UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T J.95

(09/99)

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

SERIE J: TRANSMISIONES DE SEÑALES RADIOFÓNICAS, DE TELEVISIÓN Y DE OTRAS SEÑALES MULTIMEDIOS

Servicios digitales auxiliares para transmisiones de televisión

---

Sistema de protección de la propiedad intelectual contra la copia de contenidos transmitidos a través de sistemas de televisión por cable

Recomendación UIT-T J.95

(Anteriormente Recomendación del CCITT)

RECOMENDACIONES UIT-T DE LA SERIE J

TRANSMISIONES DE SEÑALES RADIOFÓNICAS, DE TELEVISIÓN Y DE OTRAS SEÑALES MULTIMEDIOS

Recomendaciones generales	J.1–J.9
Especificaciones generales para transmisiones radiofónicas analógicas	J.10–J.19
Características de funcionamiento de los circuitos radiofónicos	J.20–J.29
Equipos y líneas utilizados para circuitos radiofónicos analógicos	J.30–J.39
Codificadores digitales para señales radiofónicas analógicas	J.40–J.49
Transmisión digital de señales radiofónicas	J.50–J.59
Circuitos para transmisiones de televisión analógica	J.60–J.69
Transmisiones de televisión analógica por líneas metálicas e interconexión con radioenlaces	J.70–J.79
Transmisión digital de señales de televisión	J.80–J.89
Servicios digitales auxiliares para transmisiones de televisión	**J.90–J.99**
Requisitos operacionales y métodos para transmisiones de televisión	J.100–J.109
Sistemas interactivos para distribución de televisión digital	J.110–J.129
Transporte de señales MPEG-2 por redes de transmisión de paquetes	J.130–J.139
Mediciones de la calidad de servicio	J.140–J.149
Distribución de televisión digital por redes locales de abonados	J.150–J.159

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

RECOMENDACIÓN UIT-T J.95

SISTEMA DE PROTECCIÓN DE LA PROPIEDAD INTELECTUAL CONTRA LA COPIA DE CONTENIDOS TRANSMITIDOS A TRAVÉS DE SISTEMAS DE TELEVISIÓN POR CABLE

Resumen

En esta Recomendación se describen los requisitos necesarios de un sistema para proteger los derechos de propiedad intelectual (IPR, *intellectual property rights*) de las entidades encargadas de la programación de televisión, contra la copia, duplicación y distribución ilegales de productos creativos de su propiedad. El sistema aquí descrito contiene aspectos que prohíben el acceso a trenes de datos MPEG criptados a personas no autorizadas. Además, se presentan técnicas destinadas a insertar una "filigrana" en señales de televisión para identificación de usuario y autorización de copias.

El material que se presenta en esta Recomendación contiene descripciones generales y el examen de distintos criterios técnicos específicos encaminados a la protección contra la copia de contenidos.

Orígenes

La Recomendación UIT-T J.95 ha sido preparada por la Comisión de Estudio 9 (1997-2000) del UIT-T y fue aprobada por el procedimiento de la Resolución N.° 1 de la CMNT el 16 de septiembre de 1999.

Palabras clave

Acceso condicional, grabación vídeo, MPEG, seguridad, televisión, televisión digital.

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 Conferencia Mundial de Normalización de las Telecomunicaciones (CMNT), 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 N.° 1 de la CMNT.

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.

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 J.95

SISTEMA DE PROTECCIÓN DE LA PROPIEDAD INTELECTUAL CONTRA LA COPIA DE CONTENIDOS TRANSMITIDOS A TRAVÉS DE SISTEMAS DE TELEVISIÓN POR CABLE

(Ginebra, 1999)

1 Introducción y antecedentes

La grabación y duplicación ilegales de la propiedad intelectual de televisión ha dado como resultado un vasto comercio ilícito en todo el mundo y ha costado a los titulares de derechos de propiedad intelectual una pérdida de beneficios significativa. La aparición de la televisión MPEG digital acentúa este problema porque la duplicación de las grabaciones digitales puede mantener su calidad original durante muchas generaciones en tanto que la fidelidad de las grabaciones analógicas se reduce en generaciones sucesivas que, de alguna manera, son inutilizables. En sistemas en que la señal digital MPEG se recibe y convierte en una señal analógica equivalente para que pueda visualizarse en un receptor de televisión sólo analógico, la calidad de esa señal analógica puede también ser objeto de piratería y, por consiguiente, debe ser protegida.

Para ayudar a cumplir estos objetivos, se han desarrollado métodos determinados a ocultar las marcas digitales en los productos de televisión digital que gozan de los derechos de propiedad intelectual de tal manera que sean indetectables e incorruptibles. Este proceso, llamado filigrana (*watermarking*), está basado en la ciencia de la criptografía aunque no se trata verdaderamente de un método criptográfico; contiene la identidad del titular de los derechos de propiedad intelectual y las reglas impuestas por ese titular con respecto a las copias de ese producto (es decir, ninguna copia, una copia para uso personal, o sin límite de copias).

Además de la filigrana, la protección contra las copias requiere que las señales de televisión digital MPEG no codificadas, o sus equivalentes analógicas, no atraviesen las líneas de señales fuera de las fronteras físicas del equipo electrónico situado en el hogar del consumidor. Para cumplir este requisito, es necesario un sistema de aleatorización secundaria para cubrir temporalmente estas señales durante su distribución en el edificio, ya sea en formato digital o analógico. Se propone un sistema criptográfico para cubrir las señales MPEG digitales y, para cubrir las señales analógicas, un sistema comercial que ya existe y que varía rápidamente la temporización.

Para que puedan iniciarse acciones judiciales contra toda persona que viole estas contramedidas, es conveniente que los procesos estén patentados y protegidos por procedimientos de concesión de licencias. No obstante, estas licencias deben concederse cuidadosamente para que no ocasionen discriminaciones y/o desventajas innecesarias a las empresas que producen estos sistemas de protección contra copias.

2 Ámbito de aplicación

En esta Recomendación se describen técnicas criptográficas para proteger el acceso a señales de televisión digitales MPEG no codificadas y, además, un proceso, conocido como filigrana, que marca indeleblemente la propiedad intelectual de su titular y los requisitos de éste con la relación a la autorización de copias. Un sistema de protección contra copias satisfactorio sobre el privilegio jurídico del titular de los derechos de propiedad intelectual para controlar la distribución del producto protegido.

Deben tenerse en cuenta los criterios relativos a la protección contra la copia de contenidos descritos en la presente Recomendación a fin de utilizarlos en otras aplicaciones que requieren una protección similar, tales como la radiodifusión por aire, la distribución de programas grabados (por ejemplo, por DVD), etc.

3 Referencias (a título informativo)

– 1394 Trade Association, Specification for AV/C Digital Interface Command Set.

– Digital Transmission Protection License Agreement, Development and Evaluation License, Digital Transmission Licensing Authority.

– Digital Transmission Licensing Administrator, 5C Digital Transmission Content Protection Specification, Volume 1, Version 0.91.

– Digital Transmission Licensing Administrator, *5C Digital Transmission Content Protection Specification*, Volume 2, Version 0.90.

– CEI 61883-1 (1998), *Digital Interface for Consumer audio/video Equipment – Digital Interface – Part 1: General*.

– IEEE Std 1394-1995, IEEE's *Standard for a High Performance Serial Bus*.

– IEEE P1363, *Editorial Contribution to Standard for Public Key Cryptography*, Preliminary Draft, P1363/D3 (11 de mayo de 1998).

– National Institute of Standards and Technology (NIST), *Secure Hash Standard (SHS)*, FIPS Publication 180-1, 17 de abril de 1995.

– Toshiba Corporation, *Efficient Implementation of an Elliptic Curve Cryptosystem* (disponible en http://www.dtcp.com).

4 Definiciones

En esta Recomendación se definen los términos siguientes.

4.1 **algoritmo**: Proceso matemático que puede utilizarse para la aleatorización y desaleatorización de un tren de datos.

4.2 **autenticación**: Proceso destinado a permitir al sistema comprobar con certeza la identificación de una parte.

4.3 **codificación de autorización**: Palabra digital que describe la personalidad de la capacidad de acceso al servicio de la unidad decodificador de abonado.

NOTA – Esta palabra de código que se basa en el acceso al servicio autorizado por el sistema de facturación, determina qué claves se distribuyen a cada cliente, y se necesitan en el decodificador de abonado para autorizar la desaleatorización de algún programa específico.

4.4 **sistema de acceso condicional (CA, *conditional access*)**: El sistema completo para asegurar que los servicios por cable son accesibles sólo a quienes están autorizados a recibirlos, y que el pedido de tales servicios no está sujeto a modificación o rechazo.

4.5 **criptoanálisis**: Ciencia de la recuperación del texto en lenguaje claro de un mensaje sin acceso a la clave (a la clave electrónica en los sistemas criptográficos electrónicos).

4.6 **ciclo de trabajo criptográfico**: Máxima capacidad segura de un proceso criptográfico, basada en el número total de bits que pueden ser criptados con seguridad antes de que resulte aconsejable cambiar la clave.

4.7 **desaleatorización**: Proceso de invertir la función de aleatorización (véase "aleatorización") para obtener imágenes, sonido y servicios de datos utilizables.

4.8 **clave electrónica**: Término que designa las señales de datos que se utilizan para controlar el proceso de desaleatorización en los decodificadores de abonado.

NOTA – Hay al menos tres tipos de claves electrónicas: las utilizadas para los trenes de señales de televisión, las utilizadas para proteger las operaciones del sistema de control, y las utilizadas para la distribución de claves electrónicas en el sistema de cable. Véase también "codificación de autorización", que también es efectivamente una clave.

4.9 **criptación**: Proceso de aleatorización de las señales para evitar el acceso no autorizado.

4.10 **servicio de conexión ordinaria permanente**: Servicio por abono que está siempre disponible para los abonados durante las horas de funcionamiento del sistema de distribución.

NOTA – En cambio, otros servicios, tales como filmes de pago por visión, sólo están disponibles durante un periodo de tiempo determinado.

4.11 **computador central**: Dispositivo con funcionalidad generalizada al que pueden conectarse módulos que contienen funcionalidad especializada.

4.12 **integridad**: Aptitud de una función para resistir su usurpación para uso no autorizado, o su modificación para conseguir resultados no autorizados.

4.13 **resistencia a la intrusión**: Aptitud de un objeto de soporte lógico para denegar el acceso físico, eléctrico, o por irradiación a funcionalidad interna por partes no autorizadas.

4.14 **módulo**: Pequeño dispositivo, que no funciona por sí mismo, destinado a realizar tareas especializadas en asociación con un computador central.

4.15 **no rechazo**: Proceso por el cual el emisor de un mensaje (por ejemplo, una petición de pago por visión) no puede negar haber enviado el mensaje.

4.16 troceo unidireccional: Algoritmo o proceso matemático por el que un mensaje de longitud variable se transforma en una palabra digital de longitud fija, de manera que es muy difícil calcular el mensaje original a partir de la palabra, y también muy difícil encontrar un segundo mensaje con la misma palabra.

4.17 pago por visión: Sistema de pago por el que el abonado puede pagar un programa individual o un periodo de tiempo especificado.

4.18 piratería: Acción de conseguir acceso no autorizado a programas, normalmente con el fin de revender dicho acceso para su recepción no autorizada.

4.19 criptografía de claves públicas: Técnica criptográfica basada en un algoritmo de dos claves, privada y pública, por el que un mensaje es criptado con la clave pública, pero puede ser descriptado con la clave privada. También conocido como sistema de clave privada-pública (PPK, *private-public key*).

NOTA – El conocimiento de la clave pública no revela la clave privada.

Ejemplo: La parte A diseñaría dicha clave privada y pública, y enviaría la clave pública abiertamente a todos quienes pudieran desear comunicar con la parte A, pero mantendría secreta la clave privada. Entonces, en tanto que cualquiera que tenga la clave privada puede criptar un mensaje para la parte A, sólo la parte A con la clave privada puede descriptar los mensajes.

4.20 aleatorización: Proceso de utilizar una función de criptación para hacer inutilizables las señales de televisión y de datos a las partes no autorizadas.

4.21 firma segura: Proceso matemático por el cual puede determinarse el origen y la integridad de un mensaje transmitido.

NOTA – Si se utiliza un sistema de firma segura, el originador no puede negar haber enviado el mensaje, y el receptor puede determinar si el mensaje ha sido modificado.

4.22 tren de transporte: Un tren de transporte MPEG-2.

5 Filigranas de propiedad intelectual de televisión digital

5.1 Antecedentes y requisitos funcionales

Uno de los requisitos básicos para definir la propiedad intelectual es incorporar de alguna manera una marca que la identifique como tal y establezca la identidad del titular de esa propiedad. En los materiales impresos, se introduce el símbolo de marca registrada universalmente reconocido y una nota al pie de página que menciona al titular de la propiedad. Suele ir seguida por una declaración que define la posición del titular con respecto a la utilización de ese producto, por ejemplo, "Prohibida la reproducción excepto para usos no comerciales". En todas las monedas se utilizan diversos métodos para distinguir entre moneda legal y falsificación.

Los productores de televisión desean marcar su propiedad intelectual de alguna manera que defina esa propiedad y las limitaciones que imponen a su utilización. A continuación figuran los requisitos de un sistema de protección por filigranas:

1) Debe enunciarse claramente la identidad del titular del derecho de propiedad intelectual aplicado a un producto determinado y las autorizaciones para la copia del mismo.

2) El marcado del producto de televisión debe estar presente en todas, o virtualmente todas, las tramas.

3) En la presentación del producto artístico, el marcado debe ser indetectable, incluso en forma subliminal.

4) Debe ser virtualmente imposible la modificación no autorizada del marcado sin que el deterioro del producto original lo sitúe por debajo de la fidelidad comercial.

5) El marcado del producto debe ser accesible en lectura automática.

6) La tasa de errores positivos falsos debe ser insignificante durante largos periodos (por ejemplo, un segundo en 30 años).

7) Los datos insertados deben ser detectables mediante adaptaciones que modifiquen el formato de la pantalla o durante las funciones de zoom.

8) Deben poder coexistir sin interferencia múltiples filigranas.

La forma en que se ofrecen estas funciones en un sistema de filigranas ha generado una cantidad considerable de criterios, dos de los cuales figuran en los apéndices I y II.

5.2 Consecuencias del método de diseño

Estos requisitos funcionales sugieren que la forma más eficaz de marcar la propiedad intelectual de televisión es utilizar algunos aspectos de la ciencia de la criptología. Al emplear técnicas distintas, el titular de la propiedad intelectual puede estar sumamente seguro de que el marcado es difícil de detectar, virtualmente imposible de modificar, puede insertarse fácilmente en cada trama, en caso necesario, y puede ser leído por el equipo electrónico de origen y el del consumidor convenientemente autorizados. El método criptográfico ocasiona en la imagen visual original un aumento muy leve del umbral mínimo de ruido de la señal. No corresponde a esta Recomendación seleccionar una serie de procesos criptográficos comunes ni elegir la forma en que esos algoritmos se implementan en los equipos.

6 Medidas de control de acceso para la protección contra copias

6.1 Antecedentes y requisitos funcionales – Señales analógicas

Las señales analógicas protegidas contra copias que se transportan por circuitos interconectados a las instalaciones del cliente tras haber sido recibidas de un sistema de cable secundario, son enviadas originalmente en formato analógico o bien convertidas del formato digital al analógico en el adaptador multimedios, deben ser protegidas utilizando un sistema o una combinación de sistemas actualmente disponibles para evitar su eventual copiado en un magnetoscopio convencional. No necesitan esta protección las señales que no gozan de una protección contra las copias, o las que se han convertido para utilizarlas en un aparato de visualización y no están disponibles en formato no codificado fuera del dispositivo de visualización.

6.2 Antecedentes y requisitos funcionales – Señales digitales MPEG

El objetivo fundamental de esta Recomendación es asegurar que no se pueda acceder con facilidad a las señales de televisión digitales MPEG no codificadas para efectuar grabaciones no autorizadas. Esto significa que todas las señales MPEG, mientras se transmiten a las instalaciones del cliente por un sistema de cable o a los dispositivos electrónicos del consumidor situadas en dichas instalaciones, deben estar protegidas contra el acceso no autorizado. La ciencia del acceso condicional, que figura en la Recomendación J.93, se aplica a las señales MPEG que se transmiten por el sistema de cable secundario. La protección contra las copias se aplica a las señales transmitidas entre los dispositivos electrónicos del consumidor situados en las instalaciones del mismo.

Para cumplir este requisito, es conveniente un sistema de criptación y descriptación de las señales MPEG que se transportan por los circuitos interconectados de las instalaciones del cliente. El sistema de criptación seleccionado debe poseer los siguientes atributos:

1) Simplicidad y rentabilidad, a fin de que pueda instalarse en el equipo del consumidor.

2) Capacidad de autorrecuperación en el caso de que se pierda la sincronización criptográfica.

3) Se implementa tanto en el formato módulo interno como en el formato módulo punto de instalación (POD, *point-of-deployment*)

4) Puede ser autorizado o desautorizado desde un punto distante y transmitir su situación al mismo.

5) Ningún fallo voluntario o involuntario producido en un punto determinado puede averiar el sistema MPEG no codificado transmitido por los circuitos de interconexión.

6.3 Funcionalidad del centro de autorización

Con el sistema criptográfico antes descrito utilizado para proteger las señales transmitidas por los circuitos de interconexión, es necesario un sistema externo que cumpla las siguientes funciones:

1) Autorizar y suministrar claves para los equipos electrónicos del consumidor recientemente instalados.

2) Desautorizar los equipos electrónicos del consumidor ilegales o robados.

3) Ayudar en los modos de recuperación tras los fallos.

4) Suministrar un sistema de seguridad y de control del funcionamiento.

5) Proporcionar información a los propietarios afectados de materiales protegidos contra copias afectados.

6) Coordinar acciones previstas con las cabeceras del sistema de cable.

Para que su funcionamiento sea eficaz, es necesario que los centros de autorización tengan como mínimo un campo de acción múltiple. Pueden cubrir una región o prestar servicios a poblaciones más pequeñas. Necesitarán un enlace de comunicaciones bidireccional en la vivienda de cada consumidor y para cada aparato apto para la funcionalidad protección contra copias. Las funciones de autorización y resolución de fallos exigirán un acceso virtual en tiempo real a los equipos electrónicos del consumidor. Por motivos de coste y eficiencia esta comunicación debe transmitirse por nuevas redes sin recargar indebidamente las operaciones existentes.

Además, serán necesarios trayectos de comunicación entre varios centros de autorización, con canales de retorno para los proveedores de televisión que pagan la protección contra las copias de sus materiales. No se conoce todavía la naturaleza de estos canales de retorno y será necesario continuar los trabajos para poder definirlos.

7 Factores relativos a la inclusión de la funcionalidad protección contra copias en la televisión por cable y en los equipos electrónicos del consumidor

7.1 Filigranas

Dado que la filigrana se instala en el vídeo original en el momento de su fabricación, y que sólo puede ser leída por ciertos equipos del consumidor en sus puntos de uso, la red de transmisión, *per se*, no es responsable de esta funcionalidad.

7.2 Control de acceso para la protección contra copias

Para los sistemas de transmisión por cable la mayor repercusión se producirá en la protección de las señales transmitidas por los circuitos de interconexión en las instalaciones del cliente. La facilidad de autorización debe estar en condiciones de autenticar cada pieza del equipo de procesamiento de vídeo situado en la vivienda del usuario final así como todos los demás aparatos pertinentes del consumidor a través de los cuales serán procesadas las señales de televisión MPEG, y de criptar y descriptar dichas señales, cuando sea necesario. Toda fuente o aparato de grabación que forme parte del equipo del consumidor, como los vídeo discos digitales (DVD), los magnetoscopios (VCR) o los adaptadores multimedios, también deben poder leer la señal de filigranas para determinar si el titular tiene la intención de que se haga una nueva grabación. Estas funciones deben normalizarse porque los medios provienen de distintos fabricantes y de distintos sectores de la industria.

7.3 Otras repercusiones

El sistema descrito requiere canales de control dúplex completo en tiempo real entre los centros de control regionales y todos los equipos interesados de esa región. Hasta ahora no se conocen los medios que se van a utilizar ni los protocolos necesarios, cuya definición será el resultado de nuevos trabajos sobre el tema.

Apéndice I

Propuesta de la UER sobre un sistema de protección de la propiedad intelectual contra la copia de programas transmitidos a través de sistemas de televisión por cable secundarios

A fin de garantizar el respeto de los derechos de propiedad intelectual aplicados a los programas de televisión, la propuesta de la UER se centra en la afirmación de que debe ser posible identificar cualquier objeto digital y vincular esa identificación a una base de datos que conserve todos los datos necesarios sobre los derechos de propiedad intelectual correspondientes. Conciliando esta propuesta con los avances de la tecnología actual con respecto a la protección de los medios digitales, la UER formula las siguientes observaciones y propone el modelo de referencia adjunto (véase la figura I.1).

1) Ningún objeto digital, por ejemplo una secuencia de televisión, debe estar disponible al público sin la protección adecuada incorporada dentro del objeto mismo; lo ideal sería que, a largo plazo, no se pudiera vender en el mercado digital ningún objeto no identificado.

2) Como los titulares de derechos de propiedad intelectual necesitan distintos tipos de información, es al parecer imposible satisfacer todas las peticiones con un marcado directo de los datos correspondientes; por consiguiente, debe utilizarse un identificador únicamente como enlace a una base de datos garantizada que contenga toda la información necesaria.

3) Cualquier parte pequeña de una secuencia que pueda ser aislada y utilizada nuevamente debe llevar el identificador que es un enlace a la base de datos de los derechos de propiedad intelectual.

4) Se ha determinado que el identificador único más corto tiene 64 bits, lo que permite un número de combinaciones de 16 cifras decimales hasta una combinación de menor cantidad de letras y cifras. Un ejemplo del proceso de identificación con 64 bits es el de ISO 10918-4 (identificación de imágenes fijas); ISBN, ISSN, ISRC, ISMN, ISWC o ISAN pueden también utilizarse en el mismo espacio de 64 bits.

5) El identificador de 64 bits debe marcarse dentro del objeto de tal forma que sea invisible y no pueda eliminarse ni modificarse sin producir efectos visibles.

6) El contenido del identificador de 64 bits debe ser concedido por una autoridad de registro y puede llamarse "placa de licencia" o LP (*license plate*).

7) El identificador puede utilizarse para vincular una base de datos que contiene la información de los derechos de propiedad intelectual (filigranas de creación) o la información de distribución (filigranas de distribución).

8) Por lo tanto, pueden insertarse dos filigranas dentro del tren de datos, con referencia a las referencias 5) a 8). Para marcar todas las tramas, si se utiliza MPEG-2, se marcará cada trama I.

9) Como un identificador no puede contener todos los datos debido a su tamaño pequeño, sólo puede utilizarse como enlace. El tipo de enlace puede ser un hiperenlace entre el objeto y la base de datos que contiene la información de interés.

10) Para garantizar la filigrana, se propone duplicar los contenidos (64 bits) en un rótulo presente en el fichero de tren de bits. A tal efecto, se ha reservado un espacio de 64 bits en MPEG-2.

11) Debe recomendarse también la utilización de un espacio de 64 bits dividido en dos mitades, los primeros 32 bits definen la autoridad de registro (REGAUT, *registration authority*) de origen que concede el identificador, y los últimos 32 bits se podrán utilizar para denominar el objeto, con una capacidad de 4 mil millones de identificadores.

12) Un identificador de este tipo actualmente utilizado es IMLP (Placa de licencia multimedios ISO para identificación de imágenes fijas) cuya estructura es la siguiente:

    /indicativo de país ISO (16 bits)/identidad REGAUT (16 bits)/número de registro (32 bits)/

13) Las tablas para obtener la dirección URL de REGAUT a partir de su identidad estarán disponibles en un sitio de la Web para permitir el enlace automático entre el objeto y los datos relativos a sus derechos de propiedad intelectual.

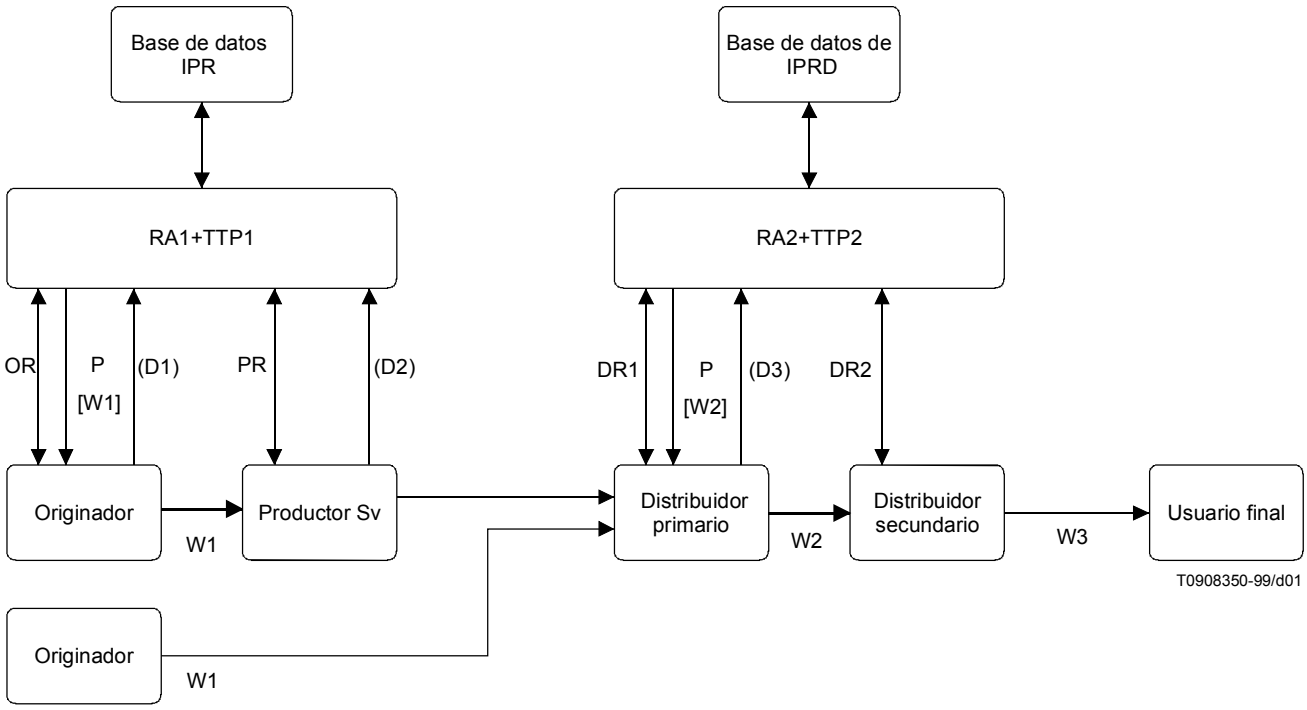
14) La verificación del tren de bits dará como resultado la lectura de las dos filigranas, y la capacidad de establecer un enlace automático a las bases de datos donde se guarda la información necesaria.

15) El contenido de la filigrana puede utilizarse con fines jurídicos, en especial si es concedido por una autoridad de registro.

16) El contenido de la filigrana se ofrece contra entrega de la presentación de información presuntamente fiable que la REGAUT guarda en lugar seguro.

17) Cada REGAUT puede definir su proceso de registro y debe garantizar la autenticidad de los datos registrados.

18) El control de acceso a los datos de interés corresponde a la gestión de la REGAUT.



OR	Registro originador	D2	Declaración del trabajo realizado (preparación o ensamblado)
P	Protección (contenido de la filigrana)	DR1	Registro de distribuidor (primario)
D1	Declaración (del trabajo relacionado con W1)	D3	Declaración (de lo que se ha distribuido)
PR	Sv Registro del productor	DR2	Registro del distribuidor (secundario)

Figura I.1/J.95 – Modelo de referencia IPR

Apéndice II

Propuesta sobre filigranas Galaxy

Resumen

Mediante la tecnología de filigrana Galaxy propuesta se insertan 8 bits de datos como filigrana digital transparente en vídeo digital no comprimido. Esta filigrana puede detectarse en el dominio de banda de base y en el dominio MPEG-2 y se denomina marca primaria. Los primeros dos bits de la marca primaria representan la información de control de copias (CCI, *copy control information*) como, por ejemplo, "ninguna copia", "una generación de copia" y "no más copias". El detector utiliza el algoritmo de detección de periodo adaptativo para detectar la marca primaria con una relación de errores positivos falsos determinada previamente. Se puede lograr una detección fiable hasta de un contenido muy degradado sin exceder la relación positiva falsa determinada previamente, que se fija a menos de 10^{-12}, valor establecido como compromiso de la extensión del tiempo de detección.

Galaxy propone que se inserte otra filigrana transparente en los dispositivos de grabación digitales para que sirva como identificación del material copiado. Esto se llama inserción de filigrana. Mediante esta tecnología se inserta otra filigrana transparente sin causar ninguna perturbación a la marca primaria previamente incorporada. La inserción de esta marca de copia puede tener lugar tanto en el dominio de banda de base como en el dominio MPEG-2 y la detección de la misma puede también efectuarse en ambos dominios. Se añade marca de copia al contenido "una generación de copia" para que cambie al estado "no más copias" a efectos del control de generación de copias. Cabe indicar que las marcas de copia insertadas en ambos dominios son idénticas.

La tecnología de filigrana Galaxy es compatible e intercambiable entre el dominio MPEG y el dominio de banda de base y, por consiguiente, los fabricantes de dispositivos tienen mucha libertad para elegir dónde colocar el detector de filigrana y el insertador de marca de copia. La decisión final se debe adoptar teniendo en cuenta los aspectos relativos a la seguridad y al coste de la implementación.

Galaxy completó el diseño y programa con el prototipo de una tecnología de filigrana unificada y ha realizado numerosas pruebas de capacidad de supervivencia y la transparencia para hacer más estable el algoritmo. Más adelante, se informa sobre las pruebas de capacidad de supervivencia realizadas. Esta tecnología ha alcanzado un grado suficiente de madurez para ser sometida a una prueba de verificación inmediata por CPAC. En este apéndice se describe también cómo el valor de umbral en la detección puede controlar la tasa de errores positivos falsos.

Finalmente, se describe la tecnología insertada automática y el sistema de insertación seguro y de fácil funcionamiento. El sistema de insertación en tiempo real es un sistema DSP basado en PC.

II.1 Arquitectura del sistema

II.1.1 Panorama general de la utilización de la filigrana

En el sistema de filigrana Galaxy, la marca primaria transporta 8 bits de información y los primeros dos bits se utilizan para la información de control de copias (CCI). La utilización de otros bits está fuera del alcance del presente apéndice pero deben ser aceptados por las partes de ICPAC pertinentes, incluidos los bits de arranque APS. Además, la tecnología Galaxy puede insertar y detectar otra filigrana independiente, llamada marca de copia, que coexiste con la filigrana primaria y se utiliza para cambiar la interpretación de la CCI de marca primaria para el control de generación de copias.

Al utilizarse CCI, se suele dar por entendido en DHSG lo siguiente.

1) El contenido distribuido por medios electrónicos, como la televisión digital, puede estar marcado (1,1), (1,0), (0,0) o puede no estar marcado.

2) Todos los contenidos distribuidos por medios DVD-ROM están marcados (1,1), (0,0) o pueden no estar marcados.

3) Todos los contenidos distribuidos por medios DVD-ROM marcados (1,1) son aleatorizados por CSS.

4) Los dispositivos de reproducción DVD son capaces de distinguir entre medios de grabación y medios de lectura solamente.

5) El estado "no más copias" sólo está permitido en los medios de grabación.

A continuación figuran ejemplos de control de grabación y control de reproducción. La tecnología de filigrana Galaxy tiene la capacidad y flexibilidad necesarias para abordar todos los posibles escenarios de implementación. La implementación real debe examinarse junto con el diseño del sistema de protección global contra copias.

Control de grabación y de generación de copias

La información de control de copias (CCI) detectada que se enumera en el cuadro II.1 puede utilizarse para activar la acción de los dispositivos de grabación digitales, como por ejemplo los dispositivos DVD. En este cuadro, CFP representa el aviso de licitación efectuado por DHSG en mayo de 1997.

Cuadro II.1/J.95 – Definición de CCI y respuesta solicitada para el control de copias en dispositivos de grabación

CCI detectada	Definición en CFP	Respuesta del dispositivo de grabación
1,1	Ninguna copia	Impedir copia
1,0	Generación de copia	Autorizar copia y añadir marca de copia
1,0 con marca de copia	No más copias	Impedir copia
0,0 o sin marca	Copia autorizada	Autorizar copia

Control de reproducción

La CCI detectada y la información de los medios de reproducción puede utilizarse para activar las acciones de lectores DVD autorizados. En el cuadro II.2 figura un ejemplo de definición. Suponiendo que la filigrana no sea detectada cuando está presente la aleatorización CSS, se asigna la respuesta "evitar reproducción" como copia no autorizada cuando se detecta CCI = (1,1) en medios DVD-ROM sin aleatorización CSS.

Cuadro II.2/J.95 – Definición de CCI y respuesta para el control de reproducción en lectores DVD

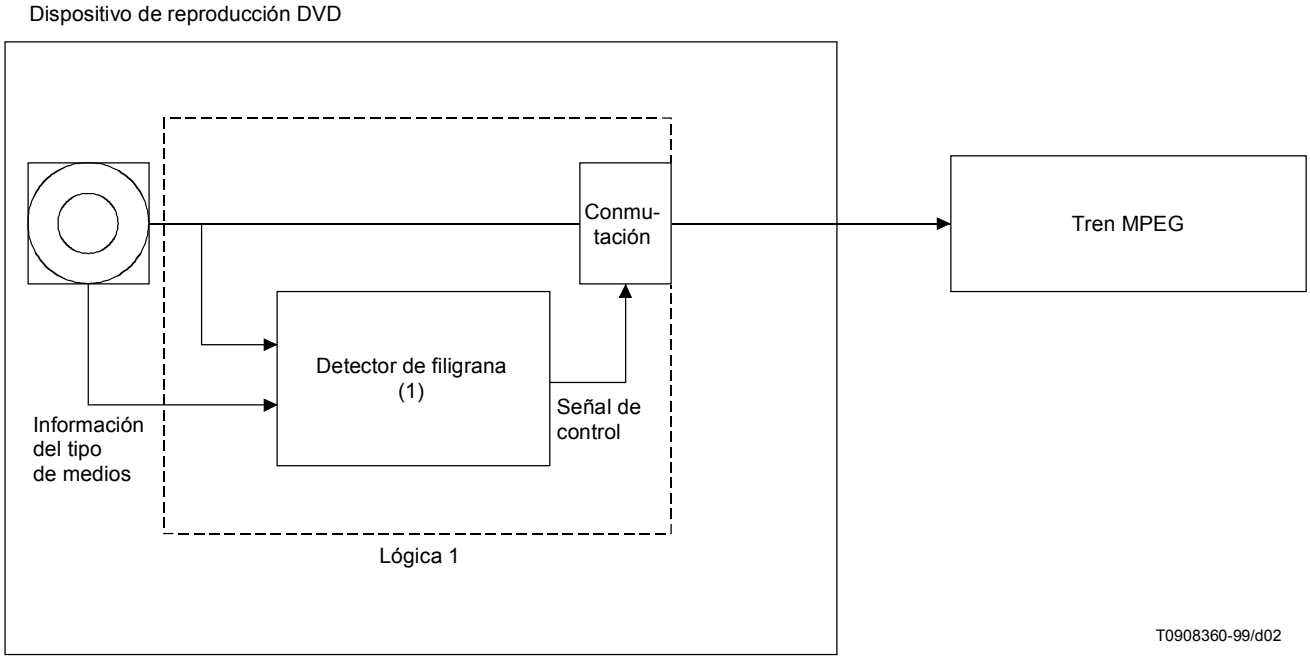
Tipo de medio detectado	CCI detectada	Respuesta del dispositivo
Lectura solamente	1,1	Impedir reproducción*
	1,0	Impedir reproducción
	1,0 con marca de copia	Impedir reproducción
	0,0 o sin marca	Autorizar reproducción
Grabable y regrabable	1,1	Impedir reproducción
	1,0	Impedir reproducción
	1,0 con marca de copia	Autorizar reproducción
	0,0 o sin marca	Autorizar reproducción

II.1.2 Configuración del sistema

En esta subcláusula se describe la configuración del sistema DVD con respecto al control de reproducción y al control de grabación utilizando tres tipos de lógicas relativas a la detección de filigrana/inserción de marca de copia, que constituyen los elementos fundamentales del diseño total del sistema de control de copias. La marca primaria puede detectarse en el dominio MPEG-2 y en el dominio de banda de base y la marca de copia puede insertarse y detectarse en ambos dominios. Gracias a esta característica, los fabricantes de dispositivos tienen gran margen de libertad para decidir dónde colocar el detector de filigrana y el insertador de marca de copia.

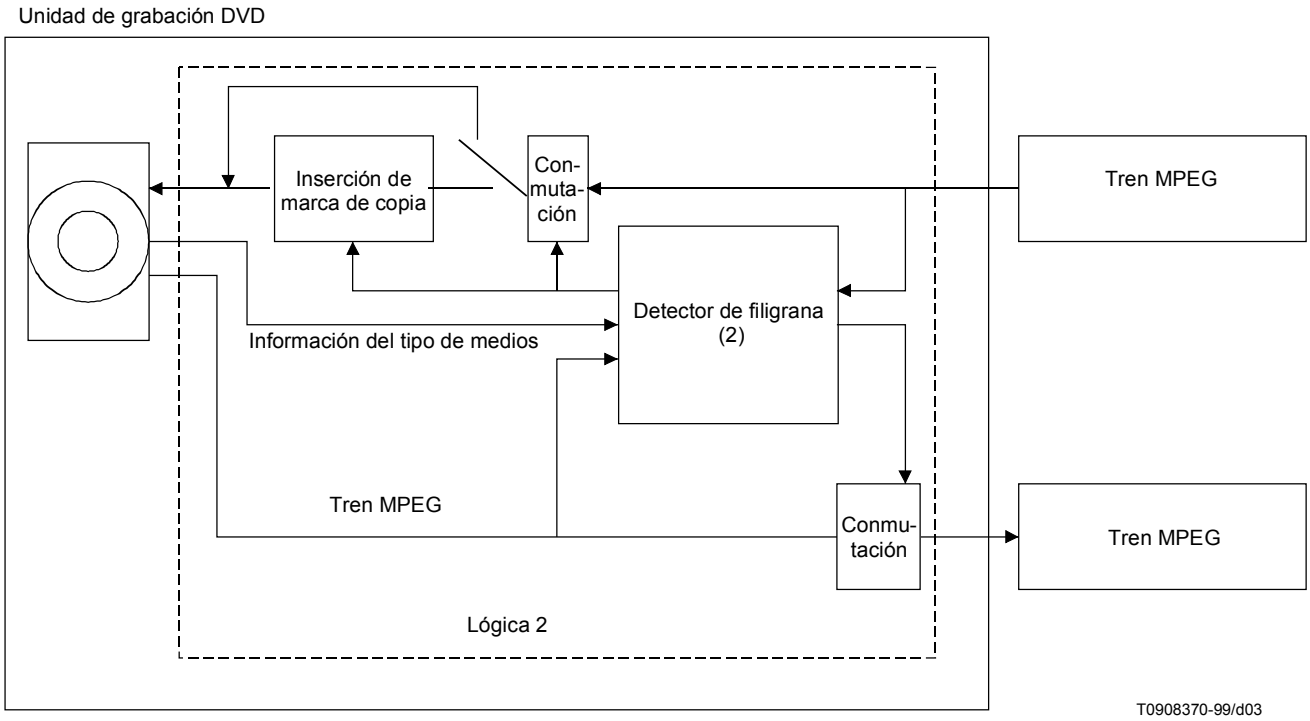
Lógica 1: Control de reproducción DVD

Esta lógica detecta directamente la marca primaria y la marca de copia a partir de los datos MPEG. La CCI y la marca de copias resultantes se utilizarán con la información del tipo de medios ofrecida por el controlador del dispositivo de reproducción DVD para el control de reproducción, según las acciones definidas en II.1.1. La casilla marcada por la línea de puntos representa el diagrama de bloques de esta lógica.



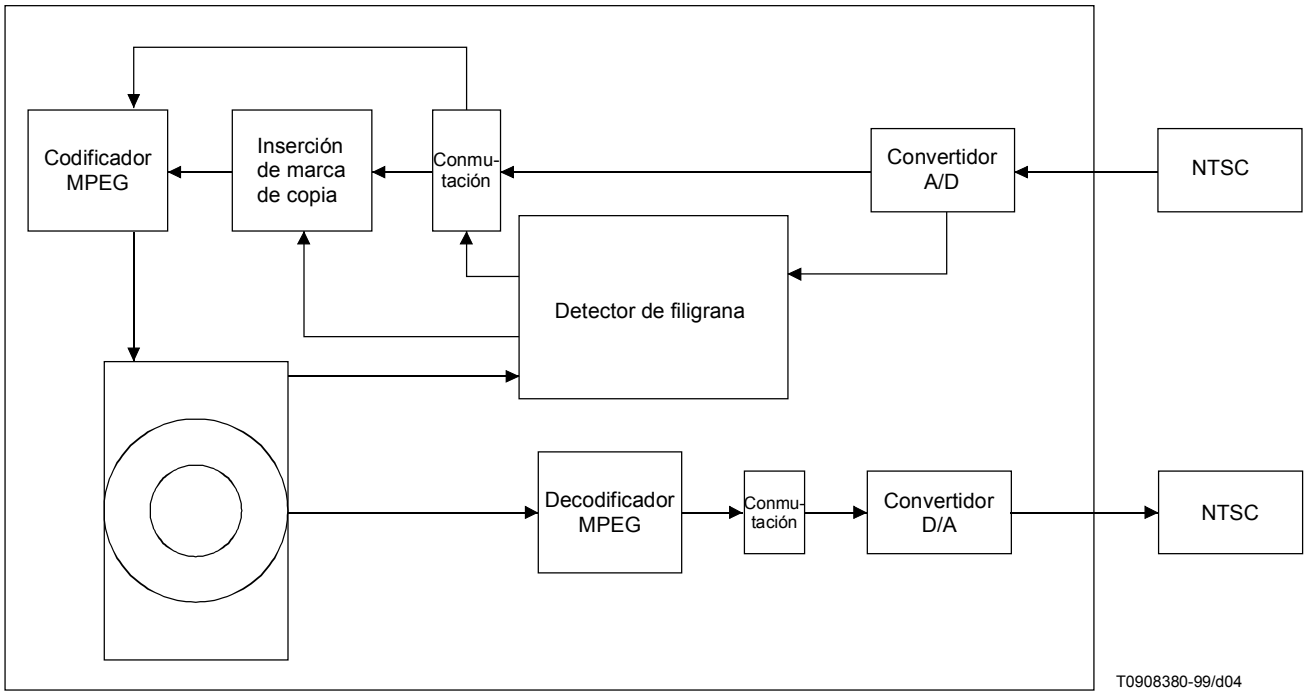
Lógica 2: Control de reproducción DVD, control de copias y de generación de copias

Además del control de reproducción, esta lógica permite el control de grabación y de generación de copias mediante la utilización de la función de inserción de marca de copia y el mismo detector de filigrana de la lógica 1. Para la reproducción es necesaria también la información del tipo de medios. En esta lógica, todas las funciones se realizan directamente para el tren de señales vídeo MPEG y, por lo tanto, puede colocarse en la unidad DVD, en caso necesario. La casilla formada por la línea de puntos representa el diagrama de bloques de la lógica 2.



Lógica 3: Control de copias y control de generación de copias en banda de base

Esta lógica se aplica al control de grabación y al control de generación de copias en dispositivos de grabación con entrada de vídeo en banda de base o magnetoscopios DVD. La funcionalidad es la misma que la descrita para la parte entrada de la lógica 2 con la diferencia de que el tren de señales vídeo previsto es el tren de datos vídeo no comprimido. En la figura siguiente se muestra un ejemplo de implementación con control de reproducción DVD.



II.2 Control de generación de copias

Mediante la tecnología Galaxy puede insertarse otra filigrana transparente llamada marca de copia sin destruir la marca primaria en el dominio de banda de base ni en el dominio MPEG-2 y detectarla también en ambos dominios. La inserción de la marca de copia en el dominio MPEG-2 tiene la finalidad de preservar estrictamente el tamaño del paquete del tren MPEG-2 a fin de cumplir con las restricciones impuestas a la realización del equipo. La presencia de la marca de copia cambiará la interpretación de CCI (1,0) de "una generación de copia" a "no más copias" a efectos del control de generación de copias indicado en los cuadros II.1 y II.2.

Al utilizar el criterio de insertar la marca de copia, el sistema puede soportar completamente tanto la transmisión digital como analógica desde el adaptador multimedios de la base de instalación sin ayuda de los dispositivos existentes en los trayectos de transmisión.

II.3 Madurez técnica

Desde comienzos de 1996 las empresas miembro del proyecto Galaxy están elaborando en forma independiente y conjunta la tecnología de filigrana aplicada a los sistemas vídeo digitales con la finalidad de aplicarla a la protección de los contenidos DVD contra copias. Se ha puesto ya en práctica la lógica de detección por FPGA (red de lógica programable) y la inserción de algoritmos por DSP, y se ha demostrado la inserción y detección en tiempo real en DHSG en 1997 y 1998. En una prueba directa del DHSG efectuada en febrero de 1998 se ha mostrado la gran capacidad de supervivencia de la filigrana y, demostrado la tecnología de remarcado para el control de generación de copias. Galaxy reconoció los conocimientos técnicos de cada miembro y anunció la fusión de las propuestas en febrero de 1999.

La tecnología de filigrana Galaxy ha alcanzado la suficiente madurez para ser sometida a una prueba de verificación inmediata por CPAC. Se han realizado las pruebas de todas las funciones que figuran en el cuadro II.3 con la transparencia, la fiabilidad y la capacidad de supervivencia de la marca primaria (PM, *primary mark*) y la marca de copia (CM, *copy mark*), que abarcan tanto el dominio MPEG como el dominio de banda de base. Se podrá disponer a la brevedad del prototipo de sistema de inserción en tiempo real para un ensayo en estudio aunque el calendario completo del producto depende del calendario de selección definitivo de CPAC.

Cuadro II.3/J.96 – Disponibilidad de funciones requeridas a partir de 1999

		Descripción funcional	Disponibilidad
Inserción de filigrana en vídeo de banda de base	Sistema en estudio	Sistema de inserción de filigrana automático con información completa de 8 bits por campo. Seudoinserción en tiempo real con UIT-R-656 I/O	Sí
Detección PM en dominio MPEG	Lógica 1, 2	Detección directa del tren MPEG en tiempo real	Sí
Detección PM en dominio de banda de base	Lógica 3	Detección tras conversión A/D	Sí
Inserción CM en dominio MPEG	Lógica 2	Inserción CM directa en tren MPEG con mantenimiento del tamaño del paquete MPEG	Sí
Inserción CM en dominio de banda de base	Lógica 3	Inserción CM al vídeo tras conversión A/D	Sí
Detección CM en dominio MPEG	Lógica 1, 2	Detección directa del tren MPEG en tiempo real	Sí
Detección CM en dominio de banda de base	Lógica 3	Detección tras conversión A/D	Sí

II.4 Análisis de cómputo de puertas

En el cuadro II.4 se enumeran los tamaños de puerta estimados de las lógicas 1, 2 y 3 de II.2.

Cuadro II.4/J.95 – Función y resumen del cómputo de puertas de las microplaquetas de detección de filigrana Galaxy

Tipo de lógica	Finalidad	Descripción funcional	Cómputo de puertas	Dispositivos previstos
1	Control de reproducción	Detección de las filigranas marca primaria y marca de copia del tren MPEG	Puertas de 30 k 5 kbyte RAM	Dispositivo de reproducción DVD
2	Control de reproducción Control de grabación Control de generación de copias	Detección de filigranas marca primaria y marca de copia, e inserción de marca de copia en tren MPEG	Puertas de 35 k 5 kbyte RAM	Unidad de grabación DVD
3	Control de reproducción Control de grabación Control de generación de copias	Detección de filigranas marca primaria y marca de copia e inserción de marca de copia, en dominio de banda de base tras conversión A/D	Puertas de 30 k 42 kbyte RAM	Dispositivos de grabación DVD con entrada de vídeo analógica

El tamaño estimado de la puerta puede variar según la arquitectura y la disponibilidad de recursos de los sistemas semiconductores de los dispositivos de grabación y/o de reproducción. El tamaño de puerta de la lógica 3 no incluye una conversión analógica/digital antes del proceso de detección.

Estos tamaños de puerta no representan necesariamente la futura especificación del producto y están sujetos a modificaciones porque los detalles de la especificación de funciones puede cambiar según los nuevos requisitos de CPAC.

II.5 Pruebas de robustez

La prueba para medir la capacidad de supervivencia se efectuó bajo las siguientes condiciones:

- Carga útil de datos: 8 bits (pueden representarse 256 estados arbitrarios).
- Tasa de errores positivos falsos inferior a 10^{-12} en periodo de detección de 10 segundos.

Estas condiciones deben especificarse antes de efectuar cualquier comparación entre distintas tecnologías porque se trata de una relación de equilibrio entre transparencia, carga útil de datos, relación de errores positivos falsos y capacidad de supervivencia de la filigrana.

El algoritmo del periodo de detección adaptable utilizado detectó 8 bits de datos de las videosecuencias de prueba con ventana de detección de un máximo de 20 segundos en ambos dominios (MPEG-2 y banda de base). Se utilizaron 20 secuencias de muestra proporcionadas por DHSG en 1997 y se aplicaron procesos sucesivos de procesamiento vídeo en estudio → compresión MPEG-2 → grabación VHS → recompresión MPEG-2 para simular la degradación prevista en el mundo real. En el cuadro II.5 se enumeran el procesamiento vídeo en estudio y los parámetros de cada proceso. Por regla general, se detectaron 8 bits correctos en un segundo o menos tras la primera compresión MPEG-2 y en el transcurso de 10 segundos en la mayoría de los casos incluso después de una recompresión MPEG-2.

Cuadro II.5/J.95 – Lista de elementos de la prueba de capacidad de supervivencia

Procesamiento vídeo en estudio (DVNR-1000)	Nota
Filtro de contención	
Aumento de abertura	
Reducción de ruido	
Reducción de velocidad (98%)	Caída de una trama cada 50 tramas
Combinación de filigranas (50%)	(prueba de referencia)
Conversión a "formato buzón"	
Conversión a "formato buzón" por desplazamiento	
Desplazamiento espacial aleatorio	Más de 10 desplazamientos cada 20 s
Desplazamiento de tonalidades	Desplazamiento de tonalidades a 30 grados

Compresión MPEG	4-10 Mbit/s, GOP distintos, campo/trama
Grabación VHS	3 DNR, TBC encendido/apagado, etc.
Recompresión MPEG	Codificador en tiempo real CBR, cambio de intervalo GOP

Además de la prueba de simulación, se han efectuado las tres pruebas siguientes de capacidad de supervivencia en entorno real:

1) Compresión MPEG → Transmisión por satélite → Transmisión analógica por cable → Grabación VHS.
2) Compresión MPEG → Transmisión por satélite → Transmisión directa de televisión → Grabación VHS.
3) Inserción de formato HD → Conversión descendente a SD → Conversión analógica → Análisis positivo falso de compresión MPEG.

II.6 Análisis positivo falso

El error positivo falso se produce cuando el detector interpreta que un segmento de vídeo no marcado es un segmento marcado. La tasa de errores positivos falsos debe ser extremadamente baja, por ejemplo de 10^{-12}, porque impide al dispositivo copiar una copia auténtica. La tecnología Galaxy puede controlar la tasa de errores positivos falsos prevista mediante un umbral de detección de filigrana determinado previamente.

Breve descripción del algoritmo

El algoritmo propuesto detecta 8 bits de CCI en cada campo del tren MPEG-2 o del vídeo de banda de base de la forma siguiente. En primer lugar, se calcula la intensidad de filigrana detectada de cada bit sumando los resultados observados de los subbloques asignados en el campo. A continuación se interpretan todos los bits cuando la intensidad de todos ellos excede un valor de umbral previamente determinado. En este caso, ε_B indica una probabilidad de que la intensidad de detección de un bit exceda el umbral. Dado que los valores de detección de los 8 bits son independientes entre sí, la probabilidad de que los 8 bits excedan el umbral en una trama no marcada se representa del modo siguiente:

$$\varepsilon = \varepsilon_B{}^8$$

Según el teorema del límite central, la distribución de la intensidad de la señal observada en las tramas no marcadas (por ejemplo, la intensidad de ruido) puede tratarse como una distribución normal y sus variaciones calcularse sobre la base de cada variación de los resultados. Esto se debe a que la intensidad es una suma lineal de un gran número de resultados aleatorios. Por lo tanto, la probabilidad de que la intensidad del ruido normalizado R exceda el valor de umbral T puede estimarse mediante una función de densidad de probabilidad normal, como se indica a continuación:

$$\varepsilon_B = \mathrm{P}(|R| > T) = 2\int_T^\infty \frac{1}{\sqrt{2\pi}} e^{-\frac{t^2}{2}} dt$$

donde "P(x)" indica probabilidad de un evento "x".

Si la intensidad de la señal normalizada es más débil que el umbral, la señal será acumulada continuamente con las tramas siguientes (campos). La acumulación de la señal continuará hasta que la intensidad de la señal acumulada alcance el umbral (filigrana detectada), o el tiempo de acumulación exceda el tiempo de corte máximo (filigrana no detectada), cualesquiera sea el primero (detección de acumulación de trama). Además, dado que el algoritmo selecciona las señales adecuadas de forma que sean independientes entre sí, la variación de la señal acumulada puede calcularse como una raíz cuadrada del número de acumulaciones *f* y, por lo tanto, el comportamiento de la señal acumulada:

$$S_f = \sum_{1}^{f} R_i$$

puede calcularse mediante una función de densidad de probabilidad normal, del modo siguiente:

$$\varepsilon_B = \mathrm{P}(|\frac{S_f}{\sqrt{f}}| > T) = 2\int_{T}^{\infty} \frac{1}{\sqrt{2\pi}} e^{-\frac{t^2}{2}} dt$$

Como el algoritmo efectúa una prueba de detección independiente al mismo tiempo que la acumulación, la tasa de errores positivos falsos total para cada bit puede expresarse de la siguiente forma:

$$\varepsilon' = 1 - (1 - \varepsilon)^f$$

donde ε es la tasa de errores positivos falsos de una prueba y *f* es el número de acumulaciones. En el cuadro II.6 se muestran algunos valores de umbral *T* y la relación de errores positivos falsos ε′ correspondiente, donde el máximo de acumulaciones se fija en 40.

Cuadro II.6/J.95 – Lista de tasa de errores positivos falsos en comparación con los umbrales

Relación prevista (ε′) de errores positivos falsos	Umbral (*T*) para detección de 8 bits
10^{-8}	1,85878
10^{-9}	1,98372
10^{-10}	2,10306
10^{-11}	2,21752
10^{-12}	2,32729
10^{-13}	2,44118

II.7 Tecnología y sistemas de inserción

En la tecnología Galaxy la inserción es un proceso de doble trayecto:

1) análisis del contenido de la imagen; y

2) proceso de modificación de luminancia.

Este proceso permite el control automático de la intensidad de inserción para satisfacer la transparencia, la robustez y la tasa de errores positivos falsos requeridas. En cada campo de vídeo digital no comprimido se insertan 8 bits de datos CCI como marca primaria.

El sistema de inserción en estudio es un sistema DSP basado en PC capaz de funcionar en tiempo real con tramas de retardo. La entrada y salida de las señales de este sistema se efectúan a través de la interfaz digital de vídeo UIT-R-656. El sistema está planificado para que un monitor en tiempo real confirme la intensidad de la señal de secuencias insertadas y ofrece una interfaz de usuario de fácil manejo para parámetros de insertación ajustables. Este sistema ofrece también funciones de seguridad, como por ejemplo el control de acceso a operadores no autorizados y la prevención de nuevas inserciones accidentales o intencionales.

II.8 Abreviaturas

A/D	Analógico a digital (*analogue to digital*)
APS	Sistema de protección analógico (*analogue protection system*)
CCI	Información de control de copia (*copy control information*)
CFP	Aviso de licitación (*call for proposal*)
CM	Marca de copia (*copy mark*)
CPAC	Comité asesor de protección contra copias (*copy protection advisory committee*)
CSS	Sistema de aleatorización de contenidos (*contents scramble system*)
D/A	Digital a analógico (*digital to analogue*)
DHSG	Subgrupo de ocultación de datos (*data-hiding sub-group*)
DSP	Procesador de señal digital (*digital signal processor*)
DVD-ROM	Disco versátil digital – memoria de lectura solamente (*digital versatile disc read-only memory*)
DVNR	Reducción de ruido vídeo digital (*digital video noise reduction*)
FPGA	Disposición de puertos programables de campo (*field programmable gate array*)
ICPAC	CPAC interino (*interim CPAC*)
MPEG-2	Grupo de expertos 2 sobre imágenes en movimiento (*moving pictures expert group 2*)
PM	Marca primaria (*primary mark*)
WM	Filigrana (*water mark*)

II.9 Informaciones útiles

En Japón

IBM Corporation
Tokyo Research Laboratory
1623-14, Shimotsuruma, Yamato-shi
Kanagawa-ken, 242-8502
Japón

NEC Corporation
1-10, Nisshincho, Fuchu-shi
Tokyo, 183-8501
Japón

Hitachi Ltd.
292, Yoshidacho, Totsuka-ku
Yokohama-shi
Kanagawa-ken, 244-0817
Japón

Pioneer Electronic Corporation
1-1, Fujimi 6 chome, Tsurugashima-shi
Saitama-ken, 350-2288
Japón

Sony Corporation
6-7-35, Kitashinagawa, Shinagawa-ku
Tokyo, 141-0001
Japón

En los Estados Unidos

Director of Licensing Development
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594
Estados Unidos de América

NEC Research Institute Inc.
4 Independence Way
Princeton, NJ
Estados Unidos de América

Apéndice III

Propuesta 5C para la protección de la propiedad intelectual contra copia de vídeo MPEG

Propiedad intelectual

La aplicación de esta especificación requiere una licencia del Administrador de concesión de licencias para transmisión digital.

Informaciones útiles

Todas las cuestiones relativas a esta especificación deben dirigirse a spec-comments@dtcp.com.

La dirección electrónica del Administrador de concesión de licencias para transmisión digital es dtla@intel.com.

El URL del sitio de la Web para el Administrador de concesión de licencias para transmisión digital es http://www.dtcp.com.

NOTA – Los documentos originales del material que figura en el presente apéndice pueden obtenerse de los titulares de derechos de autor únicamente mediante el establecimiento de un acuerdo sobre confidencialidad (NDA, *non-disclosure agreement*). Para obtener más datos sobre las fuentes adecuadas de esta información, dirigirse al Administrador de concesión de licencias para transmisión digital.

III.1 Introducción

III.1.1 Finalidad y ámbito de aplicación

En la *Especificación relativa a la protección de contenidos de transmisión digitales 5C* se define un protocolo criptográfico destinado a proteger el material audio/vídeo recreativo contra las copias, la intercepción y la manipulación no autorizadas mientras circula por mecanismos de transmisión digitales, como por ejemplo un bus serie de alto nivel de eficacia conforme a la norma IEEE 1394-1995. Serán protegidos por este sistema de protección contra copias únicamente los contenidos recreativos legítimos transmitidos a un dispositivo fuente a través de otro sistema de protección contra copias homologado (como el sistema de aleatorización de contenidos DVD).

La utilización de esta especificación y el acceso a la propiedad intelectual y a los materiales criptográficos necesarios para aplicarla estarán sujetos a la concesión de una licencia. El administrador de concesión de licencias para transmisión digital (DTLA, *digital transmission licensing administrator*) es el responsable de establecer y administrar el sistema de protección de contenidos descrito en la presente especificación.

Aunque el protocolo DTCP se ha concebido para dispositivos conectados a los bus serie definidos por la norma IEEE 1394-1995, los diseñadores anticipan que se podrá utilizar en futuras ampliaciones de esta norma, en otros sistemas de transmisión y en otros tipos de contenidos autorizados por el DTLA.

III.1.2 Panorama general

En esta especificación se describen cuatro capas de protección contra copias:

- **Información de control de copias (CCI)**

  Los titulares de la propiedad intelectual de contenidos necesitan una forma de especificar cómo pueden utilizarse esos contenidos ("una generación de copias", "ninguna copia", etc.). Este sistema de protección de contenidos es capaz de comunicar en forma segura la información de control de copias (CCI) entre dispositivos de dos maneras:

  – El indicador de modo criptación (EMI, *encryption mode indicator*) permite que la transmisión de la CCI a través de los dos bits más significativos del campo del encabezamiento de paquete isócrono sea de fácil acceso pero segura.

  – La CCI se inserta en el tren de contenidos (por ejemplo, MPEG). Esta forma de CCI se procesa únicamente mediante dispositivos que reconocen el formato del contenido específico.

- **Autenticación del dispositivo e intercambio de claves (*AKE, authentication and key exchange*)**

  Antes de intercambiar datos valiosos, un dispositivo conectado debe verificar primero si el otro dispositivo conectado es auténtico. Para lograr un equilibrio entre los requisitos establecidos por las industrias de contenidos con respecto a la protección de los mismos y los requisitos reales de los usuarios de computadoras personales y de dispositivos electrónicos (CE, *consumer electronics*), esta especificación abarca dos niveles de autenticación, completa y restringida.

  – Puede utilizarse la autenticación completa con todos los contenidos protegidos por el sistema.

  – La autenticación restringida hace posible la protección únicamente de contenidos "una generación de copias" y "no más copias". Los dispositivos utilizados para hacer copias, como los magnetoscopios digitales, emplean este tipo de autenticación.

- **Criptación de contenidos**

  Los dispositivos incluyen un subsistema de cifrado de canales que cripta y descripta el contenido que goza de los derechos de autor. A fin de asegurar el interfuncionamiento, todos los dispositivos deben soportar el cifrado específico definido como cifrado de línea de base. El subsistema puede soportar también cifrados adicionales, cuya utilización se negocia durante la autenticación.

- **Capacidad de renovación del sistema [MP1]**

  Los dispositivos que soporten la autenticación completa pueden recibir y procesar mensajes con capacidad de renovación del sistema (SRM, *system renewability messages*) creados por el DTLA y distribuidos con contenidos y nuevos dispositivos. La capacidad de renovación del sistema asegura la integridad a largo plazo del mismo mediante la revocación de dispositivos afectados.

En la figura III.1 se ofrece una visión general de la protección de contenidos, en la que se observa que el dispositivo fuente ha recibido instrucciones para transmitir un tren de protección contra copia de contenidos. En este diagrama y en diagramas subsiguientes, un dispositivo fuente es el que puede enviar un tren de contenidos y un dispositivo sumidero el que puede recibirlo. Los dispositivos multifunción como las computadoras personales y los dispositivos de grabación y reproducción, como los magnetoscopios digitales pueden ser a la vez dispositivos fuente y dispositivos sumidero.

1) El dispositivo fuente inicia la transmisión de un tren de contenidos criptados marcado con el estado de protección contra copias apropiado (por ejemplo, "una generación de copias", "ninguna copia", o "no más copias") a través de los bits EMI.[1]

2) Al recibir el tren de contenidos, el dispositivo sumidero inspecciona los bits EMI para determinar el estado de protección contra las copias del contenido. Si el contenido está marcado "ninguna copia", el dispositivo sumidero pide que el dispositivo fuente inicie la capa de protección AKE completa. Si el contenido está marcado "una generación de copias" o "no más copias", el dispositivo sumidero solicitará AKE completa, si la soporta, o AKE restringida. Si el dispositivo sumidero ya ha realizado la autenticación adecuada, puede pasar inmediatamente a la etapa 4.

---

[1] Si el contenido requerido por un dispositivo sumidero está protegido, el dispositivo fuente puede transmitir un tren de contenidos vacío hasta que, como mínimo, un dispositivo haya completado el procedimiento de autenticación adecuado necesario para acceder al tren de contenidos.

3) Cuando el dispositivo fuente recibe la petición de autenticación, la efectúa con el tipo de autenticación solicitada por el dispositivo sumidero, a menos que se soportar AKE completa y el dispositivo fuente sólo pueda soportar AKE restringida, en cuyo caso se efectúa este último nivel de autenticación.

4) Una vez que los dispositivos han completado el procedimiento AKE solicitado, pueden intercambiar una clave de criptación de canal de contenidos. Esta clave se utiliza para criptar el contenido en el dispositivo fuente y descriptarlo en el dispositivo sumidero.

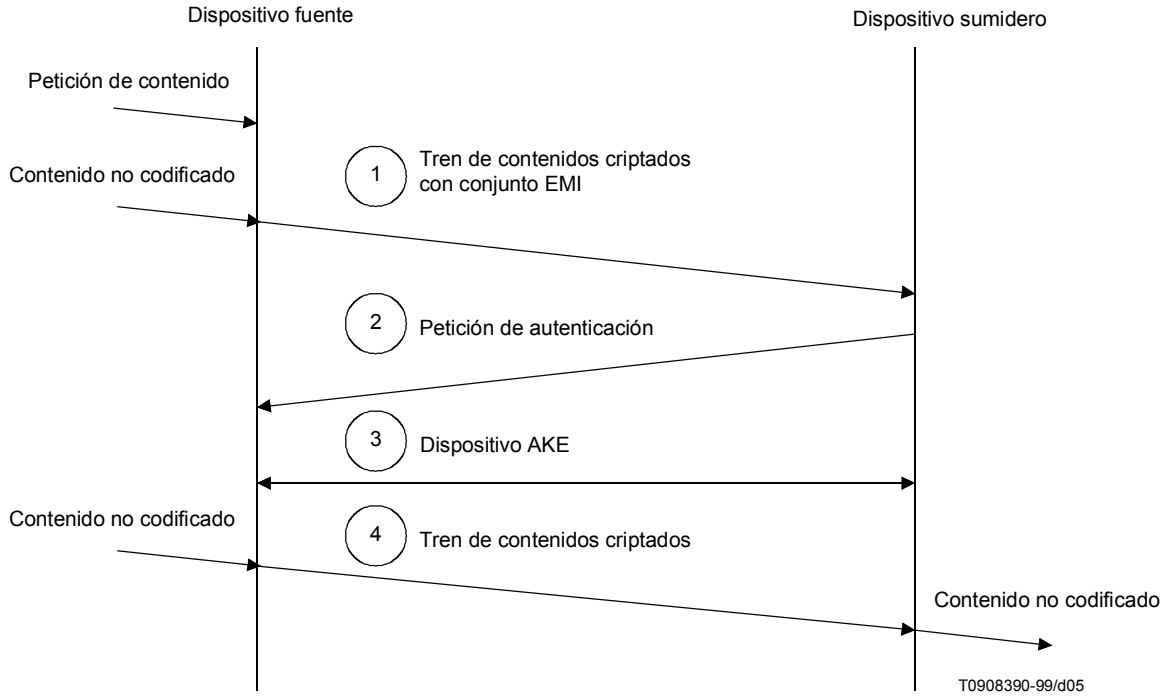


Figura III.1/J.95 – Visión general de la protección de contenidos

III.1.3 Referencias

La presente especificación será utilizada junto con las siguientes publicaciones. En el caso de que las mencionadas publicaciones hayan sido sustituidas por una revisión aprobada, se dará validez a dicha revisión.

– Digital Transmission Protection License Agreement, *Development and Evaluation License*, Digital Transmission Licensing Authority.

– 1394 Trade Association, *Specification for AV/C Digital Interface Command Set*.

– Digital Transmission Licensing Administrator, *5C Digital Transmission Content Protection Specification*, Volume 1, Version 0.91.

– Digital Transmission Licensing Administrator, *5C Digital Transmission Content Protection Specification*, Volume 2, Version 0.90.

– Digital Transmission Protection License Agreement, *Development and Evaluation License*, Digital Transmission Licensing Authority.

– IEEE Std 1394-1995, *IEEE's Standard for a High Performance Serial Bus*.

– IEEE P1363, *Editorial Contribution to Standard for Public Key Cryptography*, Preliminary Draft, P1363/D3 (11 de mayo 1998).

– CEI 61883-1 (1998), *Digital Interface for Consumer Audio/Video Equipment – Digital Interface – Part 1: General.*

– National Institute of Standards and Technology (NIST), *Secure Hash Standard (SHS)*, FIPS Publication 180-1, 17 de abril de 1995.

– Toshiba Corporation, *Efficient Implementation of an Elliptic Curve Cryptosystem,* disponible en http://www.dtcp.com/

III.1.4 Organización del presente apéndice

Esta propuesta de protección contra copias se organiza del modo siguiente:

- Subcláusula III.1: panorama general de la protección de contenidos.
- Subcláusula III.2: enumeración de los términos y abreviaturas utilizados en todo el apéndice.
- Subcláusula III.3: descripción del funcionamiento de todo el sistema de protección de contenidos de transmisión digital como máquina de estados.
- Subcláusula III.4: características particulares del nivel de autenticación completa de la autenticación de dispositivos e intercambio de claves.
- Subcláusula III.5: características particulares del nivel de autenticación restringida de la autenticación de dispositivos e intercambio de claves.
- Subcláusula III.6: detalles del establecimiento del canal de contenidos una vez que ha tenido lugar la autenticación completa o restringida.
- Subcláusula III.7: descripción de las capacidades de renovación del sistema.
- Subcláusula III.8: ampliaciones de la instrucción AV/C.

III.1.5 Notación de máquinas de estados

Para mostrar diversos estados de funcionamiento, en todo este apéndice se utilizan máquinas de estado con el estilo indicado en la figura III.2.

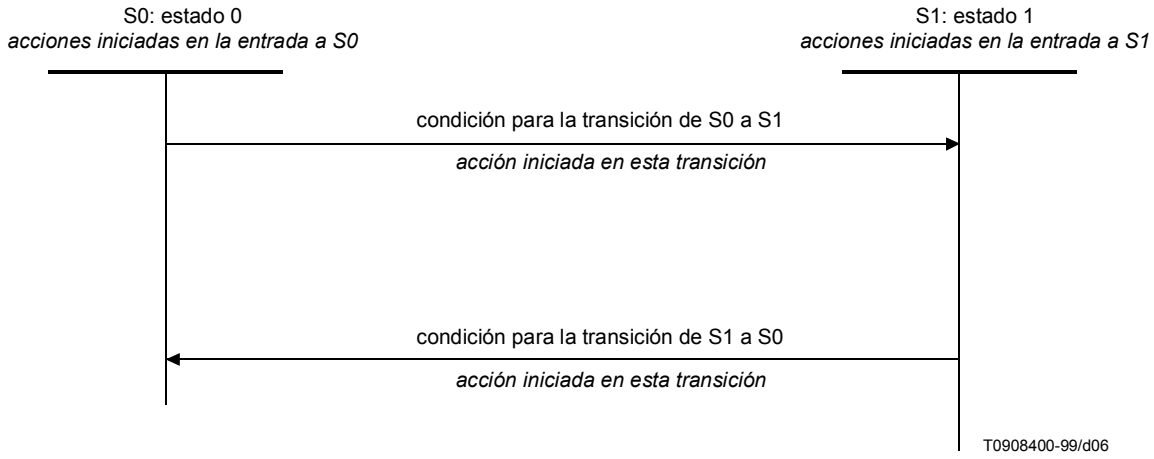


Figura III.2/J.95 – Ejemplo de máquina de estados

En las máquinas de estados se formulan tres hipótesis:

1) El tiempo transcurre únicamente dentro de estados discretos.

2) Las transiciones de estado son instantáneas de modo que únicamente las acciones efectuadas durante una transición colocan banderas y variables y envían señales.

3) Cada vez que se introduce un estado, se inician las acciones de dicho estado. Una transacción que apunta nuevamente al mismo estado iniciará las acciones desde el comienzo.

III.1.6 Notación

Se utilizará la siguiente notación:

$[X]_{msb\_z}$ = Los z bits más significativos de X.

$[X]_{lsb\_z}$ = Los z bits menos significativos de X.

$S_{X^{-1}}[M]$ = Firmar M utilizando EC-DSA con clave privada X^{-1} (En III.4 figuran más detalles del algoritmo de firma).

$V_{X^1}[M]$ = Verificar firma de M utilizando EC-DSA con clave pública X^1 (En III.4 figuran más detalles del algoritmo de verificación).

$X \,||\, Y$ = Concatenación ordenada de X con Y.

$X \oplus Y$ = O R exclusivo con bits (XOR, *exclusive-OR*) de dos cadenas X e Y.

III.1.7 Valores numéricos

En esta especificación se utilizan tres representaciones distintas de números. Los números decimales se representan sin ninguna notación especial. Los números binarios, como una cadena de dígitos binarios (0, 1) seguidos de un subíndice 2 (por ejemplo, 1010_2). Los números hexadecimales, como una cadena de dígitos hexadecimales (0…9, A…F) seguidos de un subíndice 16 (por ejemplo, $3C2_{16}$).

III.1.8 Orden de los bits

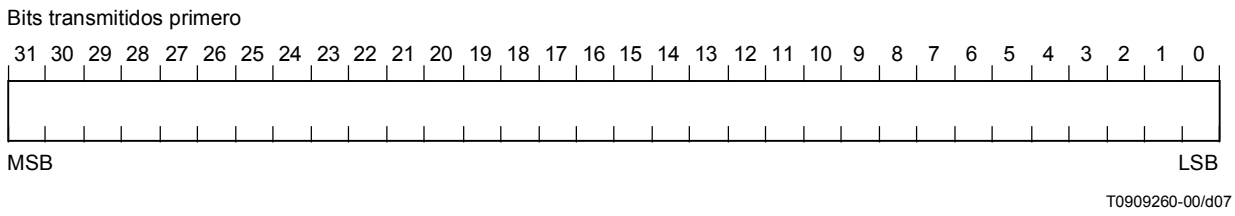


Figura III.3/J.95 – Orden de los bits

III.1.9 Formato del paquete

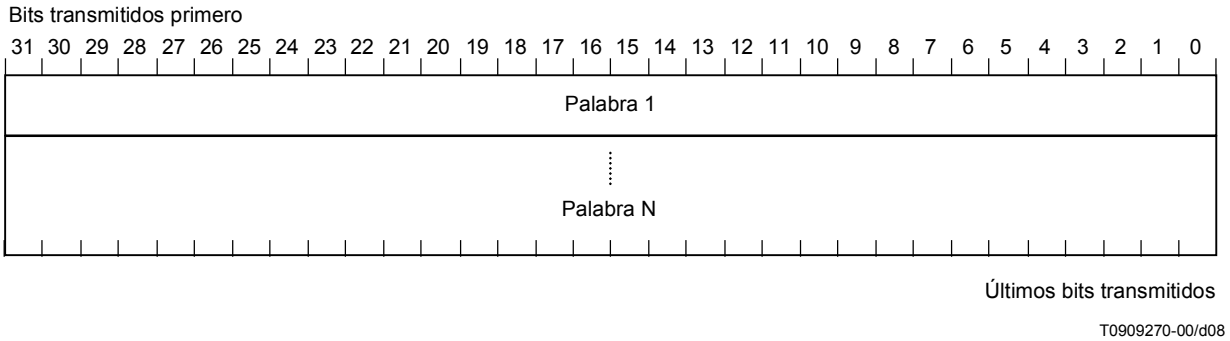


Figura III.4/J.95 – Formato del paquete

III.1.10 Tratamiento de partes opcionales de esta Especificación

Las características de esta especificación rotuladas como "opcionales" describen capacidades cuya utilización no ha sido aún establecida por el DTLA.

III.2 Términos y abreviaturas

Queda en estudio.

III.3 Sistema de protección de contenidos de transmisión digital 5C

III.3.1 Dispositivo fuente de contenidos

La figura III.5 muestra los diversos estados de funcionamiento de un dispositivo fuente de contenidos.

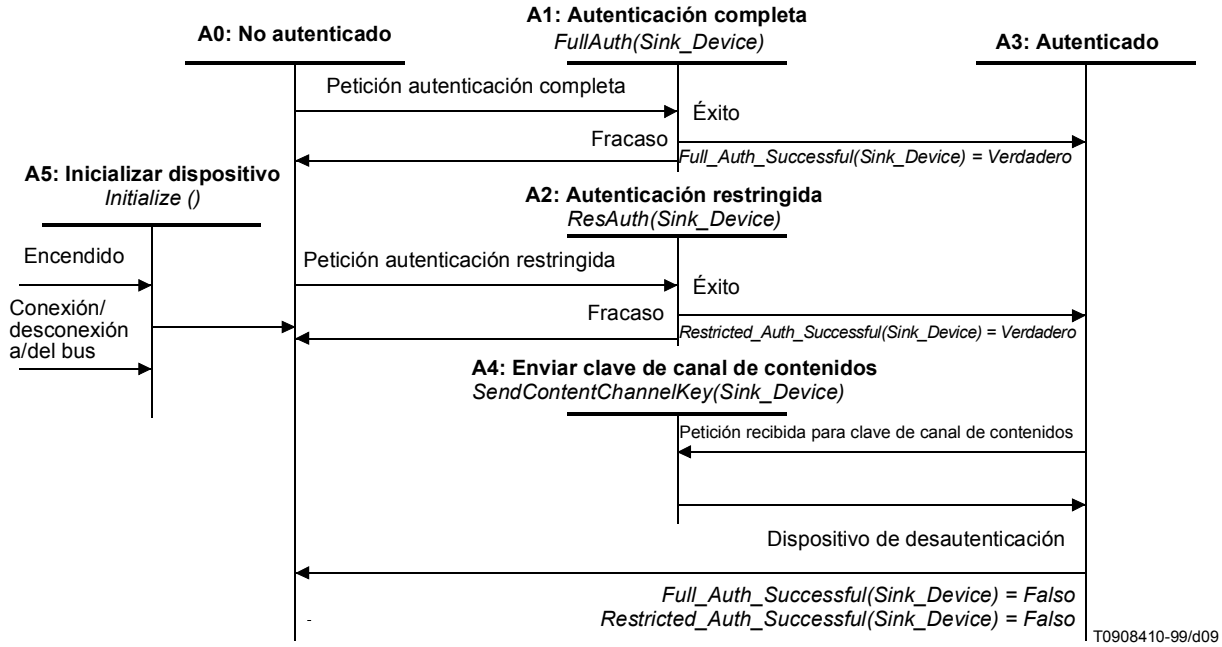


Figura III.5/J.95 – Máquina de estados del dispositivo fuente de contenidos

Un encendido o una conexión/desconexión al/del evento bus restablece esta máquina de estados en el **estado A5: Inicializar dispositivo**.

Estado 5: Inicializar dispositivo. En este estado, se inicializa el dispositivo.

Transición A5:A0. Esta transición al **estado A0: No autenticado** ocurre después de la finalización del proceso de inicialización.

Estado A0: No autenticado. Un dispositivo se halla en un estado no autenticado, en espera de recibir una petición para realizar el procedimiento de autenticación completa o autenticación restringida.

Transición A0:A1. Esta transición ocurre cuando el dispositivo recibe una petición para realizar el procedimiento autenticación completa con un dispositivo sumidero *(Sink_Device)*.

Estado A1: Autenticación completa. En este estado, se efectúa el proceso *FullAuth(Sink_Device)* (autenticación completa) (dispositivo sumidero). En III.4 se describe en forma más completa este proceso.

Transición A1:A3. Esta transición ocurre cuando se ha completado satisfactoriamente *FullAuth(Sink_Device)*.

Full_Auth_Successful(Sink_Device) = Verdadero

Transición A1:A0. Esta transición ocurre cuando *FullAuth(Sink_Device)* no tiene éxito.

Transición A0:A2. Esta transición ocurre cuando el dispositivo recibe una petición para efectuar el procedimiento autenticación restringida con un dispositivo sumidero *(Sink_Device)*.

Estado A2: Autenticación restringida. En este estado, el dispositivo ejecuta el proceso *ResAuth(Sink_Device)* (autenticación restringida) (dispositivo sumidero). En III.5 se describe en forma más completa este proceso.

Transición A2:A3. Esta transición ocurre cuando el proceso *ResAuth(Sink_Device)* se ha completado satisfactoriamente.

Restricted_Auth-Successful(Sink_Device) = Verdadero

Transición A2:A0. Esta transición ocurre cuando el proceso *ResAuth(Sink_Device)* no tiene éxito.

Estado A3: Autenticado. Cuando un dispositivo se encuentra en este estado, ha sido completado satisfactoriamente el procedimiento autenticación completa o autenticación restringida.

Transición A3:A4. Se pide a un dispositivo autenticado que envíe los valores necesarios para construir una clave de contenidos para un dispositivo sumidero.

Estado A4: Enviar clave de canal de contenidos. En este estado, el dispositivo de origen envía los valores necesarios a fin de crear una clave de contenidos para un dispositivo sumidero autenticado ejecutando S*endContentChannelKey-(Sink_Device)* [enviar clave de canal de contenidos (dispositivo sumidero)]. En III.6 se describe este proceso.

Transición A4:A3. Esta transición ocurre al completarse el proceso *SendContentChannelKey(Sink_Device)*.

Transición A3:A0.

Full_Auth_Successful(Sink_Device) = Falso

Restricted_Auth_Successful(Sink_Device) = Falso

III.3.2 Dispositivo fuente de contenidos

La figura III.6 muestra los diversos estados de funcionamiento de un dispositivo sumidero de contenidos.

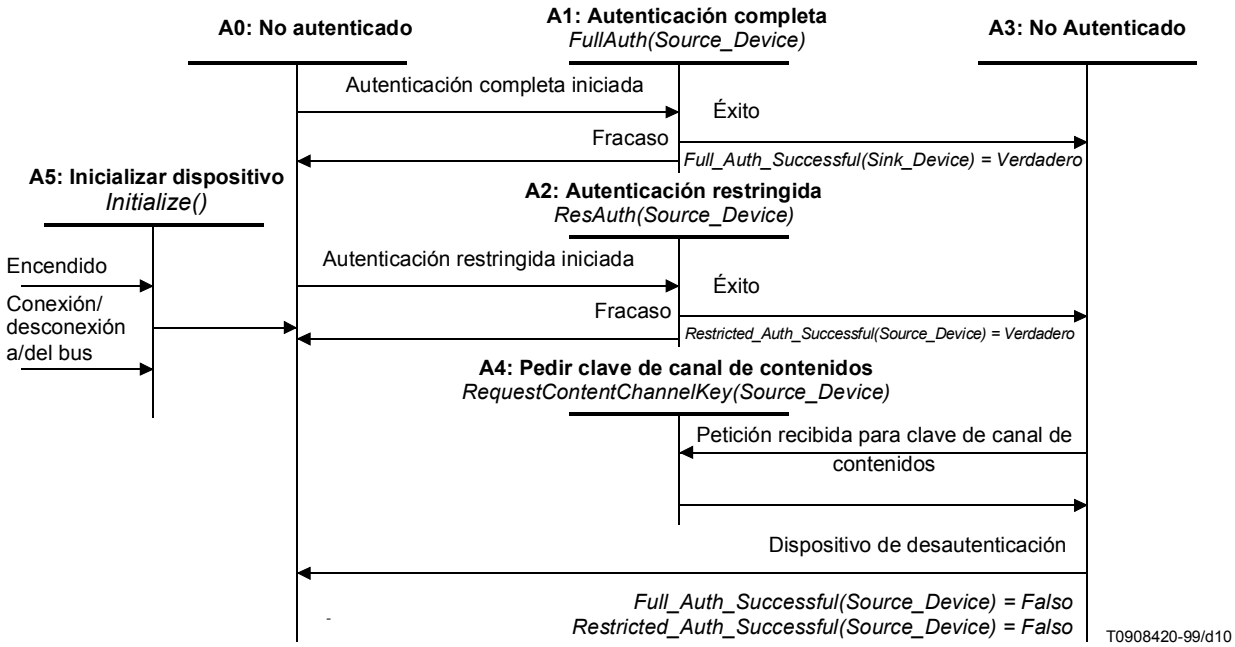


Figura III.6/J.95 – Máquina de estados del dispositivo sumidero de contenidos

Un encendido o una conexión/desconexión al/del evento bus restablece esta máquina de estados en el **estado A5: Inicializar dispositivo**.

Estado 5: Inicializar dispositivo. En este estado, se inicializa el dispositivo.

Transición A5:A0. Esta transición al **estado A0: No autenticado** ocurre después de la finalización del proceso de inicialización.

Estado A0: No autenticado. Un dispositivo se halla en un estado no autenticado, en espera de iniciar una petición para realizar el procedimiento de autenticación completa o autenticación restringida.

Transición A0:A1. Esta transición ocurre cuando el dispositivo inicia una petición para realizar el procedimiento autenticación completa con otro dispositivo (*Source_Device*).

Estado A1: Autenticación completa. En este estado, se efectúa el proceso *FullAuth(Source_Device)* (autenticación completa) (dispositivo fuente). En III.4 se describe en forma más completa este proceso.

Transición A1:A3 Esta transición ocurre cuando se ha completado satisfactoriamente *FullAuth(Source_Device)*.

Full_Auth_Successful(Source_Device) = Verdadero

Transición A1:A0. Esta transición ocurre cuando el proceso *FullAuth(Source_Device)* no tiene éxito.

Transición A0:A2. Esta transición ocurre cuando el dispositivo inicia una petición para efectuar el procedimiento autenticación restringida con otro dispositivo *(Source_Device).*

Estado A2: Autenticación restringida. En este estado, el dispositivo ejecuta el proceso *ResAuth(Source_Device)* (autenticación restringida) (dispositivo fuente). En III.5 se describe en forma más completa este proceso.

Transición A2:A3. Esta transición ocurre cuando el proceso *ResAuth(Source_Device)* se ha completado satisfactoriamente.

Restricted_Auth-Successful(Source-Device) = Verdadero

Transición A2:A0. Esta transición ocurre cuando *ResAuth(Source_Device)* no tiene éxito.

Estado A3: Autenticado. Cuando un dispositivo se encuentra en este estado, ha sido completado satisfactoriamente el procedimiento autenticación completa o autenticación restringida.

Transición A3:A4. Un dispositivo autenticado necesita pedir una clave de contenidos para acceder al contenido protegido contra copias.

Estado A4: Pedir clave de canal de contenidos. En este estado, un dispositivo sumidero autenticado pide los valores necesarios a fin de crear una clave de contenidos ejecutando el procedimiento *RequestContentChannelKey-(Source_Device)* [pedir clave de canal de contenidos (dispositivo fuente)]. En III.6 se describe este proceso.

Transición A4:A3. Esta transición ocurre al completarse el proceso *RequestContentChannelKey(Source_Device)*.

Transición A3:A0.

Full_Auth_Successful(Source_Device) = Falso

Restricted_Auth_Successful(Source_Device) = Falso

III.4 Autenticación completa

III.4.1 Introducción

En esta subcláusula se abordan las características particulares del nivel de autenticación completa de la autenticación de dispositivos e intercambio de claves. La autenticación completa emplea la clave pública basada en el algoritmo de firma digital de curva elíptica (EC-DSA, *elliptic curve digital signature algorithm*) para firma y verificación. Utiliza también el algoritmo de intercambio de claves Diffie-Hellman de curva elíptica (EC-DH, *elliptic curve Diffie-Hellman*) para generar una clave de autenticación compartida.

III.4.2 Notación

La notación introducida en esta subcláusula se utiliza para describir los procesos criptográficos. Todas las operaciones en el dominio curva elíptica se calculan en una curva elíptica E definida por GF(p).

III.4.2.1 Definiciones del DTLA

Los parámetros, claves, constantes y certificados siguientes son generados por el DTLA.

III.4.2.1.1 Elementos generales

p = Número primo superior a 3.

GF(p) = Campo finito de p elementos, representado como módulo p de enteros.

E = Curva elíptica en el campo GF(p).

a, b = Coeficientes que definen la curva elíptica E, elementos de GF(p).

G = Punto de base de la curva elíptica.

r = Orden de G.

L^{-1}, L^{1} = Par de claves EC-DSA del DTLA formada por una clave privada L^{-1} de EC, que es un entero en la gama [1, r – 1] y una clave pública L^{1} de EC, que es un punto en E, donde $L^{1} = L^{-1}G$.

Estas constantes, a excepción de L^{-1}, están disponibles en la especificación DTCP con licencia concedida por el DTLA.

III.4.2.1.2 Dispositivo X

X^{-1}, X^{1} = Par de claves EC-DSA de dispositivo formado por una clave privada X^{-1} de EC, que es un entero en la gama [1, r – 1] y una clave pública X^{1} de EC, que es un punto en E, donde $X^{1} = X^{-1}G$.

X_{Cert} = Certificado concedido por el DTLA al dispositivo X apto y utilizado durante el proceso de autenticación (para más detalles, véase la subcláusula siguiente).

Los puntos de la curva elíptica están formados por la concatenación de la coordenada x y la coordenada y, respectivamente; para un punto P de la curva elíptica = (x_P, y_P) que no es igual al punto de la curva elíptica en el infinito, $P = x_P \| y_P$.

Cuadro III.1/J.95 – Longitud de claves y parámetros de curva elíptica generados por DTLA (autenticación completa)

Claves y parámetros de curva elíptica	Tamaño (bits)
Clave pública DTLA (L^{1})	320
Clave privada de dispositivo (X^{-1})	160
Clave pública de dispositivo (X^{1})	320
Punto de base (G)	320
Coeficiente de polinomio de curva elíptica (a, b)	160 (cada uno)
Número primo (p) de campo finito GF(p)	160
Orden de puntos de base (r)	160

III.4.2.2 Notación utilizada durante la autenticación completa

Durante la autenticación completa, los dispositivos generan y utilizan los siguientes valores adicionales:

X_n = Identificador de un solo uso (impugnación aleatoria generada por RNG_F).

X_k = Valor aleatorio utilizado en el intercambio de claves EC-DH generado por RNG_F en el dispositivo (entero en la gama [1, r – 1]).

X_V = Valor de primera fase EC-DH (X_kG) calculado en el dispositivo (punto E en la curva elíptica).

X_{SRMV} = Número de versión del mensaje capacidad de renovación del sistema (SRMV) almacenado por el dispositivo (véase III.7).

X_{SRMC} = Indica el número de partes SRM que se almacenan actualmente en la memoria no volátil del dispositivo. Un valor de SRMC indica que las primeras generaciones SRMC+1 de los SRM son almacenadas actualmente por el dispositivo (véase III.7).

K_{Auth} = Clave de autenticación que son los 96 bits menos significativos de los datos compartidos creados mediante el intercambio de claves EC-DH

Cuadro III.2/J.95 – Longitud de claves y variables generadas por el dispositivo (autenticación completa)

Clave o variable	Tamaño (bits)
No más de uno (impugnación aleatoria X_n)	128
Valor aleatorio para EC-DH (X_k)	160
Valor de primera fase EC-DH (X_V)	320
X_{SRMV}	16
X_{SRMC}	4
Clave de autenticación creada mediante el intercambio de claves EC-DH (K_{Auth})	96

III.4.2.3 Formatos de certificados para dispositivos

El DTLA concede un certificado a cada dispositivo que satisface la norma. Este certificado se almacena en dicho dispositivo y se utiliza durante el proceso de autenticación.

III.4.2.3.1 Formato de línea de base

La figura III.7 muestra el formato de certificado del dispositivo de línea de base:

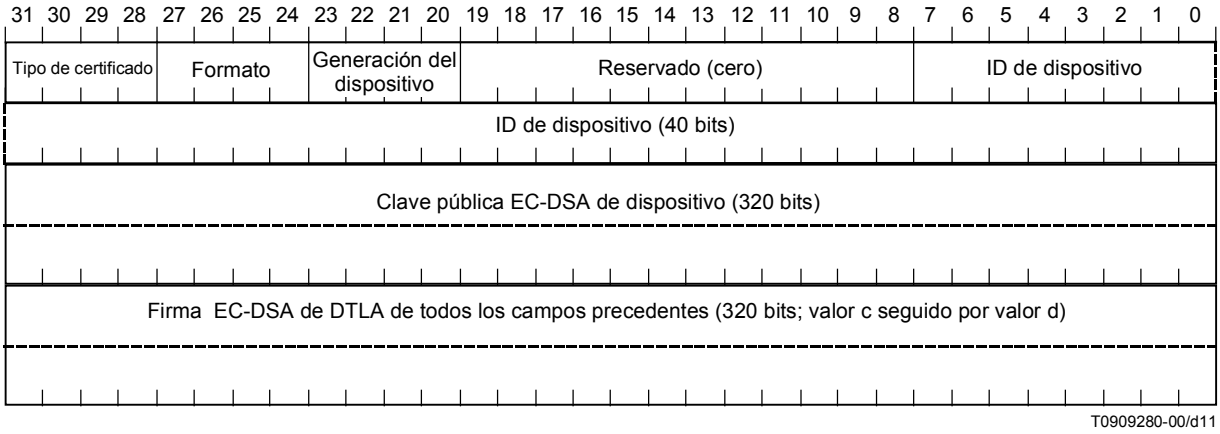


Figura III.7/J.95 – Formato de certificado del dispositivo de línea de base

Los certificados de dispositivos están formados por los siguientes campos del formato de línea de base:

- **Tipo de certificado** (4 bits). La única codificación actualmente definida es 0, que indica que el certificado corresponde a la protección de contenido IEEE 1394. Actualmente se reservan otras codificaciones.
- **Formato de certificado** (4 bits). Este campo especifica el formato de un tipo específico de certificado. Actualmente se definen tres formatos:

  Formato 0 = formato de certificado de dispositivo de autorización restringida (descrito en III.5).

  Formato 1 = formato de certificado de dispositivo de autenticación completa de línea de base.

  Formato 2 = formato de certificado de dispositivo de autenticación completa ampliada (opcional[2]).

[2] Las características de esta especificación rotuladas como "opcionales" describen capacidades cuya utilización no ha sido aún establecida por el DTLA.

Actualmente se reservan otras codificaciones.

- **Generación de dispositivo** (X_{SRMG}) (4 bits). Este campo indica la capacidad de memoria no volátil y, por consiguiente, la generación máxima de mensajes con capacidad de renovación que soporta este dispositivo (descrito en III.7). La codificación 0 indica un tamaño máximo de 128 bytes aunque actualmente se reservan otras codificaciones.
- Campo reservado (12 bits). Estos bits se reservan para una futura definición y se definen actualmente con un valor de cero.
- El número **ID de dispositivo** (X_{ID} 40 bits) asignado por el DTLA.
- La **clave pública EC-DSA** (X^1, 320 bits).
- Una **firma EC-DSA** del DTLA de los componentes enumerados anteriormente (320 bits).

El tamaño total de un formato de certificado del dispositivo de línea de base es 88 bytes.

III.4.2.3.2 Campos de formato ampliados (componentes opcionales del certificado de dispositivo)

Además de los campos de formato de línea de base, cada certificado de dispositivo puede incluir, como opción, los siguientes campos de formato ampliados[3]:

- Una **máscara de capacidad de dispositivo** que indica las propiedades del dispositivo y los códigos de canal soportados. (X_{Cap_Mask}, 32 bits).
- Una **firma EC-DSA** del DTLA de todos los componentes precedentes en el certificado de dispositivo (320 bits).

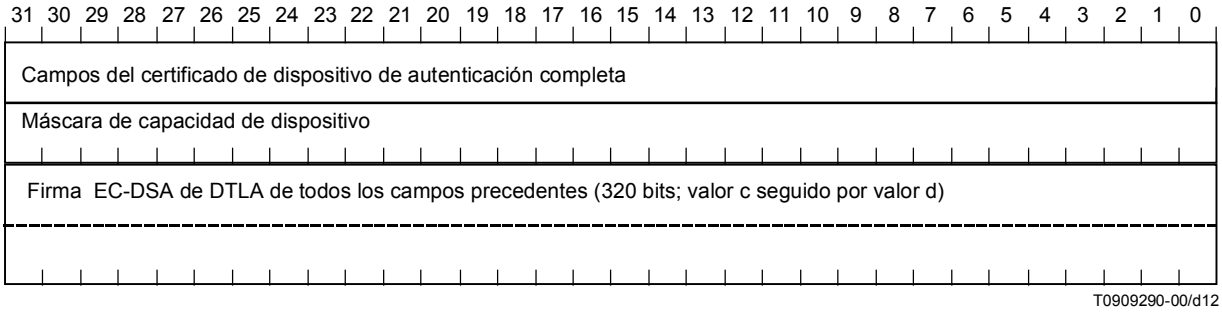


Figura III.8/J.95 – Campos del certificado de dispositivo ampliados

Máscara de capacidad de dispositivo

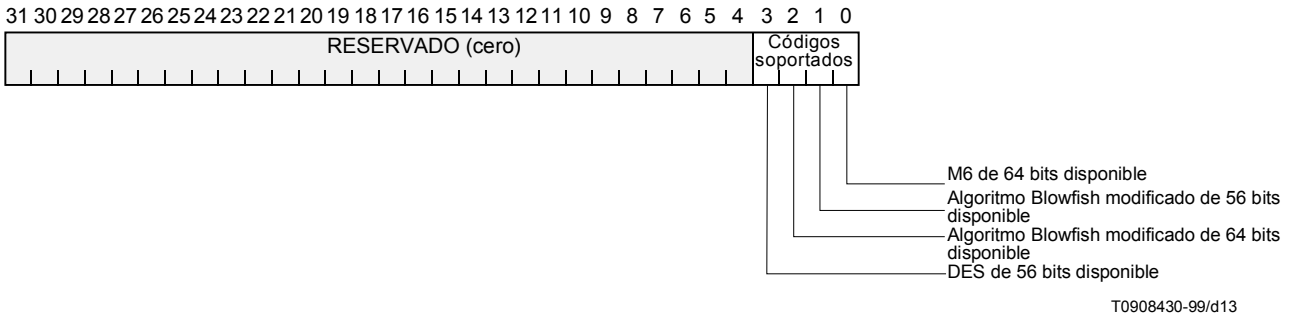


Figura III.9/J.95 – Máscara de capacidad de dispositivo

La máscara de capacidad de dispositivo describe las características de extensibilidad soportadas por un determinado dispositivo. En la figura III.9 se indica el formato de dicha máscara.

Se supone que los dispositivos que no soporten la máscara de capacidad de dispositivo soporten únicamente las características criptográficas obligatorias definidas por este sistema de protección de contenidos (por ejemplo, los códigos de línea de base M6 de 56 bits).

---

[3] Las características de esta especificación rotuladas como "opcionales" describen capacidades cuya utilización no ha sido aún establecida por el DTLA.

III.4.3 Manufactura de dispositivos aptos

A todos los dispositivos aptos que soporten la autenticación completa (es decir, a cada elemento manufacturado, independientemente de la marca y modelo) se le asignará un ID (identificador) de dispositivo único (X_{ID}) y un par de claves públicas/privadas EC-DSA de dispositivo (X^1, X^{-1}) generado por el DTLA. X^{-1} debe almacenarse dentro del dispositivo de tal forma que impida la divulgación de los datos que contiene. Además, el DTLA debe conceder un certificado a cada dispositivo apto que se almacenará en el mismo y se utilizará durante el proceso de autenticación. Asimismo, el dispositivo apto necesitará almacenar las demás constantes y claves necesarias para implementar los protocolos criptográficos.

III.4.4 Funciones criptográficas

III.4.4.1 SHA-1 (Secure Hash Algorithm, algoritmo de troceado seguro, revisión 1)

El SHA-1, descrito en FIPS PUB 180-1[4], es el algoritmo utilizado en DSS para generar un mensaje condensado de una longitud de 160 bits. Un resumen de mensaje es un valor calculado a partir del mensaje y, como concepto, es similar a una suma de verificación aunque, desde el punto de vista informático, imposible de falsificar.

III.4.4.2 Generador de número aleatorio

Para la autenticación completa es necesario un generador de número aleatorio de alta calidad. El resultado de este generador se indica mediante la función RNG_F descrita en la especificación DTCP y disponible con licencia concedida por el DTLA.

III.4.4.3 Criptografía de curva elíptica (ECC)

Estos algoritmos criptográficos se basan en sistemas criptográficos, primitivas y métodos de codificación descritos en IEEE P1363/D3 (11 de mayo de 1998), un proyecto no aprobado sujeto a modificaciones. En versiones subsiguientes de ese proyecto se pueden introducir modificaciones que interfieren la norma IEEE 1363 definitiva de los algoritmos criptográficos aquí descritos.

Se utiliza un criptosistema de curva elíptica (ECC, *elliptic curve cryptosystem*) como base criptográfica para DH y DSA.

El campo de definición clasifica implementaciones ECC. Para este sistema, el campo de definición utilizado es GF(p) donde p es un número primo grande mayor que 3. Una curva elíptica E en el campo GF(p), donde $p > 3$, se define por los parámetros a y b y el conjunto de soluciones (x, y) para la ecuación de curva elíptica junto con un punto suplementario frecuentemente llamado punto en el infinito. El punto en el infinito es el elemento de identidad del grupo abeliano (E, +). La ecuación de la curva elíptica utilizada es:

$$y^2 = x^3 + ax + b \quad \text{donde} \quad 4a^3 + 27b^2 \neq 0$$

donde a, b, x, y, son elementos de GF(p). Un punto P en la curva elíptica está formado por la coordenada x y la coordenada y de una solución de esta ecuación, o el punto en el infinito, y se designa $P = (x_p, y_p)$.

Para EC-DSA y EC-DH, se selecciona un punto de base G en la curva elíptica. Todas las operaciones en el dominio de curva elíptica se calculan en una curva elíptica E definida por GF(p). La clave pública Y^1 (un punto en la curva elíptica) y la clave privada Y^{-1} (un valor escalar que cumple la condición $0 < Y^{-1} < r$) para cada entidad satisface la ecuación:

$$Y^1 = Y^{-1}\, G$$

Al especificar la curva elíptica utilizada:

- El orden del punto de base G tendrá un factor primo grande.
- El sistema tendría la solidez necesaria para resistir ataques de reducción MOV ya que se evitan curvas elípticas de extrema singularidad.

---

[4] Instituto Nacional de Normas y Tecnología (NIST), "Norma de troceado seguro (SHS, *secure hash standard*", publicación FIPS 180-1, 17 de abril de 1995.

III.4.4.3.1 Algoritmo de firma digital de curva elíptica (EC-DSA)

Firma

El algoritmo de firma siguiente se basa en el sistema de firma digital ECSSA que utiliza la primitiva de firma DLSP-DSA y el método de codificación EMSA-SHA-1 definido en IEEE P1363/D3.

Entrada de datos:

- M = datos que deben firmarse
- X^{-1} = clave privada del dispositivo de firma (debe mantenerse secreta)
- p, a, b, G y r = parámetros de curva elíptica asociados con X^{-1}

Resultado:

- $S_{X^{-1}}[M]$ = firma de los datos, M, de 320 bits, basada en la clave privada, X^{-1}

Algoritmo:

Paso 1: Generar un valor aleatorio, u, que satisface la condición $0 < u < r$, utilizando $\mathbf{RNG_F}$. Para cada firma se genera un nuevo valor para u que no será previsible para un tercero en cada cálculo de firma. Calcular el punto de la curva elíptica, $V = uG$.

Paso 2: Calcular $c = x_V \bmod r$ *(coordenada x de V, módulo reducido r)*. Si $c = 0$, ir al **Paso 1**.

Paso 3: Calcular $f = [\text{SHA-1}(M)]_{\text{msb\_bits\_in\_}r}$, es decir, calcular el resumen SHA-1 de M y tomar los bits más significativos del resumen de mensaje que es el mismo número bits que el tamaño de r.

Paso 4: Calcular $d = [u^{-1}(f + cX^{-1})] \bmod r$ *(obsérvese que u^{-1} es el inverso modular de u mod r en tanto que X^{-1} es la clave privada del dispositivo de firma)*. Si $d = 0$, ir al **Paso 1**.

Paso 5: Colocar primero 160 bits de $S_{X^{-1}}[M]$ igual a la representación big endian de c, y los 160 bits siguientes de $S_{X^{-1}}[M]$ igual a la representación big endian de d. ($S_{X^{-1}}[M] = c \parallel d$).

Verificación

El algoritmo de verificación siguiente está basado en el sistema de firma digital ECSSA que utiliza en la primitiva de firma DLVP-DSA y el método de codificación EMSA-SHA-1 definido en la norma IEEE P1363/D3.

Entrada de datos:

- $S_{X^{-1}}[M]$ = firma de 320 bits hipotética ($c \parallel d$) de los datos, M, basada en la clave privada, X^{-1}
- M = datos asociados con la firma
- X^1 = clave pública del dispositivo de firma
- p, a, b, G y r = parámetros de curva elíptica asociados con X^{-1}

Resultado:

- "válido" o "no válido", lo cual indica si la firma hipotética es válida o no válida, respectivamente.

Algoritmo:

Paso 1: Colocar c igual a los primeros 160 bits de $S_{X^{-1}}[M]$ interpretados como representación big endian, y d igual a los 160 bits siguientes de $S_{X^{-1}}[M]$ interpretados como representación big endian. Si c no pertenece a la gama $[1, r-1]$ o d a la gama $[1, r-1]$, se indicará "no válido" y se detendrá.

Paso 2: Calcular $f = [\text{SHA-1}(M)]_{\text{msb\_bits\_in\_}r,}$ es decir, calcular el SHA-1 de M y tomar luego los bits más significativos del resumen de mensaje que es el mismo número de bits que el tamaño de r.

Paso 3: Calcular $h = d^{-1} \bmod r$, $h_1 = (fh) \bmod r$, y $h_2 = (ch) \bmod r$.

Paso 4: Calcular el punto de la curva elíptica $P = (x_P, y_P) = h_1G + h_2X^1$. Si P es igual al punto de la curva elíptica en el infinito, se indicará "no válido" y se detendrá.

Paso 5: Calcular $c' = x_P \bmod r$. Si $c' = c$, se indicará "válido"; en caso contrario, se indicará "no válido."

III.4.4.3.2 Valor de Diffie-Hellman de curva elíptica (EC-DH)

El algoritmo de derivación secreta compartido siguiente se basa en la primitiva ECSVDP-DH definida en IEEE P1363/D3.

Entrada de datos:

- Y_V = valor de la primera fase Diffie-Hellman generado por el otro dispositivo (un punto de la curva elíptica)
- p, a, b, G y r = parámetros de la curva elíptica asociados con X^{-1}

Resultado:

- X_V = valor de la primera fase Diffie-Hellman (un punto de la curva elíptica)
- coordenada x de $X_K Y_V$ = secreto compartido generado por este algoritmo (debe mantenerse el secreto de terceras partes)

Algoritmo:

Paso 1: Generar un entero aleatorio, X_K, en la gama [1, r – 1] utilizando $\mathbf{RNG_F}$. Para cada secreto compartido se genera un nuevo valor para X_K que no será previsible para un tercero. Además, calcular el punto de la curva elíptica, $X_V = X_K G$.

Paso 2: Resultado X_V.

Paso 3: Calcular $X_K Y_V$. Tomar el resultado de la coordenada x de $X_K Y_V$ como secreto compartido.

III.4.4.3.3 Implementación del criptosistema de curva elíptica

Puede implementarse una gama de aplicaciones del criptosistema de curva elíptica compatibles con las primitivas IEEE P1363 descritas en esta subcláusula.

Una eficaz implementación de este sistema puede efectuarse mediante cálculos dentro del espacio Montgomery utilizando nuevas definiciones de las operaciones aritméticas básicas de suma, resta, multiplicación y división[5].

III.4.5 Flujo de protocolos

III.4.5.1 Visión general del flujo de protocolos

Durante la autenticación completa:

1) El dispositivo sumidero pide la autenticación enviando una impugnación aleatoria y su certificado de dispositivo. Esto puede ser el resultado del intento del dispositivo sumidero de acceder a un tren de contenidos protegidos (cuyo EMI se coloca en "ninguna copia", "no más copias" o "una generación de copias"). El dispositivo sumidero puede pedir la autenticación a título especulativo antes de intentar el acceso al tren de contenidos. Si un dispositivo sumidero intenta una autenticación especulativa, la fuente puede rechazar la petición.

2) El dispositivo A devuelve luego una impugnación aleatoria y su certificado de dispositivo. Si el valor del tipo de certificado del otro dispositivo o los campos de formato están reservados, la autenticación será inmediatamente abortada. Tras el intercambio de impugnaciones aleatorias y certificados de dispositivo, cada dispositivo verifica la integridad del certificado del otro dispositivo utilizando EC-DSA. Si se determina que la firma DTLA es válida, los dispositivos examinan la lista de revocación de certificados insertada en sus mensajes de capacidad de renovación del sistema (véase III.7) para verificar que no se ha revocado el otro dispositivo. Si el otro dispositivo no se ha revocado, cada dispositivo calcula un valor de primera fase de intercambio de claves EC-DH (véase III.4.4.3.2).

3) Los dispositivos intercambian mensajes que contienen el valor de primera fase de intercambio de claves EC-DH, el número de la versión de mensaje de capacidad de renovación y la generación del mensaje de capacidad de renovación del sistema almacenado por el dispositivo, y una firma de mensaje que contiene las impugnaciones aleatorias del otro dispositivo concatenadas a los componentes precedentes.

---

[5] Número de aplicación de patente japonesa: TBD.

Los dispositivos verifican los mensajes firmados recibidos mediante la verificación de la firma de mensaje utilizando EC-DSA con la clave pública del otro dispositivo. De este modo se verifica que el mensaje no ha sido manipulado. Si no puede verificarse la firma, el dispositivo se niega a continuar.

Además, mediante la comparación de los números de versiones intercambiados, los dispositivos pueden invocar posteriormente los mecanismos de capacidad de renovación del sistema (para más detalles sobre este procedimiento, véase III.7.2).

Cada dispositivo calcula una clave de autenticación (K_{Auth}) completando el intercambio de claves EC-DH.

En la especificación DTCP disponible con licencia concedida por el DTLA puede hallarse una descripción más detallada del protocolo de autenticación completa y máquinas de estado asociadas.

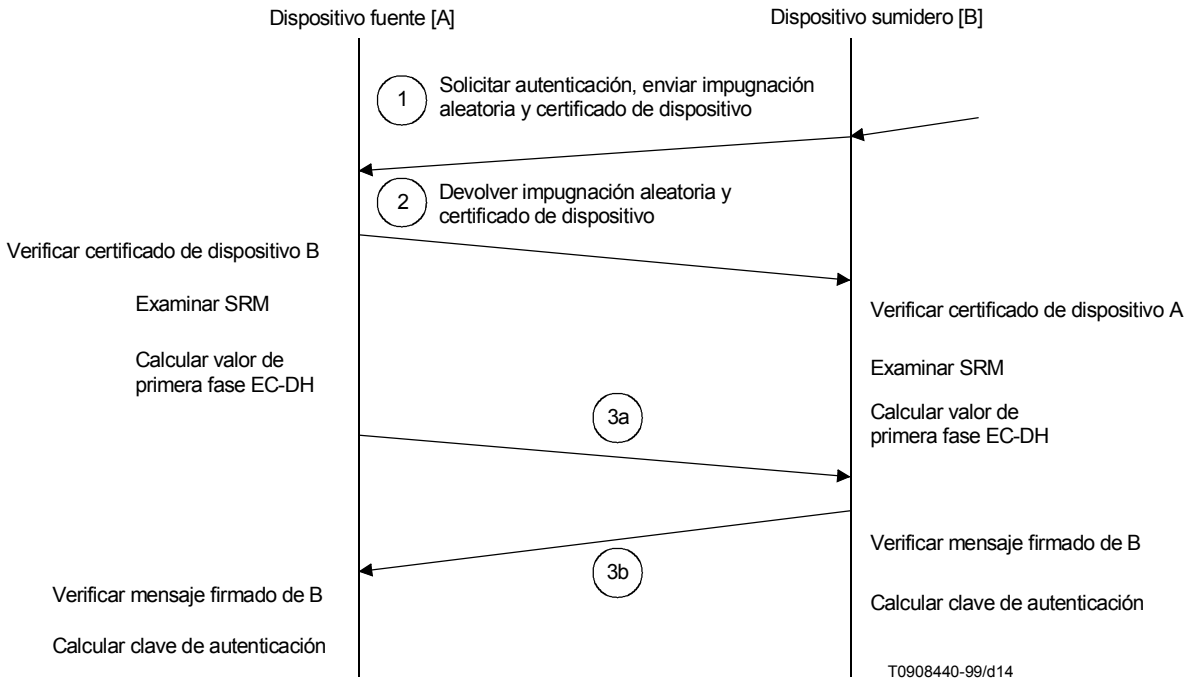


Figura III.10/J.95 – Versión general del flujo de protocolos de autenticación completa

III.5 Autenticación restringida

III.5.1 Introducción

En esta subcláusula se describen la autenticación y el intercambio de claves entre dispositivos fuente y dispositivos sumidero que emplean gestión de claves asimétricas y criptografía de claves comunes para contenidos "una generación de copias" y "no más copias". Este tipo de dispositivos, que generalmente tienen recursos de cálculo limitados, aplican un protocolo de autenticación restringida y no un protocolo de autenticación completa. La autenticación restringida se basa en la utilización de secretos compartidos y en la función troceado para responder a una impugnación aleatoria.

El método de autenticación restringida está basado en un dispositivo capaz de probar que comparte un secreto con otros dispositivos. Un dispositivo autentica otro dispositivo enviando una impugnación aleatoria. Como respuesta, se modifica esa impugnación con el secreto compartido y el resumen.

III.5.2 Notación

La notación introducida en esta subcláusula se utiliza para describir el proceso criptográfico y los protocolos utilizados para la autenticación restringida.

III.5.2.1 Definiciones del DTLA

Los parámetros, claves, constantes y certificados siguientes deben ser generados por el DTLA.

III.5.2.1.1 Elementos generales

Los parámetros definidos en III.4.2.1 son utilizados también durante la autenticación restringida por dispositivos fuente que también soportan la autenticación completa.

III.5.2.1.2 Dispositivo X

X_{Cert} = Certificado concedido por el DTLA al dispositivo X apto y utilizado durante el proceso de autenticación (para más detalles, véase III.5.2.2).

$X_{Kcosrc1} \ldots X_{Kcosrc12}$ = Cada dispositivo que es fuente del contenido "una generación de copias" recibe 12 claves de 64 bits del DTLA.

$X_{Kcosnk1} \ldots X_{Kcosnk12}$ = Cada dispositivo que es sumidero del contenido "una generación de copias" recibe 12 claves de 64 bits del DTLA.

$X_{Knmsrc1} \ldots X_{Knmsrc12}$ = Cada dispositivo que es fuente del contenido "no más copias" recibe 12 claves de 64 bits del DTLA.

$X_{Knmsnk1} \ldots X_{Knmsnk12}$ = Cada dispositivo que es sumidero del contenido "no más copias" recibe 12 claves de 64 bits del DTLA.

X_{KSV} = Este vector de selección de claves (KSV, *key selection vector*) determina qué claves se utilizarán durante el procedimiento de autenticación restringida con este dispositivo. Para los dispositivos que pueden ser fuente y sumidero de contenidos, se pide únicamente un KSV.

Cuadro III.3/J.95 – Longitud de claves y constantes creadas por el DTLA (autenticación restringida)

Clave o variable	Tamaño (bits)
Claves de dispositivo sumidero "una generación de copias" ($X_{Kcosnk1} \ldots X_{Kcosnk12}$)	64 (Cada una)
Claves de dispositivo fuente "una generación de copias" ($X_{Kcosrc1} \ldots X_{Kcosrc12}$)	64 (Cada una)
Claves de dispositivo sumidero "No más copias" ($X_{Knmsnk1} \ldots X_{Knmsnk12}$)	64 (Cada una)
Claves de dispositivo fuente "No más copias" ($X_{Knmsrc1} \ldots X_{Knmsrc12}$)	64 (Cada una)
Vector de selección de claves (X_{KSV})	12

Los dispositivos contienen las claves adecuadas al tipo de contenido y funciones que realizan.

Notación utilizada durante la autenticación restringida

Durante la autenticación restringida, los dispositivos generan y utilizan los siguientes valores adicionales:

X_n = Identificador de un solo uso (impugnaciones aleatoria generada por RNG_R)

K_V, K'_V = Clave de verificación

R, R′ = Respuestas a identificadores a un solo uso

K_{Auth}, K'_{Auth} = Clave de autenticación

Cuadro III.4/J.95 – Longitud de claves y variables generadas por el dispositivo (autenticación restringida)

Clave o variable	Tamaño (bits)
Identificadores de un solo uso (A_n, B_n)	64
Claves de verificación (K_v, K'_v)	64
Respuestas (R, R')	64
Clave de autenticación (K_{Auth}, K'_{Auth})	96

III.5.2.2 Formatos de certificados para dispositivos

En el proceso de autenticación restringida se utiliza un certificado de dispositivo de autenticación restringida. El DTLA asigna cada uno de estos certificados que incluye un ID de dispositivo y una firma generada por el DTLA. Dispondrán de este certificado todos los dispositivos sumidero aptos que soporten únicamente autenticación restringida.

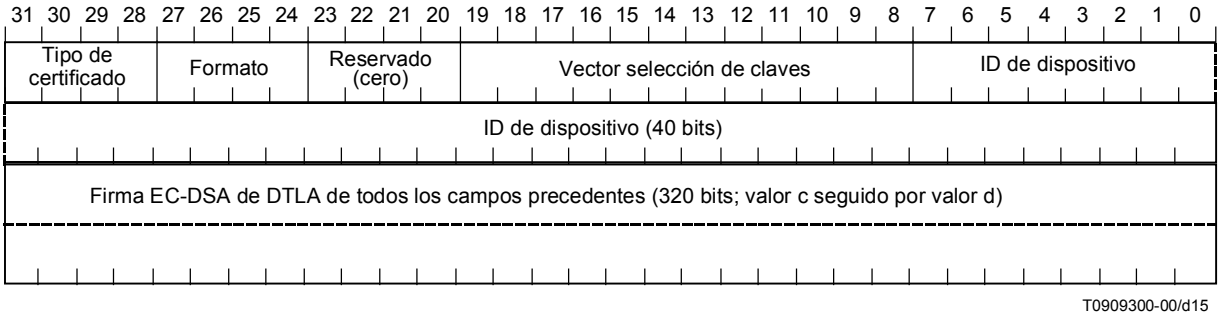


Figura III.11/J.95 – Formato de certificado del dispositivo de autenticación restringida

El certificado del dispositivo de autenticación restringida está formado por los siguientes campos (véase la figura III.11):

- **Tipo de certificado** (4 bits). (Para una descripción de la codificación, véase III.4.2.3.1.)
- **Formato de certificado** (4 bits). (Para una descripción de la codificación, véase III.4.2.3.1.)
- **Campo reservado** (4 bits). Estos bits se reservan para una futura definición y se definen actualmente con un valor de cero.
- **Vector de selección de claves** (X_{KSV}, 12 bits) asignado por el DTLA (véase la figura III.12). Este vector determina qué claves se utilizarán durante el procedimiento de autenticación restringida con este dispositivo. Este KSV se utiliza independientemente del EMI del tren que se va a tratar o que el dispositivo se utilice como fuente o sumidero del contenido. La codificación de este campo es la siguiente:
- El número **ID de dispositivo** (X_{ID}, 40 bits) asignado por el DTLA.
- Una **firma EC-DSA** del DTLA de los componentes enumerados anteriormente (320 bits)

El tamaño total de un formato de certificado de dispositivo de autenticación restringida es 48 bytes.

III.5.2.3 Generador de número aleatorio

Para la autenticación restringida se requiere un generador de número aleatorio. El resultado de este generador se indica mediante la función RNG_R. Para la autenticación restringida puede utilizarse tanto RNG_R como RNG_F, tal como se indica en la especificación DTCP disponible con licencia concedida por el DTLA.

Figura III.12/J.95 – Vector de selección de claves

III.5.3 Flujo de protocolos

III.5.3.1 Visión general del flujo de protocolos

En la figura III.13 se presenta una visión general del flujo de protocolos de autenticación restringida.

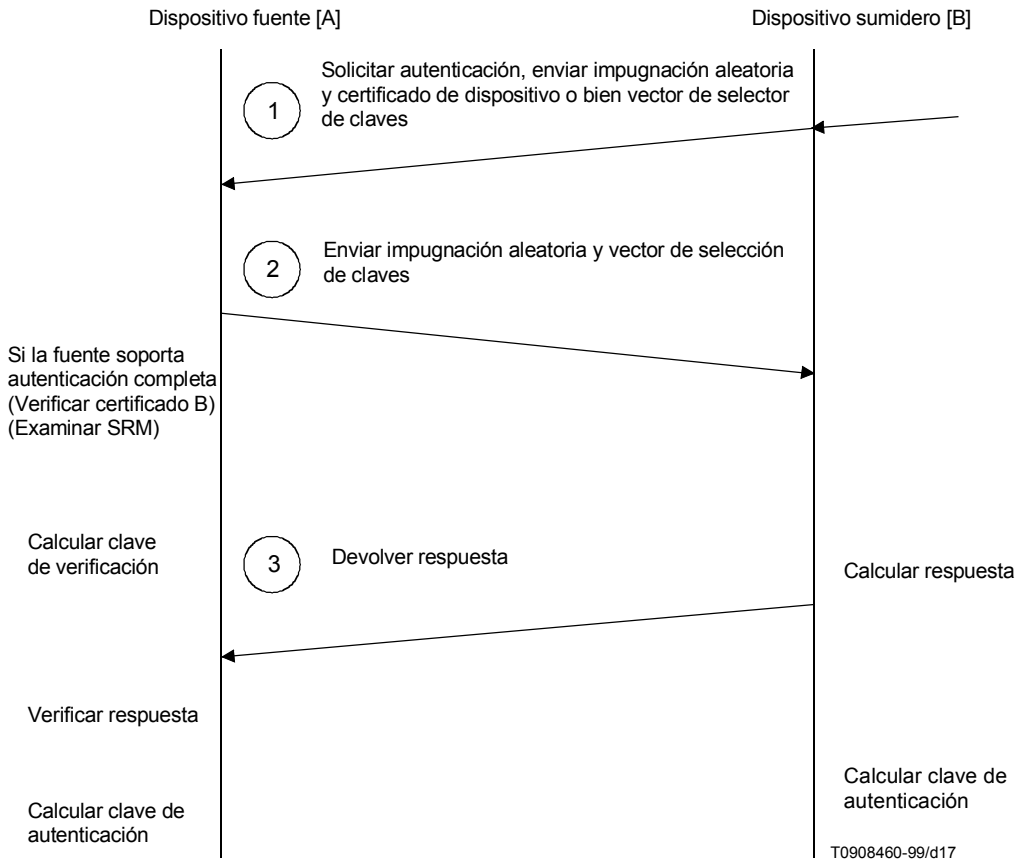


Figura III.13/J.95 – Visión general del flujo de protocolos de autenticación restringida

Durante la autenticación restringida:

1) El dispositivo sumidero inicia el protocolo de autenticación enviando una petición de impugnación asíncrona al dispositivo fuente. Esta petición contiene el tipo de clave de intercambio que compartirán los dispositivos fuente y sumidero así como el número aleatorio generado por el dispositivo sumidero utilizando RNG_R. Si el dispositivo sumidero sabe que el dispositivo fuente no tiene una capacidad de autenticación completa, envía su KSV a la fuente; en caso contrario, envía su certificado de dispositivo de autenticación restringida.

2) El dispositivo fuente genera una impugnación aleatoria utilizando RNG_R y lo envía al dispositivo sumidero. Si el dispositivo fuente soporta autenticación completa, extrae el ID de dispositivo del sumidero a partir del certificado enviado por éste. Verifica luego:

   a) que el certificado enviado por el dispositivo sumidero es válido; y

   b) que el ID de dispositivo del sumidero no figura en la lista de revocación de certificación en el mensaje capacidad de renovación del sistema almacenado en el dispositivo fuente.

Además, si el valor del tipo de certificado del otro dispositivo o los campos de formato están reservados, la autenticación será inmediatamente abortada. Si estas verificaciones se completan satisfactoriamente, la fuente continúa el protocolo calculando la clave de verificación.

3) Tras recibir una impugnación aleatoria del dispositivo fuente, el dispositivo sumidero calcula una respuesta utilizando una clave de verificación que calcula y la envía a la fuente.

4) Una vez que el dispositivo sumidero devuelve una respuesta, el dispositivo fuente la compara con datos similares generados en el lado fuente utilizando su clave de verificación. Si esa comparación coincide con su propio cálculo, el dispositivo sumidero ha sido verificado y autenticado. Si no coincide, el dispositivo fuente rechazará al dispositivo sumidero. Finalmente, cada dispositivo calcula la clave de autenticación.

En la especificación DTCP disponible con licencia concedida por el DTLA puede hallarse una descripción más completa del protocolo de autenticación restringida y máquinas de estado asociadas.

III.6 Gestión y protección del canal de contenidos

III.6.1 Introducción

En esta subcláusula se describen los mecanismos utilizados para :

1) compartir una clave de intercambio entre un dispositivo fuente y un dispositivo sumidero; y

2) establecer y gestionar el canal isócrono criptado por el que circulan los contenidos protegidos.

Antes de establecer un canal de contenidos se completará la autenticación completa o bien la autenticación restringida (según las capacidades del dispositivo).

III.6.2 Claves de la gestión de contenidos

III.6.2.1 Clave de intercambios (K_x, *exchange key*)

Se establece una serie común de claves de intercambio (K_x) entre un dispositivo fuente y todos los dispositivos sumidero que han llevado a término el procedimiento de autenticación apropiado (ya sea completa o restringida) con el dispositivo fuente necesario para tratar los contenidos con un valor EMI específico (véase III.6.4.2). Además, si los códigos[6] de contenido opcionales se soportan mutuamente, se establecen claves de intercambio para utilizarlas con ellos en el contenido "ninguna copia".

En III.6.3.1 se describe el procedimiento para establecer una clave de intercambio.

III.6.2.2 Clave de contenido (K_c, *content key*)

La **clave de contenido** (K_c) se utiliza como la clave de la máquina de criptación de contenidos. K_c se calcula a partir de los tres valores que figuran a continuación:

- Clave de intercambio K_x asignada al EMI y la longitud de códigos claves que se utilizan para proteger el contenido.

---

6 Aplicable únicamente a claves de intercambio establecidas como resultado de la autenticación completa entre dispositivos que soporten la máscara de la capacidad opcional en el certificado de dispositivo.

- Un número aleatorio N_c generado por el dispositivo fuente (utilizando la función RNG_F para dispositivos que soporten autenticación completa y la función RNG_R para los que sólo soporten autenticación restringida) que se envía con texto ordinario a todos los dispositivos sumidero en uno o varios paquetes asíncronos.
- Valor constante C_a o C_b o C_c, que corresponde al EMI en el encabezamiento de paquete.

La clave de contenido se genera del modo siguiente:

$$K_c = J[K_x, N_c, f[\text{EMI}]]$$

donde:

f[EMI] = C_a si EMI es modo A

f[EMI] = C_b si EMI es modo B

f[EMI] = C_c si EMI es modo C

C_a, C_b y C_c son constantes de secretos universales asignados por el DTLA. Los valores de estas constantes figuran en la especificación DTCP accesible con licencia concedida por el DTLA. En este apéndice se describe también la definición de función J[].

III.6.2.3 Tamaño de las claves

En el cuadro III.5 figura la longitud de las claves y constantes descritas precedentemente.

Cuadro III.5/J.95 – Longitud de claves y constantes (gestión de canal de contenidos)

Clave, variable o constante	Tamaño (bits)
Claves de intercambio (K_x)	96
Claves de intercambio aleatorizadas (K_{sx})	96
Constantes (C_a, C_b, C_c)	24
Clave de contenido para código de línea de base (K_c)	56
Clave de contenido para códigos opcionales [a] (K_c)	56-64
Indicador de un solo uso para canal de contenido (N_c)	64
[a] Las características de esta especificación rotuladas como "opcionales" describen capacidades cuya utilización no ha sido aún establecida por el DTLA.	

III.6.3 Flujo de protocolos

III.6.3.1 Establecimiento de claves de intercambio

Una vez completada la autenticación completa o restringida, el dispositivo fuente establece la clave o claves de intercambio descritas en III.6.2.1. El procedimiento utilizado para cada clave es el siguiente:

1) El dispositivo fuente asigna un valor aleatorio a la clave de intercambio (K_x) establecida.
2) A continuación aleatoriza la clave K_x utilizando K_{Auth}, cuyo resultado es K_{sx}, según la función descrita en la Especificación DTCP disponible con licencia concedida por el DTLA.
3) El dispositivo fuente envía K_{sx} al dispositivo sumidero.
4) El dispositivo sumidero desaleatoriza la clave K_{sx} utilizando K'_{Auth} para determinar la clave de intercambio compartida K_x, según la función descrita en la Especificación DTCP disponible con licencia concedida por el DTLA.

El dispositivo fuente repite los pasos mencionados para todas las claves de intercambio necesarias entre él y el dispositivo sumidero.

Finalmente, los dispositivos actualizan el SRM si se determina que es necesario durante el proceso de autenticación completa (véase III.4)

Los dispositivos siguen manteniendo su autenticación mientras conservan claves de intercambio válidas. La clave de intercambio puede utilizarse repetidamente para configurar y administrar la seguridad de los trenes de contenidos que gozan de derechos de autor sin una nueva autenticación. Se recomienda que los dispositivos fuente hagan expirar sus claves de intercambio cuando detienen todos los resultados isócronos y, además, cuando se desconectan del bus.

III.6.3.2 Establecimiento de claves de contenido

En esta subcláusula se describe el mecanismo para establecer las claves de contenido (K_c) utilizadas para criptar y descriptar los contenidos que se intercambian entre los dispositivos fuente y sumidero (véase la figura III.14).

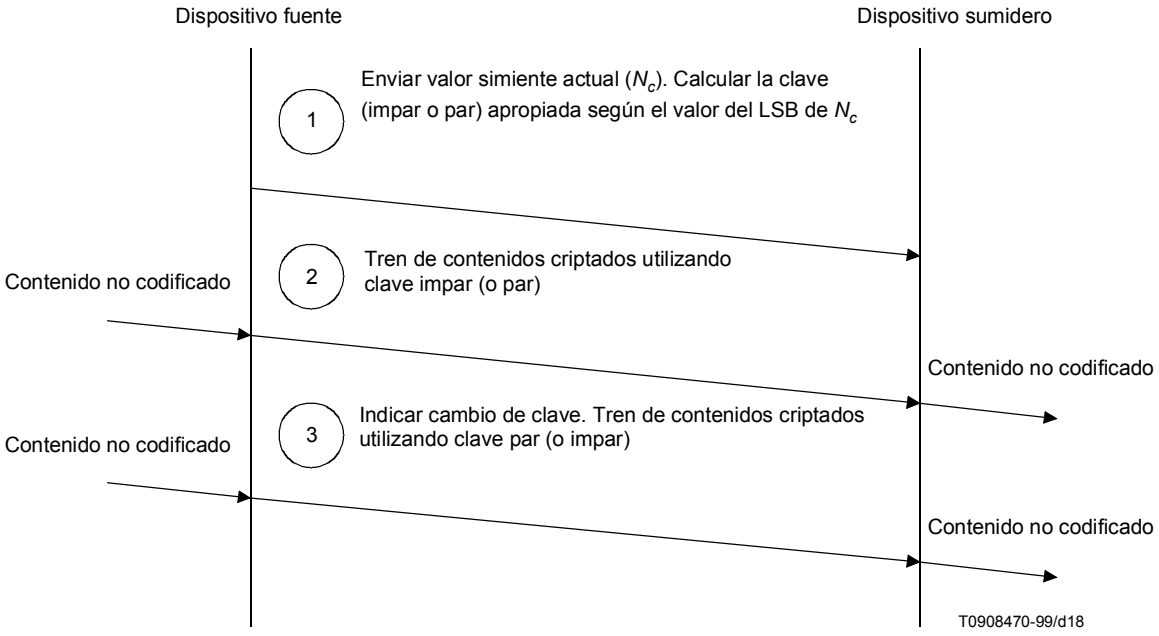


Figura III.14/J.95 – Visión general del establecimiento de canal de contenidos y del flujo de protocolos de gestión

Las claves de contenido se establecen entre el dispositivo fuente y el dispositivo sumidero del modo siguiente:

1) Cuando el dispositivo fuente empieza a enviar contenidos genera un número aleatorio de 64 bits como valor inicial de la simiente (N_c) de la clave de contenido. La simiente inicial se denomina impar o par según su bit menos significativo. Si se establecen canales de contenido subsiguientes, puede utilizarse como simiente el valor actual de N_c del canal o canales de contenidos activos.

2) El dispositivo fuente empieza a transmitir el contenido utilizando la clave de contenido impar o par (K_c) que corresponde a la referencia anterior de la simiente inicial para criptar el contenido. La clave de contenido se calcula por el dispositivo fuente utilizando la función J, la clave de intercambio K_x, la simiente (N_c) y $f[EMI]$). Se utiliza un bit en el encabezamiento de paquete IEEE 1394 para indicar cuál es la clave (IMPAR o PAR) que se utiliza para criptar un determinado paquete de contenidos. Si la simiente inicial es IMPAR, el bit impar/par en el encabezamiento de paquete IEEE 1394 se coloca en impar; de lo contrario, se coloca en par.

Al recibir la simiente N_c, el dispositivo sumidero verifica si el bit menos significativo de N_c coincide con el estado del bit impar/par. Si ambos bits son idénticos, el dispositivo sumidero calcula la clave de contenido actual utilizando la función J, K_X, *f[EMI]* y N_c. Si esos bits son distintos, esto indica que se ha cambiado la clave y el dispositivo sumidero calcula la clave de contenido actual utilizando el método siguiente:

a) se calcula $N_c + 1 \; mod \; 2^{64}$ como nueva simiente; luego

b) se calcula la clave de contenido con el método precedente utilizando la nueva simiente en lugar de la simiente original enviada desde el dispositivo fuente.

El dispositivo fuente prepara la clave de contenidos siguiente calculando K_c y utilizando el mismo proceso que para el cálculo inicial a excepción de que se incrementa la simiente (N_c).

Periódicamente el dispositivo fuente modificará las claves de contenido para conservar la solidez de la protección de contenidos. Para modificar las claves, el dispositivo fuente empieza a criptar la nueva clave calculada anteriormente e indica esta modificación pasando al estado del bit impar/par en el encabezamiento de paquete IEEE 1394. El periodo mínimo para cambiar la clave de contenido es de 30 s; el periodo máximo, de 120 s. El tiempo de duración de K_c oscila entre 30 s y 2 min. Un dispositivo fuente no debe incrementar el contador del tiempo de duración de la clave de contenido cuando está calculando únicamente contenidos marcados con un valor EMI (véase III.6.4.2) de "sin restricción de copias". Cuando un dispositivo suspende todos los resultados isócronos debe reiniciar su contador.

En III.8 figura el flujo de protocolos necesarios para establecer la clave de contenido utilizando transacciones IEEE 1394.

III.6.3.3 Bit impar/par

El bit impar/par (tercer bit del campo de sincronización del encabezamiento de paquete isócrono IEEE 1394) se utiliza para indicar cuál es la clave de contenido (K_c) que se utiliza para proteger el canal de contenidos (véase la figura III.15). El bit impar/par existe únicamente cuando el valor del campo marcador es 01A. El valor "0" indica que debe utilizarse la clave par y "1", que debe utilizarse la clave impar. La clave impar y la clave par se utilizan y actualizan alternativamente. El bit impar/par sólo puede modificarse en paquetes isócronos que contienen el comienzo de una nueva trama de criptación o bien son paquetes en reposo entre tramas de criptación. Si un paquete isócrono contiene tramos de más de una trama de criptación, la modificación en la clave se aplica a la primera trama de criptación que comienza en el paquete.

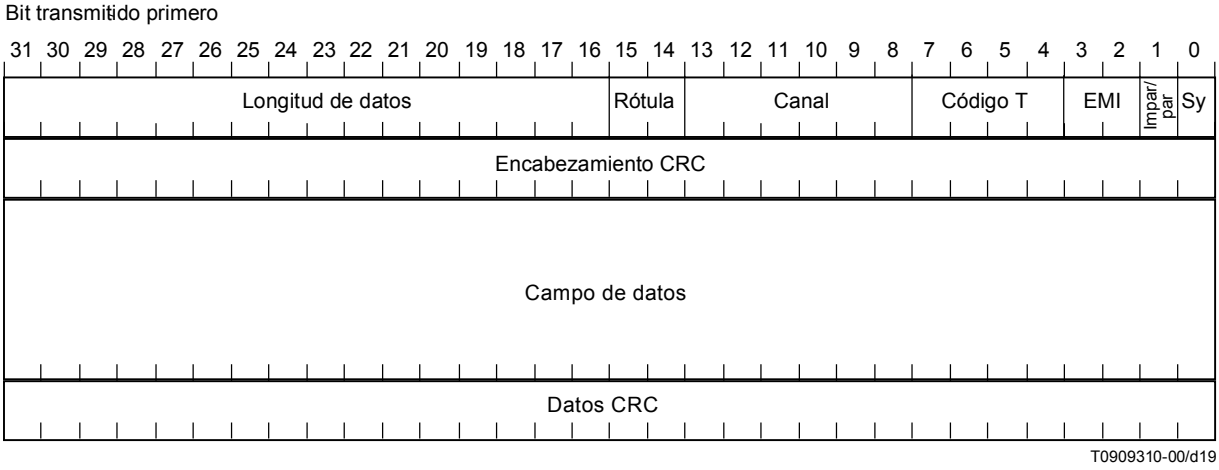


Figura III.15/J.95 – Localización del bit impar/par en el encabezamiento de paquete

III.6.4 Información de control de copias (CCI)

La **información de control de copias (CCI)** especifica los atributos del contenido con respecto al sistema de protección de ese contenido. Se soportan dos mecanismos CCI: CCI insertada e indicador de modo criptación.

III.6.4.1 CCI insertada

La CCI insertada se transporta como parte del tren de contenidos. Muchos formatos de contenido, incluido MPEG, tienen campos asignados para transportar la CCI asociada con el tren de contenidos. La integridad de la CCI insertada está asegurada porque la manipulación del tren de contenidos da como resultado una descriptación errónea del contenido.

III.6.4.2 Indicador de modo criptación (EMI)

El indicador de modo criptación (EMI) proporciona un mecanismo de fácil acceso pero seguro para indicar la CCI asociada con un tren de contenidos digitales. Para los buses serie IEEE 1394, el EMI se coloca en los dos bits más significativos del campo de sincronización del encabezamiento de paquete indicado en la figura III.16. Los bits EMI existen únicamente cuando el valor del campo marcador es 01. Al poder acceder con facilidad a la localización del EMI, los dispositivos pueden determinar inmediatamente la CCI del tren de contenidos sin necesidad de decodificar el formato de transporte de contenidos para extraer la CCI insertada. Esta capacidad es fundamental para habilitar dispositivos de grabación de trenes de bits (por ejemplo, magnetoscopios digitales) que no reconocen ni pueden decodificar formatos de contenido específico.

Los bits EMI pueden modificarse únicamente en paquetes isócronos que contienen el comienzo de una nueva trama de criptación o bien son paquetes en reposo entre tramas de criptación. Si un paquete isócrono contiene porciones de más de una trama de criptación, la modificación del EMI se aplica a la primera trama de encriptación que comienza en el paquete.

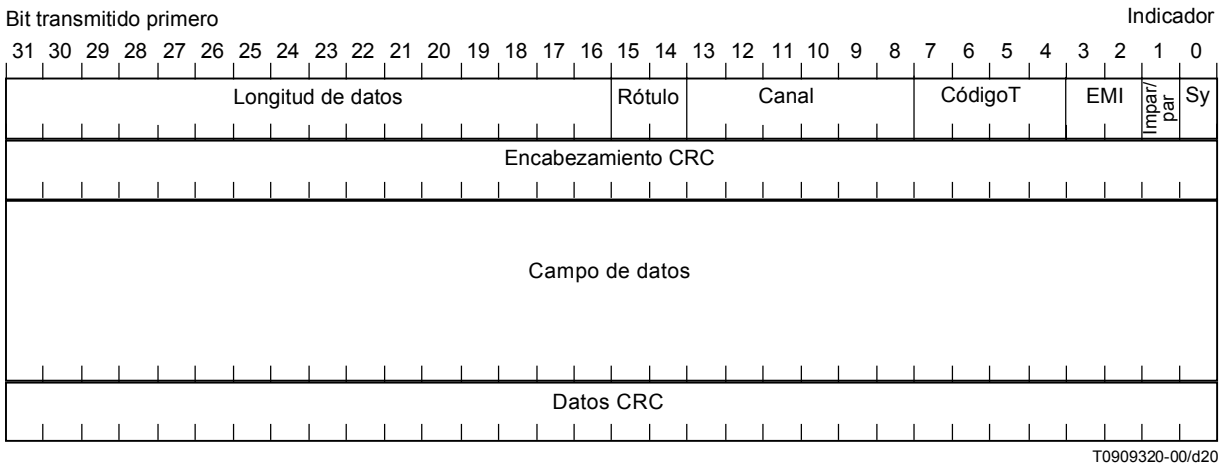


Figura III.16/J.95 – Localización de EMI

El EMI indica el modo de criptación aplicado a un tren de contenidos:

- Los dispositivos fuente con licencia seleccionarán el modo de criptación adecuado según las características del tren de contenidos y colocarán su EMI en consecuencia. Si el tren de contenidos está formado por subtrenes múltiples con distintas CCI insertadas, se utilizará la CCI insertada más estricta para colocar el EMI.

- Los dispositivos sumidero con licencia seleccionarán el modo de criptación correcto indicado por el EMI.

Si los bits EMI se manipulan, los modos criptación y descriptación no coincidirán, lo que dará como resultado una descriptación errónea del contenido.

Cuadro III.6/J.95 –Codificación EMI

Modo EMI	Valor EMI	Significado	Autenticación requerida
Modo A	11	Ninguna copia	Completa
Modo B	10	Una generación de copias	Restringida o completa
Modo C	01	No más copias	Restringida o completa
N.A.[a)]	00	Sin restricción de copias	Ninguna, no criptada
[a)] No se aplica. No se define ningún modo EMI para un codificación de 00.			

- Se utiliza una codificación de 00 para indicar que la copia del contenido no tiene restricciones. Para proteger este contenido no es necesario ninguna autenticación ni criptación.

- Si no debe hacerse ninguna copia del contenido (por ejemplo, contenido de medios grabados previamente con un valor del sistema de gestión de generación de copias (CGMS, *copy generation management system*) de 11), se utiliza una codificación EMI de 11. Este contenido puede intercambiarse únicamente entre dispositivos que han completado satisfactoriamente el procedimiento de autenticación completa.

- Una codificación EMI de 10 indica que se puede efectuar una generación de copias (por ejemplo, contenido de medios grabados previamente con un valor CGMS de 10). Los dispositivos que intercambian este contenido pueden utilizar autenticación completa o autenticación restringida.

- Si se copia un contenido con EMI = 10, los futuros intercambios a través de una interconexión digital se marcarán con una codificación EMI de 01, lo cual indica que ya se ha realizado una generación de copias.

III.6.4.3 Relación entre CCI insertada y EMI

Un tren de contenidos protegido puede estar formado por uno o más programas. A cada uno de estos programas se puede asignar un nivel diferente de CCI insertada. Como EMI está asociada al tren de contenidos completo, es posible que ese tren esté formado por múltiples programas y que el EMI no coincida con el valor de CCI insertada de cada uno de los programas protegidos. Si se produce un conflicto, para el EMI se utilizará el valor de CCI insertada más restrictivo.

Cuadro III.7/J.95 – Relación entre EMI y CCI insertada

EMI	CCI insertada para cada programa			
	00	01	10	11
Modo A (ninguna copia)	Permitida	Permitida[a)]	Permitida	Permitida
Modo B (una generación de copias)	Permitida	Prohibida	Permitida	Prohibida
Modo C (no más copias)	Permitida	Permitida	Permitida	Prohibida
N.A. (sin restricción de copias)	Permitida	Prohibida	Prohibida	Prohibida
[a)] No se utiliza habitualmente.				

III.6.4.4 Tratamiento de EMI/CCI insertada para funciones de dispositivo comunes

En esta subcláusula se presenta el comportamiento de las funciones de dispositivo comunes según su capacidad para enviar/recibir EMI y detectar/modificar la CCI insertada. Pueden autorizarse otras funciones no enumeradas en esta subcláusula mientras sean compatibles con las disposiciones de la presente especificación.

III.6.4.4.1 Función fuente con formato de reconocimiento

Una función fuente con formato de reconocimiento (veáse el cuadro III.8) puede reconocer la CCI insertada del tren de contenidos que se transmite.

Cuadro III.8/J.95 – Función fuente con formato de reconocimiento para el tratamiento de CCI

CCI de programas insertada				**EMI**
00	**01**	**10**	**11**	
Irrelevante	(Nota)	Irrelevante	Presente	Modo A (ninguna copia)
Irrelevante	No puede estar presente	Presente	No puede estar presente	Modo B (una generación de copias)
Irrelevante	Presente	No puede estar presente	No puede estar presente	Modo C (no más copias)
Presente	No puede estar presente	No puede estar presente	No puede estar presente	N.A. (sin restricción de copias)
Otras combinaciones				Transmisión prohibida
NOTA – Irrelevante, no se utiliza habitualmente.				

III.6.4.4.2 Función fuente con formato sin reconocimiento

Una función fuente con formato sin reconocimiento (véase el cuadro III.9) no necesita reconocer la CCI insertada del tren de contenidos que se transmite.

Cuadro III.9/J.95 – Función fuente con formato sin reconocimiento para el tratamiento de CCI

EMI o CCI[a] grabada de contenido de fuente	**EMI utilizada para transmisión**
Ninguna copia	Modo A (ninguna copia)
Una generación de copias	Modo B (una generación de copias)
No más copias	Modo C (no más copias)
Sin restricción de copias	N.A. (sin restricción de copias)
a) La CCI grabada es la información de control de copias no insertada en el programa de contenidos y es necesario conocer el formato del contenido para extraerla.	

III.6.4.4.3 Función grabación con formato de reconocimiento

Una función grabación con formato de reconocimiento (véase el cuadro III.10) reconoce la CCI insertada de un programa recibido antes de inscribirla en un medio de grabación.

Cuadro III.10/J.95 – Función grabación con formato de reconocimiento para el tratamiento de CCI

EMI	CCI insertada de programa			
	00	01	10	11
Modo A (ninguna copia)	Grabable	No grabar	(Nota 1)	No grabar
Modo B (una generación de copias)	Grabable	Descartar el tren de contenidos completo (Nota 2)	(Nota 1)	Descartar el tren de contenidos completo (Nota 2)
Modo C (no más copias)	Grabable	No grabar	No grabar	Descartar el tren de contenidos completo (Nota 2)
NOTA 1 – Si la función de grabación soporta la grabación de un valor CCI de no más copias, dicho valor será grabado con el programa. De lo contrario, se grabará la CCI de ninguna copia. NOTA 2 – Si la función detecta esta combinación de CCI entre los programas que está grabando, se descarta el tren de contenidos completo.				

III.6.4.4.4 Función sumidero con formato de reconocimiento

Una función sumidero con formato de reconocimiento puede reconocer la CCI insertada del contenido recibido.

En el cuadro III.11 se observa la CCI insertada de programas contenida dentro del tren de contenidos que puede ser recibido.

Cuadro III.11/J.95 – Función de sumidero de formato con reconocimiento para el tratamiento de CCI

EMI	CCI insertada de programa			
	00	01	10	11
Modo A (ninguna copia)	Disponible para el procesamiento	Disponible para el procesamiento (Nota 2)	Disponible para el procesamiento	Disponible para el procesamiento
Modo B (una generación de copias)	Disponible para el procesamiento	Descartar el tren de contenidos completo (Nota 1)	Disponible para el procesamiento	Descartar el tren de contenidos completo (Nota 1)
Modo C (no más copias)	Disponible para el procesamiento	Disponible para el procesamiento	Disponible para el procesamiento (Nota 3)	Descartar el tren de contenidos completo (Nota 1)
NOTA 1 – Si la función detecta esta combinación de CCI entre los programas que está grabando, se descarta el tren de contenidos completo. NOTA 2 – Generalmente no se utiliza. NOTA 3 – Si el dispositivo tiene una regla para tratar no más copias, este programa será tratado de conformidad con dicha regla. De lo contrario, se tratará como ninguna copia.				

III.6.4.4.5 Función grabación con formato sin reconocimiento

Una función grabación con formato sin reconocimiento (véase el cuadro III.12) puede grabar contenidos con el EMI adecuado en medios de grabación.

Cuadro III.12/J.95 – Función grabación con formato sin reconocimiento para el tratamiento de CCI

EMI del tren recibido	CCI[a)] grabada que se inscribe en medios de grabación del usuario
Modo A (ninguna copia)	No puede grabarse el tren de contenidos
Modo B (una generación de copias)	No más copias
Modo C (no más copias)	No puede grabarse el tren de contenidos
a) La CCI grabada es la información de control de copias no insertada en el programa de contenidos y no es necesario conocer el formato del contenido para extraerla.	

III.6.4.4.6 Función sumidero con formato sin reconocimiento

Para esta función, el contenido debe tratarse de forma compatible con sus categorías de dispositivo comunes EMI 6.5.

Los dispositivos pueden soportar ninguna o algunas funciones descritas en III.6.4.4.

Los tipos más comunes de dispositivos de funciones fijas comprenden los siguientes, pero no se limitan a ellos:

1) El **dispositivo de fuente de contenido grabado previamente con formato de reconocimiento** tiene una función fuente con formato de reconocimiento (por ejemplo, lector DVD).

2) El **dispositivo de fuente/decodificación de contenido de entrega en tiempo en real con formato de reconocimiento** tiene una función fuente con formato de reconocimiento y una función sumidero con formato de reconocimiento (por ejemplo, adaptador multimedios o televisión digital).

3) El **registrador y lector con formato de reconocimiento** tiene una función fuente con formato de reconocimiento, una función sumidero con formato de reconocimiento y una función grabación con formato de reconocimiento (por ejemplo, magnetoscopio DV).

4) El **registrador y lector con formato sin reconocimiento** tiene una función fuente con formato sin reconocimiento y una función grabación con formato sin reconocimiento (por ejemplo, magnetoscopio D-VHS).

5) El **puente de bus con formato sin reconocimiento** tiene una función fuente con formato sin reconocimiento y una función sumidero con formato sin reconocimiento (por ejemplo, puente de bus IEEE 1394 a IEEE 1394).

III.6.5 Códigos de canal de contenidos

Todos los dispositivos aptos soportan el código de línea de base y los códigos opcionales, posiblemente adicionales, para la protección de contenidos[7].

III.6.5.1 Código de línea de base

Para asegurar el interfuncionamiento, todos los dispositivos y aplicaciones deben soportar, como mínimo, código de bloque M6-S56 que utiliza el modo concatenación de bloque de códigos convertidos (C-CBC, *converted cipher-block-chaining*). Este código se describe en forma más completa en la especificación DTCP disponible con licencia concedida por el DTLA.

---

[7] Las características de esta especificación rotuladas como "opcionales" describen capacidades cuya utilización no ha sido aún establecida por el DTLA.

III.6.5.2 Formatos de criptación de contenidos

En el cuadro III.13 figuran los formatos de criptación de contenidos que se utilizarán con los códigos de canal de contenidos.

Cuadro III.13/J.95 – Formatos de encripción de contenidos

Formato de datos	Trama de criptación	Tamaño
Tren de transporte MPEG	Paquete del tren de transporte CEI 61883-4	188 bytes
DV (formato SD)	Unidad de transferencia isócrona CEI 61883-2	480 bytes
Audio	Datos conformes a CEI 61883-6 (CEI-PAS) CEI 958 para 2 canales	8 bytes

III.6.5.3 Soporte de códigos de canal de contenidos opcionales

El soporte de estos códigos se define en III.4 (Máscara de capacidad de dispositivos), la sección A.6 (Establecimiento de múltiples valores K_X), y en la sección A.8 (Codificación de selección de códigos en el conjunto de instrucciones de interfaz digital AV/C). Los algoritmos de códigos de canal de contenidos opcionales con el modo concatenación de bloque de códigos convertidos (C-CBC) se describen en la especificación DTCP disponible con licencia concedida por el DTLA[8].

III.7 Capacidad de renovación del sistema

III.7.1 Introducción

Los dispositivos aptos que soportan la autenticación completa pueden recibir y procesar mensajes de capacidad de renovación del sistema (SRM) creados por el DTLA y distribuidos con contenidos. Estos mensajes se utilizan para asegurar la integridad del sistema a largo plazo.

III.7.1.1 Componentes y organización del mensaje SRM

Un mensaje de capacidad de renovación del sistema (SRM) tiene diversos componentes:

- Un campo **Tipo** de mensaje (4 bits). Este campo tiene la misma codificación utilizada para el campo de tipo certificado en los certificados de dispositivo. Para una descripción del mismo, véase III.4.2.3.1. La única codificación actualmente definida es 0, que indica que el mensaje corresponde a la protección de contenidos IEEE 1394.
- Un campo **Generación** de mensaje (SRMM) (4 bits). Este campo especifica la generación del mensaje SRM y se utiliza para asegurar la extensibilidad del mecanismo SRM. Actualmente, la única codificación definida es 0, que indica un SRM de primera generación con un tamaño máximo indicado en la especificación DTCP disponible con licencia concedida por el DTLA. Actualmente, están reservadas otras codificaciones. Este valor permanece invariable incluso si el dispositivo puede almacenar únicamente una parte del SRM (por ejemplo, X_{SRMC} <= SRMM).
- Campo reservado (8 bits). Estos bits se reservan para una futura definición y se definen actualmente con un valor de cero.
- Número de versión del mensaje de capacidad de renovación del sistema (SRMV, *system renewability message version number*) que aumenta de forma monótona (16 bits). Este valor se intercambia como X_{SRMV} durante la autenticación completa. No se vuelve a colocar a cero cuando se cambia el campo de generación de mensajes.
- Longitud de la lista de revocación de certificados (CRL, *certificate revocation list*) (16 bits). Este campo especifica el tamaño (en bytes) de la CRL incluidos el campo de longitud CRL (2 bytes), las entradas CRL (longitud variable) y la firma DTLA (40 bytes).
- Entradas CRL (tamaño variable). La CRL se utiliza para revocar los certificados de dispositivos cuya seguridad se ha negociado. Su formato se describe en la siguiente subcláusula.
- La firma EC-DSA del DTLA de estos componentes utilizando L^{-1} (320 bits).

---

[8] Las características de esta especificación rotuladas como "opcionales" describen capacidades cuya utilización no ha sido aún establecida por el DTLA.

En la figura III.17 se muestra la estructura de los mensajes SRM de primera generación. Los campos en los cuatro primeros bytes del mensaje SRM comprenden el encabezamiento SRM.

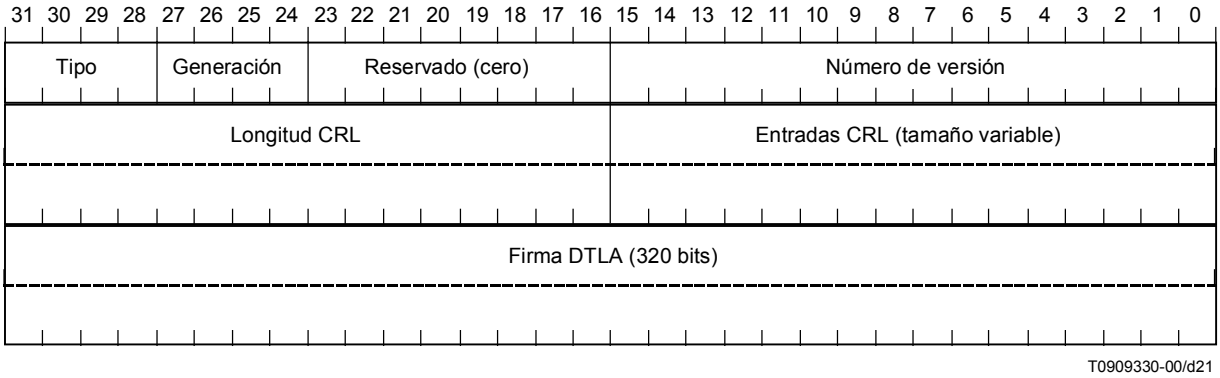


Figura III.17/J.95 – Estructura del mensaje de capacidad de renovación del sistema de primera generación

III.7.1.1.1 Lista de revocación de certificados (CRL)

La **lista de revocación de certificados (CRL)** identifica los dispositivos que ya no son aptos. Está formada por el campo de longitud CRL que indica la longitud de la lista en bytes. Este campo es seguido por una secuencia de bloques de tipo entrada (1 byte) que son seguidos a la vez por el número de entradas CLR indicadas por el bloque de tipo entrada. Se soportan dos tipos de bloque de entrada. Uno de ellos proporciona la revocación de dispositivos y el segundo, la revocación de bloques de hasta 65 535 dispositivos.

III.7.1.1.2 Firma EC-DSA del DTLA

El campo de firma EC-DSA del DTLA es una firma de 320 bits calculada en todos los campos precedentes del SRM utilizando la clave privada L^{-1} EC-DSA del DTLA. Este campo se utiliza para verificar la integridad del SRM utilizando la clave pública L^{1} EC-DSA del DTLA.

III.7.1.2 Crecimiento gradual del SRM

Para garantizar el crecimiento gradual de esta solución de capacidad de renovación, se puede ampliar el formato SRM (véase la figura III.18). Las ampliaciones de próxima generación (CRL y posiblemente otros mecanismos) de un formato SRM de actual generación deben ser adjuntados al SRM de actual generación para asegurar la compatibilidad hacia atrás con dispositivos que soporten únicamente mensajes SRM de generación anterior. Los dispositivos sólo son responsables de soportar la generación de SRM requerida por el DTLA en el momento en que se fabricó el dispositivo. En el acuerdo para la concesión de licencias del DTLA se indican las condiciones en que el DTLA autorizará los SRM de nueva generación.

III.7.2 Actualización de los SRM

Los mensajes de capacidad de renovación del sistema pueden actualizarse a partir de:

- otros dispositivos aptos (conectados por medios de transmisión digitales) que tienen una lista más reciente;
- medios de contenidos grabados previamente;
- trenes de contenidos a través de dispositivos aptos en tiempo real que pueden comunicarse externamente (por ejemplo, a través de Internet, líneas telefónicas, sistemas de cable, satélites para radiodifusión directa, etc.)

El procedimiento general para la actualización de los SRM es el siguiente:

1) Examinar el número de versión del nuevo SRM.
2) Verificar que el número de versión del SRM es mayor que el almacenado en la memoria no volátil.
3) Verificar la integridad con la clave pública DTLA (L^{1}).
4) Si el SRM es válido y nuevo, almacenar todo lo que pueda ajustarse a la versión más reciente del mensaje en la memoria no volátil del dispositivo.

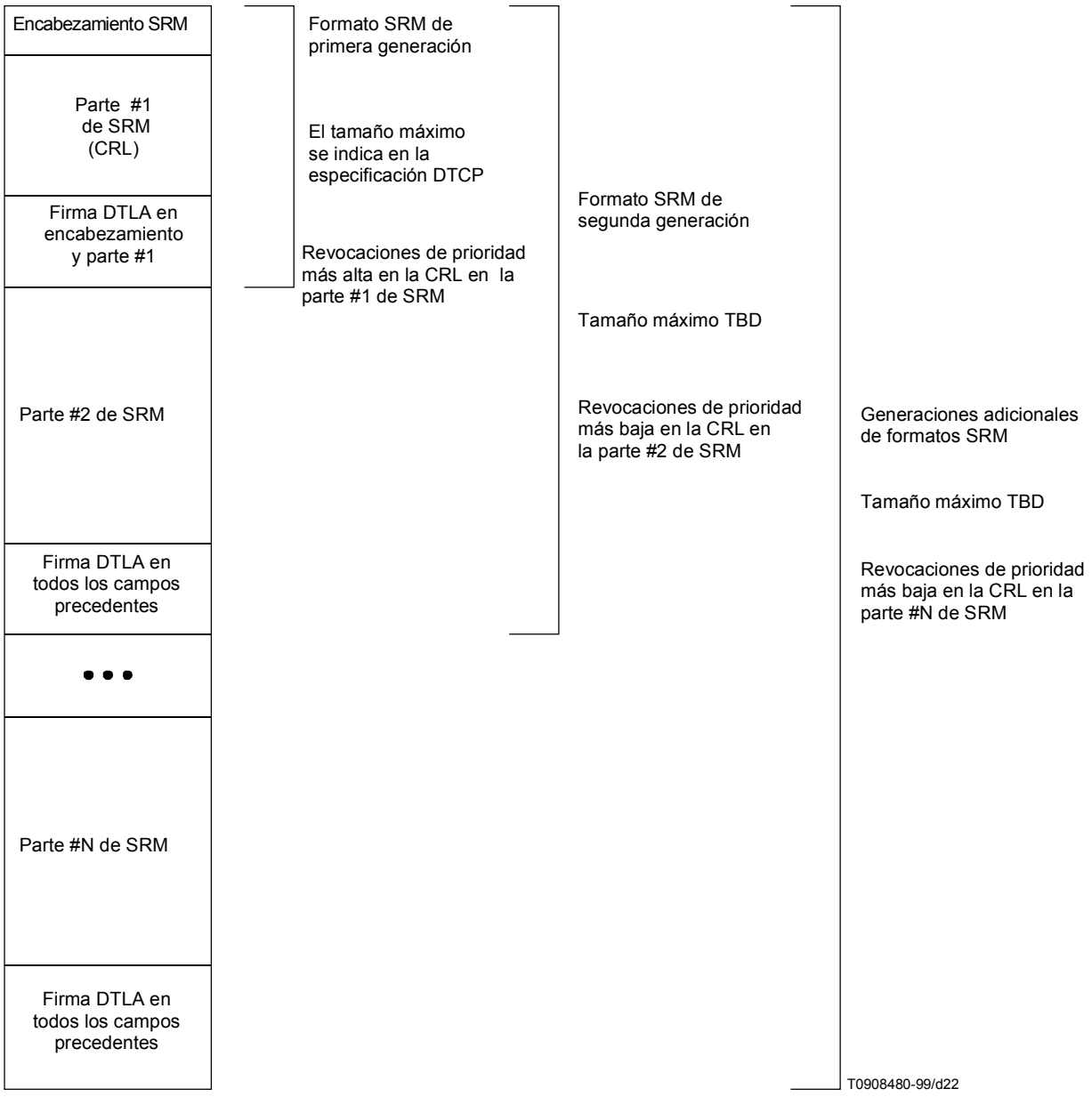


Figura III.18/J.95 – Ampliación SRM

III.8 Ampliaciones del conjunto de instrucciones de interfaz digital AV/C

III.8.1 Introducción

Por regla general, los dispositivos audio/vídeo que intercambian contenidos a través del bus serie IEEE 1394 están conformes según CEI 61883 y el conjunto de instrucciones de interfaz digital AV/C. Con respeto a las reglas generales relativas a las instrucciones y respuestas AV/C, véanse las secciones A.5, A.6 y A.7 de la *Especificación para el conjunto de instrucciones de interfaz digital AV/C* (Especificación general).

Estas especificaciones definen la utilización de paquetes asíncronos IEEE 1394 para el control y gestión de dispositivos y de paquetes isócronos IEEE 1394 para el intercambio de contenidos. En este capítulo se describen las ampliaciones del conjunto de instrucciones AV/C que soporten los protocolos de autenticación DTCP y los protocolos de intercambio de claves. En la sección A.6 se describen las ampliaciones del formato de paquete isócrono IEEE 1394.

III.8.2 Instrucción SEGURIDAD

Se define una nueva instrucción seguridad para AV/C. Esta instrucción tiene por finalidad proteger los contenidos, incluido el sistema DTCP. El formato general de la instrucción SEGURIDAD es el siguiente:

	msb		lsb
Código operacional	SEGURIDAD ($0F_{16}$)		
Operando[0]	categoría	(msb)	
Operando[1]	campo dependiente de la categoría		
:			
Operando[X]			(lsb)

El valor del código operacional instrucción seguridad es $0F_{16}$. (Instrucción unidad y subunidad comunes).

El campo **category** (**categoría**) para la instrucción SEGURIDAD se define del modo siguiente:

Valor	categoría
0	Soporte para DTCP AKE. Esto se llama instrucción AKE.
$1\text{-}D_{16}$	Reservada para futura ampliación
E_{16}	Dependiente del vendedor
F_{16}	Ampliación de campo categoría

El valor 0 del campo category (categoría) indica que esta instrucción se utiliza para soportar los protocolos de autenticación DTCP y de intercambio de claves.

La instrucción AKE se define para *ctype* de CONTROL y SITUACIÓN. Los dispositivos que soporten la instrucción AKE soportarán ambos *ctype*s.

El valor E_{16} del campo category (categoría) indica que los proveedores utilizan esta instrucción para especificar sus propias instrucciones de seguridad para la utilización autorizada mediante concesión de licencia.

III.8.3 Instrucción AKE

El destino de esta instrucción es el dispositivo previsto. Por lo tanto, el campo subunit_type (tipo de subunidad) de 5 bits de una trama instrucción/respuestas AV/C es igual a 11111_2 y el campo subunit_ID (ID de subunidad) de 3 bits de la trama es igual a 111_2.

III.8.3.1 Instrucción control AKE

Esta instrucción se utiliza para intercambiar los mensajes necesarios para aplicar los protocolos de autenticación e intercambio de claves. A continuación figura el formato de esta instrucción:

Tanto las tramas de la instrucción como de la respuesta AKE tienen el mismo código operacional y los primeros 9 operandos (operando[0-8]). El valor de cada campo en la trama de respuestas es idéntico al de la trama de instrucción excepto para los campos status (situación) y data (datos). Si alguno de los campos en los primeros 9 operandos contienen valores reservados, se devolverá una respuesta de NOT_IMPLEMENTED (no aplicado).

Si una trama de instrucción dada incluye un campo data, la trama de respuesta correspondiente no tiene un campo data. Se utilizan las instrucciones control AKE para enviar la información utilizada para el procedimiento de autenticación que se está efectuando entre el dispositivo fuente y el dispositivo sumidero. Esta información se envía en el campo data y se llama Info AKE. Se deben ignorar los valores distintos de cero en los campos Reserved_zero (cero reservado) de Info AKE.

El campo AKE_ID (ID de AKE) indica el formato del campo AKE_ID dependent (dependiente de ID de AKE). Actualmente sólo se define la codificación AKE_ID = 0. En III.8.3.3 se describirá el campo AKE_ID dependent de esta codificación. Los demás valores, de 1_{16} a F_{16}, se reservan para una futura definición.

	msb		lsb
Código operacional	$0F_{16}$		
Operando[0]	categoría = 0000_2 (AKE)	AKE_ID	
Operando[1]	(msb)		
Operando[2]	Campo dependiente AKE_ID		
Operando[3]			
Operando[4]			(lsb)
Operando[5]	AKE_label		
Operando[6]	número (opción)	situación	
Operando[7]	blocks_remaining		(msb)
Operando[8]	data_length (lsb)		
Operando[9]	datos		
:			
Operando[8 + data_length]			

El campo AKE_label (etiqueta AKE) es una indicación que se utiliza para distinguir una secuencia de instrucciones AKE asociadas con un determinado proceso de autenticación. El iniciador de un procedimiento de autenticación puede seleccionar un valor arbitrario para AKE_label. El valor seleccionado será distinto de los demás valores AKE_label que está utilizando el dispositivo que inicia la autenticación. Se utilizará el mismo valor AKE_label para todas las instrucciones de control asociadas con un procedimiento de autenticación específico entre un dispositivo fuente y un dispositivo sumidero. Para asegurar que proviene del controlador adecuado, se verificará AKE_label y el ID de nodo fuente de cada instrucción control.

El campo number (número) opcional[9] indica el número de pasos de una instrucción de control específica para identificar su posición en la secuencia de instrucciones control que forman un procedimiento de autenticación. El iniciador de un procedimiento de autenticación coloca el valor de este campo en 1 para la instrucción inicial de control AKE. El valor se incrementa en cada instrucción subsiguiente que es parte del mismo proceso de autenticación. Cuando una instrucción AKE debe ser fragmentada para transmisión [(véase, más adelante, la descripción del campo blocks_remaining (bloques entrantes)], cada fragmento utilizará el mismo valor para el campo number. Los dispositivos que no soporten este campo colocarán sus valores en 0000_2.

Se utiliza el campo status para comunicar al dispositivo que envía la instrucción el motivo de que la instrucción dé como resultado una respuesta RECHAZADO. El dispositivo que envía la instrucción coloca el valor de este campo en 1111_2. Si el dispositivo que responde rechaza la instrucción, invalida el campo status con un código que indica el motivo del rechazo. La codificación del campo status es la siguiente:

Valor	Situación	Código de respuesta
0000_2	Sin error	ACEPTADO
0001_2	Actualmente está disponible el soporte para no más procedimientos de autenticación	RECHAZADO
0010_2	Sin resultado isócrono	RECHAZADO
0011_2	Sin conexión punto a punto	RECHAZADO
0111_2	Cualquier otro error	RECHAZADO
1111_2	Sin información	Reservado para PROVISIONAL[a)]

a) Reservado para una futura utilización. No debe utilizarse la respuesta con código de respuesta PROVISIONAL.

9 Las características de esta especificación rotuladas como "opcionales" describen capacidades cuya utilización no ha sido aún establecida por el DTLA.

Los códigos de situación siguientes se utilizan únicamente como prueba. Los productos no devolverán estos códigos pero, si se dan estas condiciones, devolverán 0111_2 (cualquier otro error).

Valor	Situación	Código de respuesta
1000_2	Orden de instrucción incorrecto (únicamente para prueba)	RECHAZADO
1001_2	Fracaso de autenticación (únicamente para prueba)	RECHAZADO
1010_2	Errores de sintaxis en el campo de datos (únicamente para prueba)	RECHAZADO

Se utiliza el campo blocks_remaining cuando el tamaño de una instrucción es superior al tamaño máximo de la trama de instrucción que el dispositivo seleccionado puede recibir (un dispositivo que envía una instrucción puede determinar el tamaño del campo de datos que el dispositivo previsto puede aceptar utilizando la instrucción situación AKE). En este caso, el campo data se fragmenta en N bloques que se envían secuencialmente, cada uno en una de las N instrucciones separadas, donde cada instrucción es lo bastante pequeña como para que la memoria tampón de la instrucción del dispositivo pueda soportarla. Como mínimo, la memoria tampón debe ser capaz de retener una instrucción con un campo de datos de, como mínimo 32, bytes[10]. El tamaño del campo de datos en los primeros N – 1 fragmentos será el mismo tamaño y un múltiplo de 16 bytes superior o igual a 32 bytes.

Cada una de las tramas de N instrucciones es idéntica salvo para los valores de los campos blocks_remaining, data_length (longitud de datos), y data. Para la primera instrucción, el campo blocks_remaining se coloca en el valor de N – 1. En cada instrucción sucesiva, el campo blocks_remaining disminuye en uno hasta llegar a cero, lo que indica el último fragmento de la instrucción. Si el valor del campo block_remaining no es correcto (por ejemplo, no está en el orden correcto), el dispositivo devolverá una respuesta RECHAZADO con campo status de 0111_2 (cualquier otro error).

Como el tamaño de las tramas de instrucción y respuesta no puede exceder el límite de 512 bytes impuesto por el transporte FCP subyacente, una instrucción sólo puede fragmentarse cuando un dispositivo seleccionado tiene una capacidad de memoria tampón de trama de instrucción inferior a 512 bytes. Generalmente, el tamaño de la instrucción corresponde a la capacidad de la memoria tampón de trama de instrucción del dispositivo y la instrucción se envía sin fragmentación y con un campo blocks_remaining con valor cero.

Cuando se transmite AKE_Info utilizando múltiples instrucciones control, un controlador enviará cada instrucción únicamente después de haber recibido una respuesta ACEPTADO a la instrucción precedente.

El campo data_length indica el campo longitud de datos en bytes. Las respuestas a una instrucción utilizarán el mismo valor para sus campos data_length respectivos incluso cuando la respuesta no devuelva ningún dato. Si una respuesta tiene algunos datos cuando el código de respuesta es ACEPTADO, la instrucción correspondiente no tendrá ningún dato pero el valor del campo data_length será el mismo que el de la respuesta.

El campo data contiene los datos que se han de transferir. Los contenidos del campo data dependen del campo AKE_ID y del campo AKE_ID dependent. Para respuestas con un código de respuesta de RECHAZADO, no existe ningún campo data.

---

[10] Si futuras generaciones de mensajes de capacidad de renovación de sistema (SRMM > 0) se definen con un tamaño máximo superior a 4096 bytes, será necesario que los nuevos dispositivos soporten un aumento del tamaño mínimo de la memoria tampón.

III.8.3.2 Instrucción de situación AKE

El formato de la instrucción de situación AKE es el siguiente:

	msb		lsb
Código operacional	$0F_{16}$		
Operando[0]	categoría = 0000_2 (AKE)	AKE_ID	
Operando[1]	(msb) campo AKE_ID dependent		
Operando[2]			
Operando[3]			
Operando[4]			(lsb)
Operando[5]	FF_{16}		
Operando[6]	F_{16}	situación	
Operando[7]	$7F_{16}$		(msb)
Operando[8]	data_length (lsb)		

Las tramas de instrucción y respuesta tienen la misma estructura. Los valores de cada campo de las tramas de instrucción y respuestas son idénticas salvo en los campos AKE_ID dependent, status, y data_length.

El campo AKE_ID indica el formato del campo AKE_ID dependent. En III.8.3.3 se describirá el campo AKE_ID dependent para esta codificación. Actualmente, sólo se define la codificación de AKE_ID = 0. Los demás valores, de 1_{16} a F_{16}, se reservan para una futura definición.

El campo status es utilizado por un dispositivo para interrogar la situación de otro dispositivo. Cuando se envía la instrucción, el valor de este campo se fija a 1111_2. En la respuesta, el dispositivo previsto invalida este campo con un valor que indica su situación actual.

Valor	Situación	Código de respuesta
0000_2	Sin error	ESTABLE
0001_2	Actualmente está disponible el soporte para no más procedimientos de autenticación	ESTABLE
0010_2	Sin resultado isócrono	ESTABLE
0011_2	Sin conexión punto a punto	ESTABLE
0111_2	Cualquier otro error	ESTABLE
1111_2	Sin información[a)]	RECHAZADO

a) Se recomienda que los implementadores no utilicen la respuesta "sin información".

Los códigos de situación siguientes se utilizan únicamente como prueba. Los productos no devolverán estos códigos pero, si se dan estas condiciones, devolverán 0111_2 (cualquier otro error).

Valor	Situación	Código de respuesta
1001_2	Fracaso de autenticación (únicamente para prueba)	ESTABLE

El campo data_length indica la capacidad máxima del campo data del dispositivo en bytes. Cuando se envía la instrucción situación, el valor de este campo se coloca en $1FF_{16}$. En la respuesta, el dispositivo seleccionado invalida este campo con un valor que indica su situación actual. El valor mínimo que se soporta es 020_{16} (32 bytes).

III.8.3.3 Campo AKE_ID dependent (AKE_ID = 0)

Cuando AKE_ID = 0, el formato del campo AKE_ID dependent es el siguiente:

	msb	lsb
Operando[1]	subfunción	
Operando[2]	AKE_procedure	
Operando[3]	exchange_key	
Operando[4]	subfunction_dependent	

El campo subfunction (subfunción) indica la operación de instrucciones control. El bit más significativo del campo subfunction indica si la instrucción control tiene o no datos.

- Si el *MSB* es 0, esa instrucción tiene algunos datos y el campo data_length indica su longitud.
- Si el *MSB* es 1, esa instrucción no tiene ningún dato y el campo data_length indica la longitud del campo de datos en trama de respuesta cuyo código de respuesta es ACEPTADO.

En la especificación DTCP disponible con licencia concedida por el DTLA se describen completamente las subfunciones. En el cuadro siguiente figura un resumen de las seis subfunciones actualmente definidas:

Valor	Subfunción	Comentarios
01_{16}	CHALLENGE	Enviar valor aleatorio. Cuando se envía desde un dispositivo sumidero, esta subfunción inicia el procedimiento AKE.
02_{16}	RESPONSE	Devolver datos calculados con el valor aleatorio recibido.
03_{16}	EXCHANGE_KEY	Enviar una clave de intercambio criptada (K_x) al dispositivo sumidero de contenidos autenticado.
04_{16}	SRM	Enviar SRM a un dispositivo que tiene un SRM actualizado o más pequeño.
$C0_{16}$	AKE_CANCEL	Notificar a un dispositivo que no puede continuarse el actual procedimiento de autenticación.
80_{16}	CONTENT_KEY_REQ	Solicitar los datos necesarios para construir la clave de contenidos (K_c).

Para las instrucciones situación, el valor del campo subfunction se colocará en FF_{16}.

Cada bit del campo AKE_procedure (procedimiento AKE) corresponde a un tipo de procedimiento de autenticación, tal como se describe a continuación.

Bit	AKE_procedure
0 (lsb)	Procedimiento de autenticación restringida (rest_auth)
1	Procedimiento de autenticación restringida mejorada (en_rest_auth) (nota 1)
2	Procedimiento de autenticación completa (full_auth)
3	Procedimiento de autenticación completa ampliado (nota 2) (ex_full_auth, optional) (nota 3)
4-7 (msb)	Reservado para una futura ampliación y cuyo valor será cero
NOTA 1 – Los dispositivos fuente que soportan el procedimiento de autenticación completa verificarán el certificado del dispositivo sumidero y examinarán el SRM incluso en la autenticación restringida. En la presente subcláusula este procedimiento de autenticación se denomina autenticación restringida mejorada. NOTA 2 – Los dispositivos que soporten certificados de dispositivo ampliados utilizan el procedimiento autenticación completa ampliada descrito en esta subcláusula. NOTA 3 – Las características de esta especificación rotuladas como "opcionales" describen capacidades cuya utilización no ha sido aún establecida por el DTLA.	

Para la instrucción control, el iniciador de un procedimiento de autenticación coloca un bit en este campo para indicar cuál es el tipo de autenticación que se realizará. El valor del campo se mantiene constante durante el resto de ese procedimiento de autenticación.

Para la instrucción situación, el iniciador colocará el valor inicial de este campo en FF_{16}. El dispositivo previsto invalidará el campo, liberará los bits que indican los procedimientos de autenticación que ese dispositivo no soporta como dispositivo fuente. Por ejemplo, si un dispositivo fuente soporta la autenticación completa y la autenticación restringida mejorada, los valores del campo, AKE_procedure podrán colocarse en 06_{16}.

Antes de iniciar el protocolo de autenticación, los dispositivos sumidero deben investigar qué procedimientos de autenticación soporta un dispositivo fuente utilizando la instrucción situación. En el cuadro siguiente figura la forma de seleccionar el procedimiento de autenticación adecuado:

Procedimiento de autenticación soportado por el dispositivo sumidero / Procedimiento de autenticación soportado por el dispositivo fuente	Rest_auth y En_rest_auth	Rest_auth y Full_auth	Rest_auth, Full_auth, y Ex_full_auth
Rest_auth	Autenticación restringida	Autenticación restringida	Autenticación restringida
En_rest_auth y Full_auth	Autenticación restringida mejorada	Autenticación completa	Autenticación completa
En_rest_auth, Full_auth, y Ex_full_auth	Autenticación restringida mejorada	Autenticación completa	Autenticación completa ampliada

Cada bit del campo exchange_key (clave de intercambio) corresponde a una o más claves descritas en el cuadro que figura a continuación:

Bit	exchange_key
0 (lsb)	Clave(s) de intercambio para el contenido ninguna copia (requieren autenticación completa o autenticación completa ampliada) (nota)
1	Clave de intercambio para el contenido una generación de copias (cualquier autenticación aceptable)
2	Clave de intercambio para el contenido no más copias (cualquier autenticación aceptable)
3-7 (msb)	Reservado para una futura ampliación y cuyo valor será cero
NOTA – Si se utiliza la autenticación completa ampliada, todas las claves de intercambio para códigos opcionales mutuamente soportados se enviarán una vez que se dé por terminada la autenticación completa.	

Para la instrucción control, el dispositivo sumidero fija el valor de este campo al iniciar un procedimiento de autenticación para indicar qué clave o claves de intercambio serán proporcionadas por el dispositivo fuente una vez terminado satisfactoriamente el procedimiento. Para la autenticación completa, puede colocarse cualquier bit. Para la autenticación restringida, se colocará únicamente un bit para una generación de copias o para no más copias. Este campo sigue constante durante el resto del procedimiento de autenticación excepto cuando se realiza la subfunción EXCHANGE_KEY.

Para la instrucción situación, el iniciador colocará FF_{16} en este campo y el dispositivo previsto liberará todos los bits del campo que correspondan a una clave de intercambios que dicho dispositivo no puede proporcionar.

Por ejemplo, si el dispositivo puede proporcionar tres claves que corresponden a bit0 a bit2 en el cuadro precedente, el valor del campo exchange_key se colocará en 07_{16}.

Un dispositivo sumidero debe decidir qué clave o claves serán necesarias obteniendo por adelantado esta información del procedimiento de autenticación.

La definición del campo subfunction_dependent (dependiente de la subfunción) varía. La especificación DTCP disponible con licencia concedida por el DTLA describe las definiciones para instrucciones control. Para las instrucciones situación, el valor de este campo se coloca en FF_{16} tanto para las tramas de instrucción como para las tramas de respuesta.

III.8.4 Comportamiento de reiniciación de bus

Si el dispositivo fuente sigue transmitiendo contenidos por un canal isócrono tras una reiniciación de bus, se utilizarán las mismas claves de intercambio y claves de contenido utilizadas antes de esa reiniciación.

Si la reiniciación de bus se produce durante un procedimiento de autenticación, el dispositivo fuente y el dispositivo sumidero detendrán inmediatamente el procedimiento de autenticación. Tras la reiniciación, es posible que el campo ID de nodo de fuente (SID, *source node ID*) en el encabezamiento CIP haya cambiado y es necesario que el dispositivo sumidero reinicie el procedimiento de autenticación utilizando el nuevo SID.

III.8.5 Acción cuando se detecta el dispositivo no autorizado durante la autenticación

Tras devolver una respuesta ACEPTADO al iniciador de una instrucción, el dispositivo examina la información AKE. Si este dispositivo determina que el iniciador es un dispositivo no autorizado, detendrá inmediatamente el procedimiento AKE sin ninguna notificación.

III.8.6 Flujos de instrucciones AV/C para autenticación

Las figuras III.19 y III.20 ilustran los flujos de instrucciones AV/C utilizadas para autenticación restringida/autenticación restringida completa y mejorada.

III.8.6.1 Notación de las figuras

Las líneas llenas indican los pares instrucción/respuesta que siempre se realizan.

Las líneas de punto indican los pares instrucción/respuesta que se realizan a título condicional.

III.8.6.2 Flujo de instrucciones para autenticación completa

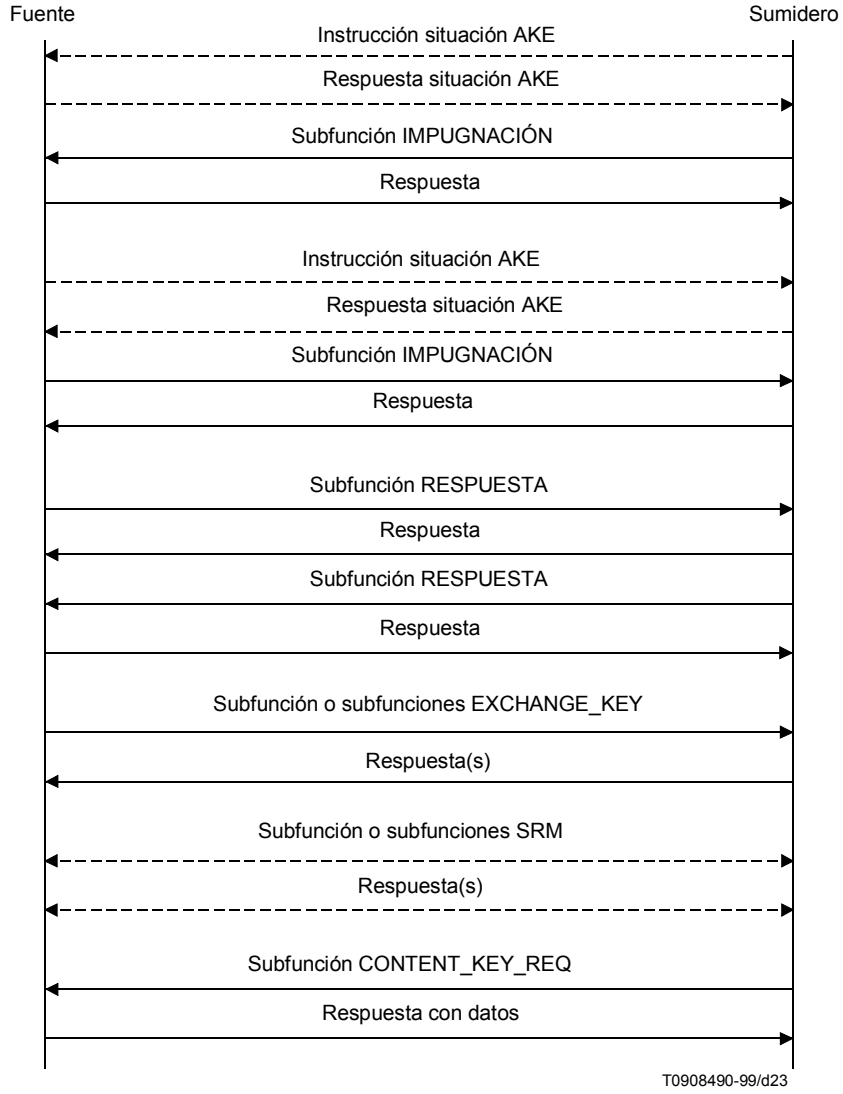


Figura III.19/J.95 – Flujo de instrucciones para autenticación completa

III.8.6.3 Flujo de instrucciones para autenticación restringida/autenticación restringida mejorada

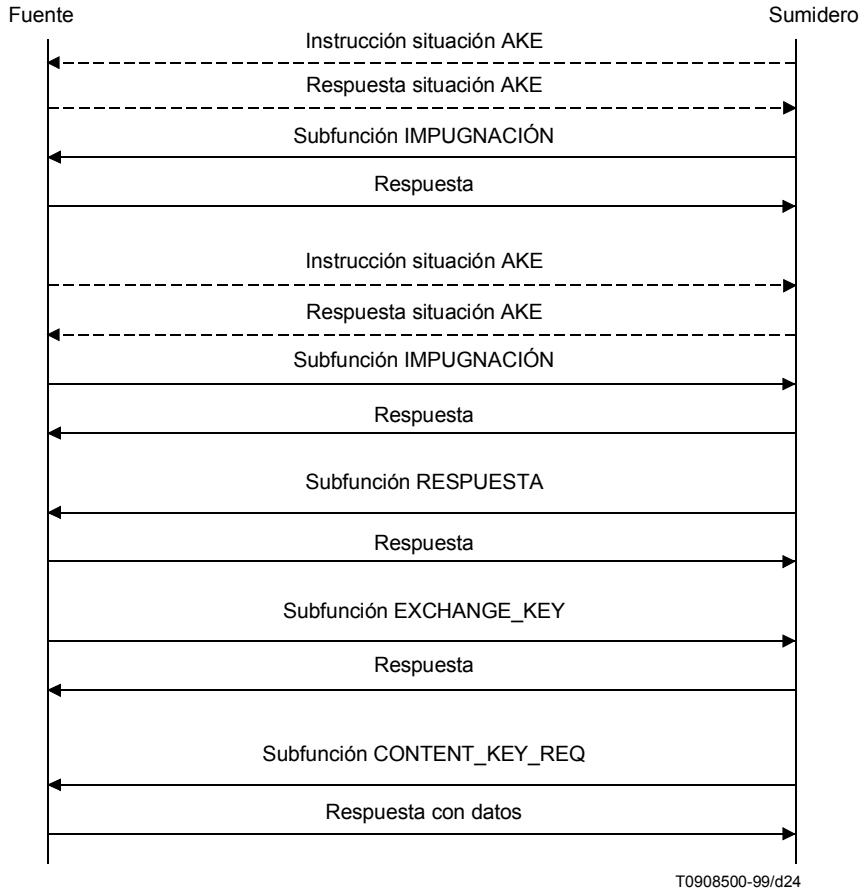


Figura III.20/J.95 – Flujo de instrucciones para autenticación restringida/autenticación restringida mejorada

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie B	Medios de expresión: definiciones, símbolos, clasificación
Serie C	Estadísticas generales de telecomunicaciones
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	**Transmisiones de señales radiofónicas, de televisión 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	RGT y mantenimiento de redes: sistemas de transmisión, circuitos telefónicos, telegrafía, facsímil y circuitos arrendados internacionales
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 y comunicación entre sistemas abiertos
Serie Y	Infraestructura mundial de la información
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Ginebra, 2001