Unión Internacional de Telecomunicaciones

UIT-T J.197

(11/2005)

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

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

Módems de cable

Requisitos de alto nivel para un puente de gestión de derechos digitales desde una red de acceso de cable a una red doméstica

Recomendación UIT-T J.197

UIT-T

ITU Unión Internacional de Telecomunicaciones

Recomendación UIT-T J.197

Requisitos de alto nivel para un puente de gestión de derechos digitales desde una red de acceso de cable a una red doméstica

Resumen

La presente Recomendación determina los requisitos de un puente de gestión de derechos digitales desde una red de acceso de cable a una red doméstica a través del cual los operadores de red puedan transferir diversos tipos de contenido (por ejemplo, vídeo, audio, etc.) con la seguridad de que el contenido no se utiliza de manera que constituya una violación de los acuerdos de servicio o requisitos impuestos por la ley.

Orígenes

La Recomendación UIT-T J.197 fue aprobada el 29 de noviembre de 2005 por la Comisión de Estudio 9 (2005-2008) del UIT-T por el procedimiento de la Recomendación UIT-T A.8.

PREFACIO

La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT) 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.

ÍNDICE

Recomendación UIT-T J.197

Requisitos de alto nivel para un puente de gestión de derechos digitales desde una red de acceso de cable a una red doméstica

1 Alcance

La presente Recomendación determina los requisitos de un puente de gestión de derechos digitales desde una red de acceso de cable a una red doméstica a través del cual los operadores de red puedan transferir diversos tipos de contenido (por ejemplo, vídeo, audio, etc.) con la seguridad de que el contenido no se utiliza de manera que constituya una violación de cualquiera de los acuerdos de servicio o requisitos impuestos por la ley.

2 Referencias

2.1 Referencias normativas

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

– NIST FIPS 140-2 (2002), *Security requirements for cryptographic modules*.

2.2 Referencias informativas

– Recomendación UIT-T J.192 (2005), *Pasarela residencial para soportar la entrega de servicios de datos por cable*.

– DTCP (2005), *Digital transmission content protection specification volume 1 (information version)*.

– Intel (2005), *High-bandwidth digital content protection system, revision 1.1*.

3 Términos y definiciones

En esta Recomendación se definen los términos siguientes.

3.1 bits de sistema de protección analógica (Bits APS): Bits 2 y 3 de la CCI que indican el estado de protección analógica de un adaptador multimedia.

3.2 reglas para garantizar el cumplimiento (en adelante "reglas de cumplimiento"): Reglas que se aplican a los adaptadores multimedia con el fin de prevenir la copia no autorizada de contenido controlado.

3.3 filigrana de consenso: Filigrana normalizada elaborada para su utilización en la gestión de derechos digitales.

3.4 imagen constreñida: Equivalente visual de no más de 520 000 píxeles por trama (por ejemplo, una imagen con una resolución de 540 líneas verticales por 960 líneas horizontales con una relación de formato 16:9). Una imagen constreñida puede ser transmitida o visualizada utilizando técnicas de procesamiento de vídeo tales como la agudización o duplicación de líneas para mejorar la calidad percibida de la imagen.

3.5 activador de imagen constreñida (CIT, *constrained image trigger*): Campo o bits utilizados para activar la producción de una "imagen constreñida**"** en la salida analógica de alta definición de los adaptadores multimedia.

3.6 protección de contenido: Aplicación de salvaguardias técnicas que impiden la duplicación y/o redistribución no autorizadas del contenido transmitido por la red.

3.7 contenido controlado: Contenido que se ha transmitido desde la red de un proveedor de servicio de vídeo con los bits de indicador de modo criptación (EMI, *encryption mode indicator*) puestos a un valor distinto de cero, cero (0,0) ("copia no restringida").

3.8 información de control de copia (CCI, *copy control information*): Campo de un byte que contiene la información que utilizan los adaptadores multimedia para controlar la copia del contenido. Véanse más detalles en el anexo A.

3.9 gestión de derechos digitales (DRM, *digital rights management*): Definición, gestión y aplicación de una serie de reglas de utilización del contenido. Estas reglas de utilización indicarán parámetros tales como el derecho de copia, visualización o distribución de un elemento concreto de contenido.

3.10 protección de contenido de transmisiones digitales (DTCP, *digital transmission content protection*): Método de criptación, descriptación, intercambio de claves y renovabilidad que se describe en la especificación "5C digital transmission content protection release 1.0".

3.11 puente DRM: Infraestructura y tecnologías de redes de distribución y doméstica creadas para aplicar la protección de contenido y la gestión de derechos digitales a contenidos transmitidos por la red y que se almacenan o distribuyen en una red doméstica.

3.12 bits de indicador de modo criptación (Bits EMI, *encryption mode indicator*): Dos bits, asociados al contenido protegido, que especifican las operaciones de copia que están permitidas en relación con el contenido.

3.13 formato o producto analógico de alta definición: Formato o producto que no es digital y cuya resolución es superior al formato o producto analógico de definición normalizada.

3.14 protección de contenido digital de elevado ancho de banda (HDCP, *high-bandwidth digital content protection*): Método de autenticación, criptación, descriptación y renovabilidad que se describe en la especificación "High-bandwidth digital content protection system, rev. 1.1".

3.15 producto: Dispositivo y/o tecnología que recibe y posiblemente distribuye contenido con control de redistribución y/o control de copia.

3.16 reglas de robustez: Reglas descritas en las cláusula 6 que se aplican a los adaptadores multimedia con el fin de impedir los intentos de modificar los adaptadores multimedia para infringir las reglas de cumplimiento.

3.17 servicio: Señales de vídeo, audio o datos, en formato digital o analógico, transmitidas por la red de un proveedor de servicio de vídeo hacia (o desde) un adaptador multimedia para recibir o transmitir contenidos de información, entretenimiento o comunicaciones.

3.18 adaptador multimedia (STB, *set top box*): Todo dispositivo que recibe contenido directamente de un proveedor de servicio de vídeo, lo que incluye tanto los dispositivos distintos de los dispositivos de visualización, como los dispositivos de visualización que tienen esa funcionalidad incorporada. El STB funciona como una pasarela de servicio para la red doméstica e incluye el sistema de acceso condicional (CA, *conditional access*) y un sistema de gestión de derechos digitales (DRM).

3.19 formato o producto analógico de definición normalizada: Formato o producto que no es digital (por ejemplo, PAL RF, NTSC RF, compuesto, S-Video, YUV, Y, R-Y, B-Y o RGB) y no tiene más de 483 líneas de exploración activas progresivas o entrelazadas.

3.20 sistema de protección de contenido de vídeo (VCPS, *video content protection system*): El sistema de protección de contenido de vídeo para la grabación de contenido criptado en medios digitales ópticos DVD+RW y DVD+R protegidos por la tecnología VCPS.

3.21 proveedor de servicio de vídeo (VSP, *video service provider*): Proveedor de servicios que ofrece el "servicio" definido en esta Recomendación.

4 Abreviaturas, siglas, acrónimos y convenios

En esta Recomendación se utilizan las siguientes abreviaturas, siglas, acrónimos y convenios.

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

AMNT Asamblea Mundial de Normalización de las Telecomunicaciones

APS Sistema de protección analógico (*analogue protection system*)

CCI Información de control de copia (*copy control information*)

CGMS-A Analógico para el sistema de administración de generación de copia (*copy generation management system analogue*)

CIT Activador de imágen constreñida (*constrained image trigger*)

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

DTCP Protección de contenido de transmisiones digitales (*digital transmission content protection*)

DVD-RW Disco versátil digital regrabable (*digital versatile disk re-writable*)

DVD+R Disco versátil digital grabable (*digital versatile disk + recordable*)

DOCSIS Especificación de interfaz del servicio de datos por cable (*data over cable service interface specification*)

DVI Interfaz visual digital (*digital visual interface*)

EEPROM Memoria de sólo lectura programable y borrable eléctricamente (*electrically erasable programmable read-only memory*)

EMI Indicador de modo criptación (*encryption mode indicator*)

HDCP Protección de contenido digital de elevado ancho de banda (*high-bandwidth digital content protection*)

HDMI *Interfaz multimedia de alta definición* (*high-definition multimedia interface*)

IP Protocolo Internet (*Internet protocol*)

LSB Bit menos significativo (*least significant bit*)

MPEG Grupo de Expertos en imágenes en movimiento (*moving picture experts group*)

NTSC RF Frecuencia radioeléctrica del National Television System Committee de los Estados Unidos

OOB Fuera de banda (*out of band*)

PAL Línea con alternancia de fase (*phase alternate line*)

PCI *Interfaz de componente periférico* (*peripheral component interface*)

PCMCIA Asociación internacional de fabricantes de tarjetas de memoria de computador personal (*personal computer memory card international association*)

QoS Calidad de servicio (*quality of service*)

RF Frecuencia eléctrica (*radio frequency*)

RGB Rojo, verde, azul (*red, green, blue*)

SRM Mensaje con capacidad de renovación del sistema (*system renewability message*)

STB adaptador multimedia (*set top box*)

S-Video Super vídeo (*super-video*)

VCPS Sistema de protección de contenido de vídeo (*video content protection system*)

VSP Proveedor de servicio de vídeo (*video service provider*)

5 Consideraciones generales

La tecnología de red doméstica y su aceptación han evolucionado de tal manera que una red doméstica puede actuar como red de entretenimiento, que permite al usuario almacenar y distribuir contenido entre los distintos dispositivos de la red doméstica. Conviene que la industria aproveche este potencial y amplíe la prestación de estos servicios en las redes domésticas. Dado que los servicios de cable generalmente proporcionan contenidos de alta calidad sometidos a los derechos de autor, es necesario definir mecanismos para proteger el contenido y aplicar reglas de utilización pertinentes por diversas razones jurídicas y económicas. La presente Recomendación establece los requisitos de un puente de gestión de derechos digitales desde una red de acceso de cable a una red doméstica y a través del cual el operador de red puede transferir contenido con la seguridad de que éste no será utilizado de manera que viole los acuerdos de servicio o los requisitos legales.

5.1 Principales objetivos

Para cumplir los objetivos de la aplicación, un puente DRM debe:

- Ser suficientemente robusto desde el punto de vista del proveedor de contenido.
- No ser intrusivo desde el punto de vista del abonado.
- Ser conforme al entorno reglamentario y jurídico.

5.2 Principales características

A continuación se enumeran las principales características de un puente DRM:

- Autenticación de todos los dispositivos que participan en la transmisión y/o consumo de contenido de vídeo.
- Extensión de un conjunto completo de reglas mercantiles para la protección de contenido y gestión de derechos digitales (restricciones de copia, cantidad de reproducciones, límites de tiempo, etc.) establecidos como parte del STB.
- Criptación y descriptación de contenido de vídeo para transmisión y consumo.

5.3 Principales características técnicas

A continuación se numeran las principales características técnicas de un puente DRM:

- El puente DRM amplía los elementos esenciales de la DRM a puntos exteriores al STB.
- El puente DRM soporta la transmisión y almacenamiento tanto del contenido transmitido por operadores de redes en cable u otras.
- El contenido con control de redistribución o de copia sólo podrá salir del STB o de los elementos subsiguientes a través de las salidas aprobadas.

- El contenido sin control de redistribución o de copia podrá consumirse y almacenarse en el STB o en los elementos subsiguientes.
- El contenido sin control de redistribución o de copia podrá salir libremente del STB o de los elementos subsiguientes.

5.4 Requisitos generales del puente DRM

G-1	**fácil para el abonado**: El puente DRM será transparente al abonado, permitirá el adecuado consumo del contenido y su utilización no presentará obstáculos.
G-2	**modelo de utilización simple**: El puente DRM empleará un modelo de utilización simple que permita utilizar el contenido comprado y entregado por el operador de red en la red doméstica de acuerdo con los derechos otorgados al contenido.
G-3	**protección del contenido**: El puente DRM impedirá la transmisión o copia no autorizadas del contenido protegido fuera de la red doméstica.
G-4	**bloqueo de robo de servicio**: El puente DRM impedirá el robo de servicio y protegerá las reglas de utilización de contenido (por ejemplo, robo de contenido en la red inalámbrica en una unidad residencial múltiple).
G-5	**compatibilidad con otras tecnologías DRM**: El puente DRM no excluirá el uso de otras tecnologías de protección del contenido entregado por redes que no son de cable.
G-6	**independencia del transporte**: La tecnología utilizada para aplicar el puente DRM será independiente de la tecnología de la red doméstica.
G-7	**compatibilidad con versiones anteriores**: La tecnología de puente DRM no afectará al comercio de distribución de vídeo existente.
G-8	**independencia de la distribución**: El puente DRM deberá soportar diversas tecnologías de distribución, incluida la radiodifusión MPEG, la difusión en directo IP y FTP.
G-9	**protección en tiempo real**: La tecnología utilizada para aplicar el puente DRM deberá ser aplicable a los medios en tiempo real (por ejemplo, para la radiodifusión MPEG y difusión en directo IP).
G-10	**integración**: La tecnología del puente DRM y sus procesos deben ser compatibles con otras normas industriales como DOCSIS (Recs. UIT-T J.112/122), IPCablecom (Recomendaciones UIT-T de la serie J.16.x y 17.x) e IPCable2Home (Recomendaciones UIT-T de la serie J.19.x).
G-11	**especificación abierta**: La especificación del puente DRM deberá permitir la interoperabilidad entre equipos de distintos fabricantes.
G-12	**factibilidad económica**: Los costos de aplicar, mantener, validar y aplicar las reglas de cumplimiento de las tecnologías y procesos del puente DRM deberán ajustarse a modelos económicos factibles.
G-13	**gestión dinámica**: La información utilizada para proteger al contenido deberá ser gestionable y configurable de manera dinámica.
G-14	**renovabilidad**: El software de seguridad del puente DRM deberá ser renovable.
G-15	**funcionamiento en caso de avería**: La distribución de contenido controlado y no controlado a la red doméstica será asegurada en caso de avería del acceso al sistema de acceso condicional.
G-16	**contenido no protegido**: El puente DRM no deberá afectar a la utilización del contenido no protegido.
G-17	**extensión de la protección del contenido**: La protección del contenido deberá aplicarse, a todas las transmisiones de vídeo de la red doméstica según lo establecido en las reglas DRM.
G-18	**extensión de las reglas DRM**: El DRM conlleva un amplio conjunto de reglas (copia, reproducción, tiempo de visualización, etc.) que deben ser gestionadas por el STB y abarcar a los elementos subsiguientes.

G-19	**autenticación del cliente**: Todos los elementos de la red doméstica que participen en la transmisión y/o consumo del contenido de vídeo admitirán la autenticación.
G-20	**criptación**: Se proporcionará criptación del contenido para las transmisiones de vídeo dentro de la red doméstica.
G-21	**revocación del dispositivo**: Se permitirá denegar el acceso al contenido a un dispositivo en concreto, incluso si en algún momento éste ha sido un elemento de red válido del puente DRM.

5.5 Antecedentes

Cuando se proporciona contenido protegido a través de una red de distribución segura, es fundamental utilizar una tecnología que impida la copia o redistribución no autorizadas del contenido. Además, el dispositivo mismo debe ser robusto y resistente para garantizar la seguridad. Esta Recomendación detalla los requisitos de la tecnología de protección del contenido así como de robustez y cumplimiento de los dispositivos que manejan la protección del contenido. Estos requisitos de robustez y de tecnología se han definido desde la perspectiva de un dispositivo receptor del consumidor (es decir, un adaptador multimedia) que recibe el contenido de un proveedor de servicios de vídeo como parte de una red de distribución de cable que debe proteger un contenido de gran valor. El contenido es criptado en el origen y protegido a lo largo de toda la red de proveedor de servicio. El objetivo de esta Recomendación es garantizar que en las redes domésticas se alcanza un nivel de seguridad comparable, con el fin de encaminar este flujo de contenido a los medios o entornos sucesivos de manera robusta y segura.

Las tecnologías de protección del contenido y de producción digital que permiten al contenido del proveedor de servicios salir de un adaptador multimedia deben garantizar que el proveedor de servicios retiene el control sobre la copia y la redistribución de dicho contenido, aunque éste ya haya pasado del adaptador multimedia a otros dispositivos. Los dispositivos posteriores al adaptador multimedia que contienen productos digitales, DRM o tecnologías de protección del contenido también tienen que cumplir las reglas de robustez y cumplimiento establecidas para el adaptador multimedia en esta Recomendación. Dichas reglas establecidas para el adaptador multimedia controlan todos los ecosistemas subsiguientes.

6 Requisitos de robustez

Los dispositivos que reciben y, posiblemente, distribuyen contenido protegido deben cumplir una serie de requisitos de robustez para garantizar la protección suficiente del contenido. Se sabe que la robustez puede variar dependiendo del contenido que se entrega al dispositivo y es posible que la robustez tenga que variar con el tiempo a medida que cambien la tecnología de seguridad y las formas de piratearla. En esta cláusula se recomienda un conjunto genérico de requisitos de robustez de los dispositivos.

6.1 Construcción

6.1.1 Aspectos generales

Los productos deberán satisfacer las reglas de cumplimiento y estarán diseñados y fabricados de manera que efectivamente frustren cualquier intento de modificar dichos productos para violar las reglas.

6.1.2 Destrucción de funciones

Los productos no comprenderán:

i) enchufes, botones, derivadores, cables específicos que puedan ser cortados o equivalentes de software de cualesquiera de los anteriores; o

ii) menús o funciones de servicio (incluidas las funciones de control remoto),

según el caso, que puedan anular el efecto de las tecnologías de protección del contenido, los sistemas de protección analógicos, la protección redundante, las restricciones de entrega, las limitaciones de grabación u otras disposiciones obligatorias de las reglas de cumplimiento, o mediante los cuales el contenido pueda exponerse a una copia no autorizada. A los efectos de esta Recomendación se entenderá por "protección redundante" la aplicación de una tecnología de protección aprobada, siempre que se requiera, al contenido controlado procedente de una red de distribución de vídeo y que ha de ser entregada por el adaptador multimedia, así como la integridad del sistema y los métodos que garantizan dicha aplicación.

6.1.3 Mantenimiento de secretos

Para frustrar todos los intentos de partes no autorizadas de comprometer la seguridad, los productos se diseñarán y fabricarán de manera que impida efectivamente cualquier intento de descubrir o revelar:

i) el número único, de una longitud de bits especificada, asignado a cada adaptador multimedia, o los números utilizados en el proceso de criptación o descriptación del contenido controlado (denominados colectivamente, "claves"); y

ii) los métodos y algoritmos criptográficos utilizados para generar dichas claves.

6.2 Trayectos de contenido controlado

El contenido no se facilitará por dispositivos de salida distintos de los especificados en las reglas de cumplimiento y, dentro de cada producto, el contenido controlado no estará presente en ninguno de los buses accesibles a los usuarios (como se define a continuación) en forma comprimida no criptada. Del mismo modo, en los buses accesibles a los usuarios no se utilizarán claves no criptadas para la criptación y/o descriptación de los datos del producto. Un "bus accesible al usuario" es un bus de datos diseñado para mejoras o acceso para el usuario final, tales como un PCI con zócalos, o que sea accesible de otra manera, tarjetas inteligentes, PCMCIA o Cardbus.

6.3 Métodos para robustecer las funciones

Los productos utilizarán al menos las siguientes técnicas para robustecer las funciones y protecciones que se especifican en esta Recomendación.

6.3.1 Funciones distribuidas

Las partes del producto que realizan la autenticación y descriptación del decodificador MPEG (o similar) estarán diseñadas y fabricadas de la manera correspondiente e integradas, de manera que el contenido controlado de cualquier manera utilizable que fluye entre estas porciones del producto tenga el nivel de protección descrito en 6.3.5 siguiente y no pueda ser interceptado ni copiado.

6.3.2 Software

Toda parte del producto que utilice una parte de la tecnología de protección del contenido en software comprenderá todas las características previstas en 6.1 y 6.2. A los efectos de esta Recomendación, se entiende por "software" la implementación de las funciones relacionadas con los requisitos establecidos por esta Recomendación a través de cualquier código de programa informático formado por instrucciones o datos distintos de los incluidos en el hardware. Estas aplicaciones deberán:

a) Ajustarse 6.1.3 utilizando cualquier método razonable, incluida, aunque no únicamente, la criptación, la ejecución de una porción de la implementación del anillo cero o el modo supervisor y/o la incorporación de una implementación física segura, además de, en cualquier implementación del software, la utilización de técnicas efectivas de ofuscación para disimular o evitar cualquier intento de descubrir los métodos utilizados.

b) Estar diseñadas para realizar la autocomprobación de la integridad de sus componentes, de manera que las modificaciones no autorizadas den como resultado que la implementación no efectúe la función de autenticación y/o descriptación autorizada. A los efectos de esta disposición se entenderá como "modificación" cualquier cambio o perturbación o invasión de las características, o interrupción de algún proceso pertinente de 6.1 y 6.2. Esta disposición requiere, como mínimo, la utilización de un código con verificación por redundancia cíclica criptado además con una clave privada o un algoritmo de troceado seguro.

c) Alcanzar el nivel de protección que se indica en 6.3.5.

d) Estar diseñadas para proporcionar mecanismos de protección contra ataques de software no autorizados.

6.3.3 Hardware

Toda parte del producto que implemente los requisitos de esta Recomendación en el hardware incluirá todas las características indicadas en 6.1 y 6.2. A los efectos de estas reglas de robustez se entenderá por "hardware" un dispositivo físico, incluido un componente, que implemente cualesquiera de los requisitos de protección de contenido que debe cumplir un producto de acuerdo con esta Recomendación y que:

i) no incluye instrucciones o datos distintos de los permanentemente incorporados en dicho dispositivo o componente; o

ii) incluye instrucciones o datos no permanentemente incorporados en dicho dispositivo o componente, cuando tales instrucciones o datos han sido adaptados para éste y no sean accesibles al usuario final a través del mismo.

Estas implementaciones deberán:

a) Ajustarse a 6.1.3 mediante cualquier método razonable, incluidas, aunque no únicamente, las claves incorporadas, los métodos de generación de claves y los algoritmos criptográficos en circuitos de silicio o soportes propios que no puedan leerse normalmente, o cualquier técnica descrita anteriormente para el software.

b) Estar diseñadas de modo que cualquier intento de reprogramar, eliminar o sustituir elementos de hardware que comprometa la seguridad o las características de protección de contenido de la tecnología examinada o del adaptador multimedia, suponga un grave riesgo de dañar el producto de tal forma que ya no pueda recibir, descriptar o decodificar el contenido controlado (por ejemplo, resulta más adecuado un componente soldado que "con zócalos").

c) Alcanzar el nivel de protección que se indica en 6.3.5.

6.3.4 Híbrido

Las interfaces entre el hardware y el software de un producto estarán diseñadas de manera que tengan un nivel de protección similar al que proporcionará puramente hardware o el software, como se describe más arriba.

6.3.5 Nivel de protección

Las funciones de criptación principales (que mantienen la confidencialidad de las claves, los métodos de generación de claves y algoritmos criptográficos, la conformidad con las reglas de cumplimiento y que impiden la copia o la visualización no autorizada del contenido controlado que no ha sido criptado) se aplicarán de acuerdo con los requisitos de "Nivel 2" de FIPS PUB 140-2 "Security Requirements for Cryptographic Modules", y, como mínimo, de tal manera que:

a) no se pueda prever razonablemente que sean neutralizados o soslayados utilizando herramientas o equipos que pueden sostenerse fácilmente a un precio asequible, como destornilladores, derivadores, clips y soldadores ("herramientas fácilmente adquiribles"), o

empleando herramientas electrónicas o software especializados también ampliamente asequibles, tales como lectores y escritores EEPROM, depuradores y decompiladores o herramientas de diseño de software similares ("herramientas especializadas"), distintos de los dispositivos y tecnologías, ya sean de hardware o software, diseñados y disponibles para el fin específico de eludir las tecnologías de protección requeridas ("dispositivos de elusión"); y

b) sólo puedan ser neutralizados o evitados difícilmente utilizando herramientas o equipos profesionales (excluidos los dispositivos de elusión y las herramientas y equipos profesionales disponibles únicamente mediante un acuerdo de no divulgación), como analizadores lógicos, sistemas de desensamblaje de chips, o emuladores de circuito u otras herramientas, equipos, métodos o técnicas no incluidas en la definición de herramientas ampliamente disponibles o herramientas especializadas del punto a) *supra*.

7 Reglas de cumplimiento

7.1 Introducción

Para que el proveedor de servicio de vídeo acepte conectar a su red un dispositivo destinado a recibir contenido protegido, este dispositivo deberá de cumplir varias condiciones.

7.2 Salidas generadas

7.2.1 Consideraciones generales

Ningún producto transmitirá contenido o lo pasará a través del servicio a otro dispositivo de salida, excepto en la medida en que lo permita esta Recomendación. A los efectos de la misma, se considerará que el dispositivo de salida efectuará, aunque no únicamente, las transmisiones a cualquier dispositivo interno de copia, grabación o almacenamiento, pero no las transmisiones internas no permanentes o transitorias que de no ser así satisfarían estas reglas de cumplimiento y las de robustez.

7.2.2 Salidas analógicas de definición normalizada

Los productos que generan salidas analógicas de definición normalizada sólo transmitirán o pasarán el contenido recibido a través del servicio si el contenido está adecuadamente protegido de conformidad con normas nacionales o regionales apropiadas para la protección contra copias del contenido analógico.

7.2.3 Salidas analógicas de alta definición

Los productos podrán restringir, cuando así lo requiera el bit CIT CCI, a una imagen constreñida la resolución del contenido de alta definición a la salida a través de una conexión capaz de transmitir contenido en forma analógica de alta definición. El producto incluirá una o más salidas digitales aprobadas. Todos los dispositivos generarán y propagarán señales CGMS-A para todas las salidas analógicas de alta definición, pero no tendrán que respetar el activador CGMS-A, a menos que así lo exija la legislación o el reglamento correspondientes.

7.2.4 Salidas digitales

Los dispositivos con salidas digitales sólo transmitirán o pasarán el contenido a través del servicio o en la medida en que lo permita esta Recomendación. En el apéndice I se enumeran las tecnologías cuya conformidad con esta Recomendación se ha comprobado.

7.2.5 No interferencia con la filigrana

Los productos y componentes NO DEBERÁN cubrir, oscurecer o interferir la filigrana de consenso del contenido controlado que ha sido descriptado.

7.3 Copia, grabación y almacenamiento de contenido controlado

7.3.1 Consideraciones generales

Los dispositivos que incluyen, sin limitación, otros productos, con capacidades inherentes o integradas de copia, grabación o almacenamiento, no copiarán, grabarán o almacenarán contenido controlado, excepto en la medida en que lo permita esta cláusula.

7.3.2 Almacenamiento en memoria tampón para visualización

Los productos podrán almacenar contenido controlado temporalmente con el único propósito de permitir su inmediata visualización, siempre y cuando:

a) dicho almacenamiento no persista una vez visualizado el contenido; y

b) los datos no estén almacenados de manera que puedan ser copiados, grabados o almacenados con otros fines.

7.3.3 Copia única

Los productos no copiarán, grabarán o almacenarán contenido controlado cuyos bits EMI indiquen que ya ha sido copiado pero no ha de ser copiado de nuevo ("copia única"), excepto en la medida en que lo permitan 7.3.2 ó 7.3.5.2.

7.3.4 Copia prohibida

Los productos que incluyan, sin limitación, un dispositivo con capacidades integradas de grabación, como los denominados "videograbador personal", no deberán copiar contenido controlado cuyos bits EMI indiquen que no ha de ser copiado nunca ("copia prohibida siempre"), excepto en la medida en que lo permita 7.3.2 o según lo siguiente:

Tales dispositivos podrán almacenar internamente este tipo de contenido, incluso para una pausa en el programa, si el contenido almacenado está circunscrito de manera segura al producto que realiza la grabación, de manera que no pueda ser extraído del mismo y no pueda ser grabado posterior ni temporalmente dentro del mismo dispositivo sin inutilizarlo, siempre y cuando el dispositivo sea conforme a los requisitos de robustez especificados para evitar la elusión de las restricciones. Cuando se almacene internamente este contenido, incluso para hacer una pausa, como indica la presente cláusula, éste se almacenará de manera que esté criptado y su seguridad no sea inferior a la norma de criptación avanzada (AES, *advanced encryption standard*) de 128 bits.

Los productos se diseñarán y fabricarán para marcar el contenido almacenado o inutilizarlo después de un determinado periodo de tiempo, de trama en trama, de minuto en minuto de megabyte en megabyte.

7.3.5 Copia de una generación

7.3.5.1 Función de copia

Los productos podrán realizar una copia de contenido controlado cuyos bits EMI indiquen que puede copiarse para una generación ("copia de una generación"), tal y como se prevé en 7.3.2 ó 7.3.4, o siempre y cuando dicha copia:

a) esté aleatorizada, criptada o circunscrita únicamente a ese dispositivo, utilizando en cada caso un tipo de protección contra copias identificado mediante una enmienda a 7.3.5, de haberla, y

b) esté marcada para que no pueda copiarse posteriormente ("copia única") de la manera identificada mediante enmienda a 7.3.5, de haberla, y que efectivamente impida que sean hechas otras copias por dispositivos capaces de recibir una transmisión de los datos así marcados a través de las salidas indicadas en 7.2.4. De no haber enmiendas a 7.3.5, no se harán copias de este contenido controlado salvo las permitidas por 7.3.2 ó 7.3.4, y en la medida en que lo permita 7.3.5.2.

7.3.5.2 Función de traslado

Un producto que realice una copia de contenido marcado en los bits CCI como "copia de una generación", de conformidad con 7.3.5, podrá trasladar dicho contenido a un medio de grabación extraíble o a un dispositivo de grabación externo únicamente cuando:

a) el dispositivo de grabación externo indique que está autorizado a realizar esta función de traslado, de conformidad con los requisitos de esta cláusula, y a copiar el contenido controlado, de acuerdo con los requisitos de 7.3.5;

b) dicho contenido controlado esté marcado para transmisión por el producto de origen como "copia de una generación";

c) el contenido controlado se transmita por una salida protegida de conformidad con 7.2.2, 7.2.3 ó 7.2.4;

d) antes de completar el traslado, la grabación del producto de origen sea inutilizada y el contenido controlado trasladado sea marcado "copia única";

e) el dispositivo al que es trasladado el medio de grabación extraíble no pueda transmitir el contenido controlado, o excepto por salidas autorizadas por estas reglas de cumplimiento; y

f) la copia sea almacenada:

   i) utilizando un protocolo de criptación aprobado por una enmienda a estas reglas, que asocie unívocamente dicha copia con un solo dispositivo, de manera que no pueda ser reproducida en otro dispositivo o, de si está almacenada en un medio extraíble, que no puedan hacerse más copias utilizables, o

   ii) aplicando los métodos indicados en 7.3.5.1.

La implementación actual sólo permite un traslado. Están en estudio otros medios de control del contenido que podrán aplicarse cuando se defina la próxima generación de sistemas DRM.

8 Control de cambios

Todo cambio material o sustancial de la tecnología debe ser reevaluado utilizando los criterios y procesos descritos en esta Recomendación. Estos cambios materiales sustanciales incluyen, aunque no únicamente:

1) la correspondencia con un nuevo transporte o medios;

2) los cambios en la codificación o el tratamiento del contenido;

3) los cambios que puedan perjudicar la integridad o seguridad de la tecnología;

4) los cambios en el método criptográfico utilizado (salvo cuando el algoritmo no se modifica y sólo se alarga la clave);

5) los cambios en el alcance de la redistribución; y

6) cualquier cambio fundamental en la naturaleza de la tecnología.

Anexo A

Información de control de copia

El proveedor de servicio de vídeo transmite la información de control de copia (CCI, *copy control information*) a través del canal de datos para informar al adaptador multimedia el nivel de protección de copia que se requiere. La CCI es enviada en claro al adaptador multimedia, pero la integridad de la información se mantiene autenticando la CCI utilizando un protocolo simple. Este proceso se repite para cada elemento subsiguiente al adaptador multimedia.

El campo CCI de un byte contiene información que el adaptador multimedia y los elementos subsiguientes utilizan para controlar la copia del contenido. Dos bits EMI controlan la copia de las salidas digitales en el adaptador multimedia, dos bits APS controlan la copia en salidas analógicas, un bit se dedica al activador de imagen constreñida y tres bits quedan reservados.

A.1 Cambio de canal

Cuando se cambia de canal, el adaptador multimedia tratará todo el contenido aleatorizado CP como si los bits EMI estuviesen puestos a "copia prohibida siempre", pero no aplicará la constricción de imagen hasta que se reciba un nuevo mensaje CCI. El adaptador multimedia empezará inmediatamente a utilizar los valores de la CCI cuando los reciba del proveedor de servicio de vídeo. Si no se recibe un nuevo mensaje CCI en el plazo de 10 segundos, el adaptador multimedia aplicará la constricción de imagen como si el bit CIT estuviese puesto a uno. El cambio del canal no originará un refresco de claves.

A.2 Definición de la CCI

La CCI es un campo de un byte, 8 bits, que va del adaptador multimedia a los elementos de red subsiguientes. Cinco de los 8 bits están definidos, y los tres bits restantes se reservan. Los bits reservados se pondrán a cero, como se muestra en el cuadro A.1. Los elementos subsiguientes utilizarán los valores de bit reservados recibidos del adaptador multimedia únicamente para ejecutar el protocolo de túnel autenticado que se describe a continuación. El adaptador multimedia ignorará los valores de los bits reservados.

Cuadro A.1/J.197 – Asignación de bits CCI

Bits CCI #	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**
El proveedor de servicio de vídeo lo configura a	0	0	0	CIT	APS1	APS0	EMI1	EMI0
El adaptador multimedia lo interpreta como	reservado	reservado	reservado	CIT	APS1	APS0	EMI1	EMI0

A.3 Bits de control de copia digital – EMI

Los dos bits menos significativos del byte CCI son los bits EMI, encargados de controlar los permisos de copia digital. Los bits EMI serán enviados a los puertos de salida digital del adaptador multimedia para controlar las copias que se hacen de estos productos. Los bits EMI están definidos en el cuadro A.2.

Cuadro A.2/J.197 – Valores EMI y contenido

Valor EMI	Permiso de copia digital	Tipo de contenido
00	Copia no restringida	No "valor alto"
01	No se permiten más copias	Valor alto
10	Se permite la copia de una generación	Valor alto
11	Copia prohibida	Valor alto

A.4 Sistema de protección analógico (APS, *analogue protection system*)

Los bits 3 y 2 de la CCI, como se muestra en el cuadro A.1, son los bits 1 y 0 APS, respectivamente. El adaptador multimedia utilizará los bits APS para controlar la codificación de protección de copia de las salidas compuestas analógicas, como se indica en el cuadro A.3.

Cuadro A.3/J.197 – Definición de los valores APS

APS	Descripción
00	Codificación de protección de copia desactivada
01	Proceso AGC activado, ráfaga alterna desactivada
10	Proceso AGC activado, ráfaga alterna de 2 líneas activada
11	Proceso AGC activado, ráfaga alterna de 4 líneas activada

A.5 Activador de imagen constreñida (CIT, *constrained image trigger*)

El bit 4 de la CCI que se muestra en el cuadro A.4 es el bit CIT. El adaptador multimedia utilizará este bit para controlar la constricción de imagen de las salidas analógicas de alta definición.

Cuadro A.4/J.197 – Valores CIT y aplicación

Valor CIT	Aplicación de constricción de imagen
0	No se requiere constricción de imagen
1	Constricción de imagen requerida

A.6 Protocolo de túnel autenticado

El adaptador multimedia calcula el valor CCI_auth utilizando el valor CCI recibido y lo compara con el valor CCI_auth recibido el proveedor de servicio de vídeo. Toda inequivalencia genera un error y el adaptador multimedia pone los bits EMI a 11 y aplica la constricción de imagen, como si el valor fuese igual a 1.

Anexo B

Lista de control de robustez

Antes de lanzar al mercado cualquier producto, el implementador de la tecnología debe realizar pruebas y análisis para garantizar la robustez de la implementación. La siguiente lista del control de robustez puede ser útil para efectuar las pruebas que determinan algunos aspectos importantes de la robustez. Dado que la lista de control de robustez no abarca todos los elementos necesarios para fabricación de un producto, se aconseja vivamente al realizador de la tecnología que evalúe muy cuidadosamente tanto los procedimientos de prueba como la conformidad de sus productos.

Cuestiones generales de implementación

1) ¿Se ha diseñado y fabricado el producto de manera que no incluya enchufes, botones, derivadores o software equivalentes a los anteriores, ni pistas específicas que puedan ser descubiertas y que permitan neutralizar las tecnologías de protección de contenido, los sistemas de protección analógicos, las restricciones de visualización, las limitaciones de grabación u otras disposiciones obligatorias de las reglas de cumplimiento, o que expongan el contenido controlado a copias no autorizadas?

2) ¿Se ha diseñado y fabricado el producto de manera que no comprenda menús de servicio ni funciones (funciones de control remoto, enchufes, cajas de control u otros medios) que puedan interceptar el flujo de contenido controlado o exponerlo a copias no autorizadas?

3) ¿Se ha diseñado y fabricado el producto de manera que no comprenda menús de servicio ni funciones (tales como funciones de control remoto, enchufes, cajas de control u otros medios que puedan desactivar los sistemas de protección analógicos, las restricciones de visualización, las limitaciones de grabación u otras disposiciones obligatorias de las reglas de cumplimiento?

4) ¿Tiene el producto menús de servicio, funciones de servicio o características de servicio que puedan alterar o exponer el flujo de contenido controlado dentro del dispositivo?

   En caso afirmativo, describa estos menús, funciones o características de servicio y las medidas que se adoptan para garantizar que dichas herramientas no se utilicen para exponer o encaminar erróneamente el contenido controlado.

5) ¿Tiene el dispositivo menús de servicio, funciones de servicio o características de servicio que puedan desactivar los sistemas de protección analógica, las restricciones de visualización, las limitaciones a la grabación u otras disposiciones de las reglas de cumplimiento?

   En caso afirmativo, describa estos menús, funciones o características de servicio y las medidas que se adoptan para garantizar que dichas herramientas no se utilizan para destruir las características de criptación del producto (incluida la observación de las reglas de cumplimiento).

6) ¿Tiene el dispositivo buses accesibles al usuario (como se define en 6.2 de las reglas de robustez)?

   De ser así, ¿se transporta el contenido controlado por este bus?

   En caso afirmativo:

   identifique y describa el bus y si el contenido controlado está comprimido o no. Si los datos están comprimidos, explique detalladamente cómo y por qué medios los datos son recriptados como se exige en 6.2 de las reglas de robustez.

7) Explique detalladamente cómo el producto protege la confidencialidad de todas las claves.

8) Explique detalladamente cómo el producto protege la confidencialidad de los algoritmos criptográficos confidenciales que utiliza.

9) Si el producto transfiere contenido controlado de una parte a otra del mismo, ya sea entre módulos de software, circuitos integrados o de otro tipo, o una combinación de éstos, explique cómo se han diseñado, asociado o integrado las partes del producto que realizan la autenticación y descriptación y el decodificador MPEG (o similar) de manera que el contenido controlado esté asegurado contra cualquier posible intercepción o copia, como exige 6.3.1 de las reglas de robustez.

10) ¿Tiene el hardware funciones de protección del contenido?

En caso afirmativo, responda a las siguientes cuestiones relativas al hardware.

11) ¿Se realizan en el software funciones de protección del contenido?

En caso afirmativo, responda a las siguientes las cuestiones relativas al software.

Cuestiones relativas a la implementación del software

12) Describa el método utilizado para almacenar en el producto todas las claves de manera segura.

13) ¿Resulta imposible descubrir las claves en imágenes binarias de los dispositivos de memoria permanente utilizando la instrucción grep o equivalente?

14) Describa el método utilizado en el producto para ocultar los algoritmos criptográficos confidenciales y las claves utilizadas en el software.

15) Describa el método utilizado en el producto para crear valores criptográficos intermedios (por ejemplo, valores creados durante el proceso de autenticación entre módulos o dispositivos dentro de un producto) y mantenerlos protegidos.

16) Describa el método utilizado para impedir el uso de herramientas de descontaminación o descompilación fácilmente adquiribles, (por ejemplo, Softice) para descompilar o examinar directamente el funcionamiento de las funciones de protección de contenido aplicadas en el software.

17) Describa el método utilizado por el producto para autocomprobar la integridad de sus componentes, en caso de que las modificaciones causen un fallo de la función de autorización o decriptación, como se indica en 6.3.2b de las reglas de robustez. Describa qué ocurre cuando se viola la integridad.

18) Para garantizar que se realiza la autocomprobación de la integridad, realice una prueba para estar seguro de que un ejecutable no funcionará si se utiliza un editor binario para modificar un byte aleatorio de la imagen ejecutable que contiene funciones de protección del contenido, y describa el método y los resultados de dicha prueba.

Cuestiones relativas a la implementación del hardware

19) Describa el método utilizado en el producto para almacenar las claves de manera segura y cómo se mantiene su confidencialidad.

20) ¿Resulta imposible descubrir las claves en imágenes binarias de los dispositivos de memoria permanente utilizando la instrucción grep o equivalente?

21) Describa cómo se han implementado en el producto los algoritmos criptográficos confidenciales y las claves utilizadas se han incorporado en los circuitos de silicio y soportes privados de manera que no puedan ser leídos.

22) Describa el método aplicado en el producto para crear valores criptográficos intermedios (por ejemplo, valores creados durante el proceso de autenticación entre módulos o dispositivo dentro de un producto) y mantenerlos protegidos.

23) Describa los métodos utilizados para impedir cualquier intento de sustitución, traslado o alteración de elementos o módulos del hardware utilizados para implementar las funciones de protección del contenido.

24) En el producto, la eliminación o sustitución de elementos o módulos del hardware que comprometerían las características de protección del producto (incluidas las reglas de cumplimiento y de robustez) ¿dañarían el producto incapacitándolo para recibir, decriptar o decodificar contenido controlado?

Apéndice I

Salidas digitales

Resultará necesario probar la conformidad de las salidas digitales con los requisitos establecidos en la presente Recomendación. A este respecto han sido probadas las salidas digitales consignadas en la siguiente lista, que se presenta con fines informativos. Se espera que en el futuro otros productos se adapten a los requisitos aquí expuestos.

I.1 Cable Television Laboratories ha probado el siguiente producto y ha determinado su conformidad con esta Recomendación:

- **1394 con DTCP**. El producto puede transmitir contenido controlado a una salida en formato digital por interfaces IEEE 1394, siempre y cuando el producto esté protegido por un DTCP. El producto debe soportar la "autenticación plena" DTCP y además la "autenticación restringida" DTCP. De así requerirlo la licencia correspondiente para DTCP, el contenido que *no* es contenido controlado será extraído a través de la interfaz IEEE 1394 sin protección DTCP.

I.2 Cable Television Laboratories ha probado el siguiente producto y ha determinado conformidad con esta Recomendación:

- **DVI/HDMI con HDCP**. El producto puede transmitir contenido recibido a través del servicio y pasarlo a una salida a través del mismo en formato digital a través de interfaces DVI, incluidas las HDMI, siempre y cuando salida tenga el HDCP activado. El producto deberá pasar todos los SRM HDCP recibidos legalmente a la función HDCP.

Apéndice II

Criterios de examen

Dependiendo del producto o la tecnología específicos de que se trate, los criterios de evaluación serán los siguientes:

II.1 Transporte de vídeo

¿Hay métodos definidos para la traducción y entrega de la CCI desde el adaptador multimedia al entorno o perfil del dispositivo propuesto?

i) *Salidas digitales comprimidas*

- ¿Se utiliza el sistema de compresión digital original en la interfaz o se recomprime la señal?
- En caso de recompresión ¿qué sistema, perfil, resolución y velocidad de datos se requieren?
- Si se preserva la compresión original ¿se envía todo el múltiplex de transporte a través de la interfaz o se limita ésta a trenes monoprograma enviados después de la demultiplexación?
- Si la salida transporta todo el tren de transporte ¿cómo es transportada la información del sistema (por ejemplo, datos OOB)?
- ¿Qué métodos se utilizan para garantizar el flujo ininterrumpido de programas a través de la interfaz, independientemente de la presencia de otro tipo de tráfico en esta interfaz (calidad de servicio)?
- ¿Cuál es el caudal de datos mínimo garantizado en la interfaz?
- ¿Qué métodos se utilizan para la entrega, decodificación o visualización de los datos de subtitulado codificado digital y analógico, la calificación moral del contenido y los mensajes del sistema de alerta de emergencia en banda?
- ¿Cómo se preserva sin interrupción los sistemas de programación analógica en esta interfaz?

ii) *Salidas digitales no comprimidas*

- ¿Cuál es el caudal de datos mínimo garantizado en la interfaz?
- ¿Cómo se preservan sin interrupción los servicios de programación analógica en esta interfaz?
- ¿Qué métodos se utilizan para la entrega, decodificación o visualización de datos de subtitulado codificado digital y analógico, la calificación moral del contenido y los mensajes del sistema de alerta de emergencia en banda?

II.2 Interfaces de seguridad

- ¿Cómo se utiliza la seguridad en el transporte de vídeo y cómo se asocia éste con los perfiles de protección del contenido y los métodos para autenticar y proteger los perfiles de protección de contenido?
- ¿Qué métodos de generación, protección e intercambio de clave se utilizan?
- ¿Hay zonas evidentes de presentación del contenido en claro?

II.3 Puntos débiles y vulnerables del sistema

- ¿Puede ser neutralizada la tecnología en algún punto?
- ¿Cuáles son las protecciones más susceptibles de ser atacadas?
- ¿Dónde se efectuarán los ataques de piratería y con cuáles recursos?

- ¿Cuáles son los posibles puntos débiles/amenazas y cuál es la relación entre seguridad y costos aplicados?

II.4 Efectividad de la tecnología propuesta

- ¿Se protege adecuadamente la tecnología propuesta al contenido que pasa por el medio digital, o que se graba o almacena de manera segura para una reproducción posterior?
- ¿Cuál es el alcance de la redistribución del contenido? ¿La tecnología digital o DRM protegen efectivamente el contenido contra la redistribución no autorizada mediante un control de ubicación u otro tipo de restricciones geográficas o de usuario?

II.5 Procesamiento de seguridad

- ¿Están protegidas las claves y secretos contra la lectura y escritura durante los cálculos criptográficos?
- ¿Están protegidos en el diseño del sistema la CCI, la constricción de imagen y otro tipo de controles?

II.6 Revocación y renovación de claves

- ¿Cuenta el producto con un método de revocación de claves del sistema?
- ¿Cuenta el dispositivo con un método de renovación de claves del sistema?
- ¿Qué criterios y procesos se utilizan para la revocación y la renovación? ¿Quiénes participan en el proceso?
- ¿Cuál es el tamaño mínimo y máximo del mensaje con capacidad de renovación del sistema (SRM, *system renewability message*) y en qué formato se presenta?
- ¿Cómo suele entregarse generalmente el SRM? Desde el punto de vista operativo y de la infraestructura ¿qué repercusiones tendría el mecanismo de revocación/renovación en la red de proveedor de servicio de vídeo (incluida la inversión de capital y las mejoras de equipos y de la red que puedan necesitarse)? ¿Qué debe hacer un proveedor de servicio de vídeo para adoptar los mecanismos de revocación/renovación propuestos?

II.7 Nuevos algoritmos

- ¿Cuál es la resistencia relativa del algoritmo?
- ¿Cuál es la resistencia relativa de la autenticación con respecto a otras tecnologías?

II.8 Preservación de la integridad del servicio

- ¿Interfiere el producto/tecnología propuestos con el cumplimiento por parte del adaptador multimedia de otras obligaciones en materia de licencias o pruebas? ¿Requiere la salida digital propuesta la conmutación a la fuente analógica o el traspaso a la alta definición?
- ¿Proporciona el producto una manera de preservar las aplicaciones de servicio y la navegación del proveedor de servicios?
- ¿Interfiere el producto/tecnología propuestos con otros dispositivos e interfaces comercializados?
- ¿Plantea el producto/tecnología propuestos problemas de interoperabilidad con otros dispositivos e interfaces comercializados?
- ¿Puede funcionar la interfaz propuesta con los productos de otros fabricantes o se trata de un sistema privado o exclusivo?
- ¿Está la interoperabilidad definida por normas industriales (indíquese cuáles) o licencias, o ambas?
- ¿Necesita la tecnología una prueba de conformidad para garantizar la interoperabilidad?

II.9 Condiciones de la concesión de licencias

- Las condiciones de la concesión de licencias deben conformarse con las prácticas de la UIT y a los requisitos nacionales.

II.10 Repercusión general en la red de distribución de vídeo

- ¿Desde el punto de vista operacional y de infraestructura ¿qué repercusiones tendría la tecnología propuesta en la red de distribución de vídeo (incluidas la inversión en capital o las mejoras de la red que puedan necesitarse)?
- ¿Qué debe hacer un proveedor de servicio de vídeo para adoptar la tecnología propuesta?

Apéndice III

Documentación de elementos para el análisis de tecnologías

Las tecnologías que abarcan el proceso de evaluación recomendado incluyen las interfaces digitales protegidas, la grabación, almacenamiento y reproducción seguros de contenido, así como la gestión de derechos digitales. Las medidas de seguridad específicas utilizadas por estas tecnologías pueden variar. Además, cada una de ellas puede emplear mecanismos de transporte y protocolos que requieran determinadas limitaciones o restricciones de aplicación. En este apéndice se identifican varios elementos cruciales que deben ser comunes a todas las tecnologías analizadas, pero no se trata de una lista exhaustiva que excluye otro tipo de información que pueda resultar necesaria para evaluar plenamente una tecnología concreta. En la documentación presentada no se deberá omitir ni falsear las especificaciones de material, hechos u otros detalles necesarios para realizar un análisis completo y exacto de la tecnología.

Las tecnologías examinadas pueden incorporar elementos mixtos de tecnologías de interfaces digitales protegidas, grabación y almacenamiento seguros de contenido, y gestión de derechos digitales. En las siguientes cláusulas se esbozan los elementos que se recomienda presentar para hacer un análisis cabal de las tecnologías.

III.1 Condiciones de la concesión de licencias

Las condiciones de la concesión de licencias deben adaptarse a las prácticas de la UIT y a los requisitos nacionales.

Nota sobre las reglas de robustez y cumplimiento – Los dispositivos subsiguientes al adaptador multimedia que contienen una tecnología de salida digital, DRM o de protección del contenido deberán también satisfacer las reglas de robustez y cumplimiento establecidas para el adaptador multimedia en esta Recomendación. Estas reglas controlan todo el ecosistema subsiguiente. Por tanto, las reglas de robustez y cumplimiento de las licencias de tecnología de los fabricantes no deberán contradecir las reglas de robustez y cumplimiento que se detallan en la presente Recomendación.

III.2 Aspectos generales de seguridad

La especificación y documentación sobre seguridad debe incluir una introducción e información sobre la seguridad que incluya:

1) Un resumen general de la arquitectura de seguridad, sus componentes (por ejemplo, servidor de empaquetado, servidor de licencias, cliente, etc.), sus funciones e interfaces clave; requisitos de conectividad para los productos/seguridad.
2) Un diagrama de bloques detallado de la arquitectura de seguridad que identifiquen los componentes clave y las interfaces necesarias para la implementación del sistema de extremo a extremo, incluido el receptor y otros elementos de medios (PC, almacenamiento, visualización, etc.).
3) Este resumen general también deberá identificar claramente las opciones de transporte de vídeo, cuando existan alternativas. Por ejemplo, los algoritmos de cifrado de transporte de vídeo (AES, 3-DES, etc.) y los algoritmos de intercambio de claves (Diffie-Hellman, RSA, etc.).
4) Una descripción detallada de la correspondencia entre las reglas o licencias de protección de contenido del adaptador multimedia y la tecnología de protección del contenido propuesta que se incorporará en los dispositivos "subsiguientes", indicando específicamente cómo se mantiene la seguridad en general y la protección del contenido en todo el ecosistema de distribución.

III.3 Transporte de vídeo

La especificación de seguridad debe de incluir detalles relativos al método de transporte de vídeo y especificar cómo la información de control de copia (CCI) presentada por el adaptador multimedia se traduce en el entorno/perfil propuesto. Esta especificación debe asimismo detallar cómo está asociado el transporte de vídeo con los perfiles de protección de contenido y a los métodos para autenticar y proteger los perfiles de protección de contenido.

Además, deberá proporcionarse especificaciones u otras descripciones técnicas de manera que expliquen plenamente cómo los productos digitales propuestos soportan uno o más protocolos de transporte de vídeo capaces de proporcionar todos los servicios de audio-vídeo definidos[1] asociados con el adaptador multimedia sin interrumpir, impedir o menoscabar la prestación de dichos servicios en el dispositivo de visualización. Estos servicios deberán incluir, aunque no únicamente, la presentación, decodificación y visualización de datos de subtítulos codificados digitales y analógicos, la calificación moral del contenido y los mensajes del sistema de alerta de emergencia.

Deberá examinarse la tecnología de cada mecanismo de transporte y protocolo correspondiente a la tecnología de protección del contenido. Estos análisis se harán para cada transporte o para cada medio. Si una tecnología en concreto cumple todos los criterios que aquí se enumeran, no deberá considerarse que ha obtenido la "aprobación general" para cualquier transporte o protocolo.

III.4 Perfiles de protección del contenido

La especificación de seguridad debe incluir detalles relativos al formato y utilización de los perfiles de protección de contenido con firma digital utilizados en el sistema. La especificación de seguridad debe definir igualmente la estructura y opciones que se emplean en ese sistema y toda la mensajería y señalización que necesita su implementación.

III.5 Algoritmos de intercambio de claves

La especificación de seguridad debe incluir detalles relativos a la autenticación de los dispositivos receptores, los dispositivos de almacenamiento y todos aquellos conectados a éstos. La especificación de seguridad debe incluir asimismo los métodos de autenticación del servidor de licencias, el servidor de empaquetado y el cliente. Todas las claves de sesión intercambiadas y protocolos criptográficos utilizados deberán estar bien definidos para poder realizar un examen completo. Podrán emplearse también alternativas no criptadas pero deberán explicarse muy detalladamente.

III.6 Interfaces de seguridad

La especificación debe incluir detalles que definan completamente las interfaces de seguridad de todo el sistema y la creación y protección de claves simétricas y asimétricas. Han de definirse también detalladamente los componentes de seguridad implementados en el hardware y el software para poder analizar las interfaces de seguridad.

III.7 Procesamiento de seguridad

La especificación debe incluir detalles que demuestren cómo se protegen las claves y secretos contra la lectura y escritura durante los cálculos criptográficos y cómo la CCI, la constricción de imagen y otros parámetros están protegidos en todo el sistema.

---

[1] Véase, por ejemplo, ANSI/SCTE 40-2004; sección 8.1.

III.8 Gestión de certificados

La especificación debe incluir detalles que definan completamente la utilización de certificados, los métodos de protección de claves privadas, los métodos de revocación y cómo los certificados se relacionan con el contenido y los servidores de empaquetado/licencias. Se incluirán también detalles sobre la instalación, firma, encadenamiento a la raíz, estructura general, validación de seguridad y protección contra el clonaje de certificados.

III.9 Revocación/renovación de claves

La especificación debe incluir detalles sobre cómo funcionan los sistemas de revocación y de renovación de claves.

III.10 Posibles puntos débiles/vulnerables

La especificación debe incluir exámenes o análisis de amenazas previsibles para considerar los posibles puntos débiles/peligros así como su relación con los costos aplicados. También se proporcionarán análisis de seguridad independientes. Según convenga, podrá aplicarse al análisis restricciones de divulgación.

III.11 Uso comercial

Los datos presentados deben incluir todos los usos comerciales conocidos del producto o tecnología propuestos, así como los efectos conocidos sobre el funcionamiento de los dispositivos y la interoperabilidad. El solicitante deberá proporcionar una lista de usuarios (implementadores) y proveedores (propietarios, diseñadores de contenido, etc.), e identificar toda sus relaciones comerciales con los propietarios del contenido.

III.12 Información de contacto

El documento presentado debe incluir los nombres e información de contacto de los especialistas en seguridad y otras personas que puedan ser consultadas sobre cuestiones relativas a la información presentada.

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 multimedios
Serie I	Red digital de servicios integrados
Serie J	**Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedios**
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	Calidad de transmisión telefónica, instalaciones telefónicas y redes locales
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

Impreso en Suiza
Ginebra, 2006