

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1191

(02/2009)

SERIE X: REDES DE DATOS, COMUNICACIONES DE
SISTEMAS ABIERTOS Y SEGURIDAD

Aplicaciones y servicios con seguridad – Seguridad en
la TVIP

Requisitos funcionales y arquitectura para los aspectos de seguridad de la TVIP

Recomendación UIT-T X.1191

RECOMENDACIONES UIT-T DE LA SERIE X
REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	X.1–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	
Aspectos generales de la seguridad	X.1000–X.1029
Seguridad de las redes	X.1030–X.1049
Gestión de la seguridad	X.1050–X.1069
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	X.1120–X.1139
Seguridad en la web	X.1140–X.1149
Protocolos de seguridad	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	X.1200–X.1229
Lucha contra el correo basura	X.1230–X.1249
Gestión de identidades	X.1250–X.1279
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T X.1191

Requisitos funcionales y arquitectura para los aspectos de seguridad de la TVIP

Resumen

En esta Recomendación se abordan los requisitos funcionales, la arquitectura y los mecanismos que se refieren a los aspectos de seguridad de los contenidos, servicios, redes, terminales y abonados (usuarios finales) de la TVIP.

Orígenes

La Recomendación UIT-T X.1191 fue aprobada el 20 de febrero de 2009 por la Comisión de Estudio 17 (2009-2012) del UIT-T por el procedimiento de la Resolución 1 de la AMNT.

Palabras clave

Aleatorización, arquitectura de seguridad, autenticación, autorización, encriptación, protección de la privacidad, protección de servicios y contenidos, seguridad, TVIP.

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/>.

© UIT 2009

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 Términos y definiciones	1
3.1 Términos definidos en otros documentos.....	1
3.2 Términos definidos en la presente Recomendación	3
4 Abreviaturas y acrónimos	5
5 Convenios	6
6 Requisitos de seguridad	6
6.1 Requisitos generales de seguridad.....	6
6.2 Requisitos de la seguridad de contenidos.....	6
6.3 Requisitos de la seguridad del servicio	9
6.4 Requisitos de seguridad de la red	11
6.5 Requisitos de seguridad de los terminales.....	12
6.6 Requisitos de seguridad del abonado	13
7 Arquitectura de seguridad.....	13
7.1 Arquitectura general de seguridad.....	14
7.2 Arquitectura de protección de contenidos	16
7.3 Arquitectura de protección del servicio.....	19
7.4 Descripción de las funciones y bloques funcionales de las arquitecturas de seguridad de la TVIP	20
8 Mecanismos de seguridad.....	23
8.1 Mecanismos de seguridad relativos a la protección de contenidos	23
8.2 Mecanismos de seguridad relativos a la protección del servicio.....	24
8.3 Mecanismos de seguridad relativos a la protección de redes	25
8.4 Mecanismos de seguridad relativos a la protección de dispositivos de aparatos terminales	25
8.5 Mecanismos de seguridad relativos al abonado o usuario final	26
Anexo A – Protección de la seguridad del abonado	27
A.1 Protección de los datos del usuario	27
A.2 Control parental, protección de menores de edad a efectos legales y control de acceso	28
Apéndice I – Amenazas de seguridad	29
I.1 Modelo de amenazas de seguridad	29
Apéndice II – Interoperabilidad de la SCP	33
II.1 Introducción a la interoperabilidad de la SCP.....	33
II.2 Escenarios de la SCP interoperable.....	33
II.3 Ámbito técnico de interoperabilidad de la SCP	34

	Página
II.4 Arquitecturas interoperables de la SCP	35
II.5 Escenarios de la SCP-B o de la SCP-IX instalados en el TD.....	37
Apéndice III – Ejemplo de proceso de protección de contenidos TVIP	39
Apéndice IV – Protección de contenidos y gestión de copias para DVB.....	40
IV.1 Introducción.....	40
IV.2 Definiciones.....	40
IV.3 Abreviaturas y acrónimos.....	42
IV.4 La arquitectura CPCM.....	42
IV.5 Modelo de referencia y entidades funcionales CPCM	44
IV.6 Dominio autorizado CPCM.....	44
IV.7 Reglas de utilización de contenidos CPCM	44
IV.8 Metadatos de información del estado de utilización	45
IV.9 Contenidos CPCM.....	45
IV.10 El Dispositivo CPCM.....	45
IV.11 Reglas de utilización e información del estado de utilización	45
Apéndice V – Esquema transcodificable seguro.....	46
V.1 Introducción al esquema transcodificable seguro.....	46
Bibliografía	47

Introducción

Los servicios de TVIP, los contenidos que se entregan a través de ellos y los dispositivos terminales utilizados para el procesamiento y entrega de tales servicios requieren que se tengan en cuenta muchos aspectos de seguridad. En esta Recomendación se presentan los requisitos, modelos de arquitectura, entidades funcionales, interfaces, mecanismos y otra información para describir y solucionar los problemas que plantea la seguridad.

Recomendación UIT-T X.1191

Requisitos funcionales y arquitectura para los aspectos de seguridad de la TVIP

1 Alcance

En esta Recomendación se abordan los requisitos funcionales, la arquitectura y los mecanismos que se refieren a los aspectos de seguridad y protección de los contenidos, servicios, redes, terminales y abonados de la TVIP. La intención de esta Recomendación es que los requisitos y funciones pertinentes identificadas en la misma puedan aplicarse adecuadamente, en función del servicio de TVIP y de los modelos empresariales, que pueden exigir distintos niveles de capacidades de seguridad.

2 Referencias

Las Recomendaciones del UIT-T relacionadas a continuación y demás 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 demás 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 demás referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. La referencia a un documento en la presente Recomendación como documento autónomo, no le confiere el carácter de Recomendación.

[UIT-T X.509] Recomendación UIT-T X.509 (2008) | ISO/CEI 9594-8:2008, *Tecnología de la información – Interconexión de sistemas abiertos – El Directorio: Marcos para certificados de claves públicas y atributos*.

[UIT-T Y.1910] Recomendación UIT-T Y.1910, *Arquitectura funcional de la TVIP*.

3 Términos y definiciones

3.1 Términos definidos en otros documentos

En la presente Recomendación se utilizan los siguientes términos definidos en otros documentos:

3.1.1 control de acceso [b-UIT-T X.800]: Prevención del uso no autorizado de un recurso, incluida la prevención del uso de un recurso de una manera no autorizada.

3.1.2 aplicación [b-UIT-T Y.101]: Conjunto estructurado de capacidades que proporcionan una funcionalidad de valor añadido soportada por uno o más servicios.

3.1.3 autenticación [b-UIT-T X.800]: Véanse autenticación del origen de los datos y autenticación de entidad par.

3.1.4 autorización [b-UIT-T X.800]: Atribución de derechos, que incluye la concesión de acceso basada en derechos de acceso.

3.1.5 disponibilidad [b-UIT-T X.800]: Propiedad de ser accesible y utilizable sobre pedido por parte de una entidad autorizada.

3.1.6 confidencialidad [b-UIT-T X.800]: Propiedad de una información que no está disponible ni es divulgada a personas, entidades o procesos no autorizados.

3.1.7 autenticación del origen de los datos [b-UIT-T X.800]: Confirmación de que la fuente de los datos recibidos es la que se alega.

3.1.8 denegación de servicio [b-UIT-T X.800]: Prevención de acceso autorizado a recursos o retardo deliberado de operaciones críticas desde el punto de vista del tiempo.

3.1.9 firma digital [b-UIT-T X.800]: Datos añadidos a una unidad de datos, o transformación criptográfica (véase criptografía) de una unidad de datos que permite al receptor de la unidad de datos demostrar el origen y la integridad de la unidad de datos y protegerla contra la falsificación (por ejemplo, por el receptor).

3.1.10 tren elemental [b-UIT-T H.222.0]: Término genérico para designar un tren de bits de vídeo codificado, de audio codificado o de otro tipo de codificación dentro de un paquete PES.

NOTA – PES significa tren elemental paquetizado (*packetized elementary stream*).

3.1.11 arquitectura funcional [b-UIT-T Y.2012]: Conjunto de entidades funcionales y puntos de referencia, entre ellos utilizados para describir la estructura de una red de próxima generación. Estas entidades funcionales vienen separadas por puntos de referencia y, por consiguiente, definen la distribución de las funciones.

3.1.12 entidad funcional [b-UIT-T Y.2012]: Entidad que comprende un conjunto indivisible de funciones específicas. Las entidades funcionales son conceptos lógicos, mientras que los agrupamientos de entidades funcionales se utilizan para describir implementaciones prácticas y físicas.

3.1.13 integridad [b-UIT-T X.800]: Propiedad que garantiza que los datos no han sido alterados ni destruidos de una manera no autorizada.

3.1.14 clave [b-UIT-T X.800]: Secuencia de símbolos que controla las operaciones de cifrado y descifrado.

3.1.15 gestión de claves [b-UIT-T X.800]: Generación, almacenamiento, distribución, supresión, archivo y aplicación de claves, de acuerdo con una política de seguridad.

3.1.16 usurpación de identidad (o impostura) [b-UIT-T X.800]: Pretensión de una entidad de hacerse pasar por otra diferente.

3.1.17 proveedor de red [b-UIT-T Q.1290]: Organización que mantiene y explota los componentes de red necesarios para la funcionalidad de la TVIP.

NOTA 1 – Un proveedor de red puede opcionalmente actuar también como proveedor de servicios.

NOTA 2 – Aunque se consideran dos entidades independientes, el proveedor de servicios y el proveedor de red pueden opcionalmente constituir una entidad organizativa.

3.1.18 autenticación de entidad par [b-UIT-T X.800]: Corroboración de que una entidad par en una asociación es la pretendida.

3.1.19 privacidad [b-UIT-T X.800]: Derecho de las personas a controlar, o influir en, la información relacionada con ellos que pueda recogerse o almacenarse y las personas a las cuales, o por las cuales, esta información puede ser revelada.

3.1.20 repudio [b-UIT-T X.800]: Negación de una de las entidades implicadas en una comunicación de haber participado en toda la comunicación o en parte de ella.

3.1.21 etiqueta de seguridad [b-UIT-T X.800]: Marca vinculada a un recurso (que puede ser una unidad de datos) que denomina o designa los atributos de seguridad de dicho recurso.

NOTA – La marca y/o vinculación puede ser explícita o implícita.

3.1.22 política de seguridad [b-UIT-T X.800]: Conjunto de criterios para la prestación de servicios de seguridad.

3.1.23 proveedor de servicios [b-UIT-T M.1400]: Referencia general a un operador que proporciona servicios de telecomunicación a clientes y otros usuarios en base a un cuadro de tarifas o a un contrato. Un proveedor de servicios puede opcionalmente explotar una red. Un proveedor de servicios puede opcionalmente ser cliente de otro proveedor de servicios.

3.1.24 amenaza [b-UIT-T X.800]: Violación potencial de la seguridad.

3.2 Términos definidos en la presente Recomendación

En esta Recomendación se definen los siguientes términos:

3.2.1 adquisición: Proceso de obtención de contenidos por parte del usuario final.

3.2.2 exportación de contenidos: Proceso de exportar con seguridad el contenido de TVIP desde el terminal TVIP a otro terminal propiedad del usuario con derecho a utilizarlo.

3.2.3 protección de contenidos: Garantía de que los usuarios finales sólo pueden utilizar los contenidos que ya han adquirido con arreglo a los derechos que les han sido otorgados por el titular de éstos. La protección de contenidos conlleva la preservación de éstos frente a la copia o distribución ilegal, la interceptación, manipulación, uso ilegítimo, etc.

3.2.4 rastreo de contenidos: Proceso que permite la identificación del origen (arbitrario) de un contenido y/o de su responsable (por ejemplo, un usuario final) a fin de facilitar la investigación subsiguiente en el caso de uso de contenidos sin autorización, por ejemplo la copia o redistribución de contenidos.

NOTA – La información de rastreo de contenidos puede acompañar al propio contenido ya sea como metadatos o como filigrana forense.

3.2.5 derechos adquiridos: En relación con los niveles de autorización y en particular con el acceso condicional, la información que puede utilizar un abonado para tener acceso a determinados servicios de la TVIP en su aparato terminal (TD, *terminal device*) de TVIP.

3.2.6 protección del aparato terminal (TD) de la TVIP: Verificación de que el TD utilizado por un usuario final en la recepción de un servicio puede utilizar con fiabilidad y seguridad los contenidos sin perjuicio del respeto de los derechos de utilización concedidos para dichos contenidos ni de la protección física y electrónica de la integridad del TD y de la confidencialidad de los contenidos y parámetros de seguridad críticos (por ejemplo, de las claves salvadas) que no estén protegidos.

3.2.7 TV lineal: Servicio de radiodifusión de TV semejante a la forma tradicional de servicios de televisión proporcionados por operadores de cable, de televisión terrenal y de televisión por satélite directa al hogar; aunque, en este caso, los contenidos de programas se transmiten con arreglo a un horario definido y pensado para el consumo en tiempo real por parte del usuario final.

3.2.8 metadatos para la aplicación de la filigrana: Metadatos creados para facilitar la posterior inserción de filigrana por los dispositivos subsiguientes

3.2.9 peska (*phishing*): Adquisición de información personal o sensible tal como el nombre del usuario, su fecha de nacimiento o detalles de su tarjeta de crédito, haciéndose pasar por una entidad digna de confianza.

3.2.10 derechos legales: Se refiere a la capacidad de ejecutar una serie predefinida de funciones de uso sobre un elemento de contenido; entre estas funciones de usos se encuentran los permisos (por ejemplo, visionar/oír, copiar, modificar, grabar, extraer, muestrear, conservar durante un cierto tiempo, distribuir), las restricciones (por ejemplo, reproducir/visionar/oír varias veces, reproducir, visionar/oír un cierto número de horas), y obligaciones (por ejemplo, pago, rastreo de contenidos) que se aplican al contenido y permiten la libertad de uso otorgada al usuario final.

3.2.11 expresión de los derechos: Plasmación sintáctica de los derechos legales en un formato concreto y formal

3.2.12 SCP de extremo a extremo: Modo de funcionamiento de la protección del servicio y contenidos en el cual se accede o modifica el contenido por parte de dispositivos de extremo con arreglo a los derechos otorgados utilizando un único sistema de protección del servicio y contenidos.

3.2.13 SCP en puente: Modo de funcionamiento de la protección del servicio y contenidos en el cual se encuentran operativos dos o más sistemas de protección del servicio y contenidos en un único dispositivo que hace de puente entre dichos sistemas de protección del servicio y contenidos. Se puede acceder a los contenidos adquiridos a través de un sistema de protección del servicio y contenidos a través de otro sistema de protección del servicio y contenidos en el puente de acuerdo con los derechos otorgados.

3.2.14 SCP con intercambio: Modo de funcionamiento de protección del servicio y contenidos más genérico que afecta a dos o más dispositivos y en el que cada dispositivo tiene uno o más sistemas de protección del servicio y contenidos. Los contenidos adquiridos por un dispositivo a través de uno de sus sistemas de protección del servicio y contenidos pueden ser transferidos con seguridad a otro dispositivo, en el que se tenga acceso, a través de un sistema distinto de protección del servicio y contenidos con arreglo a los derechos otorgados.

3.2.15 aleatorización: Proceso diseñado para proteger los contenidos multimedia; normalmente la aleatorización utiliza tecnología de encriptación para proteger los contenidos.

3.2.16 algoritmo de aleatorización: Algoritmo utilizado en los procesos de aleatorización y desaleatorización.

3.2.17 esquema transcodificable seguro: Tipo de esquema de seguridad que permite que un nodo de red intermedio ejecute las transcodificación sin desencriptación manteniendo la seguridad extremo a extremo; este esquema puede ejecutarse combinando la codificación escalonable, la encriptación progresiva y la paquetización. El esquema transcodificable seguro puede ofrecer tanto confidencialidad como integridad/autenticación de los mensajes.

3.2.18 protección del servicio: Garantía de que el usuario final sólo puede adquirir un servicio y, por extensión, el contenido alojado en el mismo, de acuerdo con su derecho adquirido a la recepción del mismo; la protección del servicio comprende también su preservación de accesos no autorizados durante el recorrido de los contenidos de TVIP por las conexiones de servicio TVIP.

3.2.19 protección de servicios y contenidos: Combinación de protección del servicio y protección de contenidos o bien sistema o implementación de los mismos.

3.2.20 simulación (*spoofing*): Actividad mediante la cual una fuente falsificada (simulada) (por ejemplo una persona o programa informático) se hace pasar con éxito por fuente legítima falsificando datos con el fin de obtener información u ocultar la fuente verdadera de modo que la falsificada pueda llevar a cabo actividades no autorizadas tales como la propagación de programas informáticos dañinos (por ejemplo, virus), etc.

3.2.21 resistente a la manipulación: Producto, paquete o sistema al que se puede acceder física o lógicamente resistente a la manipulación por parte de los usuarios/atacantes.

3.2.22 transcodificación: Proceso de transformación de contenidos multimedia tales como imágenes, texto, audio o vídeo, de un formato original a un formato o calidad diferente.

3.2.23 protección de la privacidad del usuario: Garantía de que la información que se considera privada (o confidencial) por parte de un usuario final se mantiene confidencial sin perjuicio de que pueda ser revelada obligatoriamente por prescripción legal.

3.2.24 firma de vídeo: Metadatos (o característica visual) que permiten identificar un contenido de vídeo; a diferencia de la filigrana insertada manipulando el contenido de vídeo original, la firma de vídeo se extrae del propio contenido de vídeo sin riesgo de deterioro de su calidad.

4 Abreviaturas y acrónimos

En la presente Recomendación se utilizan las siguientes abreviaturas y acrónimos:

AAA	Autenticación, autorización y contabilización (<i>authentication, authorization, and accounting</i>)
AD	Dominio autorizado (<i>authorized domain</i>)
CBC	Encadenado de bloque cifrado (<i>cipher block chaining</i>)
CDN	Red de entrega de contenidos (<i>content delivery network</i>)
DNG	Pasarela de red de entrega (<i>delivery network gateway</i>)
DNGF	Función de pasarela de red de entrega (<i>delivery network gateway function</i>)
DoS	Denegación de servicio (<i>denial of service</i>)
ECB	Libro de códigos eléctricos (<i>electric code book</i>)
ECM	Mensaje de control de derechos (<i>entitlement control message</i>)
EMM	Mensaje de gestión de derechos (<i>entitlement management message</i>)
EPG	Guía de programas electrónica (<i>electronic program guide</i>)
HN	Red doméstica (<i>home network</i>)
HN-TD	Dispositivo terminal de la red doméstica (<i>home network terminal device</i>)
ID	Identificador (<i>identifier</i>)
TVIP	Televisión de protocolo Internet (<i>Internet protocol television</i>)
MIKEY	Introducción de claves en multimedios de Internet (<i>multimedia Internet KEYing</i>)
NAT	Traducción de direcciones de red (<i>network address translation</i>)
OFB	Retroalimentación de salida (<i>output feedback</i>)
P2P	Par a par (<i>peer to peer</i>)
PDA	Agenda electrónica (<i>personal digital assistant</i>)
PIN	Número de identificación personal (<i>personal identification number</i>)
PKI	Infraestructura de claves públicas (<i>public key infrastructure</i>)
PVR	Grabador personal de vídeo (<i>personal video recorder</i>)
QoE	Calidad percibida (<i>quality of experience</i>)
QoS	Calidad de servicio (<i>quality of service</i>)
REL	Lenguaje de expresión de derechos (<i>rights expression language</i>)
SCP	Protección del servicio y contenidos (<i>service and content protection</i>)
SCP-B	SCP en puente (<i>SCP bridge</i>)
SCP-EE	SCP extremo a extremo (<i>SCP end-to-end</i>)
SCP-IX	SCP con intercambio (<i>SCP interchange</i>)
STS	Esquema transcodificable seguro (<i>secure transcodable scheme</i>)
TD	Aparato terminal conforme con TVIP (<i>IPTV-compliant terminal device</i>)
USB	Bus de serie universal (<i>universal serial bus</i>)
VoD	Vídeo a la carta (<i>video on demand</i>)

5 Convenios

En la presente Recomendación:

La expresión "**se le exige que**" indica un requisito que debe cumplirse estrictamente, no permitiéndose desviación alguna si la Recomendación pretende reclamar su conformidad.

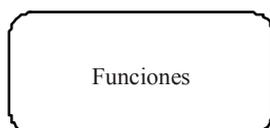
La expresión "**se recomienda**" indica un requisito recomendado pero que no se exige con carácter taxativo. Por ello no es necesario cumplir este requisito para reclamar su conformidad.

La expresión "**se le prohíbe**" indica un requisito que debe cumplirse estrictamente, sin permitirse desviación alguna si la Recomendación pretende ser conforme.

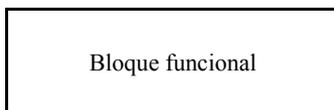
La expresión "**puede opcionalmente**" indica un requisito opcional admisible que no reviste en absoluto el carácter de recomendación. Esta expresión no pretende dar a entender que la implementación del fabricante deba suministrar una opción o característica que puedan ser activadas opcionalmente por el operador de red o proveedor del servicio. Más bien significa que el fabricante puede proporcionar opcionalmente esta característica sin menoscabo de su derecho de reclamar la conformidad con la especificación.

En el contexto de la arquitectura de seguridad de la TVIP en la presente Recomendación:

Las "**funciones**" se definen como un conjunto de funcionalidades y se representan por el siguiente símbolo:



El "**bloque funcional**" se define como un grupo de funcionalidades no subdivididas al nivel de detalle descrito en la presente Recomendación y se representa mediante el siguiente símbolo:



6 Requisitos de seguridad

6.1 Requisitos generales de seguridad

- Se recomienda que la arquitectura TVIP tenga en cuenta la influencia/repercusión sobre la calidad de funcionamiento, la calidad de servicio, la utilizabilidad, la escalonabilidad y las limitaciones de índole económica que afectan al desarrollo de la seguridad.
- La arquitectura TVIP puede opcionalmente soportar la protección de contenidos compartidos por el usuario final.

6.2 Requisitos de la seguridad de contenidos

En esta cláusula se especifican los requisitos relacionados, individual o colectivamente, con la seguridad y protección de contenidos.

Requisitos de la arquitectura

- Se requiere que la arquitectura TVIP soporte la protección de contenidos definida en la cláusula 3.

- Se requiere que la arquitectura TVIP soporte la asociación de contenidos con metadatos de protección y gestión de contenidos.
- Se requiere que la arquitectura TVIP soporte la entrega segura de protección de contenidos y metadatos de gestión de contenidos, entre ellos los metadatos de derechos de utilización.
- Se requiere que la arquitectura TVIP soporte los metadatos de derechos de utilización de contenidos que distinguen entre derechos de utilización y, en particular, de reproducción (visionado), almacenamiento, (re)distribución y combinaciones de éstos.
- Se requiere que la arquitectura TVIP soporte la protección de contenidos distribuidos simultáneamente a un gran número de abonados (escalabilidad).
- Se requiere que la arquitectura TVIP soporte la protección de contenidos transferidos sobre trenes multidifusión y/o unidifusión.
- Se requiere que la arquitectura TVIP soporte la recuperación de contenidos almacenados con arreglo a los derechos de utilización otorgados.
- Si se utiliza el rastreo de contenidos, se requiere que la arquitectura TVIP soporte un rastreo de contenidos robusto fuera de línea (en diferido) (por ejemplo, contenidos de VoD).
- Se prohíbe que la arquitectura TVIP impida el soporte de medios de transporte de información de rastreo de contenidos (por ejemplo, metadatos de facilitación de la filigrana).
- Se prohíbe que la arquitectura TVIP impida la aplicación de tecnología de rastreo de contenidos en la salida del TD a los efectos de identificar de manera exclusiva una sesión (por ejemplo, un canal, una hora/fecha), un TD, y/o un operador de red. Los ejemplos de la tecnología de rastreo de contenidos pueden utilizar información visible o invisible con carácter opcional.
- Se prohíbe que la arquitectura TVIP impida la recuperación de toda la información de rastreo de contenidos a partir del propio contenido.
- Se prohíbe que la arquitectura TVIP impida el soporte de la interoperabilidad de la protección del servicio y contenidos en la que se permita la utilización de los contenidos de TVIP únicamente a los usuarios y dispositivos autorizados, incluso tras su transferencia otro sistema de seguridad.
- Se prohíbe que la arquitectura TVIP impida el soporte de la interoperabilidad de la protección del servicio y contenidos para mantener la información de identificación de tal modo que puedan identificarse coherentemente los contenidos de TVIP con independencia de los esquemas de identificación utilizados y del sistema de seguridad al que se hayan transferido los contenidos.
- Se prohíbe que la arquitectura TVIP impida la interoperabilidad de la protección del servicio y contenidos para evitar degradar el nivel de seguridad cuando los contenidos se transfieren a otro sistema de seguridad.
- Se prohíbe que la arquitectura TVIP impida el soporte de la interoperabilidad de la protección del servicio y contenidos en la que sólo se otorguen derechos a los dispositivos de confianza.
- Se prohíbe que la arquitectura TVIP impida el soporte de la interoperabilidad de la protección del servicio y contenidos a fin de proporcionar un entorno seguro para el intercambio de datos de la interoperabilidad de la protección del servicio y contenidos (por ejemplo, información de autenticación, metadatos, información de claves, etc.).
- Se prohíbe que la arquitectura TVIP impida el soporte de la interoperabilidad de servicios y contenidos de modo que ésta no dependa de un equipo físico ni de un soporte lógico específico.

- Se prohíbe que la arquitectura TVIP exija al mecanismo de protección del servicio y contenidos de cualquiera de los dos esquemas SCP que interoperan, que se especifiquen abiertamente para intentar conseguir la interoperabilidad.
- Se prohíbe que la arquitectura TVIP impida el soporte de una interoperabilidad de la protección del servicio y contenidos que sea flexible y ampliable para soportar varios modelos de negocio.
- Se prohíbe que la arquitectura TVIP impida el soporte de la interoperabilidad de la protección del servicio y contenidos entre varios sistemas de seguridad con diferentes mecanismos de seguridad a los efectos de soportar el servicio con desplazamiento en el tiempo (gracias al cual los abonados pueden almacenar los contenidos para recuperarlos más tarde) y con desplazamiento geográfico (gracias al cual los abonados pueden visionar los contenidos en cualquier parte) sin solución de continuidad, incluso con distintos mecanismos de seguridad.
- Se prohíbe que la arquitectura TVIP impida que el soporte de la interoperabilidad de la protección del servicio y contenidos mantenga la transparencia para los usuarios.
- Se prohíbe que la arquitectura TVIP impida el soporte de múltiples mecanismos de protección del servicio y contenidos con independencia de los requisitos específicos del equipo físico o del soporte lógico.

Recomendaciones para la arquitectura

- Si el contenido de la TVIP emplea una tecnología de rastreo de contenidos, se recomienda que ésta sea imperceptible.
- Se recomienda que la arquitectura TVIP soporte un rastreo de contenidos robusto en tiempo real (por ejemplo, para contenidos de radiodifusión).
- Se recomienda que la arquitectura TVIP soporte la capacidad de autenticación y autorización de usuarios finales a los efectos de compartición de servicios (por ejemplo, la exportación y redistribución de contenidos), si se soporta la compartición de contenidos.
- Si la implementación de la arquitectura TVIP utiliza tecnología de rastreo de contenidos basada en la facilitación de filigrana, se recomienda la inserción de los metadatos relevantes en el tren elemental de contenidos utilizando las disposiciones para "datos del usuario" tales como las estipuladas en el esquema de codificación específico.
- Si un dispositivo terminal (TD, *terminal device*) o un dispositivo terminal de la red doméstica (HN-TD, *home network terminal device*) dentro de la arquitectura TVIP soporta múltiples mecanismos de protección de contenidos y servicios, se recomienda utilizar una función de traducción normalizada, dado que existe la posibilidad de vincular más de un sistema SCP y realizar entre ellos la traducción de manera compatible, asegurando al mismo tiempo la compatibilidad de cualquier TD o HN-TD conectado que participe en el mecanismo de traducción.

Opciones de arquitectura

- La arquitectura TVIP puede opcionalmente soportar la inclusión de información de rastreo de contenidos. Ésta puede opcionalmente contener el ID del operador, el ID del propietario de los contenidos, el ID del TD y otras informaciones.

Requisitos del algoritmo de aleatorización

- Se requiere que los algoritmos de aleatorización de trenes de radiodifusión soporten la actualización periódica de las claves criptográficas necesarias.
- Se requiere que los algoritmos de aleatorización para TVIP se construyan utilizando algoritmos criptográficos normalizados y públicamente disponibles.

Recomendaciones para los algoritmos de aleatorización

- Se recomienda que los algoritmos de aleatorización para TVIP tengan una entropía de claves suficientemente grande para proteger efectivamente el contenido frente al criptoanálisis.
- No se prohíbe a la arquitectura TVIP impedir el soporte de algoritmos de aleatorización ampliamente utilizados.
- Se recomienda que la arquitectura TVIP se abstenga de impedir el soporte de múltiples sistemas de aleatorización.
- Se recomienda que los algoritmos de aleatorización para TVIP se puedan implementar con eficiencia tanto en las realizaciones de equipo físico como en las de soporte lógico.
- Se recomienda que los algoritmos de aleatorización para TVIP sean escalonables y con futuro, es decir, que lo sean sus parámetros criptográficos (por ejemplo, la longitud de las claves, los periodos de encriptación, etc.) y los modos criptográficos (por ejemplo, CBC, OFB, ECB, etc.).

Opciones de los algoritmos de aleatorización

- Los algoritmos de aleatorización para TVIP pueden opcionalmente aplicar algoritmos criptográficos de diversa fuerza a tipos de contenidos diferentes.

6.3 Requisitos de la seguridad del servicio

En esta cláusula se especifican los requisitos que se refieren, individual o colectivamente, a los servicios y a la protección de éstos.

Requisitos de la arquitectura

- Se requiere que la arquitectura TVIP soporte la protección del servicio definida en la cláusula 3.
- Se prohíbe a la arquitectura TVIP impedir el soporte de actualización de la SCP o la renovación de la SCP en el TD desde el lado servidor.
- Se requiere que la arquitectura TVIP soporte la autorización y autenticación de usuarios (abonados) finales.
- Se requiere que la arquitectura TVIP soporte un mecanismo de señalización para indicar al TD que utilice un algoritmo de aleatorización específico basado en un marco normalizado.
- Se requiere que la arquitectura TVIP tenga la capacidad de utilizar sistemas de gestión de clave estándar (por ejemplo, MIKEY, EMM/ECM) requeridos para la interoperabilidad.
- Se requiere que la arquitectura TVIP soporte la capacidad de actualización y consulta del sistema SCP en relación con los algoritmos de aleatorización para TVIP y de otros algoritmos de aleatorización cualesquiera seleccionados por el operador en el lado servidor a través de las interfaces de la SCP.
- Se requiere que la arquitectura TVIP soporte mecanismos de SCP que sean independientes de formatos de contenidos específicos.
- Se requiere que la arquitectura TVIP soporte un mecanismo para proporcionar la protección de la integridad y la autenticación del origen de los datos para metadatos sensibles.
- Se requiere que la arquitectura TVIP soporte un mecanismo para la entrega segura a los TD de derechos de propiedad e información de control de acceso a los contenidos.
- Se requiere que la arquitectura TVIP soporte el control de utilización de contenidos (por ejemplo, la reproducción).

- Se requiere que la arquitectura TVIP soporte diferentes modos de reproducción, por ejemplo con la limitación del número de visionados, con limitación del tiempo de visionado o con restricciones sobre el retroceso o el avance rápido.
- Se requiere que la arquitectura TVIP soporte un mecanismo que permita el mantenimiento de la confidencialidad de los mensajes de señalización entre el servidor SCP y el cliente SCP.
- Se requiere que la arquitectura TVIP soporte un mecanismo que permita el mantenimiento de la autenticidad de los mensajes de señalización entre el servidor SCP y el cliente SCP.
- Se requiere que la arquitectura TVIP soporte un mecanismo que permita el mantenimiento de la integridad de los mensajes de señalización entre el servidor SCP y el cliente SCP.
- Se requiere que la arquitectura TVIP soporte un mecanismo para recuperar con seguridad los parámetros de la SCP del TD (por ejemplo, la configuración, el estado).
- Se requiere que la arquitectura TVIP soporte un mecanismo de actualización segura de los parámetros de la SCP del TD (por ejemplo, configuración).
- Se prohíbe que la arquitectura TVIP impida el soporte de la capacidad de activar y desactivar la función de rastreo de contenidos de modo programado (por ejemplo, tomando como base el tiempo, un evento, el contenido o un canal).
- Si emplea un sistema de gestión de claves, se requiere el diseño del mismo contemple su escalabilidad, fiabilidad e interoperabilidad.
- Se prohíbe que la arquitectura TVIP impida el soporte de la instalación y explotación de varias soluciones de protección del servicio sin sustitución del equipo físico, excepto de los dispositivos extraíbles (tales como las llaves USB y las tarjetas SIM).
- Se prohíbe que la arquitectura TVIP impida el soporte de un mecanismo de identificación que implemente las soluciones de protección del servicio disponibles y que sea capaz de satisfacer el requisito específico para la protección de los contenidos relacionados.
- Se prohíbe que la arquitectura TVIP impida el soporte de un mecanismo de descubrimiento del sistema SCP que pueda soportar un método de descubrimiento y adaptarse al mismo siempre que un contenido específico exija un sistema de protección del servicio específico.
- Se prohíbe que la arquitectura TVIP impida el soporte de un mecanismo destinado a la selección de un sistema SCP de entre los sistemas SCP disponibles sin sustitución de equipo físico, excepto los dispositivos extraíbles.
- Se prohíbe que la arquitectura TVIP impida el soporte de descarga segura de un sistema SCP. El sistema SCP descargado puede opcionalmente depender de los requisitos específicos de protección del servicio.
- Si se instala un SCP descargables, se requiere que la arquitectura TVIP ejecute la protección de la integridad y la autenticación del origen de los datos para el sistema SCP descargado.
- Si se soporta la descarga segura de un programa de aplicación al TD, se requiere que la arquitectura TVIP ejecute la protección de la integridad y la autenticación del origen de los datos para las aplicaciones descargadas.

Recomendaciones para la arquitectura

- Se recomienda que la arquitectura TVIP permita la confidencialidad de los contenidos.
- Se recomienda que la arquitectura TVIP soporte varios algoritmos de aleatorización.
- Se recomienda que la arquitectura TVIP soporte la capacidad de autenticar y autorizar a los usuarios finales para los servicios de compartición de contenidos (por ejemplo, la exportación y redistribución de contenidos).

- Si la arquitectura TVIP emplea un sistema de gestión de claves y éste se ajusta a un esquema jerárquico, se recomienda que soporte la escalabilidad.
- Si la arquitectura TVIP emplea un sistema de gestión de claves que utiliza un protocolo de gestión de claves de grupo, la gestión de claves es jerárquica y hay una alternativa de algoritmo de gestión de claves, se recomienda que ésta soporte la escalabilidad.
- Si la arquitectura TVIP emplea un sistema de gestión de claves que utiliza claves a corto plazo, se recomienda el establecimiento del trayecto de medios de tal modo que las limitaciones de paso y de anchura de banda del NAT no afecten al intercambio de claves.
- Se recomienda que la arquitectura TVIP soporte como mínimo el mismo grado de protección (a los efectos de controlar los accesos no autorizados) de la información de rastreo de contenidos que el aplicado al correspondiente contenido rastreado.
- Se recomienda que la arquitectura TVIP soporte la transmisión conjunta de contenidos e información de rastreo de los mismos, manteniendo al mismo tiempo la sincronización de los contenidos y de la información de rastreo de éstos durante su transporte.
- Si la arquitectura TVIP emplea PIK para autenticar el TD, el servicio o el proveedor de contenidos, considerando el carácter jerárquico multinivel de la PIK, se recomienda soportar la escalabilidad, la fiabilidad y la interoperabilidad.
- Si la arquitectura TVIP emplea PIK para el servicio TVIP, utilizando un formato de certificados normalizado públicamente disponible, se recomienda una lista de revocación de certificados o un protocolo de estado de certificados en línea.
- Se recomienda que la arquitectura TVIP soporte la descarga segura de programas de aplicación al TD.
- Se recomienda que la arquitectura TVIP soporte un mecanismo para limitar los derechos de visionado de ciertos programas a ciertos grupos de abonados (por ejemplo, bloqueando el visionado a los residentes de una zona específica, lo que puede ser útil, por ejemplo, para acontecimientos deportivos).

Opciones de arquitectura

- Para ofrecer un servicio TVIP escalable para una terminal propiedad del usuario cuya resolución sea distinta de la del terminal de usuario, la arquitectura TVIP puede opcionalmente soportar la capacidad de un esquema de transcodificación seguro como el definido en la cláusula 3.

6.4 Requisitos de seguridad de la red

En esta cláusula se especifican los requisitos que, individual o colectivamente, afectan a las redes y a su protección.

Requisitos de la arquitectura

- Se requiere que la arquitectura TVIP soporte la capacidad de mitigar un ataque DoS.
- Se requiere que la arquitectura TVIP soporte la habilitación de medidas de seguridad para bloquear tráfico ilegal o indeseado.
- Se requiere que la arquitectura TVIP sea resistente a los ataques a su capacidad multidifusión.
- Se recomienda que la arquitectura multidifusión soporte la capacidad de autenticar a una entidad par en el entorno multidifusión general o superpuesto (entre entidades pares).
- Se requiere que el enlace de comunicación entre aparatos terminales de la red doméstica esté protegido a efectos de la seguridad de contenidos, cuando transporte un contenido con recargo (es decir pagado por el consumidor) que no esté protegido.

- Se requiere que la arquitectura TVIP soporte la autenticación DNG por parte de la función de gestión TVIP.
- Se requiere que la arquitectura TVIP soporte la autenticación de la función de gestión TVIP por parte de la DNG.

Recomendaciones para la arquitectura

- Para proteger la red doméstica de accesos maliciosos o no autorizados, se recomienda que la arquitectura TVIP soporte la capacidad de función de pasarela de red de entrega (DNGF, *delivery network gateway function*) a fin de establecer unos cortafuegos configurable a distancia con varios niveles de seguridad y pasarelas adecuadas a nivel de la aplicación.
- Se recomienda que la arquitectura TVIP soporte la capacidad de la gestión TVIP para configurar a distancia el NAT y la función de protección frente a intrusiones de la DNG.
- Se recomienda que la arquitectura TVIP soporte la capacidad de configurar a distancia el NAT y la función de protección contra intrusiones de la DNG por parte de la función de gestión TVIP a distancia.
- Se recomienda que la arquitectura TVIP proteja la gestión a distancia del TD en el caso de que se soporte la gestión a distancia.
- Se recomienda que la arquitectura TVIP soporte la utilización de la información de etiquetas del contenido para controlar la entrega de los contenidos.

6.5 Requisitos de seguridad de los terminales

En esta cláusula se especifican los requisitos que, individual o colectivamente, afectan a los TD o a su protección.

Requisitos de la arquitectura

- Se requiere que la arquitectura TVIP soporte la protección del TD definida en la cláusula 3.
- Se requiere que la arquitectura TVIP soporte la autenticación del TD.
- Se requiere que la arquitectura TVIP soporte la resistencia a la manipulación física del TD.
- Se requiere que la arquitectura TVIP soporte un medio de detectar la manipulación física del TD.
- Si se utiliza la SCP descargable, se requiere que la arquitectura TVIP soporte la descarga e instalación segura del código operativo de la SCP a los TD.
- Se requiere que la arquitectura TVIP soporte un medio seguro de ejecutar procesos críticos para la seguridad en los TD tales como la gestión de las claves y la serialización de los medios a fin de abortar la reproducción de contenidos en el caso de un mal funcionamiento relacionado con la seguridad, de que se haya detectado una manipulación o de que exista otra indicación de uso indebido.
- Se requiere que la arquitectura TVIP ofrezca protección física a los procesos vulnerables que proporcionan la seguridad y a los componentes implicados en el proceso de transmisión y almacenamiento de los contenidos de valor en el TD cuando falta una protección lógica (tal como la encriptación o las filigranas de serialización). Entre estos procesos se encuentran la desaleatorización y la serialización de medios.
- Se requiere que la arquitectura TVIP reconozca la necesidad de protección física (frente al sondeo o manipulación del sistema de funciones de la SCP en el TD) de los procesos vulnerables que proporcionan la seguridad en el TD, entre ellos la desaleatorización y la serialización de medios (rastreo de contenidos) y de los datos críticos que soportan dichos procesos así como de todos los componentes implicados en el procesamiento, transmisión y

almacenamiento de cualquier contenido de valor carente de protecciones lógicas tales como la encriptación o las filigranas de rastreo de contenidos.

- Se prohíbe que la arquitectura TVIP impida el soporte para el intercambio de contenidos entre el TD y otros dispositivos (físicos o lógicos) siempre que los usos concedidos para este contenido comprendan dicho intercambio.
- Se requiere que la arquitectura TVIP soporte un mecanismo que permita que el TD autentique a los servidores SCP.
- Se prohíbe que la arquitectura TVIP impida el soporte de la renovación de la SCP en el TD.
- Se requiere que la arquitectura TVIP soporte la protección de contenidos digitales o analógicos según exige la ACP de almacenamiento fuera del dispositivo del cliente, en caso de que el TD disponga de salida vídeo/audio digital o analógica.

Recomendaciones para la arquitectura

- Se recomienda que la arquitectura TVIP soporte la exportación de contenidos de los TD permitiendo la transferencia segura de contenidos TVIP desde los terminales TVIP a otros terminales propiedad del usuario con derecho a utilizarlos.

6.6 Requisitos de seguridad del abonado

En esta cláusula se especifican los requisitos que, individual o colectivamente, afectan a los abonados y usuarios finales o a su protección.

Requisitos de la arquitectura

- Se requiere que la arquitectura TVIP soporte la protección de privacidad del usuario definida en la cláusula 3.
- Se requiere que la arquitectura TVIP permita a los usuarios establecer mecanismos de control de acceso (por ejemplo, mediante contraseñas) para restringir el acceso a los contenidos y servicios.
- Se requiere que la arquitectura TVIP sea capaz de indicar la razón por la que se le niega a un usuario el acceso a un contenido.
- Se requiere que la arquitectura TVIP soporte un mecanismo que permita a un abonado solicitar ampliaciones (por ejemplo, más visionados o más tiempo de visionado) de los derechos de utilización asociados a elementos de contenido específicos.

Recomendaciones para la arquitectura

- Se recomienda que la arquitectura TVIP permita al usuario final (con arreglo a los derechos legales) la modificación, por ejemplo la sustitución, de un TD sin que ello afecte intrínsecamente a los derechos a consumir los contenidos.
- Se recomienda que la arquitectura TVIP soporte un mecanismo para la calificación de los programas en función de su contenido.

NOTA – La información de calificación debe utilizarse para el control de acceso, por ejemplo, para el control parental.

7 Arquitectura de seguridad

En esta cláusula se define una arquitectura de seguridad TVIP en términos de una arquitectura de seguridad general, una arquitectura de protección de contenidos y una arquitectura de protección del servicio así como entidades funcionales de seguridad para satisfacer los requisitos descritos en las cláusulas anteriores.

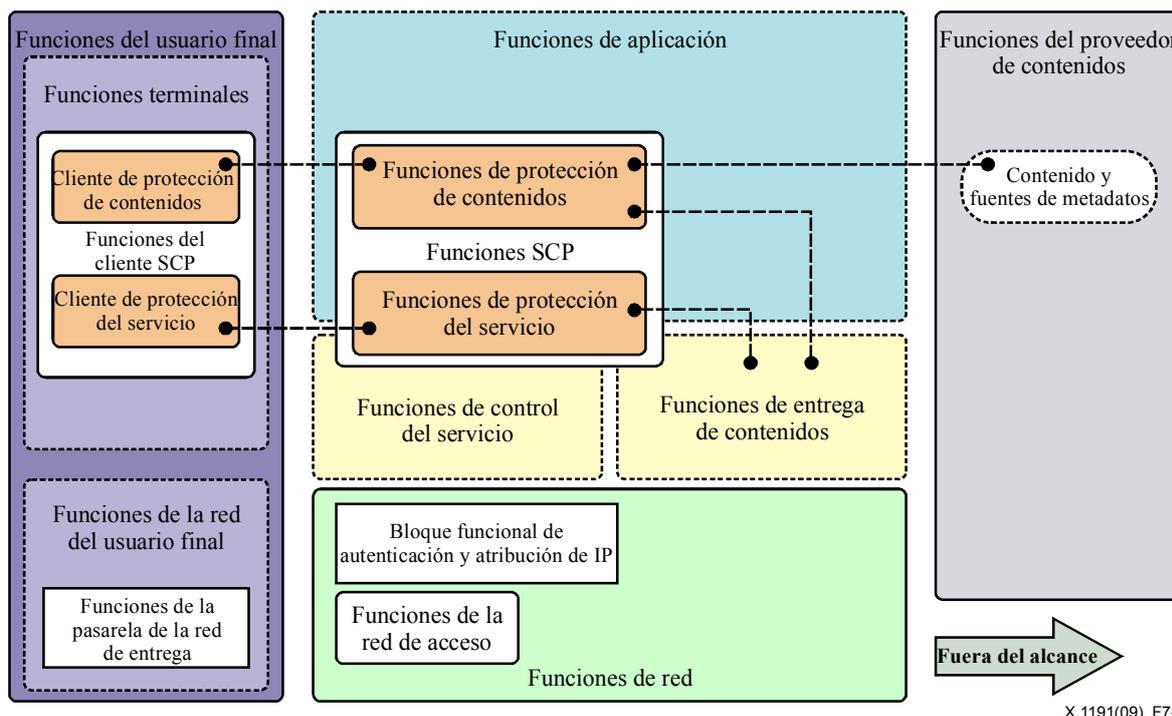
La arquitectura de seguridad TVIP descrita a continuación se supone diseñada para ser utilizada en el contexto de los dominios funcionales TVIP y del marco de arquitectura funcional TVIP definidos en las cláusulas 6 y 8 de [UIT-T Y.1910], respectivamente.

7.1 Arquitectura general de seguridad

En la figura 7-1 se representa una arquitectura general de seguridad para la TVIP. Esta arquitectura general se divide en dos zonas principales: una se considera dentro del alcance de la presente Recomendación, mientras que la otra se considera ajena al mismo. La primera zona comprende los dominios del usuario final, del proveedor de red y del proveedor de servicios, mientras que la segunda comprende el dominio del proveedor de contenidos.

En esta segunda zona, todos los aspectos de seguridad del dominio del proveedor de contenidos y la interconexión entre proveedores de contenidos y proveedores de servicios están sujetos a acuerdos privados entre las partes interesadas que operan en estos dominios. Por este motivo, se consideran fuera del alcance de la presente Recomendación.

Aunque el dominio del proveedor de contenidos y la interconexión entre éste y el dominio del proveedor de servicios se considera fuera del alcance del presente contexto, se incluye el dominio del proveedor de contenidos en las siguientes figuras y descripciones para que sean más completos. A este respecto, cualquier afirmación que afecte a dichos dominios necesita ser considerada como de carácter informativo o explicativo.



NOTA 1 – La función de protección de contenidos y las funciones de protección del servicio de esta figura constituyen las partes más importantes de la arquitectura de seguridad TVIP. La explicación detallada de estas funciones puede consultarse en la figura 7-2 (Arquitectura de la protección de contenidos) y en la figura 7-3 (Arquitectura de protección del servicio).
 NOTA 2 – Se han omitido algunas funciones y bloques funcionales de la arquitectura TVIP sin relación directa con la seguridad TVIP, en aras de su sencillez.

Figura 7-1 – Arquitectura general de seguridad de la TVIP

La arquitectura general de seguridad se divide de manera aproximada en cuatro zonas funcionales del siguiente modo:

- Funciones del proveedor de contenidos (técnicamente ajena a este documento)

Se supone que los proveedores de contenidos proporcionan a los proveedores de servicios el acceso a los contenidos siempre que se hayan establecido relaciones entre ellos. En ciertos casos, el propio proveedor de contenidos puede actuar como proveedor de servicios; en tal caso, esta relación se considera interna.

Al ofrecer a los proveedores de servicio acceso a los contenidos, los proveedores de contenidos pueden utilizar mecanismos estándar o privados para controlar y permitir el acceso a los contenidos; cabe observar, no obstante, que estos mecanismos se consideran fuera del alcance de la presente Recomendación y sujetos únicamente a acuerdo privado entre las partes.

- Funciones de la protección del servicio y contenidos (SCP) (que se solapan con ciertas partes de las funciones de la aplicación, de las funciones de control del servicio y de las funciones de entrega de contenidos)

Las funciones SCP desempeñan un papel primordial en la arquitectura general de seguridad de la TVIP, especialmente en el dominio del proveedor de servicios. Más concretamente, las funciones de protección del servicio permiten proteger tanto la infraestructura de servicios como el control de acceso a los servicios y contenidos alojados en los mismos. Por otra parte, las funciones de protección de contenidos permiten controlar la utilización de los servicios y contenidos con arreglo a los usos para los que se ha otorgado licencia. Las funciones específicas y los bloques funcionales de las funciones SCP están repartidos en tres subzonas: funciones de la aplicación, funciones del control del servicio y funciones de entrega de contenidos.

Un proveedor de servicios viene obligado por la licencia de los proveedores de contenidos a dar acceso a éstos sólo en determinadas condiciones de utilización, por ejemplo visionado de una sola vez pero sin grabación, grabación de una sola vez con múltiples visionados, grabación de una sola vez con transferencia de los derechos de grabación, etc. El objetivo principal de los aspectos de la protección de contenidos de las funciones SCP es permitir que el proveedor de servicios satisfaga dichas obligaciones de una manera objetivamente verificable.

El objetivo principal de los aspectos de protección del servicio de las funciones SCP es evitar el acceso no autorizado a los recursos de servicios y a la información considerada confidencial por las entidades en diversos dominios: servicio, red, aparato terminal y usuario final (abonado).

Un objetivo secundario de los aspectos de la protección del servicio de las funciones SCP es proteger la infraestructura de servicios del daño provocado por la mala utilización, deliberada o accidental, del recurso.

En las figuras 7-2 (*Arquitectura de protección de contenidos*) y 7-3 (*Arquitectura de protección del servicio*) se representan los bloques funcionales detallados de las funciones de protección de contenidos y de protección del servicio, respectivamente.

- Funciones de red

Las funciones de seguridad relacionadas con el dominio de la red se centran en la autenticación de entidades y en la autorización del acceso a las redes a través de las cuales se entregan, o entregarán, los servicios TVIP. Una función secundaria es la de proteger la integridad de la propia red: físicamente, electrónicamente y operacionalmente (por ejemplo, detectando y frustrando ataques de denegación de servicio contra la red de acceso o la red portadora).

- **Funciones del usuario final**

Entre los aspectos de la seguridad aplicables al usuario final (abonado) se encuentran la protección de la integridad del TD en las instalaciones del abonado y la protección de la privacidad del usuario final.

En ciertas circunstancias, se puede considerar que la DNG entre un TD y el dominio de la red está dentro del dominio del usuario final y sujeto a las medidas de seguridad del usuario final.

Por último, se recomienda la aplicación de mecanismos de integridad para garantizar la integridad de los contenidos recibidos por un TD y posteriormente redistribuidos a otros dispositivos dentro de la red doméstica o fuera de ésta. (Esto constituye un solapamiento entre los aspectos del usuario final y los aspectos de seguridad de los contenidos.)

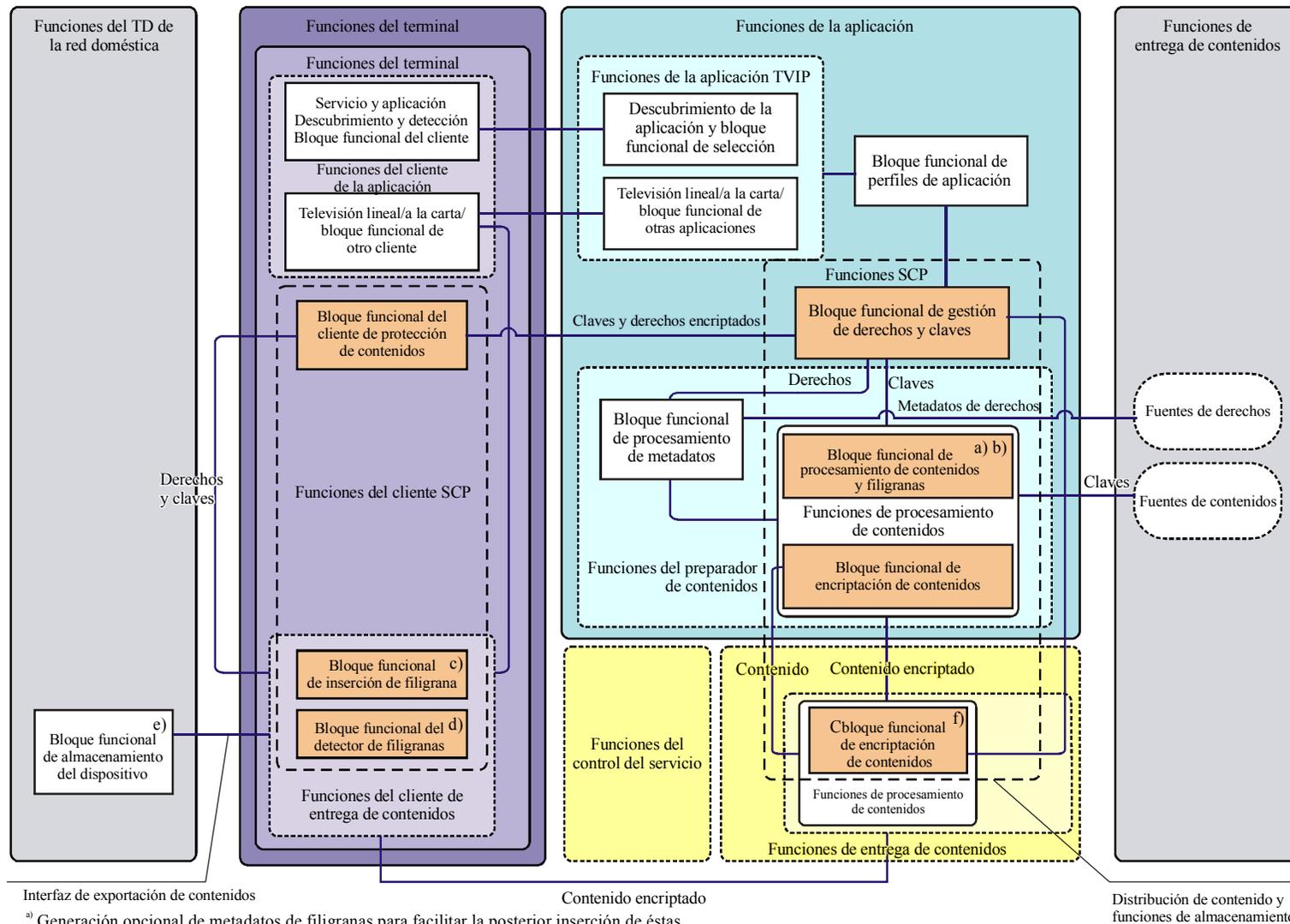
En la cláusula 7.4.1 se presentan descripciones detalladas de las funciones y bloques funcionales de la figura 7-1.

7.2 Arquitectura de protección de contenidos

En la figura 7-2, a continuación, se representa la arquitectura de protección de contenidos para la TVIP.

La función principal de la arquitectura de protección de contenidos es delinear el flujo y el proceso de información relativa a los derechos de utilización de contenidos y de la información necesaria para gestionar y facilitar dichos derechos.

En última instancia, los derechos de utilización de contenidos nacen de los proveedores de contenidos; obsérvese, no obstante, que estos derechos pueden modificarse (por ejemplo restringirse o incluso ampliarse) por parte de unos proveedores de servicios con arreglo a sus acuerdos con los proveedores de contenidos y a sus políticas operacionales y empresariales.



Interfaz de exportación de contenidos

Contenido encriptado

Distribución de contenido y funciones de almacenamiento

a) Generación opcional de metadatos de filigranas para facilitar la posterior inserción de éstas.

b) Inserción opcional de filigranas para singularizar los contenidos en las entregas a redes, servidores y unidifusión.

c) Integración opcional de filigranas para singularizar instancias de contenidos multidifusión.

d) Detector opcional para la protección contra copia de las filigranas.

e) Almacenamiento opcional fuera del aparato: dispositivo de almacenamiento en el interior del TD de la red doméstica.

f) El bloque funcional de encriptación de contenidos situado en las funciones de entrega y almacenamiento es opcional.

NOTA – Los bloques funcionales de protección de contenidos de esta figura comprenden las funciones de protección de contenidos y las funciones del cliente de protección de contenidos.

X.1191(09)_F7-2

Figura 7-2 – Arquitectura de protección de contenidos de la TVIP

La arquitectura de protección de contenidos mostrada anteriormente consta de funciones que residen principales en dos zonas funcionales.

- Las funciones de protección de contenidos y servicios (que se solapan con las funciones de la aplicación y con las funciones de entrega de contenidos)

El contenido y sus derechos asociados se obtienen de los proveedores de contenidos, se agregan y se procesan para su entrega al usuario final, viniendo gestionado el proceso global por varias funciones tales como las de preparación de contenidos, que utilizan datos que describen los derechos del usuario final y las condiciones relacionadas.

La información sobre contenidos, derechos legales y claves (utilizada para otorgar acceso a los contenidos y permitir su utilización) se organizan en un formato apropiado para la aplicación específica, por ejemplo visionado de televisión lineal. Los derechos y la información clave se entregan al bloque funcional del cliente de protección de contenidos en el aparato terminal como un derecho (por ejemplo, EMM) por parte del bloque funcional de gestión de derechos y claves; opcionalmente se procesa el contenido para insertar metadatos de rastreo de contenidos (por ejemplo, filigranas) y posteriormente se encripta, en las funciones de preparación de contenidos, antes de su entrega. En ciertos casos (por ejemplo, en los servicios IP en tiempo real) también pueden encriptarse los contenidos por parte de las funciones de entrega de contenidos como opción.

En el contexto de la arquitectura de protección de contenidos TVIP (en contraposición a la arquitectura de protección del servicio TVIP que se describirá más adelante), el objetivo radica principalmente en la gestión, el procesamiento y la entrega de derechos y claves en contraposición a la encriptación de esta información o de los contenidos sujetos a estos derechos.

- Funciones del usuario final

Las funciones de terminal que operan en el dominio del usuario final son las encargadas de hacer cumplir las reglas de utilización de contenidos asociadas a la información de derechos (conocidas también como metadatos de protección de contenidos). Esta entidad funcional interpreta las claves y derechos de los contenidos obtenidos del bloque funcional de gestión de derechos y claves, y, en función de lo interpretado, controla la forma de procesar los contenidos y de exponerlos a los usuarios ya sea mediante dispositivos de presentación integrados (por ejemplo, sistemas de reproducción de pantallas o audio) o mediante interconexiones físicas con dispositivos externos.

En los casos en los que el TD transmite contenidos protegidos a un dispositivo externo (por ejemplo, a una pantalla de visualización), los derechos de contenidos pueden traducirse a otro formato; los contenidos a los que se aplica esta utilización pueden como opción procesarse a su vez para insertar información de rastreo de contenidos (por ejemplo, filigranas) en el lado del cliente o volver a encriptar los contenidos para ejecutar el control de acceso posteriormente.

En la cláusula 7.4 se ofrece una descripción más detallada de los bloques arquitectónicos representados en la figura 7-2.

En la figura 7-2, la interfaz de exportación de contenidos es una interfaz lógica que conecta el TD de la TVIP y el TD de la red doméstica. El TD de la red doméstica puede consumir contenidos o exportarlos a otros TD de la red doméstica. Las funciones del cliente de entrega de contenidos pueden adaptar la correspondiente etiqueta de seguridad para garantizar que sólo el sistema TD de red doméstica autorizado puede consumir y exportar contenidos.

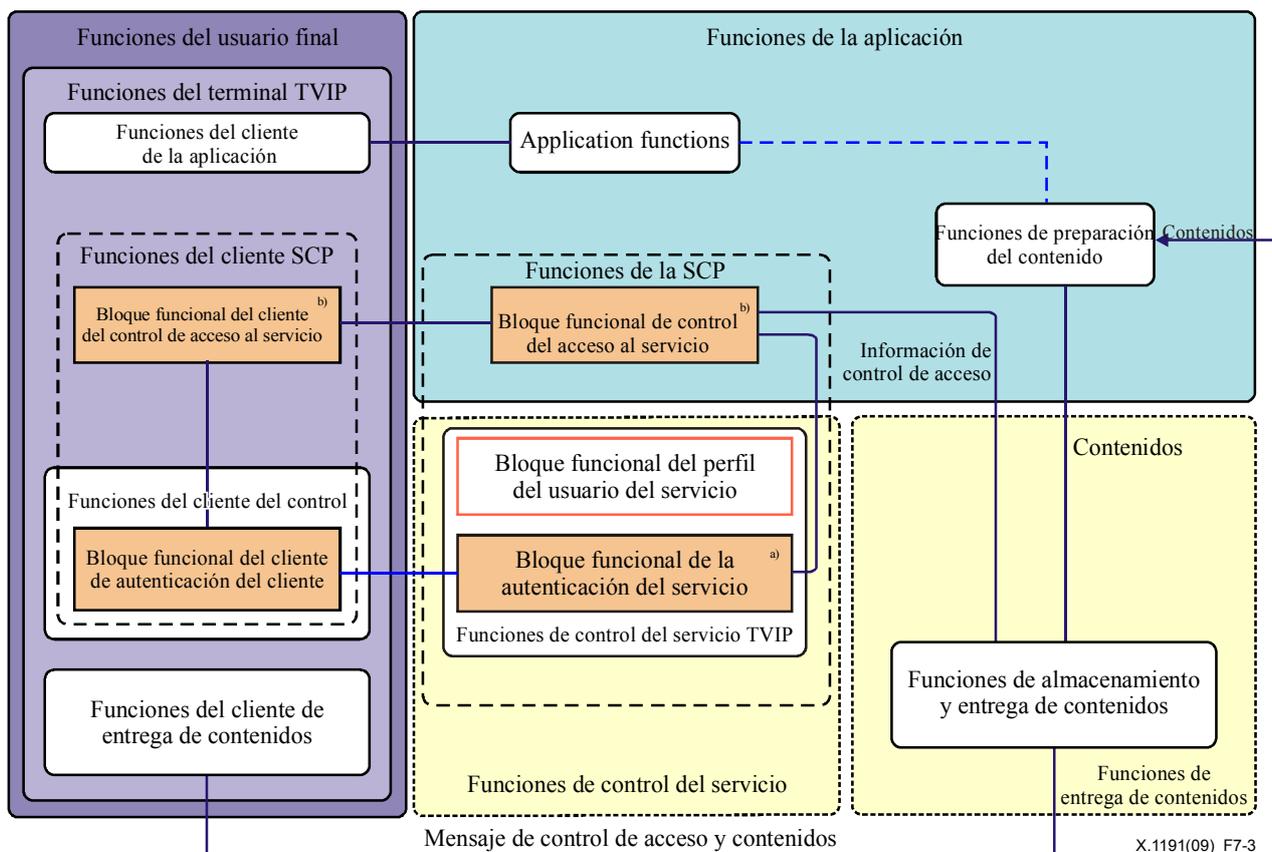
7.3 Arquitectura de protección del servicio

Un caso típico de los servicios gestionados con contenidos protegidos es aquél en el que el usuario final (abonado) y el TD deben ser autenticados y autorizados tras la autenticación positiva para acceder a los servicios y contenidos alojados en el mismo.

Dependiendo de las circunstancias, las funciones de autenticación y autorización pueden ejecutarse por separado en el TD y en los usuarios finales. En otros casos, es posible que haya dispositivos adicionales en las instalaciones del usuario final, tales como la pasarela de red de entrega y otros dispositivos del usuario final, que requieran la autenticación antes de autorizar el acceso al servicio.

La combinación de autenticación y autorización puede utilizarse para controlar el acceso tanto al servicio TVIP como al TD para la adquisición de servicios y contenidos antes de su utilización.

En la figura 7-3, a continuación, se representa la arquitectura de protección del servicio para la TVIP.



^{a)} Autenticación: Define el nombre del abonado y el ID con el privilegio asignado.

^{b)} Control de acceso al servicio: Permite proteger un servicio frente a cualquier actualización ilegal.

NOTA – Los bloques funcionales de protección del servicio de esta figura comprenden las funciones de protección del servicio y las funciones del cliente de protección del servicio.

Figure 7-3 – Arquitectura de protección del servicio TVIP

Entre las funciones básicas de la arquitectura de protección del servicio se encuentran:

- La autenticación del abonado y del TD
 - Esta función se encarga de la autenticación del abonado y del TD.
 - Autenticación del abonado: proceso de verificación de la autenticidad del usuario.
 - Autenticación del TD: proceso de verificación de la autenticidad del TD.

En los casos en los que se utilizan certificados con arreglo a X.509 como credenciales para la autenticación, se requiere una función de revocación.

- Autenticación del servidor
 - En un TD, función que permite autenticar al servidor para realizar la autenticación mutua.
- Control de acceso al servicio
 - Función que permite restringir la adquisición y acceso a los servicios por parte de los usuarios autorizados utilizando mecanismos de seguridad tales como la aleatorización y la encriptación.

En la cláusula 7.4 se presenta una descripción detallada de los bloques arquitectónicos representados en la figura 7-3.

7.4 Descripción de las funciones y bloques funcionales de las arquitecturas de seguridad de la TVIP

En la presente cláusula se ofrecen más detalles descriptivos de las funciones y bloques funcionales representados en los modelos arquitectónicos de las cláusulas 7.1 (*Arquitectura general de seguridad*), 7.2 (*Arquitectura de protección de contenidos*) y 7.3 (*Arquitectura de protección de los servicios*). Estas funciones y bloques funcionales se definen sólo en términos descriptivos generales estando divididos en tres partes que se corresponden con estas tres cláusulas.

7.4.1 Funciones y bloques funcionales de la arquitectura general

Funciones de la red de acceso: Recoger y agregar el tráfico de control y datos con origen en las redes; Habilitar la QoS/QoE y en particular la gestión de la memoria intermedia, la gestión y planificación de colas, el filtrado de paquetes, la clasificación del tráfico, el marcado, la vigilancia y la conformación del tráfico.

NOTA 1 – Estas funciones son independientes de las funciones de protección del servicio y contenidos desde el punto de vista de la protección del servicio y contenidos de la TVIP.

Funciones de la aplicación: Estas funciones están divididas entre el lado del servidor (proveedor de servicios) y el lado del cliente (instalaciones del usuario final), y consisten en componentes funcionales que preparan, originan, reciben y procesan aplicaciones TVIP a nivel del servicio tales como la TV lineal, el VoD y contenidos relacionados, por ejemplo, información de accesibilidad, aplicaciones interactivas, etc.

Bloque funcional de atribución de IP y autenticación: Proporciona la funcionalidad para autenticar el bloque funcional de pasarela de la red de entrega que conecta las funciones de red así como la atribución de direcciones IP a las funciones del terminal TVIP.

Funciones de protección de contenido: Son aquéllas que proporcionan mecanismos que permiten cumplir las políticas de utilización de contenidos, entre ellas la agregación, distribución y gestión de derechos legales y claves, la generación opcional e inserción (incrustación) de la información de rastreo de contenidos (por ejemplo, filigranas) y la encriptación de contenidos (bajo el control de las funciones de protección del servicio).

NOTA 2 – Los bloques funcionales específicos que constituyen las funciones de protección de contenidos se explican más detalladamente en las cláusulas 7.2 y 7.4.2.

Funciones del cliente de protección de contenidos: Son aquéllas que interaccionan con las funciones de protección de contenidos en el lado del servidor para aplicar las políticas de utilización de contenidos.

Funciones del proveedor de contenidos: Son aquéllas que se encargan de entregar los contenidos y los derechos de los contenidos y metadatos de las claves a los proveedores de servicios.

Funciones de la pasarela de la red de entregas: Son aquéllas que proporcionan conectividad entre el aparato terminal y la red de entrega; gestionan la conectividad de la IP local (instalaciones del usuario final), obtienen direcciones IP y la configuración IP para el TD.

NOTA 3 – Estas funciones son independientes de las funciones de protección del servicio y contenidos desde el punto de vista de la protección del servicio y contenidos de la TVIP.

Funciones de protección del servicio: Son aquéllas que proporcionan mecanismos para ejecutar la autenticación y autorización y que controlan el acceso a los servicios y contenidos de la TVIP, entre ellos el control y la implementación directa de la señal de control y la encriptación del intercambio de contenidos, ya sea independientemente o conjuntamente con las funciones de protección de contenidos.

NOTA 4 – Estas funciones son independientes de las funciones de protección del servicio y contenidos desde el punto de vista de la protección del servicio y contenidos de la TVIP.

NOTA 5 – Los bloques funcionales específicos que integran las funciones de protección del servicio se tratan más detalladamente en las cláusulas 7.3 y 7.4.3.

Funciones del cliente de protección del servicio: Son aquéllas que interaccionan con las funciones de protección del servicio en el lado del servidor para efectuar el control del acceso al servicio y otras funciones de protección.

Funciones del terminal: Son aquéllas que proporcionan la protección del servicio y los clientes de protección de contenidos para la descryptación y que aplican las políticas de utilización de servicios y contenidos con arreglo a los metadatos de derechos de utilización; ejecutan la encriptación en la capa de enlace y la traducción (intercambio) de la SCP requerida para la posterior salida o redistribución de los contenidos y el almacenamiento interno (o externo) de éstos, y además soportan conductos de procesamiento de medios seguros (resistentes a la manipulación), el almacenamiento de secretos (por ejemplo, claves) a nivel local, la capacidad de renovación de los programas informáticos de seguridad, la autenticación y verificación de los activos de soporte lógico descargados y la protección de los datos del usuario intercambiados y almacenados localmente respetando las consideraciones de privacidad del usuario final.

7.4.2 Funciones y bloques funcionales de la arquitectura de protección de contenidos

Funciones del cliente de la aplicación: Son el punto principal de coordinación y control de la interacción entre el usuario final y los servicios ofrecidos por las funciones de aplicación de la TVIP; para aplicaciones normales tales como el visionado de TV lineal, proporcionan la interfaz primaria del usuario y el paradigma de funcionamiento a través del cual el usuario final obtiene el servicio.

- **Bloque funcional del cliente de descubrimiento y selección de la aplicación:** Permite que el usuario final o el aparato terminal descubran la existencia y selección de las aplicaciones y servicios de aplicaciones que ofrecen los proveedores de servicios.

Funciones de la aplicación TVIP: Entidades lógicas que constituyen el punto de origen de ciertos servicios TVIP tales como la TV lineal, el VoD, etc.; se encargan de organizar todas las facilidades de los proveedores de servicios para habilitar la existencia de ciertos servicios operacionalmente.

- **Bloque funcional de descubrimiento y selección de la aplicación:** Interacciona con el bloque funcional del cliente de descubrimiento y selección de la aplicación antes citado, para que el usuario final o el aparato terminal puedan descubrir la existencia y selección de aplicaciones y servicios de aplicación.

Bloque funcional del perfil de la aplicación: Almacena y gestiona información de la configuración sobre aplicaciones y servicios ya sean de carácter mundial o del carácter específico de un usuario final (abonado); se utiliza típicamente para permitir que los servidores de aplicaciones adapten servicios y contenidos para el usuario final, interaccionen frecuentemente con diversos sistemas de contabilización o los implementen (internamente).

Funciones de preparación de contenidos: Ejecutan diversos tipos de procesamiento de contenidos antes de su entrega tales como el análisis del rastreo de contenidos (por ejemplo, mediante filigranas) y la generación de metadatos, el multiplexado de contenidos y metadatos de contenidos y la encriptación de contenidos.

- **Bloque funcional de procesamiento de contenidos y filigranas:** Pasos opcionales de procesamiento que analizan los contenidos para producir metadatos de rastreo de contenidos (por ejemplo filigranas) para ser utilizados en procesamientos posteriores, en particular el proceso de singularización de dichos metadatos (identificados con información por parte de la fuente que los asocia).
- **Bloque funcional de procesamiento de los metadatos:** Gestiona y procesa los metadatos relacionados con el programa y la información de derechos de utilización entregada por el proveedor de contenidos.
- **Bloque funcional de encriptación de contenidos:** Ejecuta la encriptación de contenidos protegidos (o los aleatoriza) para facilitar el control de acceso y la confidencialidad de dichos contenidos durante el proceso de entrega de los mismos. Los contenidos pueden encriptarse en tiempo real o ser encriptados previamente fuera de línea (la encriptación de contenidos puede opcionalmente soportar la transcodificación segura sin desencriptación).

NOTA 1 – La encriptación de los contenidos puede implementarse en las funciones de preparación de contenidos de la capa de aplicación. En ciertos casos, también puede opcionalmente implementarse en las funciones de entrega de contenidos.

Bloque funcional de gestión de derechos y claves: Correlaciona los derechos y las claves con los contenidos y gestiona su distribución al bloque funcional del cliente de protección de contenidos en el apartado terminal.

Bloque funcional del cliente de protección de contenidos: Obtiene o recibe los derechos y claves utilizando esta información para controlar la desencriptación de los contenidos y aplicar las reglas de utilización; este bloque funcional necesita ser resistente a la manipulación.

Funciones de entrega de contenidos: Ejecutan funcionalidades de memoria intermedia y almacenamiento, y la entrega de contenidos con arreglo a las peticiones de las funciones del usuario final; las funciones de entrega de contenidos pueden opcionalmente procesar (por ejemplo codificar o encriptar) los contenidos.

Funciones del cliente de entrega de contenidos: Se encarga de la recepción de contenidos en las funciones del terminal TVIP; ejecuta la desencriptación de los medios de los contenidos, demultiplexación, decodificación y posterior procesamiento de presentación y almacenamiento de los contenidos (estas funciones necesitan asimismo tener la capacidad de ser resistentes a la manipulación).

- **Bloque funcional detector de filigranas:** De estar presente, detecta la utilización de filigranas en los contenidos recibidos de los proveedores de servicios para verificar o implementar las reglas de utilización de contenidos deseadas en el aparato terminal o interfaces posteriores al aparato terminal.
- **Bloque funcional de inserción de filigranas:** De estar presente, efectúa la singularización de la instancia de contenidos para su presentación y posterior almacenamiento o redistribución.

Fuentes de derechos: Son aquéllas que originan metadatos de contenidos relativos a los derechos de utilización de contenidos.

Fuentes de contenidos: Son aquéllas en las que se originan los contenidos para ser agregados, procesados y posteriormente entregados a los usuarios finales por medio de aplicaciones de servicio tales como la TV lineal, el VoD, etc.

Bloque funcional de almacenamiento fuera del dispositivo: Mecanismos de almacenamiento de contenidos posteriores a la recepción que son físicamente externos al TD y cuyo almacenamiento y utilización de contenidos no está gestionado por el TD.

NOTA 2 – De existir un almacenamiento externo, cuya utilización está controlada por el TD en cada momento, puede ser considerado como almacenamiento interno al dispositivo mediante una interfaz autorizada y protegida, dependiendo de las reglas aplicables de conformidad y robustez del aparato terminal.

7.4.3 Funciones y bloques funcionales de la arquitectura de protección del servicio

Bloque funcional de control del acceso al servicio: Se encarga fundamentalmente del control del acceso al servicio; este bloque funcional utiliza mecanismos de seguridad tales como la aleatorización y la encriptación para evitar que los usuarios accedan a servicios, o los adquieran, sin permiso.

Bloque funcional del cliente de control de acceso al servicio: Ejecuta tareas relacionadas con la protección del servicio en el cliente con arreglo a lo definido por el bloque funcional de control de acceso al servicio en el lado del servidor.

Bloque funcional de autenticación del servicio: Ejecuta la autenticación para verificar la autenticidad del usuario y del TD; soporta asimismo las peticiones de autenticación procedentes del TD para verificar al servidor.

Bloque funcional del cliente de autenticación del servicio: Además de ejecutar tareas relacionadas con la autenticación del abonado en el lado del cliente, comprende la función de verificar la autenticidad del lado servidor de la protección del servicio para la autenticación mutua.

8 Mecanismos de seguridad

En esta Recomendación no se definen mecanismos ni soluciones de seguridad específicos; por contra, se describen a grandes rasgos ciertos mecanismos de seguridad que pueden considerarse a los efectos de definir e implementar mecanismos que contemplen requisitos de seguridad, entidades funcionales de la arquitectura de seguridad y amenazas de seguridad.

El conjunto de mecanismos de seguridad descritos a continuación no contempla exhaustivamente todos los requisitos de seguridad citados anteriormente.

8.1 Mecanismos de seguridad relativos a la protección de contenidos

Los mecanismos de seguridad de contenidos comprenden un conjunto de funciones que operan entre las fuentes de contenidos y los TD para garantizar que los contenidos puedan ser distribuidos (o transmitidos) con seguridad por una red y puedan ser adquiridos, consumidos, exportados, almacenados y redistribuidos (o retransmitidos) con seguridad por un usuario final.

Los mecanismos de seguridad de contenidos pueden aplicarse a la distribución, adquisición, consumo, almacenamiento, exportación y redistribución de contenidos. Para satisfacer los requisitos de la protección de contenidos y servicios de la TVIP pueden utilizarse los siguientes mecanismos (todos ellos con carácter opcional).

8.1.1 Encriptación de contenidos

En muchos casos, pueden encriptarse los contenidos para evitar su utilización ilegal durante la entrega.

8.1.2 Identificación y rastreo de contenidos

El rastreo de contenidos permite identificar y rastrear el origen (fuente) del contenido y/o la parte responsable (por ejemplo, usuario final) a fin de facilitar la subsiguiente investigación en el caso de que se haya producido un acceso no autorizado al contenido o una utilización ilegal del mismo.

La información de rastreo del contenido puede adjuntarse al contenido ya sea como metadatos o como filigrana forense. Las filigranas para el rastreo de contenidos suelen estar diseñadas para ser robustas e imperceptibles a fin de protegerlas contra su supresión deliberada o involuntaria.

Se recomienda facilitar la identificación de los contenidos mediante una tecnología de firma de vídeo.

8.1.3 Aplicación de filigranas

La aplicación de filigranas es el proceso de añadir información al contenido mediante la alteración de ciertas características del mismo. Se trata de un ámbito de estudio denominado *esteganografía*.

La filigrana es la solución preferible para muchas aplicaciones debido a la dificultad de suprimir esta información del contenido. En un servicio TVIP, la filigrana puede consistir en la inclusión de una información oculta directamente en un tren de vídeo o audio de un contenido multiplexado. Lo ideal es que las filigranas sean invisibles e inaudibles para el ser humano y que no se pierdan en la conversión entre formatos de medios.

8.1.4 Etiquetado de contenidos

El etiquetado de contenidos es el proceso de inserción y asociación de metadatos a los contenidos para describir la naturaleza de los mismos así como algunos aspectos y características de éstos. Los contenidos etiquetados con estos metadatos pueden ser ordenados, filtrados o categorizados con mayor facilidad por parte de dispositivos intermedios en la cadena de entrega de contenidos.

Algunas regiones, administraciones o desarrollos específicos de la TVIP pueden exigir la presencia de ciertos tipos de etiquetas de contenidos tales como una información de clasificación para permitir un cierto grado de control por parte del usuario final (abonado) sobre el acceso a contenidos considerados inadecuados o perjudiciales.

8.1.5 Esquema transcodificable seguro

El esquema transcodificable seguro (STS, *secure transcodable scheme*) es un tipo de esquema de seguridad que permite a un nodo intermedio de la red ejecutar la transcodificación sin descryptación, sin perjuicio de la conservación de la seguridad extremo a extremo. Este esquema puede conseguirse por medio de la combinación de una encriptación progresiva codificada escalonable y de una paquetización.

En el STS se distinguen tres entidades, a saber: un emisor, un nodo intermedio de la red y un usuario con un aparato TVIP. El emisor ejecuta una función transcodificable segura que produce paquetes encriptados escalonables a partir del vídeo y añade un encabezamiento sin encriptar para enviar la información; el nodo intermedio de la red lee el encabezamiento sin encriptar y utiliza su información para truncar o descartar los paquetes apropiados con arreglo a la operación de transcodificación deseada, mientras que el terminal TVIP descrypta los paquetes encriptados y descodifica el paquete en texto claro para producir el vídeo. El apéndice V de la presente Recomendación contiene una descripción detallada de esto.

NOTA – La presente cláusula no pretende definir ni describir mecanismos adicionales de STS. Este tema necesita ser tratado con más profundidad en otras Recomendaciones.

8.2 Mecanismos de seguridad relativos a la protección del servicio

Entre los mecanismos de seguridad de servicios cabe citar la autenticación y la autorización. También pueden recibir esta consideración algunas implementaciones de mecanismos de control de acceso específicos tales como los sistemas de encriptación y descryptación.

8.2.1 Autenticación de servicios

En el caso de servicios gestionados en los que un usuario final (abonado) tiene una relación directa con un cierto proveedor de servicios, el proveedor de servicios requerirá, normalmente, que se autenticuen el aparato terminal y el usuario final (abonado) de un modo seguro antes de prestar el servicio; en este caso, la autenticación supone la producción y presentación de una manera segura de credenciales/información que pueda ser correlacionada con la base de datos de abonados del proveedor de servicios para verificar la autenticidad del aparato terminal y del usuario final a los efectos de la entrega del servicio.

8.2.2 Autorización de servicios

Tras la autenticación del usuario final (abonado) y del aparato terminal a los efectos de entrega del servicio, se utiliza un mecanismo de autorización de servicios para autorizar y otorgar el acceso a servicios y contenidos específicos allí alojados con arreglo a la prestación pactada entre el proveedor de servicios y el abonado.

8.2.3 Control de acceso a servicios

En la mayor parte de los casos, si no en todos, un sistema de protección del servicio contendrá mecanismos que puedan ejecutar la encriptación (aleatorización) y desencriptación (desaleatorización) tanto del tráfico de señalización de control del servicio como del tráfico de contenidos. Lo normal es que se encripte el tráfico bidireccional de control del servicio en ambos sentidos, tanto del servidor al cliente como del cliente al servidor. También es normal que los trenes de contenidos se encripten únicamente del servidor (proveedor de servicios) al cliente (aparato terminal). No obstante, hay escenarios de utilización en lo que puede enviarse el tren de contenidos desde un cliente al servidor, en cuyo caso dicho contenido puede encriptarse en el aparato terminal a los efectos de la telecarga (por ejemplo, para garantizar que sólo un proveedor de servicios autenticado y autorizado pueda tener acceso al contenido telecargado).

8.3 Mecanismos de seguridad relativos a la protección de redes

En la presente Recomendación no se definen ni describen mecanismos relativos a la seguridad de la red. En general, cabe esperar que las implementaciones de redes medulares, ya sean de acceso, portadoras o de entrega, permitan implementar los mecanismos que se consideren necesarios para proteger la integridad operacional de la red, entre ellos, por ejemplo, la detección y prevención de la Denegación de Servicio (DoS, *denial of service*). Generalmente, los mecanismos de seguridad empleados por los proveedores de servicios TVIP y por los TD serán transparentes a estas redes, siempre que dichos mecanismos de seguridad funcionen al nivel de los elementos de datos útiles, o por encima de éstos, suministrados por las capas de red.

8.4 Mecanismos de seguridad relativos a la protección de dispositivos de aparatos terminales

Entre los mecanismos de seguridad de los aparatos terminales se encuentra una amplia gama de funcionalidades, entre ellas el almacenamiento seguro y resistente a la manipulación de datos secretos, la autenticación de servicios, la autorización de servicios, la encriptación y desencriptación de las señales de control, la desencriptación de contenidos, la decodificación de metadatos de derechos de contenidos, la aplicación de formas de utilización de contenidos, la detección e inserción de filigranas, la autenticación y verificación de contenidos de los programas, la protección del servicio y contenidos en puente y con intercambio, la encriptación del puerto (interfaz) de salida digital, la resistencia a la manipulación del trayecto de los medios, los procesadores y componentes de seguridad extraíbles y renovables, ya sea basados en el equipo físico como en el soporte lógico, etc.

8.5 Mecanismos de seguridad relativos al abonado o usuario final

Los mecanismos de seguridad del abonado o usuario final están relacionados principalmente con la recogida, almacenamiento y transmisión de información sujeta, en su caso, a consideraciones de privacidad o confidencialidad del usuario final. Por ello, estos mecanismos pueden dividirse entre el punto de recogida, el aparato terminal y el proveedor de servicios, susceptibles de capturar, mantener o reutilizar esta información. Por consiguiente, cabe esperar que las descripciones y definiciones de estos mecanismos se incluyan en apartados que describan la seguridad del servicio y del aparato terminal.

En la actual edición de la presente Recomendación no se definen mecanismos de seguridad del abonado o usuario final. Cabe esperar que en futuras ediciones se traten estos temas con mayor profundidad.

En el anexo A se ofrece información adicional sobre la seguridad del abonado.

Anexo A

Protección de la seguridad del abonado

(Este anexo es parte integrante de la presente Recomendación)

A.1 Protección de los datos del usuario

Cuando se implementan servicios de TVIP entre usuarios genéricos, es imprescindible prestar atención a la seguridad a fin de proteger los datos del abonado.

Entre los datos del abonado también puede figurar la información de datos de seguimiento tales como el número de canal anterior y posterior a un cambio de canal, la hora de cambio y la información del usuario para el servicio EPG, la identificación del paquete, la hora de reproducción, etc. Los datos mencionados tienen carácter personal y confidencial. La protección contra abusos de estos datos del abonado exige que el proveedor del servicio TVIP se plantee cuestiones de protección de la privacidad del usuario.

- El servicio TVIP puede opcionalmente manejar el mínimo de datos personales del abonado necesarios para la entrega de los servicios TVIP.
- El servicio TVIP puede opcionalmente explicar el uso que se pretende hacer de los datos personales del abonado y obtener el consentimiento de éste antes de recoger la información necesaria para la entrega de los servicios TVIP.
- El servicio TVIP puede opcionalmente destruir los datos personales del abonado que dejen de ser necesarios para la continuidad de los servicios TVIP.
- Cuando el proveedor del servicio administra los datos personales del abonado, el servicio TVIP puede opcionalmente almacenar los datos recogidos en condiciones de estricta seguridad.

Hay muchos modos posibles de que se produzcan fugas de datos personales del abonado: pueden producirse fugas en la empresa de servicios, en la red y en el hogar, por ejemplo desde el aparato terminal. A continuación, se presentan varios métodos de proteger los datos personales del abonado para cada una de dichas rutas de fuga.

A los efectos de la prevención de fugas de los datos del abonado se recomienda que el proveedor del servicio TVIP preste la máxima atención a los siguientes extremos:

- Clasificar los datos personales del abonado en aquéllos que requieren control y aquéllos que no.
- Administrar con seguridad los datos personales del abonado que requieren control.
- Verificar que los datos personales del abonado que requieren control no se utilicen para fines distintos de los previstos.

Se recomienda que los proveedores de servicios TVIP presten la máxima atención a los puntos siguientes relativos a los servicios y transacciones que afectan a la manipulación de los datos personales del abonado.

- Clasificar los datos personales del abonado en aquéllos que requieren control y aquéllos que no.
- Utilizar canales de comunicación encriptados para la transmisión de los datos personales del abonado que requieren control.

Algunas veces, los proveedores de servicios TVIP almacenan datos personales del abonado en aparatos terminales a fin de mejorar la eficiencia del servicio. En estos casos, se recomienda presten la máxima atención a los puntos siguientes. Se recomienda además, considerar los aspectos de la seguridad cuando se tengan que sustituir los TD.

- Verificar que ningún tercero pueda leer los datos personales del abonado que se guardan en el interior del TD.
- El proveedor del servicio TVIP puede opcionalmente controlar el acceso a los datos personales del abonado almacenados en el TD.
- Verificar que los datos personales del abonado almacenados en el TD puedan ser suprimidos por completo por un abonado o proveedor de servicios.
- Lo ideal es que en un futuro próximo se requiera que los TD queden protegidos de las infecciones provocadas por programas informáticos maliciosos tales como los virus y los programas espía.

A.2 Control parental, protección de menores de edad a efectos legales y control de acceso

En la plataforma TVIP puede utilizarse un mecanismo de protección de los menores de edad a efectos legales para restringir los contenidos de TVIP a los que puedan tener acceso dichos menores. En un esquema de utilización típico, un aparato terminal para servicios TVIP lo comparten en un hogar varias personas, entre ellos menores de edad a efectos legales. En relación con los aparatos terminales, se recomienda que el proveedor del servicio TVIP:

- Garantice la posibilidad de establecer un mecanismo de clasificación parental de contenidos cuando sea necesario.
- Garantice que los dispositivos terminales puedan manejarse con arreglo a la clasificación parental.
- Garantice que los aparatos terminales sean capaces de modificar los parámetros de la clasificación parental.
- Garantice que los aparatos terminales sean capaces de utilizar controles basados en contraseña de modo que sólo los tutores de menores puedan modificar los parámetros de la clasificación parental.
- Garantice que la clasificación de los contenidos pueda establecerse para diferentes grupos de edades.
- Garantice que puedan atribuirse privilegios de abonado a distintos grupos de edad.
- Garantice que pueda otorgarse autorización a menores de edad en los aparatos terminales para que visionen un canal o contenido particular, por ejemplo, solicitando previamente un PIN.
- Garantice que los tutores que no se encuentren cerca de los menores de edad puedan supervisar y recibir a distancia, del almacenamiento de copia de la red, los contenidos para menores.

Obsérvese que puede ser necesario considerar las condiciones de cada administración o región en relación con organizaciones de terceros para la eliminación de contenidos perjudiciales, ya que ello está relacionado con el control del flujo y acceso a contenidos. Considerando el carácter simultáneo de las retransmisiones de radiodifusión, cabe suponer que el creador del contenido original presta atención suficiente al mismo en el momento de su producción; esto subraya la necesidad de otorgar la atención suficiente a los retardos de la transmisión y a los costes de la distribución.

Apéndice I

Amenazas de seguridad

(Este apéndice no es parte integrante de la presente Recomendación)

En este apéndice se describe un conjunto de amenazas de seguridad identificadas, contempladas en algunos requisitos o mecanismos de la presente Recomendación.

El enfoque del modelo de amenazas de seguridad y otros contenidos esenciales se ha efectuado con arreglo a las siguientes Recomendaciones del UIT-T:

- [b-UIT-T X.800] en la que se definen los elementos arquitectónicos generales relacionados con la seguridad que pueden aplicarse adecuadamente en las circunstancias en que se requiera la protección de la comunicación entre sistemas abiertos.
- [b-UIT-T X.805] en la que se define una arquitectura de seguridad de red que garantiza la seguridad de las comunicaciones extremo a extremo.

Se invita a las partes interesadas en las consideraciones relativas a la seguridad de la TVIP a que lean estas Recomendaciones de seguridad básicas; se supone que el lector de la presente Recomendación conoce la información presentada en dichas Recomendaciones.

En [b-UIT-T X.800] y [b-UIT-T X.805] se identifican las siguientes amenazas de seguridad para las redes (que también constituyen amenazas de seguridad para la aplicación de servicios y contenidos en el contexto de la TVIP):

- La destrucción de información y de otros recursos.
- La corrupción y modificación de información.
- El robo, supresión y pérdida de información y de otros recursos.
- La revelación de información.
- La interrupción de servicios.

I.1 Modelo de amenazas de seguridad

Las amenazas de seguridad para la TVIP pueden clasificarse en los siguientes tipos: Amenazas de seguridad para los contenidos, amenazas de la seguridad para los servicios, amenazas de seguridad para las redes, amenazas de seguridad para los aparatos terminales y amenazas de seguridad para los abonados.

En la figura I-1 se representa el modelo de amenazas de seguridad en el que pueden verse las relaciones entre cada una de estas amenazas.

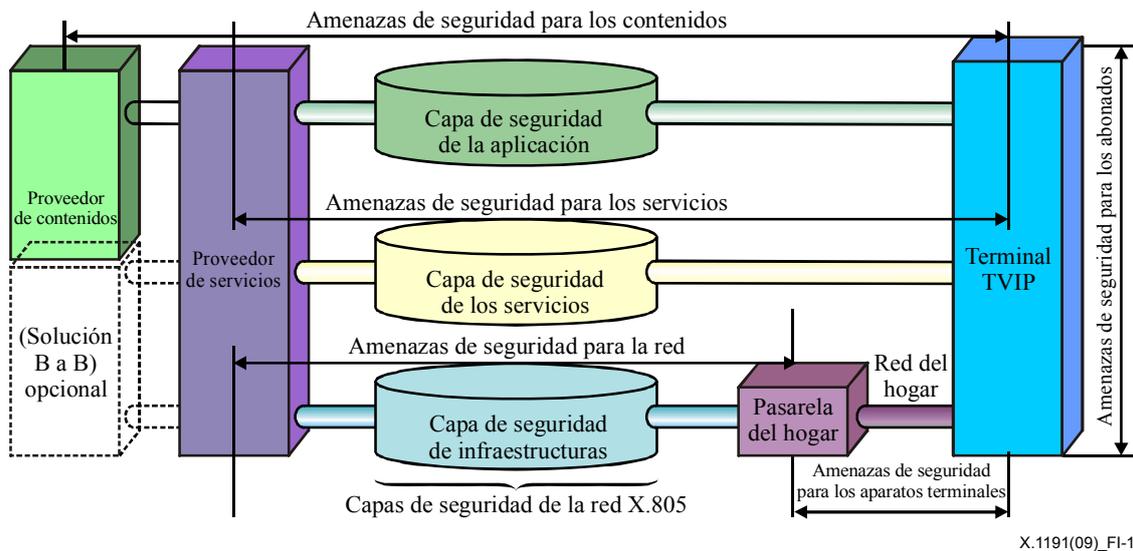


Figura I-1 – Modelo de amenazas de seguridad

I.1.1 Amenazas de seguridad para los contenidos

Activos de los contenidos: Son aquellos activos que pertenecen a un proveedor de contenidos, a un proveedor de servicios o a ambos y que pueden ser consumidos por el usuario final a través del TD.

Entre los activos de contenido que deben protegerse se encuentran: los contenidos de la TV lineal, los contenidos del VoD, los contenidos del VoD asimétrico, los contenidos del grabador personal de vídeo (PVR, *personal video recorder*), las aplicaciones descargadas, etc.

Las amenazas contra los contenidos son las siguientes:

- Interceptación: vulneración de la confidencialidad del contenido digital efectuado por supervisión ilegal de las redes de servicio.
- Visionado no autorizado.
- Reproducción o redistribución no autorizadas.

I.1.2 Amenazas de seguridad para los servicios

Activos de servicios: Activos que pertenecen a un proveedor de servicios. Entre ellos se encuentran los servidores de medios, los servidores SCP y la información de explotación tal como los registros históricos del servicio y la información de facturación, como mínimo.

Las amenazas contra los servicios son las siguientes:

- Menoscabo de los derechos de autor de los programas proporcionados por la plataforma de servicios TVIP a los abonados.
- Impostura/falsificación del proveedor de servicios TVIP.
- Amenazas maliciosas dirigidas contra los servidores TVIP (servidores SCP, servidores de medios, etc.); pueden comprender el pirateo aprovechando las fugas de seguridad en los programas informáticos de la aplicación o en el protocolo de comunicaciones, los ataques de denegación de servicio, etc.
- Robo de información del abonado (por ejemplo, información identificativa, información de facturación o información del abono) utilizando a menudo programas maliciosos tales como los troyanos.

I.1.3 Amenazas de seguridad para las redes

Activos de red: Activos que pertenecen al proveedor de la red; entre ellos se pueden considerar los equipos físicos (por ejemplo encaminadores y conmutadores) y los recursos de red (por ejemplo, ancho de banda, servicios multidifusión, etc.).

Las amenazas contra las redes son las siguientes:

- Amenazas deliberadas dirigidas a los equipos o recursos de la red (ancho de banda): ataques maliciosos a la red portadora tales como los de denegación de servicio.
- Amenazas de seguridad para la técnica multidifusión utilizada por la red portadora TVIP, por ejemplo, impostura/falsificación de las fuentes de TV multidifusión o de miembros del grupo multidifusión ilegítimos.
- Ataques maliciosos (tales como los de DoS y pirateo) a los nodos de la red de distribución de contenidos.

I.1.4 Amenazas de seguridad para los aparatos terminales

Activos de terminal: Activos que pertenecen a un dispositivo terminal y que puede utilizarse por parte del usuario final para procesar y almacenar contenidos y otra información pertinente para el servicio de TVIP.

Las amenazas contra los terminales son las siguientes:

- Acceso ilegal a contenidos claros tras manipular el equipo físico o el soporte lógico del aparato; por ejemplo, los contenidos claros pueden copiarse por interceptación de los datos que circulan por el bus o por pirateo del soporte lógico SCP.
- Acceso ilegal a claves o a otra información secreta residente en los aparatos mediante el pirateo de soporte lógico o manipulación del equipo físico; los atacantes pueden manipular la memoria de los aparatos o analizar el flujo de datos para obtener las claves y otros secretos (la exposición de las claves de los contenidos se traduce en fuga de éstos, y la fuga de claves de los aparatos permite la suplantación de éstos).
- Provocar el mal funcionamiento de los aparatos por métodos físicos tales como el control del sistema de reloj del aparato para desactivar las funciones de los sistemas SCP o por métodos lógicos tales como la instalación de virus para agotar los recursos del aparato.
- Descarga, ejecución y almacenamiento en los aparatos terminales de aplicaciones no autorizadas (tales como programas informáticos).
- Fallo de los equipos terminales (tanto del equipo físico como del soporte lógico) provocado por códigos maliciosos o virus de la red.
- Aparatos terminales sin autenticar que se conectan a la red doméstica.
- Uso no autorizado por parte de los abonados.

I.1.5 Amenazas de seguridad para los abonados

Activos de abonados: Activos que pertenecen a un abonado; pueden consistir en información sobre el abonado, sobre el hogar del abonado, sobre sus transacciones de TVIP, etc.

La seguridad del abonado exige un mecanismo que se encargue de la seguridad de contenidos y de otro que se encargue del trabajo de seguridad del servicio en cooperación recíproca debido a que el servicio TVIP comprende un servicio en el que la seguridad de contenidos y la seguridad del servicio cooperan recíprocamente.

En el cuadro I-1 se presentan ejemplos de amenazas para el abonado.

Cuadro I-1 – Categorías de seguridad de los abonados

	Seguridad del abonado		
	Ejemplo de servicio	Amenazas representativas	Ejemplo de mecanismo de protección
Seguridad de los contenidos	TV lineal, servicio de VoD	Copia ilegal	Identificación del TD (protección del servicio, protección de los contenidos)
Seguridad del servicio	Servicio bidireccional	Peska (<i>phishing</i>)	Identificación personal (protección de datos personales, PIN/contraseña)
	Parental	Falsificación	Identificación personal (PIN/contraseña, autenticación)
Seguridad de la red	No se especifica	Escucha clandestina	Identificación de la línea del abonado Datos de encriptación, control conjunto multidifusión
Seguridad del aparato terminal	Servicio P2P	Copia ilegal	Protección de contenidos (P2P)

Apéndice II

Interoperabilidad de la SCP

(Este apéndice no es parte integrante de la presente Recomendación)

II.1 Introducción a la interoperabilidad de la SCP

Hay varios escenarios de la SCP interoperable: SCP: SCP-EE, SCP-B y SCP-IX. La SCP interoperable puede aplicarse o bien al dominio del proveedor de servicios o bien al del usuario final. En este apéndice se contempla únicamente el lado del terminal.

II.2 Escenarios de la SCP interoperable

Los escenarios de la SCP interoperable se clasifican como mínimo en tres modos: SCP extremo a extremo (SCP-EE), SCP en puente (SCP-B) y SCP de intercambio (SCP-IX).

1) SCP extremo a extremo (SCP-EE)

SCP-EE: Mediante una única SCP, dos o más dispositivos intercambian contenidos y acceden a los mismos con arreglo a los derechos otorgados. Este modo es el más sencillo de implementar debido a que sólo se utiliza una sola SCP.

2) SCP en puente (SCP-B)

SCP-B: En un único TD, se instalan dos o más SCP. Puede accederse a los contenidos adquiridos por un sistema SCP (por ejemplo, de una red) mediante otra SCP que resida en el mismo dispositivo con arreglo a los derechos otorgados.

3) SCP de intercambio (SCP-IX)

SCP-IX: Este caso se caracteriza por la presencia de dos o más dispositivos, teniendo cada uno de ellos uno o más SCP instaladas. Los contenidos adquiridos por un dispositivo a través de una de sus SCP pueden ser objeto de transferencia y acceso seguro en otro dispositivo a través de una SCP diferente con arreglo a los derechos otorgados.

En la figura II-1 se representa un modelo del caso citado.

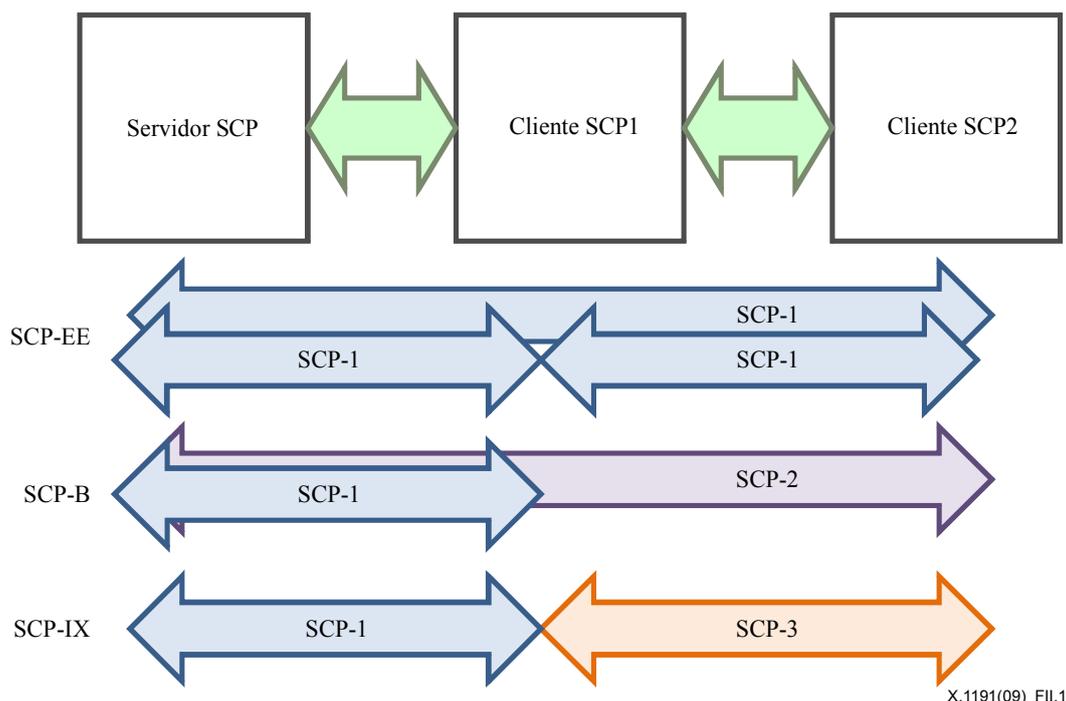


Figura II-1 – Modo de interoperabilidad de la SCP

II.3 Ámbito técnico de interoperabilidad de la SCP

Los siguientes campos representan los elementos de interoperabilidad clave requeridos por los modos SCP-EE, SCP-B y SCP-IX:

1) Autenticación de dispositivos, usuarios y SCP

Antes de que puedan intercambiarse contenidos entre entidades, deben establecerse con seguridad el identificador del aparato terminal y, en su caso, el usuario o usuarios. Además, dado que los proveedores de contenidos tal vez no confíen en SCP específicos, debe ser posible autenticar los SCP receptores o implementar niveles antes del intercambio de contenidos. Dicha autenticación debe tener una sólida base criptográfica y puede emplear diversas técnicas de firma digital conocidas, en particular la criptografía de claves públicas, que ofrece un mecanismo sólido de firma digital para protocolos de autenticación.

2) Intercambio de la expresión de derechos

Las diferentes SCP utilizan lenguajes de expresión y formatos de licencia diferentes. Para que funcionen los modos SCP-B y SCP-IX se requiere un medio de expresión de derechos común. Éste puede adoptar la forma de un lenguaje de expresión de derechos común (REL, *rights expression language*) o de un traductor de expresiones de derechos. Otro mecanismo posible de intercambio de expresiones de derecho es el de negociación de licencias.

3) Algoritmos de encriptación comunes para el intercambio de contenidos

Para que los contenidos pasen con seguridad del control de una SCP a otra, o en el seno de una misma SCP aunque en distintos dispositivos físicos, se requiere su encriptación. Esto hace que los contenidos no se puedan utilizar, salvo por las entidades que poseen las claves adecuadas o necesarias para efectuar la desencriptación. Hay muchos tipos distintos de algoritmos de encriptación (por ejemplo, cifrado de bloques, cifrado de trenes, algoritmos de encriptación basados en claves públicas, etc.) aunque los que utilizan claves simétricas suelen ser los más adaptados al

intercambio de contenidos a alta velocidad. Para la interoperabilidad, debe escogerse un pequeño número de algoritmos previamente acordados. Lo ideal es que se especifique un algoritmo por defecto.

4) Gestión e intercambio de claves para los algoritmos de encriptación comunes

Antes de que pueda efectuarse el intercambio de contenidos seguro, las claves que se deban utilizar en instancias específicas deben intercambiarse o generarse comúnmente por parte de las entidades autenticadas. La gestión de claves suele ser la parte más difícil de implementar en un sistema de seguridad. Técnicas tales como la criptografía de claves públicas han permitido simplificar la distribución de claves de los dispositivos aunque exija una infraestructura de claves públicas (PKI, *public key infrastructure*) que mantenga la validez de dichas claves. Esta infraestructura podría ser sancionada y mantenida por una autoridad expedidora de licencias, responsable de la protección de contenidos (en contraposición a una seguridad general de la red).

5) Descarga segura del cliente SCP

En un caso ideal, cualquier TD debería poder intercambiar los contenidos obtenidos (legítimamente) a través de otros dispositivos o utilizando cualquier SCP de acuerdo con los derechos concedidos (es decir en el modo *SCP-IX*). Obsérvese no obstante que precargar los TD, en el momento de su fabricación, con cada uno de los sistemas SCP que demandan las fuerzas del mercado resulta poco práctico; de aquí la necesidad de disponer de un mecanismo seguro para la descarga y ejecución en un aparato terminal de un sistema SCP seleccionado. Elementos tales como los cargadores de arranque seguros y los protocolos de descarga seguros juegan un papel importante en este ámbito de la interoperabilidad.

NOTA – Cuando se instala la interoperabilidad SCP en dispositivos y sistemas finales, los dispositivos TVIP deben tener una arquitectura de confianza para soportar la interoperabilidad de la seguridad de contenidos.

6) Exportación segura de derechos

Para exportar los derechos digitales con seguridad, el cliente SCP TVIP deben comprobar si está permitida la exportación de los derechos de utilización que afectan al sistema SCP. Los derechos digitales pueden tener expresiones de derechos que permitan que el sistema SCP objetivo exporte derechos. En tal caso, el cliente SCP TVIP debe verificar estas expresiones de derechos y autorizar la exportación de derechos digitales a los sistemas SCP objetivo adecuados.

II.4 Arquitecturas interoperables de la SCP

Pueden contemplarse dos tipos de arquitecturas posibles de la SCP interoperable; una de ellas se basa en la arquitectura de interoperabilidad basada en mediador, que utiliza un sistema mediador situado entre dos sistemas SCP para procesar la transmisión interoperable. El otro consiste en una arquitectura basada en un protocolo estándar que utiliza interfaces y protocolos estándar para transformar los contenidos digitales protegidos y asociar información entre dos sistemas SCP distintos.

En las figuras II.2 y II.3 se muestran las dos arquitecturas posibles.

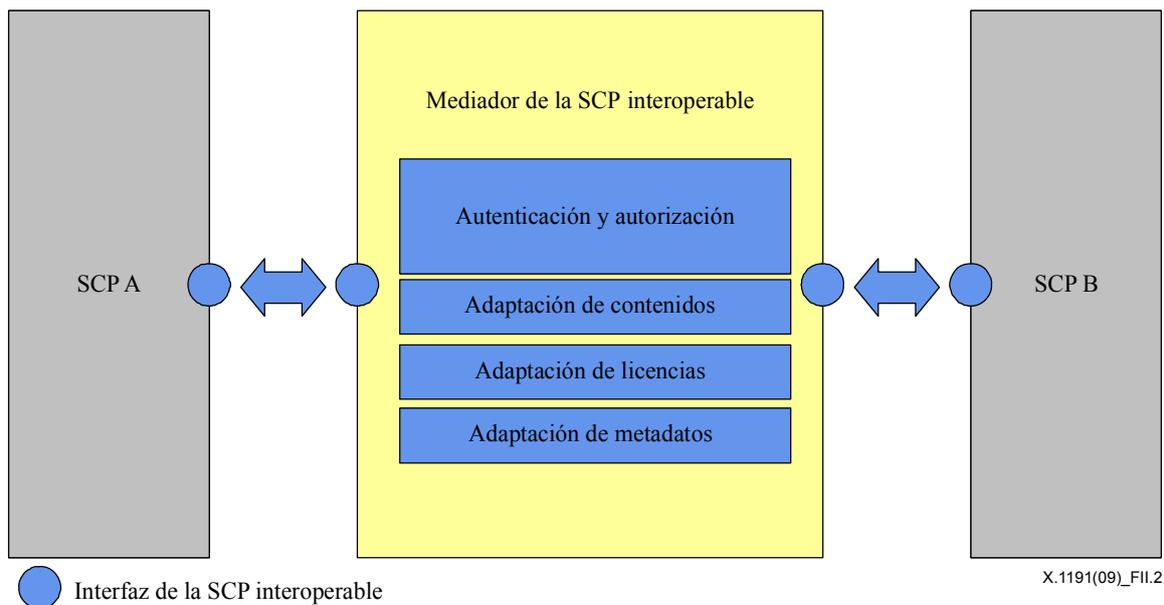


Figura II-2 – Arquitectura de la SCP interoperable basada en mediador

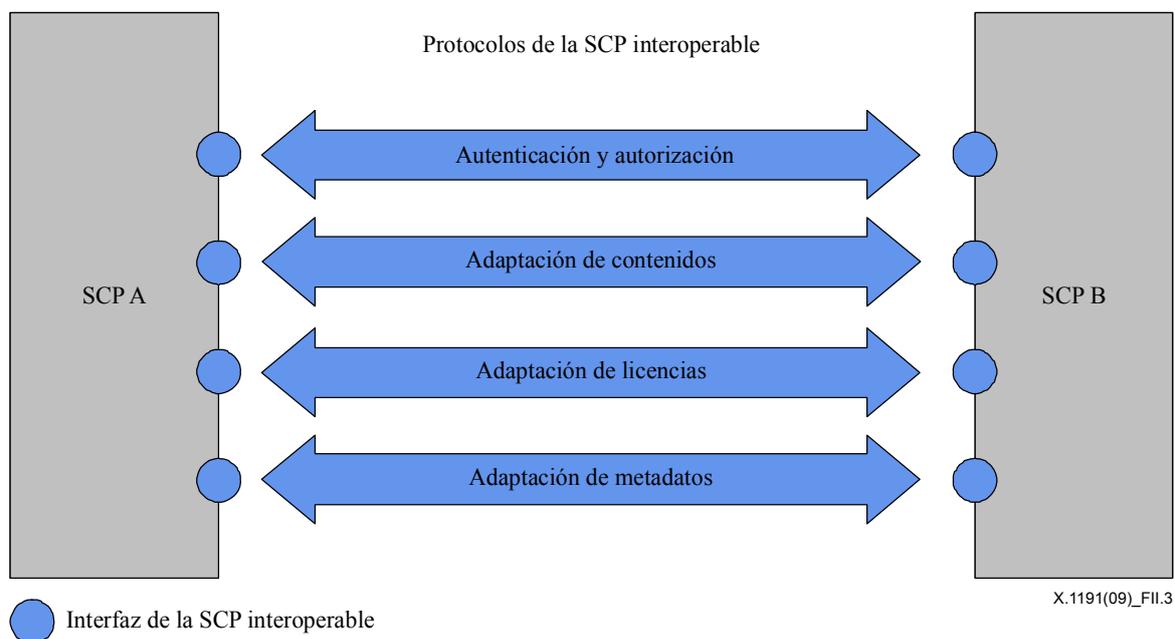


Figura II-3 – Arquitectura de la SCP interoperable basada en un protocolo normal

Descripción de los bloques funcionales:

- **Adaptación de contenidos:** La adaptación de contenidos es la encargada del algoritmo criptográfico de conversión. Los diversos algoritmos de encriptación estándar predefinidos facilitarán estos procesos.

- **Adaptación de licencias:** La adaptación de licencias es la encargada de convertir las licencias. Toda licencia temporal o normal conocida por ambas partes debe mantener prácticamente los mismos comportamientos de permiso (pares de activos de medios y permisos de consumo) que los definidos en la licencia original. Puede incluirse una correspondencia del conjunto de derechos (correspondencia de expresiones de derechos y correspondencia semántica) en la adaptación de la licencia. Además, la adaptación de la licencia puede encargarse de volver a empaquetar la información de derechos y entregarla con seguridad a sus clientes SCP nativos.
- **Adaptación de metadatos:** La adaptación de metadatos es la encargada de convertir la información de metadatos. Los metadatos temporales o normales conocidos por ambas partes deben mantener la misma información que la que contenían los metadatos originales. Puede incluirse un conjunto de correspondencias de metadatos (correspondencia sintáctica y semántica) en la adaptación de metadatos. Por otra parte, la adaptación de metadatos puede encargarse de volver a empaquetar la información de metadatos y entregarla con seguridad a la otra parte SCP.
- **Autenticación y autorización:** Cada una de las partes SCP debe juzgar si la otra es un objetivo adecuado para lograr la interoperabilidad SCP. Suele venir acompañada de un proceso de autenticación mutua entre las dos partes SCP como paso preliminar.

Caso excepcional: Si la SCP A y la SCP B están situadas dentro del mismo dispositivo, o en el caso de que exista un canal de comunicaciones seguro y dedicado entre las dos SCP, es posible que el proceso de adaptación de contenidos no necesite un procesamiento interoperable.

II.5 Escenarios de la SCP-B o de la SCP-IX instalados en el TD

En esta cláusula se describen tres escenarios posibles que requieren el intercambio de la SCP entre la seguridad de servicios y la seguridad de contenidos.

II.5.1 Definición de los términos utilizados en el diagrama

- SCP_IN: Puerto de entrada por el que se recibe el contenido de TVIP protegido por la SCP.
- SCP_OUT: Puerto de salida por el que se emite el contenido de TVIP protegido por la SCP.

II.5.2 Escenario 1: SCP con SCP_IX

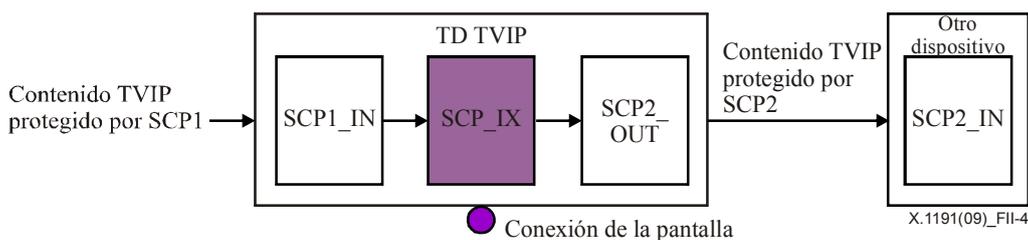


Figura II-4 – SCP con SCP_IX

El TD (aparato terminal, *terminal device*) TVIP, en este caso, tiene SCP con SCP_IX para soportar la interoperabilidad entre el TD TVIP sin almacenamiento que adopta sólo la seguridad de un servicio específico y el dispositivo externo con almacenamiento que sólo tiene protección de un contenido específico.

Para soportar la conectividad segura y flexible a cualquier tipo de dispositivo externo adoptando diversos mecanismos de protección de contenidos, el TD TVIP debe tener SCP_IX y no una implementación individualizada para la conexión de seguridad entre dos dispositivos.

II.5.3 Escenario 2: SCP con SCP-B opcional y almacenamiento

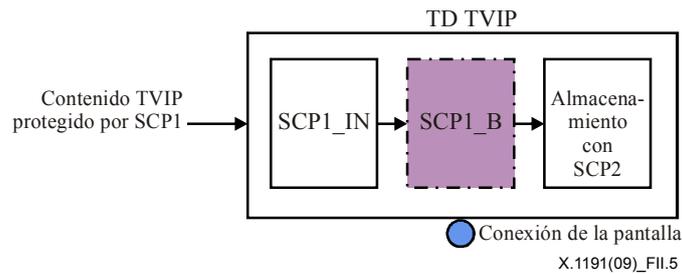


Figura II-5 – SCP con SCP-B opcional y almacenamiento

El TD TVIP en este caso tiene SCP con SCP-B para soportar la interoperabilidad entre la protección del servicio y la protección de contenidos en un solo dispositivo.

El fabricante del TD TVIP puede adoptar el mecanismo propietario de protección de contenidos para el almacenamiento interno. En tal caso, ya no es necesaria la SCP_B y el almacenamiento puede utilizar la SCP1.

Para soportar la conectividad flexible con cualquier tipo de almacenamiento interno que adopte varios mecanismos de protección de contenidos, se recomienda que el TD TVIP tenga SCP_B y no una implementación individualizada para la conexión de seguridad entre la protección del servicio y la protección de contenidos.

II.5.4 Escenario 3: SCP con almacenamiento y SCP_IX

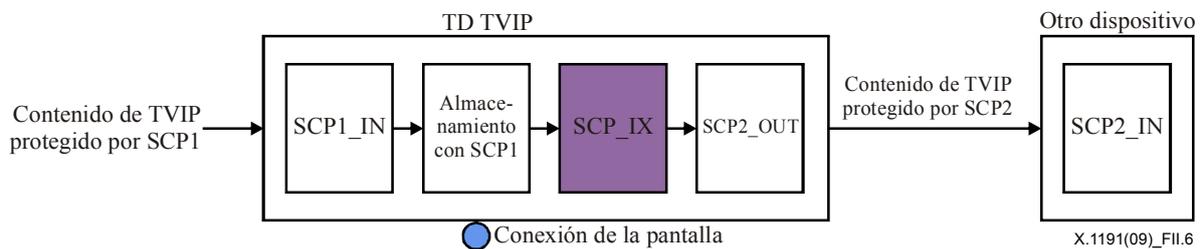


Figura II-6 – SCP con almacenamiento y SCP_IX

En este caso, el TD TVIP tiene SCP con almacenamiento y SCP_IX para soportar la interoperabilidad entre el mecanismo interno de protección de contenidos y el externo.

Para soportar la conectividad flexible con cualquier tipo de almacenamiento externo que adopte varios mecanismos de protección de contenidos, se recomienda que el TD TVIP tenga SCP_IX en vez de una implementación individualizada para la conexión de seguridad entre el mecanismo interno de protección de contenidos y el externo.

Apéndice III

Ejemplo de proceso de protección de contenidos TVIP

(Este apéndice no es parte integrante de la presente Recomendación)

A continuación se describe un ejemplo de proceso de aplicación VoD para protección de contenidos:

- *Fase de autenticación del abonado*
 - El abonado selecciona una aplicación VoD mediante el "bloque funcional servicio y descubrimiento de la aplicación y selección de cliente".
 - Las "funciones de la aplicación TVIP" enviarán la petición una vez recibido el "bloque funcional del perfil de la aplicación para verificar la identidad de este abonado. En caso positivo, la información de autorización pertinente a este abonado se almacenará en memoria caché dentro del "bloque funcional del perfil de la aplicación" para su consulta posterior.
- *Fase de selección de contenidos*
 - El abonado puede seleccionar un contenido de medios específico utilizando la información de la ECG, y el "bloque funcional de la aplicación VoD" entregará la información de la situación del contenido seleccionado (URL) al TD.
 - El "bloque funcional del cliente VoD" del TD recibe la situación del contenido para su transmisión a las "funciones del cliente de entrega de contenidos".
- *Fase de entrega de contenidos encriptados*
 - Las "funciones del cliente de entrega de contenidos" solicitan el contenido de medios "encriptado" utilizando la información de situación del contenido; asimismo solicitan los derechos y claves asociadas a este contenido al "bloque funcional del cliente de protección de contenidos".
- *Fase de distribución de derechos y claves*
 - Si no dispone de los derechos y claves, el "bloque funcional del cliente de protección de contenidos" los solicitará al "bloque funcional de gestión de derechos y claves" del proveedor de servicios TVIP.
 - El "bloque funcional de gestión de derechos y claves" solicitará la información de autorización asociada a este abonado al "bloque funcional de perfil de la aplicación" para comprobar si el abonado tiene derecho a consumir este contenido utilizando la información.
 - En caso afirmativo, los derechos y claves correspondientes a los contenidos seleccionados se entregarán al "bloque funcional del cliente de protección de contenidos".
 - Una vez recibidos, el "bloque funcional del cliente de protección de contenidos" transferirá la claves y derechos a las "funciones del cliente de entregas de contenidos" para descryptar los contenidos y controlar su utilización.

Apéndice IV

Protección de contenidos y gestión de copias para DVB

(Este apéndice no es parte integrante de la presente Recomendación)

Este apéndice presenta un resumen del conjunto de especificaciones de gestión de copias y protección de contenidos de la DVB (DVB-CPCM, *DVB content protection and copy management*), elaboradas por la ETSI.

DVB-CPCM es un ejemplo de sistema de protección de la televisión y otros contenidos en una red doméstica y fuera de ésta, totalmente normalizado. DVB-CPCM puede adquirir contenidos de un mecanismo de protección del servicio TVIP definido por la UIT (u otro) y mantener la protección de contenidos TVIP a lo largo de la vida útil del contenido desde su adquisición hasta su consumo pasando por el almacenamiento, procesamiento y exportación del contenido protegido a otros mecanismos de seguridad TVIP, sin perjuicio del mantenimiento de la correcta utilización autorizada.

IV.1 Introducción

DVB-CPCM es un sistema de protección de contenidos y gestión de copias de contenidos digitales comerciales de libre emisión y entrega a productos de consumo y redes domésticas. CPCM gestiona la utilización de los contenidos desde la adquisición por el sistema CPCM hasta el consumo final o exportación desde el sistema CPCM con arreglo a las reglas particulares de utilización de dicho contenido. CPCM se ha diseñado para ser utilizado en la protección de todo tipo de contenidos, por ejemplo audio, vídeo y aplicaciones y datos asociados. CPCM proporciona especificaciones para facilitar la interoperabilidad de dichos contenidos tras su adquisición e introducción en CPCM por parte de dispositivos de los consumidores en red, tanto para redes domésticas como para acceso remoto. Esta especificación está integrada por varias secciones, en algunas de las cuales se especifica la señalización y las acciones necesarias para su conformidad técnica, mientras que en otras se explica el fundamento de la especificación así como las directrices de implementación. Hay un modelo de referencia que proporciona el marco para el sistema CPCM y sirve como base de construcción de los restantes elementos de esta especificación.

IV.2 Definiciones

En este apéndice se definen los siguientes términos, además de los ya definidos en el cuerpo de la Recomendación.

IV.2.1 adquirir: Supone recibir e ingerir contenidos exteriores al sistema CPCM por parte de éste.

IV.2.2 punto de adquisición (AP, *acquisition point*): Entidad funcional CPCM abstracta en la que tiene lugar la adquisición de los contenidos.

IV.2.3 adquisición: Recepción e ingestión de contenidos exteriores al sistema CPCM por parte de éste.

IV.2.4 dominio autorizado (AD, *authorized domain*): Conjunto distinguible de dispositivos conformes con DVB-CPCM que son poseídos, alquilados o controlados por los miembros de un solo hogar; el hogar se considera una unidad social compuesta de todos los individuos que conviven como ocupantes del mismo domicilio (sin establecer hipótesis alguna sobre la ubicación física de los dispositivos poseídos, alquilados o controlados por los miembros del hogar).

IV.2.5 utilización autorizada: Utilización permitida del contenido CPCM; consta de un conjunto de aserciones de reglas de utilización aplicadas a dichos contenidos.

IV.2.6 consumir: Supone reproducir tangiblemente contenidos o darles salida sin impedir ninguna otra utilización.

IV.2.7 punto de consumo (CP, *consumption point*): Entidad funcional CPCM abstracta en la que se ejecuta el Consumo.

IV.2.8 consumo: Reproducción tangible de contenidos o salida de dispositivo que contenga una transformación o una señal destinada a inhibir cualquier utilización distinta de la conversión inmediata del contenido en sonido e imagen.

IV.2.9 elemento de contenido: Instancia discreta de contenido de duración finita, por ejemplo programa, evento o fragmento incompleto de los mismos.

IV.2.10 licencia de contenido: Estructura de datos comunicada y mantenida con seguridad que contiene la información necesaria para gestionar la seguridad de un elemento de contenido CPCM.

IV.2.11 contenido: Datos que debe proteger el sistema CPCM; se refiere normalmente a contenidos audiovisuales, con los datos opcionales de acompañamiento tales como subtítulos, imágenes/gráficos, animaciones, páginas web, texto, juegos, programas informáticos (tanto código fuente como objeto), guiones o cualquier otra información que haya de entregarse a un usuario para ser consumido por éste.

IV.2.12 copia: Proceso gestionado por CPCM mediante el cual se crea un nuevo elemento de contenido almacenado a partir del contenido adquirido o a partir de un elemento de contenido previamente almacenado.

IV.2.13 dispositivo CPCM: Dispositivo que aloja una o varias instancias CPCM.

IV.2.14 sistema CPCM: Conjunto de todos los dispositivos CPCM conformes.

IV.2.15 aplicación del dispositivo: Cualquier funcionalidad no CPCM de un dispositivo CPCM.

IV.2.16 punto de exportación (EP, *export point*): Entidad funcional CPCM abstracta en la que el contenido CPCM sale del sistema CPCM.

IV.2.17 exportación: Liberación de la protección y gestión explícita del contenido CPCM por parte del sistema CPCM a una CPS controlada, a una CPS de confianza o a un espacio no fiable.

IV.2.18 movimiento: Proceso de efectuar una copia en la que el original se suprime, se borra o su reproducción ya no es posible.

IV.2.19 salida: Interfaz de dispositivo o CPS utilizada para transmitir contenidos CPCM, contenidos consumidos o contenidos exportados.

IV.2.20 entidad procesadora (PE, *processing entity*): Entidad funcional abstracta CPCM en la que se procesan los contenidos CPCM.

IV.2.21 procesamiento: Operación conforme con CPCM sobre contenidos encriptados o desencriptados con independencia de su consumo o exportación. Por ejemplo, un contenido CPCM se somete a una transformación permitida de su forma original para crear un nuevo contenido CPCM transformado o información tal como niveles de volúmenes de audio, o bien se extraen imágenes fijas del contenido.

IV.2.22 información del estado de utilización (USI, *usage state information*): Metadatos del contenido CPCM que señalan la utilización autorizada para cada elemento de contenido CPCM.

IV.2.23 visionar: Consumir.

NOTA – Esto comprende asimismo la escucha de contenidos de audio exclusivamente.

IV.2.24 visionado: Consumo.

NOTA – Esto incluye asimismo la escucha de contenido de audio exclusivamente.

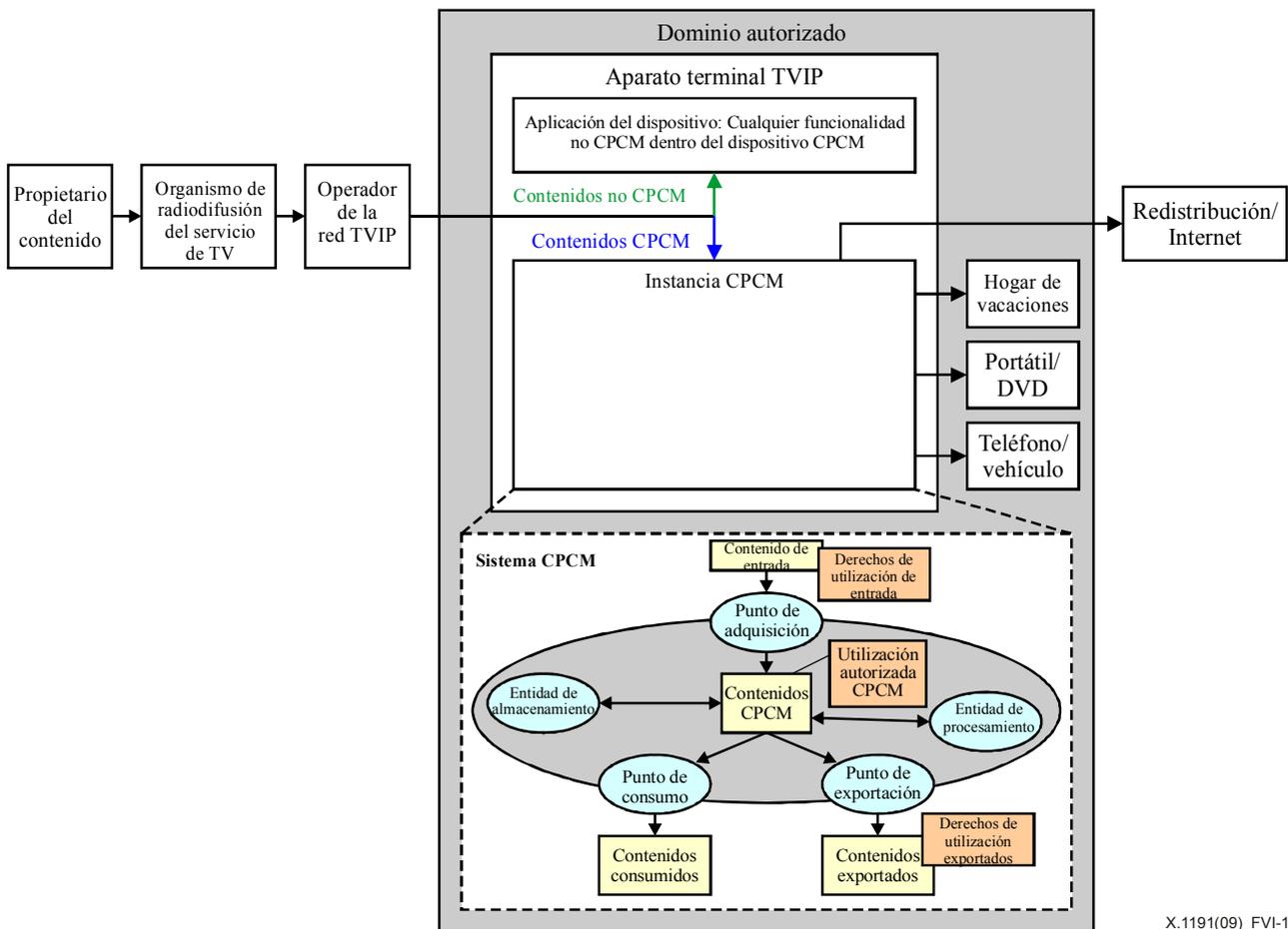
IV.3 Abreviaturas y acrónimos

En este apéndice se utilizan las siguientes abreviaturas, además de las del cuerpo de la Recomendación.

AP	Punto de adquisición (<i>acquisition point</i>)
APECS	Adquisición, procesamiento, exportación y almacenamiento (<i>acquisition, processing, export, consumption, storage</i>)
CL	Licencia de contenido (<i>content license</i>)
CP	Punto de consumo (<i>consumption point</i>)
CPCM	Protección de contenidos y gestión de copias (<i>content protection and copy management</i>)
CPE	Equipo en las instalaciones del cliente (<i>customer premise equipment</i>)
CPS	Sistema de protección de contenidos (<i>content protection system</i>)
DVB	Radiodifusión de vídeo digital (<i>digital video broadcasting</i>)
EP	Punto de exportación (<i>export point</i>)
PE	Entidad de procesamiento (<i>processing entity</i>)
SE	Entidad de almacenamiento (<i>storage entity</i>)
USI	Información del estado de utilización (<i>usage state information</i>)

IV.4 La arquitectura CPCM

En el corazón de la CPCM se encuentra el "dominio autorizado", conjunto de dispositivos pertenecientes a un hogar, aunque se encuentren fuera del mismo. El concepto AD reconoce que la vinculación de los contenidos a un único adaptador multimedios (TD) y pantalla de televisión anexa resultan insuficientes en la era del entretenimiento en red. CPCM toma el contenido de una fuente de confianza tal como un sistema SCP TVIP, como materialización de un TD o de parte del mismo, y protege el contenido, tren, o fichero recibido, gestionando el modo en que puede visionarse, moverse o copiarse. Como modelo de gestión básico de contenidos CPCM, el contenido de entrada introduce el sistema CPCM para convertirlo en contenido CPCM. El contenido CPCM se gestiona y protege en el seno del sistema CPCM, y sale del sistema CPCM cuando ha sido consumido por el usuario o exportado a otro sistema.



X.1191(09)_FVI-1

Figura IV-1 – Flujo de contenidos en un entorno CPCM

La CPCM soporta una diversidad de usos de los contenidos en una red doméstica; puede gestionar asimismo el acceso a los contenidos desde puntos remotos tales como un ordenador portátil conectado a Internet mediante un enlace de banda ancha. Gracias a la CPCM los proveedores de servicios pueden indicar a los fabricantes de dispositivos los escenarios admisibles para cada tipo de contenido. Esto amplía muchos de los métodos de protección vigentes hoy en día tales como los materializados en las tecnologías SCP TVIP en los que los contenidos se suelen restringir a un único cable de interconexión punto a punto entre el dispositivo origen de los contenidos (tal como un adaptador multimedia) y el dispositivo de visualización digital.

La CPCM supera esta protección localizada y ofrece a los organismos de radiodifusión, operadores de red y propietarios de contenidos la opción de permitir el acceso a un determinado miembro de un hogar desde una ubicación remota tal como un hotel durante un viaje de negocios o unas vacaciones.

La CPCM puede asimismo permitir a los usuarios la copia de contenidos a dispositivos portátiles y a unidades de almacenamiento extraíbles tales como el DVD. Siempre que el dispositivo reproductor pertenezca al mismo dominio autorizado, el dispositivo será capaz de reproducir el contenido aunque esté desconectado del hogar y del proveedor de servicios original. El contenido CPCM no requiere la autorización del proveedor de servicios en línea para añadir o suprimir dispositivos del dominio autorizado.

El sistema de protección de contenidos CPCM no es una entidad autónoma; está incorporado/superpuesto al sistema de distribución global SCP TVIP extremo a extremo. Por ello, coexiste con el sistema SCP TVIP y no constituye una sustitución del mismo. En todo TD, la instancia CPCM es opcional; de no estar presente, no obstante, no se le concederá acceso a ningún

contenido protegido por CPCM. Sin embargo, el TD no necesita implementar todos los elementos de la CPCM. Sólo se exigirá ejecutar la funcionalidad necesaria a aquéllos que sean útiles para el TD. Por ejemplo, un dispositivo sencillo sólo puede implementar funcionalidades de adquisición y consumo CPCM si no tiene almacenamiento CPCM ni requisitos de exportación.

IV.5 Modelo de referencia y entidades funcionales CPCM

El modelo de referencia CPCM define un conjunto de cinco funciones abstractas de gestión de contenidos que cubren todos los escenarios de utilización de contenidos pertinentes en el entorno del consumidor: adquisición, almacenamiento, procesamiento, consumo y exportación. Estas funciones se corresponden con las cinco entidades funcionales CPCM: punto de adquisición, entidad de almacenamiento, entidad de procesamiento, punto de consumo y punto de exportación. En la figura VI-1 se representa un esquema del sistema CPCM en términos del conjunto de entidades funcionales abstractas.

Así pues, el contenido de entrada que se introduce en el sistema CPCM entra gracias a su Adquisición en un punto de adquisición por parte de un dispositivo CPCM que implementa dicho punto de adquisición para convertirse en contenido CPCM. El contenido CPCM puede ser almacenado o procesado por parte de las entidades funcionales correspondientes (entidad de almacenamiento, entidad de procesamiento) implementadas en un dispositivo CPCM. El contenido CPCM sale del sistema CPCM una vez consumido en un punto de consumo o exportado en un punto de exportación. Estas entidades funcionales pueden implementarse también dentro de cualquier dispositivo CPCM.

IV.6 Dominio autorizado CPCM

Los dispositivos CPCM pueden agruparse lógicamente en dominios autorizados. Si todos esos dispositivos pertenecen a un mismo hogar, constituirán un dominio autorizado (AD) del hogar. De este modo, el dominio autorizado proporciona un destino para el contenido, que se corresponde con los límites de un solo hogar. Por lo general, puede considerarse que el AD es la agrupación lógica de todos los dispositivos CPCM que pertenecen a un hogar: los ubicados en el domicilio principal, los ubicados en otro domicilio (por ejemplo la casa de vacaciones), los portátiles que sólo se conectan intermitentemente a los dispositivos estacionarios citados, y los conectados a los vehículos que pertenecen a dicho hogar. El AD se ha diseñado para constituir un grupo lógico autónomo de dispositivos y no requiere de ninguna administración externa. Obsérvese, no obstante, que en muchos casos el AD está vinculado a un proveedor de servicios particular que puede ofrecer la administración del AD como parte del servicio prestado al consumidor.

IV.7 Reglas de utilización de contenidos CPCM

La utilización autorizada de cualquier elemento de contenido CPCM consiste en el conjunto de aserciones de utilización expresadas en las reglas de utilización CPCM vinculadas al contenido. Las reglas de utilización CPCM pueden ser fijadas por el contenido o por el proveedor de servicios o deducirse de la forma de entrega (por ejemplo, radiodifusión de emisión libre). El grado de ejecución de las operaciones de almacenamiento, consumo y exportación puede estar sometido a la utilización autorizada del contenido. CPCM define un conjunto común de reglas de utilización de las que cualquier proveedor de contenidos puede seleccionar y derivar la utilización autorizada deseada para el contenido del sistema CPCM. El conjunto de reglas de utilización CPCM se ha diseñado para ser lo suficientemente flexible como para cubrir todos los modelos de protección y gestión de contenidos aplicables así como lo suficientemente conciso como para mantener modelos de utilización de contenidos relativamente claros y sencillos para el consumidor.

IV.8 Metadatos de información del estado de utilización

La utilización autorizada de un elemento de contenidos se codifica como metadatos de contenidos CPCM denominados información del estado de utilización (USI, *usage state information*). El contenido CPCM se gestiona y protege con arreglo a la USI aplicada a cada elemento de contenido. Además de las transiciones de estados USI conformes, realizadas implícitamente por el sistema CPCM, las entidades que disfrutan de una autorización legítima sobre los contenidos dentro del sistema CPCM pueden ejecutar otras modificaciones al estado de la USI del elemento del contenido tras su adquisición en el sistema CPCM.

IV.9 Contenidos CPCM

"Contenidos" se refiere por lo general a material audiovisual más los datos opcionales que les acompañan tales como subtítulos, imágenes/gráficos, animaciones, páginas web, textos, juegos, programas informáticos (tanto código fuente como objeto), guiones y cualquier otra información que deba entregarse al usuario para ser consumido por éste. Los contenidos CPCM están sujetos a protección y gestión de contenidos por el sistema CPCM y de conformidad con éste. Un elemento de contenido es una instancia discreta de contenido de duración finita. Cada elemento de contenido CPCM viene acompañado de una licencia de contenido que transporta la USI asociada junto con más metadatos CPCM. El sistema CPCM puede manejar la licencia de contenido y el propio elemento de contenido de diferentes maneras en función de la funcionalidad objetivo y/o aplicación de las reglas de utilización requeridas por la USI.

IV.10 El Dispositivo CPCM

Un dispositivo CPCM es aquél que implementa cualquier funcionalidad CPCM de una manera conforme. La implementación de la funcionalidad CPCM se denomina instancia CPCM. Un dispositivo CPCM es pues aquél que aloja una o más instancias CPCM. Puede contener asimismo otras funciones no conformes con CPCM además de las de funcionalidad CPCM. El manejo del contenido CPCM se ejecuta sólo por la Instancia CPCM existente en el dispositivo. La parte no CPCM del dispositivo no tiene acceso al contenido CPCM. El dispositivo CPCM puede asimismo alojar la funcionalidad segura no CPCM para la adquisición segura de contenidos de otros sistemas de protección o exportación segura (y posiblemente consumo) del contenido CPCM.

IV.11 Reglas de utilización e información del estado de utilización

Una regla de utilización en CPCM consiste en una operación o comportamiento particular del contenido que ha de controlarse dentro del ámbito del sistema CPCM. El conjunto completo de aserciones de las reglas de utilización para un elemento de contenido CPCM particular se denomina utilización autorizada de dicho elemento de contenido CPCM. La utilización autorizada de un elemento de contenido se expresa mediante su codificación en la información de estado de utilización (USI), consistente en los metadatos de contenido CPCM que indican la utilización autorizada para dicho contenido específico.

Apéndice V

Esquema transcodificable seguro

(Este apéndice no es parte integrante de la presente Recomendación)

V.1 Introducción al esquema transcodificable seguro

La transcodificación de contenidos ha sido objeto de especial atención debido a la creciente popularidad de diversos tipos de dispositivos tales como los PDA, dispositivos distintos del PC, teléfonos móviles y terminales móviles inteligentes. La transcodificación es el proceso de transformar contenidos multimedios tales como imágenes, texto, audio y vídeo desde su formato original a un formato o calidad diferentes.

La transcodificación pretende reducir el retardo de la descarga de contenidos de multimedios con enlaces de acceso de pequeña anchura de banda tales como los que utilizan módem y los de acceso inalámbrico, y resolver la desadaptación entre el formato de codificación soportado por un dispositivo del cliente y el utilizado por un proveedor de contenidos multimedios. Permite asimismo que un terminal con una capacidad limitada de computación pueda mostrar contenidos codificados en base a su capacidad de transcodificación.

En el esquema transcodificable seguro se definen tres entidades: el emisor, el nodo intermedio de la red y el usuario dotado de un terminal TVIP. La función de transcodificación reside en un nodo intermedio de la red situado entre el proveedor de contenidos y el dispositivo cliente. Hay dos tipos de arquitecturas de transcodificación: la arquitectura de transcodificación tradicional y la arquitectura de transcodificación segura.

En la arquitectura de transcodificación tradicional, se utiliza un apoderado de transcodificación como nodo intermedio de la red entre el servidor de contenidos y el dispositivo cliente. El emisor encripta el contenido con una compresión adecuada y lo envía al nodo intermedio de la red denominado apoderado de transcodificación. El apoderado de transcodificación desencripta el contenido encriptado y lo descomprime. A continuación modifica el tamaño del contenido o su formato comprimiéndolo de nuevo y por último vuelve a encriptar los datos de transcodificación para su transmisión al dispositivo cliente. El dispositivo cliente desencripta el contenido encriptado y descomprime el contenido utilizando un nuevo algoritmo de compresión. Obsérvese, no obstante, el problema de seguridad que se plantea en el apoderado de transcodificación, a saber, una vez desencriptado el contenido en el apoderado de transcodificación y antes de ser encriptado de nuevo, el contenido desencriptado reside en el apoderado de transcodificación. Dicho de otro modo, un observador puede tener acceso al contenido desencriptado mediante escucha clandestina. Este contenido desencriptado debilita la garantía de seguridad de la privacidad extremo a extremo, en la que se supone que sólo el emisor y el cliente legítimo tienen acceso al contenido en un estado desencriptado.

Para abordar este problema de seguridad se propone una arquitectura de transcodificación segura. Un esquema de transcodificación seguro es un tipo de esquema de seguridad que permite que un nodo intermedio de la red ejecute la transcodificación sin desencriptación preservando al mismo tiempo la seguridad de extremo a extremo. Este esquema puede ejecutarse mediante una combinación de codificación escalonable, encriptación progresiva y paquetización. El emisor ejecuta una función transcodificable segura para producir paquetes encriptados escalonables a partir del vídeo y añade el encabezamiento desencriptado para enviar la información; el nodo intermedio de la red lee el encabezamiento desencriptado y utiliza la información para truncar o descartar los paquetes adecuados de acuerdo con la operación de transcodificación deseada; por último, el terminal TVIP desencripta los paquetes encriptados y decodifica los paquetes en texto claro para producir el vídeo.

Bibliografía

- [b-ITU-T H.222.0] Recomendación UIT-T H.222.0 (2006) | ISO/IEC 13818-1:2007, *Tecnología de la información – Codificación genérica de imágenes en movimiento e información de audio asociada: Sistemas*.
- [b-ITU-T H.622.1] Recomendación UIT-T H.622.1 (2008), *Requisitos de arquitectura funcional para el soporte de servicios TVIP en redes domésticas*.
- [b-ITU-T M.1400] Recomendación UIT-T M.1400 (2006), *Designaciones para interconexiones entre operadores de red*.
- [b-ITU-T Q.1290] Recomendación UIT-T Q.1290 (1998), *Glosario de términos utilizados en la definición de redes inteligentes*.
- [b-ITU-T X.800] Recomendación UIT-T X.800 (1991), *Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT*.
- [b-ITU-T X.805] Recomendación UIT-T X.805 (2003), *Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo*.
- [b-ITU-T Y.101] Recomendación UIT-T Y.101 (2000), *Terminología de la infraestructura mundial de la información: Términos y definiciones*.
- [b-ITU-T Y.1901] Recomendación UIT-T Y.1901 (2009), *Requisitos del servicio TVIP*.
- [b-ITU-T Y.2012] Recomendación UIT-T Y.2012 (2006), *Requisitos y arquitectura funcional de las redes de la próxima generación, versión 1*.
- [b-ETSI TS 102 825] ETSI TS 102 825 (all parts), *Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM)*.
<<http://pda.etsi.org/pda/AQuery.asp>>
- [b-ATIS 0800001] ATIS 08000001, *IPTV DRM Interoperability Requirements, ATIS-IIF*, abril de 2007.
<<https://www.atis.org/docstore/product.aspx?id=21212>>
- [b-ATIS 0800006] ATIS 0800006, *IIF Default Scrambling Algorithm (IDSA) IPTV Interoperability Specification*, febrero de 2007.
<<https://www.atis.org/docstore/product.aspx?id=22663>>

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios generales de tarificación
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	Construcción, instalación y protección de los cables y otros 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	Terminales y métodos de evaluación subjetivos y objetivos
Serie Q	Conmutación y señalización
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 y Redes de la próxima generación
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación