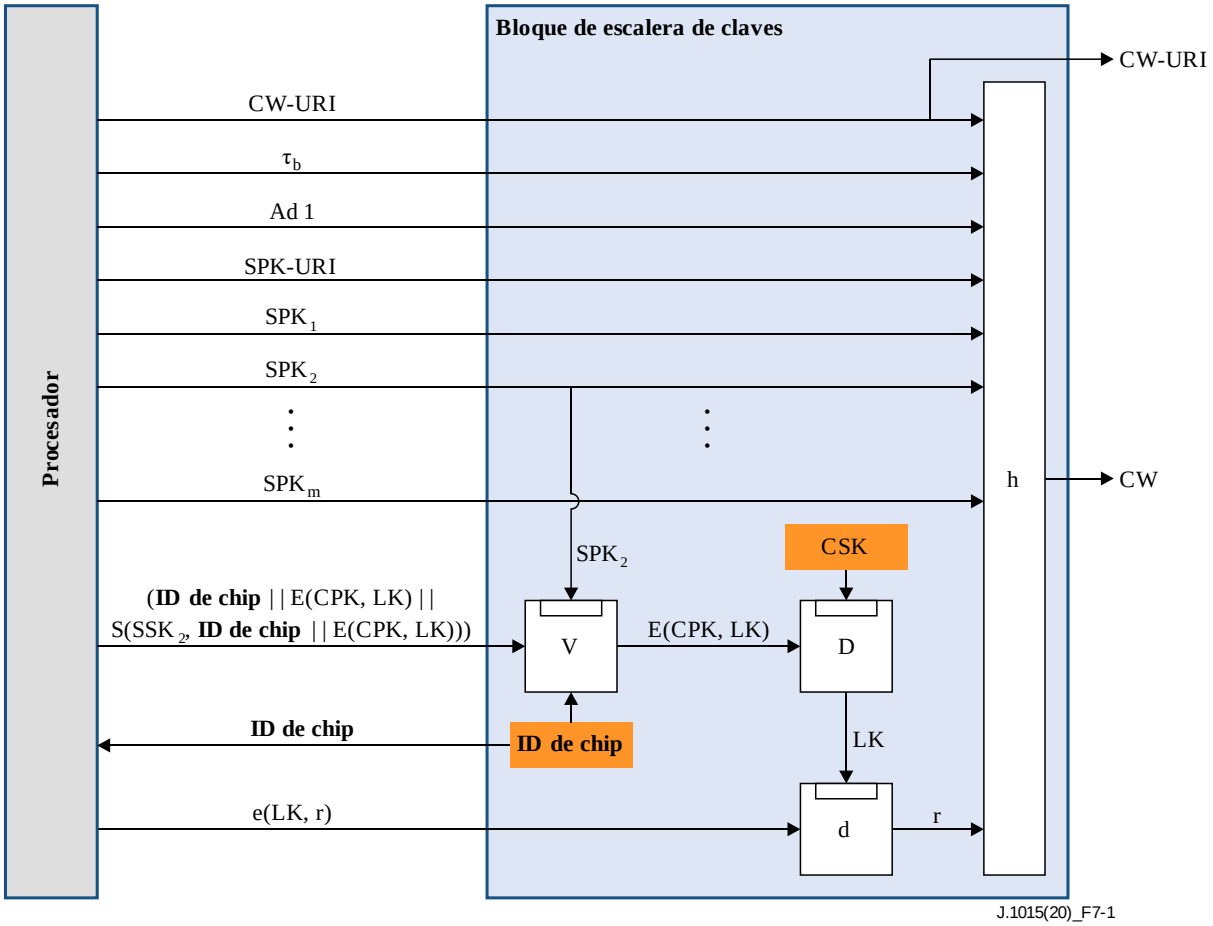

Figura 7-1 – Escalera de claves

Como se especifica en la cláusula 6, el par (CSK, CPK) está asociado con un **esquema de encriptación con clave pública**. Las operaciones de encriptación y desencriptación correspondientes se denominan respectivamente E y D. E y D son operaciones de criptografía con clave y cada una de ellas necesita dos entradas: una entrada de clave y una entrada de mensaje. En esta Recomendación se supone que la primera entrada de una operación o algoritmo de criptografía con clave es la clave.

Ejemplo: La encriptación del mensaje M utilizando E y la clave pública de chip (CPK) se escribe E(CPK, M).

Los mecanismos especificados en la presente Recomendación utilizan también un **esquema de firma digital**, donde S y V denotan respectivamente la operación de generación de firma y la operación de verificación de firma. El emisor tiene asociado un par de claves del **esquema de firma digital** consistente en una clave secreta/privada de emisor (SSK) y una clave pública de emisor (SPK). En esta Recomendación se supone que el emisor es un **sistema de protección de contenido**. Como se muestra en la Figura 7-1 una serie de distintas SPK, a saber, SPK_1, SPK_2, ..., SPK_m ($m \geq 1$), alimentan el bloque de escalera de claves. El bloque de escalera de claves deberá soportar escaleras de claves para todos los valores de m, como $1 \leq m \leq 16$. En la práctica, cada par de claves (SSK_i, SPK_i) con $1 \leq i \leq m$ estará típicamente asociado a un **sistema de protección de contenido**, aunque también es posible que ese par de claves esté compartido entre múltiples sistemas.

Asociada a SPK_1, SPK_2, ..., SPK_m está la SPK-URI. Esta entrada del bloque de escalera de claves determinar la URI para SPK_1, SPK_2, ..., SPK_m. La SPK-URI y las reglas de utilización asociadas se especifican en la cláusula 7.3.2. Como se muestra en la Figura 7-1 una de las SPK y la operación de verificación, V, se utilizan para verificar la firma del mensaje de entrada (**ID de chip** || E(CPK, LK) || S(SSK_i, **ID de chip** || E(CPK, LK))). Este mensaje de entrada firmado (SIM) también se denomina

SIM_{KL} en las cláusulas siguientes. En la Figura 7-1 se asume que i = 2 y que la SPK-URI y las reglas de utilización permiten utilizar SPK_2 para verificar la firma.

La escalera de claves también implementa un **esquema de encriptación simétrica**. En este esquema las operaciones de encriptación y desencriptación se denominan, respectivamente, e y d. la escalera de claves utiliza una clave de enlace (LK) como clave del esquema y un número aleatorio, r (u otra LK, como se indica en la cláusula 7.4 siguiente), como mensaje. El número aleatorio, r, se representa como una cadena de bits y debe tener 128 bits de longitud.

Por último, el bloque de escalera de claves implementa una función h. Esta función se basa en una **función hash criptográfica** (véase la especificación de h en la cláusula 10.4.

Como se muestra en la Figura 7-1, las otras dos entradas del bloque de escalera de claves son τ_b y los Datos Asociados 1 (AD1). Estas dos entradas se representan como cadenas de bits:

- La longitud de τ_b será de 8 bits. La utilización de τ_b se especifica en la cláusula 7.5.
- La longitud de AD1 será de 256 bits. La especificación del contenido de AD1 queda fuera del alcance de la presente Recomendación, donde se asume que el bloque de escalera de claves no procesa AD1 más que como entrada para h. El bloque de escalera de claves puede transmitir AD1, o parte de AD1, junto con la CW-URI y la CW al **desaleatorizador de contenido**.

En la presente Recomendación se supone que las claves simétricas, los mensajes de texto cifrado y las firmas se representan como cadenas de bits, cuyas longitudes se especifican en la cláusula 10, en la que también se especifica la representación de las claves asimétricas.

7.2 Cálculos de la escalera de claves

El emisor asociado al par de claves (SSK_i, SPK_i) para algunos $1 \leq i \leq m$ pueden crear el mensaje de entrada firmado, SIM_{KL}, es decir:

(**ID de chip** || E(CPK, LK) || S(SSK_i, **ID de chip** || E(CPK, LK)))

siguiendo los pasos que se indican a continuación.

Calcular SIM_{KL} (emisor)

1) Generar una LK.
2) Calcular el texto cifrado E(CPK, LK).
3) Concatenar el **ID de chip** y E(CPK, LK). La cadena de bits resultante se denota mediante (**ID de chip** || E(CPK, LK)).
4) Firmar la cadena de bits (**ID de chip** || E(CPK, LK)) utilizando SSK_i. La firma se denota mediante S(SSK_i, **ID de chip** || E(CPK, LK))).
5) Anexar esta firma a la cadena de bits (**ID de chip** || E(CPK, LK)).

Una vez recibidas la SIM_{KL} y la clave pública de emisor, SPK_i, el bloque de escalera de claves realizará los pasos siguientes para extraer la LK (en la Figura 7-1 se supone que los tres primeros pasos los realiza V).

Calcular LK (bloque de escalera de claves)

1) Verificar si el **ID de chip** recibido es igual al **ID de chip** almacenado. Si los dos valores no son iguales, el bloque de escalera de claves abortará el cálculo.
2) Comprobar si SPK-URI y las reglas de utilización, especificadas en la cláusula 7.3.2, permiten a V utilizar SPK_i para verificar la firma. De no ser así, el bloque de escalera de claves abortará el cálculo.
3) Utilizar las SIM_{KL} y SPK_i recibidas para verificar la firma. Si la firma no es válida, el bloque de escalera de claves abortará el cálculo.

4) Calcular LK = D(CSK, E(CPK, LK)).

A continuación, el bloque de escalera de claves utilizará la LK para procesar el mensaje de entrada e(LK, r) (véase también la Figura 7-1). El emisor puede crear este mensaje siguiendo los pasos que se indican a continuación.

Calcular e(LK, r) (emisor)

1) Generar una cadena de bits aleatoria, r.

2) Calcular e(LK, r).

Tras recibir e(LK, r) y haber calculado LK, el bloque de escalera de claves calculará r de la siguiente manera (véase también la Figura 7-1).

Calcular r (bloque de escalera de claves)

1) r = d(LK, e(LK, r)).

A continuación, el bloque de escalera de claves utilizará la función h para calcular la CW. Como se muestra en la Figura 7-1, las entradas de h son CW-URI, τ_b, AD1, SPK-URI, SPK_1, SPK_2, ..., SPK_m y r. La implementación de la escalera de claves deberá garantizar que la clave pública utilizada para verificar la autenticidad de la SIM_{KL} (o, más precisamente, de la SIM_{KL} que contiene la clave de enlace asociada con el número aleatorio, r) se facilita como entrada SPK a h cuando la CW se deriva de r. Entonces el bloque de escalera de claves transmitirá la CW-URI y la CW al **desaleatorizador de contenido**.

7.3 Información de reglas de utilización

7.3.1 Información sobre las reglas de utilización – palabra de control

La CW-URI tendrá 64 bits de longitud. Esos bits se numeran de 0 a 63 de izquierda a derecha. El valor de la CW-URI determina la utilización permitida de la CW (véase también el Cuadro 7-1) siguiendo la siguiente regla de utilización: si el valor de un bit es 1, se permite la utilización especificada; en caso contrario, no se permite. El **desaleatorizador de contenido** deberá aplicar esta regla de utilización. El **desaleatorizador de contenido** ignorará:

i) el valor de los bits reservados para utilización futura; y

ii) el valor de los bits correspondientes a implementaciones que el **desaleatorizador de contenido** no soporta.

Cuadro 7-1 – Definición de la CW-URI

Número de bit	Descripción
0	Encriptar
1	Desencriptar
2 … 7	Reservado para utilización futura
8	Algoritmo 2 de aleatorización común (CSA2) para la radiodifusión de vídeo digital (DVB) [b-ETSI TS 100 289]
9	DVB CSA3 [b-ETSI TS 100 289]
10 … 15	Reservado para utilización futura
16	Algoritmo de aleatorización común orientado a software de TVIP (CISSA) para la DVB versión 1 [b-ETSI TS 103 127]
17 … 23	Reservado para utilización futura
24	Algoritmo común de aleatorización/desaleatorización del Comité para Sistemas de Televisión Avanzados [b-ATSC A70-1]
25 … 31	Reservado para utilización futura
32	Esquema de encriptación común – esquema de protección cenc [b-ISO/IEC 23001-7]
33	Esquema de encriptación común – esquema de protección cbc1 [b-ISO/IEC 23001-7]
34	Esquema de encriptación común – esquema de protección cens [b-ISO/IEC 23001-7]
35	Esquema de encriptación común – esquema de protección cbcs [b-ISO/IEC 23001-7]
36 … 39	Reservado para utilización futura
40	ChinaDRM – modo encadenamiento de bloque cifrado [b-GY/T 277-2014]
41	ChinaDRM – modo contador [b-GY/T 277-2014]
42 … 63	Reservado para utilización futura

7.3.2 Información sobre las reglas de utilización – clave pública del emisor

La SPK-URI tendrá una longitud de 64 bits, que se numeran de 0 a 63 de izquierda a derecha. La SPK-URI se define en el Cuadro 7-2. Concretamente, si SPK_1, SPK_2, ... y SPK_m se introducen en la escalera de claves junto con la SPK-URI (como se muestra en el Cuadro 7-2), los bits 0, 1, …, m-1 y los bits 16, 17, .., 16+m-1 de la SPK-URI se utilizan para definir dos subseries de {SPK_1, SPK_2, ..., SPK_m}: SPK_i (i = 1, 2, …, m) es un elemento de la primera subserie única y exclusivamente si el valor del bit i-1 es igual a uno, y SPK_i es un elemento de la segunda subserie única y exclusivamente si el valor del bit i+15 es igual a uno. A continuación estas dos subseries se denominan S_1 y S_2, respectivamente. Utilizando esta notación, la escalera de claves aplicará la siguiente regla de utilización:

Regla de utilización SPK 1: en la escalera de claves V puede utilizar la SPK_i para verificar la firma de la SIM_{KL} única y exclusivamente si $SPK_i \in S_1$.

El bloque de escalera de claves aplicará la regla de utilización SPK 1.

La serie S_2 se utiliza cuando se reencripta contenido. Si el contenido se reencripta, se necesitan las dos series de entradas indicadas en la Figura 7-1: una asociada con la CW utilizada para desencriptar el contenido y otra asociada con la CW utilizada para encriptar el contenido. En este caso, la siguiente regla de utilización vincula estas dos series de entradas:

Regla de utilización SPK 2: en la escalera de claves V puede utilizar la SPK_i para verificar la firma de la SIM_{KL} de la CW utilizada para la encriptación del contenido única y exclusivamente si $SPK_i \in S_2$ asociada con la CW es utilizada para desencriptar el contenido.

Si el **desaleatorizador de contenido** soporta la reencriptación de contenido, el bloque de escalera de claves debe aplicar la regla de utilización SPK 2. Si el bloque de escalera de claves no aplica esta regla de utilización, otro componente del chip deberá aplicar la regla de utilización SPK 2 y la implementación garantizará que el valor de la SPK-URI que sirve de entrada para la función h es igual al valor de la SPK-URI utilizada para aplicar la regla de utilización SPK 2.

Cuadro 7-2 – Definición de la Información sobre las reglas de utilización – Clave pública del emisor

Número de bit	Descripción
0	spk1_in_set1
1	spk2_in_set1
2	spk3_in_set1
…	…
15	spk16_in_set1
16	spk1_in_set2
17	spk2_in_set2
18	spk3_in_set2
…	…
31	spk16_in_set2
32 … 63	Reservado para utilización futura

7.4 Capas de claves adicionales

7.4.1 Generalidades

La especificación de las cláusulas 7.1 y 7.2 supone que una capa de claves de la escalera de claves está asociada con las LK. La escalera de claves también soportará capas de claves adicionales para las claves de enlaces, como se muestra en la Figura 7-2 (sólo se muestran los bloques de construcción de la escalera de claves pertinentes para esta cláusula).

Como se muestra en la Figura 7-2, t denota el número de LK de la escalera de claves. El bloque de la escalera de claves soportará escaleras de claves para todos los valores de t $1 \leq t \leq 24$. Téngase en cuenta que el esquema en que t = 1 se especifica en las cláusulas 7.1 y 7.2.

7.4.2 Cálculos de la escalera de claves

El emisor puede generar los mensajes de entrada t para el bloque de escalera de claves siguiendo los pasos que se indican a continuación.

Calcular $e(LK_1, LK_2)$, $e(LK_2, LK_3)$, … , $e(LK_{t-1}, LK_t)$ y $e(LK_t, r)$ (emisor)

1) Generar las LK_i, para i = 1, 2, …, t y una cadena de bits aleatoria, r.
2) Calcular $e(LK_{i-1}, LK_i)$ para i = 2, 3, ..., t.
3) Calcular $e(LK_t, r)$.

Tras recibir $e(LK_1, LK_2)$, $e(LK_2, LK_3)$, … , $e(LK_{t-1}, LK_t)$ y $e(LK_t, r)$, el bloque de escalera de claves calculará r de la siguiente manera (véase también la Figura 7-2).

Calcular r (bloque de escalera de claves)

1) Calcular $LK_i = d(LK_{i-1}, e(LK_{i-1}, LK_i))$ para i = 2, 3, ..., t.
2) Calcular $r = d(LK_t, e(LK_t, r))$.

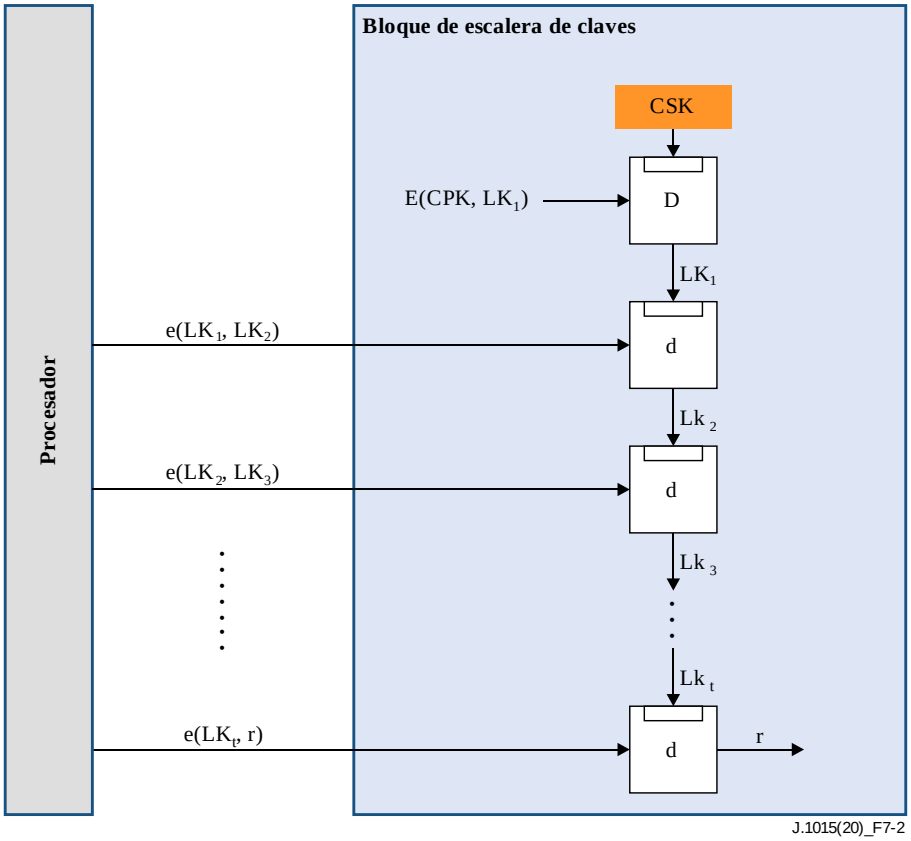

Figura 7-2 – Capas de claves adicionales

7.5 Datos Asociados 2

El emisor puede optativamente enviar datos asociados (AD2), junto con e(LK_t, r) a la escalera de claves. El valor de la cadena de bits τ_b (presentada en la cláusula 7.1) señala la presencia de AD2. Como se especifica en la cláusula 7.1, la longitud de τ_b es de 8 bits. A continuación, τ denota la representación en enteros de τ_b, donde el bit menos significativo de τ corresponde al bit más a la derecha de τ_b. La escalera de claves soportará todos los valores de $\tau \in \{0, 64, 96, 128\}$. Si $\tau = 0$, AD2 no estará presente y se utilizará el esquema presentado en las cláusulas 7.1 a 7.4. En la siguiente descripción se supone que $\tau \neq 0$. En tal caso, AD2 estará presente. El bloque de escalera de claves verificará si la τ recibida $\in \{64, 96, 128\}$. De no ser así, el bloque de escalera de claves abortará el cálculo.

En esta Recomendación se supone que AD2 está representado por una cadena de bits. Lon denota la longitud en bits de AD2. El bloque de escalera de claves soportará todos los valores de Lon cuando $1 \leq Lon \leq 256$.

Lon_b denota la representación binaria del entero Lon – 1, donde el bit más a la derecha de Lon_b corresponde al bit menos significativo de Lon – 1. Lon_b tendrá 8 bits de longitud.

La cadena de bits AD2 estará criptográficamente ligada al texto cifrado e(LK_t, r) correspondiente durante su transporte a la escalera de claves. Para ello, el emisor y el bloque de escalera de claves utilizarán un **algoritmo de código de autenticación de mensaje** (mac). Las entradas para este algoritmo son la clave MAC secreta (MK), el mensaje Lon_b || e(LK_t, r) || AD2 y τ. La salida del mac es una etiqueta, T, cuya longitud es de τ bits. El algoritmo MAC se especifica en la cláusula 10.5.

Sea 00…0 la cadena de bits todo ceros de 128 bits. El emisor puede seguir los pasos que se indican a continuación para generar el mensaje Lon_b || e(LK_t, r) || AD2 || T de entrada para la escalera de claves (como se muestra en la Figura 7-3).

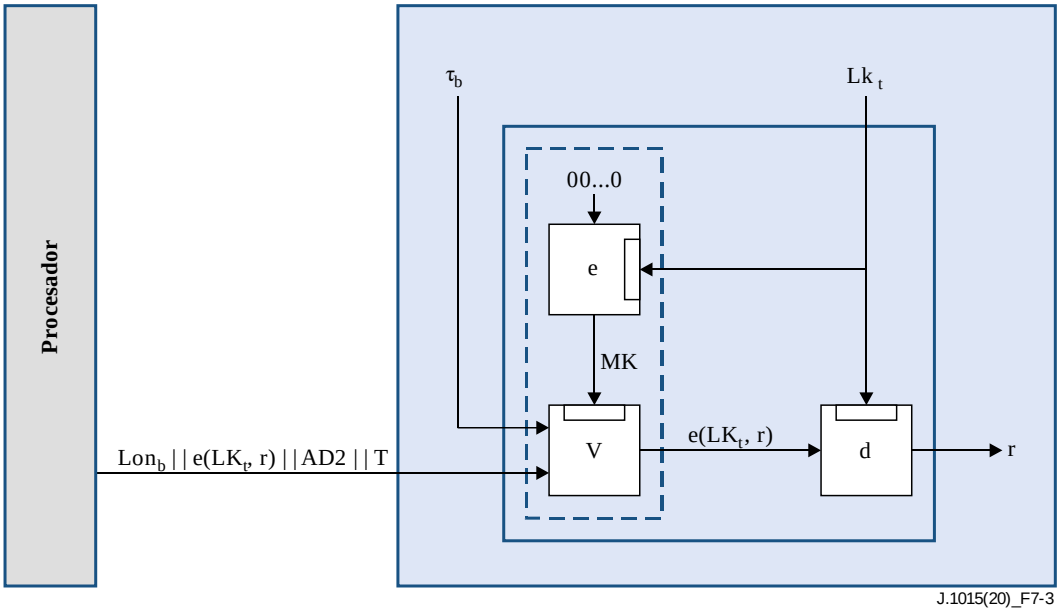

Figura 7-3 – Datos asociados 2

Calcular Lon_b || e(LK_t, r) || AD2 || T (emisor)

1) Calcular MK = e(LK_t, 00…0).
2) Anteponer Lon_b a la cadena de bits e(LK_t, r) || AD2.
3) Calcular T = mac(MK, Lon_b || e(LK_t, r) || AD2, τ).
4) Añadir T a la cadena de bits Lon_b || e(LK_t, r) || AD2.

El mensaje Lon_b || e(LK_t, r) || AD2 || T sustituye al mensaje e(LK_t, r) que se utiliza si τ = 0. Tras recibir Lon_b || e(LK_t, r) || AD2 || T, el bloque de escalera de claves calculará e(LK_t, r) siguiendo los pasos que se indican a continuación (los Pasos 2 – 4 están representados por v en la Figura 7-3).

Calcular e(LK_t, r) (bloque de escalera de claves)

1) Calcular MK = e(LK_t, 00…0).
2) Calcular T = mac(MK, Lon_b || e(LK_t, r) || AD2, τ).
3) Verificar si la T recibida es igual a la T calculada. Si los dos valores no son iguales, el bloque de escalera de claves abortará el cálculo.
4) Extraer e(LK_t, r) del mensaje recibido.

Queda fuera del alcance de esta Recomendación especificar el contenido de AD2. En esta Recomendación se supone que el bloque de escalera de claves no procesa AD2 más que para utilizarlo como entrada para el algoritmo MAC. El bloque de escalera de claves puede transmitir AD2, o parte de AD2, junto con la CW-URI y la CW al **desaleatorizador de contenido**.

Si $\tau \neq 0$, la implementación de la escalera de claves garantizará que el valor de τ_b presentado junto con Lon_b || e(LK_t, r) || AD2 como entrada para el algoritmo MAC también se presenta como entrada para h cuando la CW se deriva de r.

Sólo el bloque de escalera de claves podrá acceder a la CSK, la LK_i ($1 \leq i \leq t$), la MK y r sin encriptar.

8 Mecanismo de autenticación

8.1 Generalidades

En esta cláusula se presenta el diseño funcional del mecanismo de autenticación del bloque de escalera de claves. El mecanismo de autenticación se ilustra en la Figura 8-1. Este mecanismo está

estrechamente relacionado con la escalera de claves, como se indica en la cláusula 7, y, concretamente, utiliza las mismas operaciones V, D, además de la función h, y utiliza los mismos **ID de chip** y CSK. Sin embargo, el mecanismo de autenticación no utiliza las LK y la CW-URI, la SPK-URI y la τ_b no son entradas para el mecanismo de autenticación ni la función h. Además, el producto de h no es una CW utilizada para la encriptación o desencriptación de contenido (concretamente, el mecanismo de autenticación no tiene una interfaz directa con el **desaleatorizador de contenido**), sino una clave de autenticación (AK), que es una clave del mismo **esquema de encriptación simétrica** que se utiliza en la escalera de claves. Como se muestra en la Figura 8-1, en la implementación del mecanismo de autenticación sólo se emplea la operación de desencriptación, d.

El mensaje de entrada (**ID de chip** || E(CPK, r) || S(SSK_i, **ID de chip** || E(CPK, r))) también se denomina SIM_{AUTH} en las cláusulas siguientes.

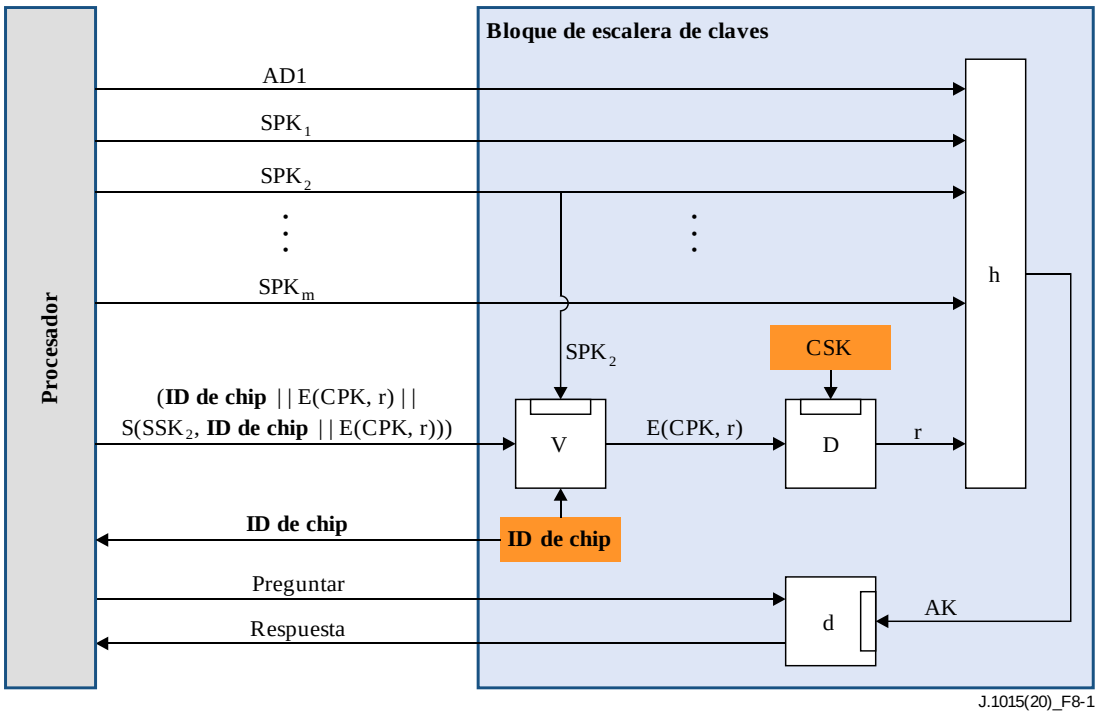

Figura 8-1 – Mecanismo de autenticación

8.2 Cálculos del mecanismo de autenticación

El emisor asociado al par de claves (SSK_i, SPK_i) para algunos $1 \leq i \leq m$ puede crear el SIM_{AUTH}, es decir:

(**ID de chip** || E(CPK, r) || S(SSK_i, **ID de chip** || E(CPK, r))),

siguiendo los pasos que se indican a continuación.

Calcular SIM_{AUTH} (emisor)

1) Generar una cadena de bits aleatoria, r.
2) Calcular el texto cifrado E(CPK, r).
3) Concatenar **ID de chip** y E(CPK, r); la cadena de bits resultante se denomina (**ID de chip** || E(CPK, r)).
4) Firmar el mensaje (**ID de chip** || E(CPK, r)) utilizando la SSK_i; la firma se denota mediante S(SSK_i, **ID de chip** || E(CPK, r)).
5) Añadir esta firma a la cadena de bits (**ID de chip** || E(CPK, r)).

Una vez recibida la SIM_{AUTH} y la SPK_i, el bloque de escalera de claves seguirá los pasos que se indican a continuación para extraer r (en la Figura 8-1 los dos primeros pasos están representados por V).

Calcular r (bloque de escalera de claves)

1) Verificar que el **ID de chip** recibido es igual al **ID de chip** almacenado. Si los dos valores no son idénticos, el bloque de escalera de claves abortará el cálculo.

2) Utilizar las SIM_{AUTH} y SPK_i recibidas para verificar la firma. Si la firma no es válida, el bloque de escalera de claves abortará el cálculo.

3) Calcular r = D(CSK, E(CPK, r)).

En el mecanismo de autenticación V puede utilizar cualquier SPK_i cuyo valor sea $1 \leq i \leq m$ para verificar la firma de SIM_{AUTH} (en la Figura 8.1 se supone que i = 2).

A continuación, AD1, SPK_1, SPK_2, ..., SPK_m y r se facilitarán como entradas para la función h. El producto de h es la clave de autenticación (AK). La implementación del mecanismo de autenticación garantizará que la clave pública utilizada para verificar la autenticidad de SIM_{AUTH} (o, más exactamente, la SIM_{AUTH} que contiene el número aleatorio, r) se facilita como entrada SPK a h cuando la AK se deriva de r.

Entonces el emisor puede crear un mensaje de entrada, denominado Pregunta. Tras recibir la Pregunta del procesador, el mecanismo de autenticación calculará la Respuesta de la siguiente manera.

Calcular Respuesta (bloque de escalera de claves)

1) Calcular Respuesta = d(AK, Pregunta).

Como se muestra en la Figura 8-1, el mecanismo de autenticación devolverá la Respuesta al procesador.

Sólo el bloque de escalera de claves podrá acceder a la AK sin encriptar.

9 Primitivas de conversión de datos

9.1 BS2OSP

La primitiva cadena de bits a cadena de bytes, BS2OSP, se utiliza para determinar el **esquema de encriptación con clave pública** de la cláusula 10.2 y el **esquema de firma digital** de la cláusula 10.3.

Función: BS2OSP(x)

Entrada: x una cadena de bits de longitud $8j$ ($j \geq 1$).

Producto: X una cadena de bytes de longitud j.

Pasos:

1) Sea x_i un bit para $0 \leq i \leq 8j - 1$ y sea $x = x_0\ x_1\ \ldots\ x_{8j-1}$.

2) Sea X_i el byte determinado por $X_i = x_{8i+1}\ \ldots\ x_{8i+7}$ para $0 \leq i \leq j\text{-}1$.

3) Obtener la cadena de bytes $X = X_0\ X_1\ \ldots\ X_{j-1}$.

9.2 OS2BSP

La primitiva cadena de bytes a cadena de bits, OS2BSP, se utiliza para determinar la primitiva I2BSP de la cláusula 9.3 y el **esquema de encriptación con clave pública** de la cláusula 10.2.

Función: OS2BSP(X)

Entrada: X una cadena de bytes de longitud j ($j \geq 1$).

Producto: x una cadena de bits de longitud $8j$.

Pasos:

1) Sea X_i un byte para $0 \leq i \leq j\text{-}1$ y sea $X = X_0\ X_1\ \ldots\ X_{j-1}$.

2) Sea x_i un bit para $0 \leq i \leq 8j\text{-}1$ y sea que estos bits se determinan mediante $X_i = x_{8i+1}\ \ldots\ x_{8i+7}$ para $0 \leq i \leq j\text{-}1$.

3) Obtener la cadena de bits $x = x_0\ x_1\ \ldots\ x_{8j-1}$.

9.3 I2BSP

La primitiva entero a cadena de bits, I2BSP, se utiliza para determinar la función h de la cláusula 10.4.

Función: I2BSP(x)

Entrada: x un entero de 2 048 bits.

Producto: una cadena de bits de longitud 2 048.

Paso: Si la primitiva de conversión de entero a cadena de bytes, I2OSP(x, xLon), es la especificada en [IETF RFC 8017], I2BSP(x) = OS2BSP(I2OSP(x, 256)).

10 Operaciones criptográficas

10.1 Esquema de encriptación simétrica

El **esquema de encriptación simétrica** utilizado en el bloque de escalera de claves deberá ser la norma de encriptación avanzada de 128 bits (AES-128) [NIST FIPS 197] en modo de funcionamiento libro de código electrónico (ECB).

10.2 Esquema de encriptación con clave pública

El **esquema de encriptación con clave pública** será RSAES-PKCS1-v1_5 [IETF RFC 8017]. Este esquema consiste en una operación de encriptación y una operación de desencriptación. Recuérdese de las cláusulas 7 y 8 que sólo la operación de desencriptación se efectúa en el bloque de escalera de claves y que de la operación de encriptación se ocupa el sistema del emisor.

La clave pública de chip (CPK) será igual a la clave pública Rivest, Shamir y Adleman (RSA) del receptor (*n*, *e*) en [IETF RFC 8017]. En esta Recomendación la longitud en bits de *n* será de 2 048, es decir, la longitud en bytes de *n*, denominada *k* en [IETF RFC 8017], será igual a 256. La clave secreta/privada (CSK) será igual a la clave privada RSA del receptor, *K*, de [IETF RFC 8017]. La representación de la CSK será igual a una de las representaciones de *K* especificadas en [IETF RFC 8017].

El mensaje que se ha de encriptar se denomina *M* en [IETF RFC 8017] y se representa como una cadena de bytes. En esta Recomendación, *M* se determina por *M* = BS2OSP(LK) para la escalera de claves y como *M* = BS2OSP(r) para el mecanismo de autenticación. Por tanto, en esta Recomendación la longitud en bytes de *M* es de 16.

CPK y *M* son las entradas para la operación de encriptación:

RSAES-PKCS1-v1_5-Encrypt(CPK, *M*)

El producto de esa operación es un texto cifrado, denominado *C* y representado como una cadena de bytes en [IETF RFC 8017]. En esta Recomendación la longitud en bytes de *C* es de 256. *C* es igual a BS2OSP(E(CPK, LK)) para la escalera de claves y a BS2OSP(E(CPK, r)) para el mecanismo de autenticación.

CSK y *C* son las entradas para la operación de desencriptación:

RSAES-PKCS-v1_5-Decrypt(CSK, *C*)

Esta operación se ejecuta en el bloque de escalera de claves. El producto de esta operación es el mensaje *M*, representado como una cadena de bytes. A continuación, el bloque de escalera de claves calculará LK = OS2BSP(*M*) para la escalera de claves y r = OS2BSP(*M*) para el mecanismo de autenticación.

10.3 Esquema de firma digital

El **esquema de firma digital** será RSASSA-PKCS1-v1_5 [IETF RFC 8017]. Este esquema consiste en una operación de generación de firma y una operación de verificación de firma. Recuérdese de las cláusulas 7 y 8 que sólo la operación de verificación de firma se ejecuta en el bloque de escalera de claves y que la operación de generación de firma se ejecuta en el sistema del emisor.

La clave pública RSA del firmante se denomina (*n*, *e*) y está representada por un par de enteros en [IETF RFC 8017]. En esta Recomendación, la longitud del módulo *n* de la clave pública RSA del firmante es de 2 048 bits, es decir, que la longitud en bytes de *n*, denominada *k* en [IETF RFC 8017], es de 256. Además, en esta Recomendación el valor del exponente público, *e*, será $2^{16} + 1$. Un chip conforme almacenará permanentemente este valor y aplicará medidas de protección de su integridad. La SPK será igual al módulo *n*, lo que implica que la longitud de SPK es de 2 048 bits y que SPK se representa con un entero. La SSK será igual a la clave privada RSA del firmante, *K*, en [IETF RFC 8017].

El mensaje que se ha de firmar se denomina *M* y se representa como una cadena de bytes en [IETF RFC 8017]. En esta Recomendación *M* se determina de la siguiente manera:

$$M = \text{BS2OSP}(\textbf{ID de chip} \,||\, \text{E(CPK, LK)})$$

para la escalera de claves y

$$M = \text{BS2OSP}(\textbf{ID de chip} \,||\, \text{E(CPK, r)})$$

para el mecanismo de autenticación. Como resultado, la longitud en bytes de *M* es 8 + 256 = 264 en ambos casos.

SSK y *M* son las entradas para la operación de generación de firma:

$$\text{RSASSA-PKCS1-v1_5-Sign(SSK, } M\text{)}$$

El producto de la operación de generación de firma es una firma, *S*, representada como una cadena de bytes en [IETF RFC 8017]. La longitud en bytes de *S* es de 256 en esta Recomendación. *S* es igual a BS2OSP(S(SSK_i, **ID de chip** || E(CPK, LK))) para la escalera de claves y a BS2OSP(S(SSK_i, **ID de chip** || E(CPK, r))) para el mecanismo de autenticación.

(SPK, $2^{16} + 1$), *M* y *S* son las entradas para la operación de verificación de firma:

$$\text{RSAES-PKCS-v1_5-Verify((SPK, } 2^{16} + 1\text{), } M\text{, } S\text{)}$$

Esta operación se ejecuta en el bloque de escalera de claves. El resultado de esta operación es "firma válida" o "firma no válida".

10.4 Función h

En esta cláusula se especifica la función h. Recuérdese de las cláusulas 7 y 8 que las entradas para h son:

- CW-URI, τ_b, AD1, SPK-URI, SPK_1, SPK_2, ..., SPK_m y *r* para la escalera de claves.
- AD1, SPK_1, SPK_2, ..., SPK_m y *r* para el mecanismo de autenticación.

Si el bloque de la escalera de claves no recibe una de estas dos series de entradas, o si la longitud de una entrada no es la especificada en esta Recomendación, el bloque de escalera de claves abortará los cálculos. En caso contrario, h aplicará en primer lugar la primitiva de conversión de datos I2BSP a cada una de sus entradas SPK. A continuación, h concatenará las cadenas de bits que representan sus entradas de la siguiente manera para obtener el mensaje *M*. En el caso de la escalera de claves:

$$M = r \,||\, \text{CW-URI} \,||\, \tau_b \,||\, \text{AD1} \,||\, \text{SPK-URI} \,||\, \text{I2BSP}(SPK_1) \,||\, \text{I2BSP}(SPK_2) \,||\, ... \,||\, \text{I2BSP}(SPK_m),$$

y en el caso del mecanismo de autenticación:

$$M = r \,||\, \text{AD1} \,||\, \text{I2BSP}(SPK_1) \,||\, \text{I2BSP}(SPK_2) \,||\, ... \,||\, \text{I2BSP}(SPK_m)$$

Recuérdese que las longitudes de r, CW-URI, τ_b, AD1, SPK-URI y I2BSP(SPK_i) son respectivamente de 128 bits, 64 bits, 8 bits, 256 bits, 64 bits y 2 048 bits. Por tanto, la longitud en bits de *M*, denominada *l* en [NIST FIPS 180-4], es de 520 + 2 048 m, siendo m el número de elementos I2BSP (SPK_m) en el bloque de mensaje M, en el caso de la escalera de claves y de 384 + 2 048m en el caso del mecanismo de autenticación.

A continuación, h calculará el algoritmo hash seguro de 256(*M*) [SHA-256(*M*)] como se especifica en [NIST FIPS 180-4].

En el caso del mecanismo de autenticación, h truncará este mensaje de 256 bits en 128 bits y dará como resultado el mensaje truncado. En el caso de la escalera de claves, el bloque de escalera de claves transmitirá el producto de 256 bits de SHA-256 al **desaleatorizador de contenido,** y, si la longitud de CW es *N* bits, el **desaleatorizador de contenido** truncará el producto en N bits. En ambos casos, se utilizará el método de truncado especificado en [NIST SP 800-107].

10.5 Algoritmo de código de autenticación de mensaje

En esta cláusula se especifica el algoritmo MAC presentado en la cláusula 7.5. Este **algoritmo de código de autenticación de mensaje** es el especificado en [ISO/IEC 9797-1] con las siguientes características:

- El cifrado de bloque será AES-128.
- El relleno del mensaje se hará con el Método de Relleno 3. Este método que la longitud en bits del mensaje e(LK_t, *r*) || A sin relleno sea igual a Lon + 129.
- Se utilizará el Algoritmo MAC 1 para calcular el MAC del mensaje y la clave secreta.
- La longitud del MAC será de τ bits.

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 que incorporar los requisitos de la especificación de protección mejorada del contenido (ECP) de MovieLabs [b ECP]. Las Recomendaciones [b-ITU-T J.1011], [b-ITU-T J.1012], [b-ITU-T J.1013], [b-ITU-T J.1014], ITU-T J.1015 y [b-ITU-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 (CE9) 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 CE9, 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 de 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-ITU-T J.1010] Recommendation ITU-T J.1010 (2016), *Embedded common interface for exchangeable CA/DRM solutions; Use cases and requirements*.

[b-ITU-T J.1011] Recommendation ITU-T J.1011 (2016), *Embedded common interface for exchangeable CA/DRM solutions; Architecture, definitions and overview*.

[b-ITU-T J.1012] Recommendation ITU-T J.1012 (2020), *Embedded common interface for exchangeable CA/DRM solutions; CA/DRM container, loader, interfaces, revocation*.

[b-ITU-T J.1013] Recommendation ITU-T J.1013 (2020), *Embedded common interface for exchangeable CA/DRM solutions; The virtual machine*.

[b-ITU-T J.1014] Recommendation ITU-T J.1014 (2020), *Embedded common interface for exchangeable CA/DRM solutions; Advanced security – ECI-specific functionalities*.

[b-ITU-T J.1015.1] Recommendation ITU-T J.1015.1 (2020), *Embedded common interface for exchangeable CA/DRM solutions; The advanced security system – Key ladder block: Authentication of control word-usage rules information and associated data 1*.

[b-SG9 Report 17 Ann.1] ITU-T SG9 meeting report, SG9-R17-Annex 1 (2020), Annex 1 to Report 17 of the SG9 fully virtual meeting held 16-23 April 2020. https://www.itu.int/md/T17-SG09-R-0017/en

[b-ISO/IEC 23001-7] ISO/IEC 23001-7:2016: *Information technology – MPEG systems technologies – Part 7: Common encryption in ISO base media file format files*.

[b-ATSC A/70-1] ATSC Standard A/70 Part 1:2010, *Conditional access system for terrestrial broadcast*. https://www.atsc.org/standard/a70-part-12010-conditional-access-system-for-terrestrial-broadcast/

[b-ETSI GS ECI 001-5-2] ETSI GS ECI 001-5-2 V1.1.1 (2017-07), *Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 5: The Advanced Security System; Sub-part 2: Key Ladder Block*. https://www.etsi.org/deliver/etsi_gs/ECI/001_099/0010502/01.01.01_60/gs_ECI0010502v010101p.pdf

[b-ETSI TS 100 289] ETSI TS 100 289 V1.1.1 (2011), *Digital video broadcasting (DVB); Support for use of the DVB scrambling algorithm version 3 within digital broadcasting systems*: https://www.etsi.org/deliver/etsi_ts/100200_100299/100289/01.01.01_60/ts_100289v010101p.pdf

[b-ETSI TS 103 127] ETSI TS 103 127 V1.1.1 (2013), *Digital video broadcasting (DVB); Content scrambling algorithms for DVB-IPTV services using MPEG2 transport streams*: https://www.etsi.org/deliver/etsi_ts/103100_103199/103127/01.01.01_60/ts_103127v010101p.pdf

[b-GY/T 277-2014] ChinaDRM Lab, GY/T 277-2014: 互联网电视数字版权管理技术规范 [Technical specification for digital rights management for internet television].

[b-IEEE-OUI] IEEE Standards Association (2017), *Guidelines for use of extended unique identifier (EUI), organizationally unique identifier (OUI) and company ID (CID)*.
https://standards.ieee.org/develop/regauth/tut/eui.pdf

[b-ROEL] Roelse, P. (2014). *A new key establishment protocol and its application in pay-TV systems*.
https://arxiv.org/pdf/1308.4371.pdf

[b-ECP] MovieLabs Specification for Enhanced Content Protection – Version 1.2
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