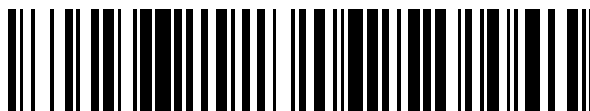


19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 461 184**

51 Int. Cl.:

H04H 60/15 (2008.01)

H04N 21/647 (2011.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **17.05.2011** **E 11720099 (8)**

97 Fecha y número de publicación de la concesión europea: **19.03.2014** **EP 2559177**

54 Título: **Proveedor de flujo de transporte, proveedor de señal DAB, analizador de flujo de transporte, receptor DAB, procedimiento, programa informática y señal de flujo de transporte**

30 Prioridad:

08.02.2011 EP 11153693

19.05.2010 DE 102010029114

45 Fecha de publicación y mención en BOPI de la traducción de la patente:

19.05.2014

73 Titular/es:

**FRAUNHOFER-GESELLSCHAFT ZUR
FÖRDERUNG DER ANGEWANDTEN
FORSCHUNG E.V. (100.0%)
Hansastraße 27c
80686 München, DE**

72 Inventor/es:

**BARTEL-KURZ, BIRGIT;
DÖHLA, STEFAN y
PROSCH, MARKUS**

74 Agente/Representante:

PONTI SALES, Adelaida

ES 2 461 184 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Proveedor de flujo de transporte, proveedor de señal DAB, analizador de flujo de transporte, receptor DAB, procedimiento, programa informática y señal de flujo de transporte

Campo técnico

[0001] Los ejemplos de realización según la invención se refieren a un proveedor de flujo de transporte para la provisión de una multiplicidad de paquetes de flujo de transporte que describen una información de medios digitales. Otros ejemplos de realización según la invención se refieren a un proveedor de señal DAB. Otros ejemplos de realización según la invención se refieren a un analizador de flujo de transporte para la provisión de una información de restricción de acceso para la descryptación de una información de medios digitales restringida de acceso en base a un flujo de transporte. Otros ejemplos de realización según la invención se refieren a un receptor DAB. Otros ejemplos de realización según la invención se refieren a procedimientos correspondientes y programas informáticos correspondientes. Otros ejemplos de realización según la invención se refieren a una señal de flujo de transporte. Otros ejemplos de realización según la invención se refieren a una estructura base para el acceso condicionado para la radiodifusión multimedia digital (DMB) para el transporte ahorrando tasa de bits de informaciones referentes al acceso condicionado.

Antecedentes de la invención

[0002] La radiodifusión multimedia digital, que se conoce por la abreviatura DMB ("digital multimedia broadcasting"), es una extensión de la radiodifusión de audio digital actual, que se conoce por la abreviatura DAB ("digital audio broadcasting"), a contenidos audiovisuales. La radiodifusión multimedia digital DMB "hereda" toda la funcionalidad DAB, pero está complementada con la posibilidad de transmitir adicionalmente flujos de transporte codificados MPEG2 con contenidos de video y/o contenidos de audio.

[0003] En el lado de emisión se complementa para ello el multiplexor DAB existente con una pasarela DMB que recibe el flujo de transporte MPEG2 de un codificador DMB (DMB-Encoder).

[0004] La fig. 14 muestra una representación esquemática de un tratamiento de señales DMB. El tratamiento de señales DMB 1400 según la fig. 14 recibe una información multimedia 1410 que comprende, por ejemplo, una señal de audio y/o una señal de video. El tratamiento de señales DMB 1400 comprende además un codificador DMB 1420 (también designado como "DMB-Encoder") que está diseñado para generar, en base a la información multimedia 1410, un flujo de transporte MPEG2 1422. El tratamiento de señales 1400 comprende además una pasarela DMB 1430 que está diseñada para recibir el flujo de transporte 1422 y generar en base a él un subcanal DAB 1432 (también designado como "DAB-Subchannel"). El tratamiento de señales 1400 comprende además un multiplexor DAB 1440 que está diseñado para añadir el subcanal DAB 1432 a una señal DAB que reúne, por ejemplo, una multiplicidad de subcanales DAB. Por consiguiente se obtiene, por ejemplo, una señal multiplexada DAB.

[0005] Para los detalles de cómo se puede obtener una señal conforme a DMB o una señal DAB que comprende informaciones DMB se remite, por ejemplo, a las publicaciones correspondientes de la Unión Europea de Radiodifusión ("European Broadcasting Union" o EBU). Los detalles se describen, por ejemplo, en la publicación ETSI TS 102 428, V1.2.1 con el título "Digital Audio Broadcasting (DAB); DMB video services; User application specification" y los documentos aquí referenciados.

[0006] La radiodifusión multimedia digital DMB es una tecnología con la que se debe ver la "televisión" sobre equipos receptores móviles. DMB representa por consiguiente una alternativa a tecnologías, como por ejemplo DVB-H.

[0007] Una aplicación interesante es la televisión de pago (también conocida como "PAY-TV"), en la que los contenidos se transmiten de forma protegida (encriptada) y sólo están a disposición de usuarios autorizados. Este concepto se designa a continuación como restricción de acceso o restricción de entrada. Un sistema para el acceso condicionado (o para la entrada condicionada) asume la encriptación de los contenidos y la provisión de los mensajes adicionales necesarios, sistema que a veces también se designa como "Conditional Access System" o de forma abreviada como "CA". Los mensajes adicionales son, por ejemplo, mensajes de autorización (también designados como "EMM") o mensajes que contienen la clave de contenido actual ("Content key") (también designada como "ECM"). Los mensajes de autorización se designan en parte también como mensajes de gestión de

autorización EMM. Los mensajes que contienen la clave de contenido actual también se designan a veces como mensajes de control de autorización ECM. Los mensajes adicionales también se denominan a continuación de forma abreviada "informaciones CA" y se transfieren igualmente a través del canal de radiodifusión. Un objetivo es mantener tan baja como sea posible la sobrecarga o "overhead" que se origina por la emisión de informaciones CA (informaciones para el acceso o entrada condicionados).

[0008] En consideración a esto el objetivo de la presente invención es crear un concepto que haga posible transmitir de forma eficiente (con bajo consumo de recursos) una información de medios restringida de acceso.

10 Resumen de la invención

[0009] Un ejemplo de realización según la invención crea un proveedor de flujo de transporte para la provisión de una multiplicidad de paquetes de flujo de transporte que describen una información de medios digitales. El proveedor de flujo de transporte está diseñado para proveer un paquete de flujo de transporte de un primer tipo de paquete con una tabla de asociación de programa y una información de restricción de acceso con una información de clave para la encriptación de una información de medios encriptada. La tabla de asociación de programa contiene una asociación entre un número de programa y un identificador de tipo de paquete (PID) de otro paquete de flujo de transporte de un segundo tipo de paquete. El proveedor de flujo de transporte está diseñado además para proveer un paquete de flujo de transporte del segundo tipo de paquete (con un identificador de tipo de paquete correspondiente) de modo que el paquete de flujo de transporte del segundo tipo de paquete contenga una referencia a los identificadores de tipo de paquete de los paquetes de datos útiles del flujo de transporte que describen los contenidos de distintos tipos de contenido de la información de medios digitales.

[0010] Una idea nuclear de la presente invención es que una inclusión eficiente en recursos de una información de restricción de acceso (CA-Information), que comprende una información de clave para la descryptación de una información de medios encriptada, se pueda realizar en paquetes de flujo de transporte con una tabla de asociación de programa. Así se ha descubierto precisamente que los paquetes de flujo de transporte (por ejemplo en DMB) en la tabla de asociación de programa presentan en general capacidades de bits libres. Por ejemplo, se trata en el caso de DMB de un flujo de datos SPTS (flujo de transporte de programa individual, también designado en inglés como "single program transport stream") y por consiguiente sólo está contenido exactamente un programa en el flujo de datos. Entonces se puede realizar la inclusión de la información de restricción de acceso sin introducir una información adicional en los paquetes de datos útiles del flujo de transporte o usar paquetes de flujo de transporte adicionales. Entonces una cantidad de datos, que se debe transmitir en conjunto en los paquetes de flujo de transporte del primer tipo de paquete con la tabla de asignación de programa, es habitualmente claramente menor que la cantidad de datos que se debe transmitir mediante paquetes de datos útiles del flujo de transporte. Por lo demás los paquetes de datos útiles del flujo de transporte ya están completamente llenos en general (o con frecuencia) de datos útiles sin el uso de un mecanismo de restricción de acceso. Esto viene por ello de que un codificador de datos útiles (por ejemplo codificador de audio o un codificador de vídeo) trabaja típicamente independientemente de si los datos de audio o datos de vídeo codificados se proveen de un mecanismo de restricción de acceso. Por ello un codificador de audio o codificador de vídeo semejante procurará habitualmente usar toda la capacidad de datos de los paquetes de datos útiles del flujo de transporte a fin de obtener con ello una calidad de audio o calidad de vídeo óptima.

[0011] Se ha descubierto con ello que una introducción de la información de restricción de acceso en los paquetes de datos útiles del flujo de transporte, o también el uso de paquetes de flujo de transporte adicionales, conduciría a que un codificador de audio o codificador de vídeo no podría usar todo la tasa de datos que se pueden transmitir mediante los paquetes de datos útiles del flujo de transporte, a fin de dejar con ello espacio en los paquetes de datos útiles del flujo de transporte, o que se deberían reempaquetar los paquetes de datos útiles del flujo de transporte si la información de restricción de acceso se debiera incluir en los paquetes de datos útiles del flujo de transporte completamente llenos de datos útiles. Por otro lado se ha descubierto que los paquetes de flujo de transporte del primer tipo de paquete que contienen la tabla de asociación de programa presentan en muchas aplicaciones de manera fiable y regular capacidades de datos libres que se pueden usar por la inclusión de la información de restricción de acceso.

[0012] Además, se ha descubierto que la inclusión de la información de restricción de acceso en los paquetes de flujo de transporte del primer tipo de paquete hace posible un acceso especialmente rápido a las informaciones de medios encriptadas, dado que con ello se consigue que las informaciones de restricción de acceso ya estén disponibles inmediatamente después de la evaluación del paquete de flujo de transporte del primer tipo de paquete. Pero de todos modos es necesaria obligatoriamente una evaluación del paquete de flujo de transporte del primer tipo

de paquete, en particular de la tabla de asociación contenida en él, para evaluar o poder reproducir una información de medios digitales. En tanto que el concepto según la invención hace posible crear un mecanismo de restricción de acceso que se las arregla sin retardos adicionales perceptibles en la reproducción de la información de medios digitales.

5

[0013] En un ejemplo de realización preferido, los paquetes de flujo de transporte de los diferentes tipos de paquete, es decir, en particular los paquetes de flujo de transporte del primer tipo y del segundo tipo, así como los paquetes de datos útiles del flujo de transporte, presentan longitudes de paquete idénticas. Esto facilita la transmisión de los paquetes de flujo de transporte en algunas redes. Simultáneamente esta característica da lugar a

10 que en los paquetes de flujo de transporte del primer tipo de paquete se puedan incluir, adicionalmente a la tabla de asociación de programa, cantidades de datos proporcionalmente grandes. Esto hace posible en particular la inclusión de la información de restricción de acceso adicionalmente a la tabla de asociación de programa.

[0014] En un ejemplo de realización preferido, el proveedor de flujo de transporte está diseñado para añadir la

15 información de restricción de acceso en un campo de información adicional del paquete de flujo de transporte del primer tipo de paquete, y para señalar una presencia del campo de información adicional mediante un marcador. La inclusión de la información de restricción de acceso en un campo de información adicional del paquete de flujo de transporte del primer tipo de paquete hace posible en este caso que, pese a la adición de la información de restricción de acceso, el paquete de flujo de transporte del primer tipo de paquete esté en concordancia con los

20 estándares válidos que no plantean especificaciones con vistas a los contenidos de datos que estén incluidos en el campo de información adicional. En tanto que el concepto de la invención hace posible usar informaciones de restricción de acceso sin infracción de los estándares existentes y, no obstante, obtener una funcionalidad mejorada en comparación a los sistemas estandarizados. Entonces el concepto de la invención hace posible utilizar el mecanismo de restricción de acceso ya en el plano de flujo de transporte, pudiéndose añadir el mecanismo de

25 restricción de acceso con bajo coste a una información de medios digitales ya codificada y paquetizada.

[0015] En un ejemplo de realización preferido, el proveedor de flujo de transporte está diseñado para proveer los paquetes de flujo de transporte de modo que cada uno de los paquetes de flujo de transporte presente un

30 identificador de tipo de paquete, que identifica un tipo de paquete, en una posición predeterminada de un preámbulo del paquete de flujo de transporte. El proveedor de flujo de transporte está diseñado en este caso para proveer los paquetes de flujo de transporte de modo que un paquete de flujo de transporte con la tabla de asociación de programa y la información de restricción de acceso presente una referencia a un identificador de tipo de paquete de otro paquete de flujo de transporte con una tabla de reproducción de programa que comprende los identificadores de

35 tipo de paquete para uno o varios tipos de flujos de datos, sin que el mismo paquete de flujo de transporte con la tabla de asociación de programa y la información de restricción de acceso describa el contenido útil de la información de medios digitales. En tanto que se puede conseguir una separación jerárquica entre paquetes de flujo de transporte, que contienen informaciones de gestión (por ejemplo la tabla de asociación de programa y la información de restricción de acceso) y paquetes de flujo de transporte que describen el contenido útil de la información de medios digitales (es decir, informaciones de audio codificadas y/o informaciones de imagen

40 codificadas y/o informaciones de video codificadas). Por consiguiente la inclusión de la información de restricción de acceso es independiente del contenido útil de la información de medios digitales.

[0016] En un ejemplo de realización preferido, el proveedor de flujo de transporte está diseñado para proveer el paquete de flujo de transporte con la tabla de asociación de programa y la información de restricción de acceso, de

45 modo que el paquete de flujo de transporte correspondiente del primer tipo de paquete presente una secuencia de secciones de informaciones de restricción de acceso diferentes. En este caso una de las secciones presenta un mensaje de gestión de autorización (por ejemplo un mensaje EMM) o una referencia a un mensaje de gestión de autorización, y otra de las secciones presente un mensaje de clave de autorización (por ejemplo un mensaje ECM) o una referencia a un mensaje de clave de autorización. Las secciones de la información de restricción de acceso

50 presentan respectivamente un identificador de tabla que describe el tipo de la información de restricción de acceso contenida en la sección. Además, las secciones de la información de restricción de acceso todavía presentan una información de longitud que describe una longitud de las informaciones contenidas en la sección.

[0017] Mediante el concepto correspondiente es posible incluir de manera estructurada distintas informaciones de

55 restricción de acceso en un único paquete de flujo de transporte. La inclusión por secciones hace posible en particular en el lado del decodificador un acceso efectivo a la información realmente necesaria, dado que en el lado del decodificador simplemente se pueden saltar las secciones cuyo contenido de información no se necesita durante la evaluación. Esto se hace posible en particular mediante el identificador de longitud. Por lo demás el tipo descrito de la inclusión de la información de restricción de acceso, que se puede realizar, por ejemplo, en un campo de

información adicional, también permite añadir otras informaciones al paquete de flujo de transporte correspondiente que no se refieran a la restricción de acceso.

[0018] Por lo demás es posible opcionalmente que existan referencias cruzadas entre secciones individuales con informaciones de restricción de acceso diferentes. Por ejemplo, se puede diferenciar entre secciones con referencias cruzadas y secciones que presentan los verdaderos datos de restricción de acceso. De este modo también se hace posible estructurar de forma jerárquica las informaciones de restricción de acceso y/o reproducir referencias entre paquetes de flujo de transporte de diferentes tipos de paquete dentro del campo de información adicional.

[0019] En un ejemplo de realización preferido, el proveedor de flujo de transporte está diseñado para proveer el flujo de transporte de modo que el flujo de transporte comprenda una referencia a un canal separado en el que se transmiten los mensajes de gestión de autorización (por ejemplo mensajes EMM). Esto concepto es ventajoso cuando el volumen de datos de los mensajes de gestión de autorización es muy grande y/o los mensajes de gestión de autorización contienen una información que es importante para varios programas multimedia.

[0020] Un ejemplo de realización según la invención crea un proveedor de señal DAB para la provisión de una señal DAB que comprende una información de medios restringida de acceso. El proveedor de señal DAB comprende un proveedor de flujo de transporte, según se ha descrito anteriormente. El proveedor de flujo de transporte está diseñado en este caso preferiblemente para proveer paquetes de flujo de transporte de un primer tipo de paquete que comprenden una tabla de asociación de programa y una información de restricción de acceso. El proveedor de flujo de transporte está diseñado además para proveer los paquetes de flujo de transporte de un segundo tipo de paquete, de modo que los paquetes de flujo de transporte del segundo tipo de paquete contengan una referencia a los identificadores de tipo de paquete de los paquetes de datos útiles del flujo de transporte que describen los contenidos de diferentes tipos de contenido de la información de medios digitales. El proveedor de flujo de transporte está diseñado además para proveer paquetes de flujo de transporte de otros tipos de paquete (por ejemplo de un tercer tipo de paquete y de un cuarto tipo de paquete, así como eventualmente tipos de paquete adicionales), que describan respectivamente el contenido de un tipo de medio (por ejemplo datos de audio o datos de vídeo codificados) de la información de medios restringida de acceso. Por ejemplo, el tercer tipo de paquete y el cuarto tipo de paquete pueden describir los contenidos de tipos de medios diferentes de la información de medios restringida de acceso. En este caso se encripta un contenido de al menos alguno de los paquetes de flujo de transporte de los otros tipos de paquete.

[0021] Los paquetes de flujo de transporte del primer tipo de paquete, del segundo tipo de paquete y de los otros tipos de paquete son en este caso parte de un flujo de transporte MPEG2. La información de restricción de acceso, que está contenida en los paquetes de flujo de transporte del primer tipo de paquete, comprende una información de clave para la desenscriptación de los contenidos encriptados de los paquetes de flujo de transporte de los otros tipos de paquete.

[0022] En un ejemplo de realización hay los cuatro tipos de paquete PAT (tabla de asociación de programa), PMT (tabla de reproducción de programa), audio y vídeo. Pero en la práctica todavía pueden estar presentes adicionalmente otros tipos, por ejemplo, descriptores y escenas.

[0023] El proveedor de señal DAB comprende además un combinador de servicios DAB que está diseñado para combinar el flujo de transporte MPEG2 con uno o varios otros servicios DAB a fin de obtener la señal DAB. El proveedor de señal DAB hace posible difundir los servicios DAB junto con una información multimedia, estando encriptadas las informaciones multimedia que se añaden a los otros servicios DAB en el plano de los paquetes de flujo de transporte. De este modo se hace posible que la restricción de acceso a los contenidos multimedia se manipule independientemente de algunas restricciones de acceso a los servicios DAB restantes. Dado que por lo demás la restricción de acceso ya se realiza en el plano de los paquetes de flujo de transporte, todos los mecanismos para la protección frente a errores que se utilizan en las combinaciones de los servicios DAB son efectivos sin limitaciones con vistas a la información multimedia protegida de acceso y las informaciones de clave correspondientes, de modo que aquí se da una fiabilidad elevada en la transmisión de datos.

[0024] Además, según el concepto de la invención es posible la adición de informaciones de restricción de acceso sin modificación del protocolo DAB.

[0025] Además, mediante el concepto según la invención se puede usar casi óptimamente la tasa de datos disponible, ya que la información de restricción de acceso (con la información de clave) no se incluye en los paquetes de datos útiles del flujo de transporte (es decir, los paquetes de flujo de transporte de los otros tipos de

paquete, por ejemplo, del tercer tipo de paquete o del cuarto tipo de paquete), sino en los paquetes de flujo de transporte del primer tipo de paquete que contienen la tabla de asociación de programa. En estos paquetes del primer tipo de paquete todavía está disponible suficiente espacio (en el sentido de bits) típicamente así con uso completo de los paquetes de datos útiles del flujo de transporte por parte de los datos multimedia. En tanto que el concepto mencionado hace posible la realización de un mecanismo de restricción de acceso que satisface, por un lado, los requisitos de los estándares relevantes y es independiente, por el otro lado, de la necesidad de la tasa de bits instantánea de la información multimedia restringida de acceso.

[0026] Un ejemplo de realización según la invención crea por lo demás un analizador de flujo de transporte para la provisión de una información de restricción de acceso para la descryptación de una información de medios digitales restringida de acceso en base a un flujo de transporte. El analizador de flujo de transporte comprende un identificador de tipo de paquete que está diseñado para identificar un paquete de un primer tipo de paquete predeterminado, que presenta un primer tipo de identificador de paquete predeterminado y contiene una tabla de asociación de programa, como un paquete identificado. El analizador de flujo de transporte comprende además un analizador de paquete que está diseñado para buscar el paquete identificado según la información de restricción de acceso y proveer una información de restricción de acceso encontrada. El analizador de flujo de transporte correspondiente se basa en el conocimiento de que un paquete de flujo de transporte que contiene una tabla de asociación de programa es apropiado especialmente adecuadamente para una inclusión de una información de restricción de acceso, según ya se ha explicado arriba detalladamente. Por ello el identificador de tipo de paquete está diseñado para identificar exactamente paquetes de flujo de transporte semejantes y extraer de ellos la información de restricción de acceso.

[0027] En un ejemplo de realización preferido, el analizador de flujo de transporte está diseñado para evaluar la tabla de asociación de programa en el paquete de flujo de transporte del primer tipo de paquete predeterminado y determinar, en base a la tabla de asociación de programa, un segundo identificador de tipo de paquete que esté asociado a un paquete de flujo de transporte con una tabla de reproducción de programa. El analizador de flujo de transporte comprende además un determinador de asociación de tipo de paquete que está diseñado para identificar, en base al segundo identificador de tipo de paquete determinado, un paquete de flujo de transporte con una tabla de reproducción de programa en el flujo de transporte y evaluar la tabla de reproducción de programa a fin de obtener una información sobre que identificadores de tipo de paquete están asignados a los paquetes de datos útiles del flujo de transporte que contienen los contenidos de medios de la información de medios digitales restringida de acceso. Por consiguiente el analizador de flujo de transporte hace realidad un concepto jerárquico en el que a partir de los paquetes de flujo de transporte del primer tipo de paquete y del segundo tipo de paquete sólo se extraen información de gestión, mientras que por el contrario los datos útiles apropiados se extraen de los paquetes de datos útiles del flujo de transporte (por ejemplo de un tercer tipo de paquete y de un cuarto tipo de paquete que se diferencian del primer y del segundo tipo de paquete).

[0028] En un ejemplo de realización preferido, el analizador de flujo de transporte comprende además un descryptador que está diseñado para descryptar contenidos de medios encriptados que están contenidos en los paquetes de datos útiles del flujo de transporte con los identificadores de tipo de paquete descritos en la tabla de reproducción de programa, usando la información de restricción de acceso contenida en el paquete de flujo de transporte del primer tipo de paquete predeterminado.

[0029] En otro ejemplo de realización preferido, el analizador de paquete está configurado para buscar el paquete identificado del primer tipo de paquete predeterminado en cuanto a si un campo de información adicional presenta una o varias tablas que están caracterizadas por identificadores de tabla predeterminados y contienen una información de restricción de acceso. El analizador de paquete está diseñado además para proveer la información de restricción de acceso contenida en las tablas identificadas. Por consiguiente mediante el analizador de paquete se evalúa un campo de información adicional (por ejemplo un campo de datos privados) por lo que, sin contravenir los estándares existentes, se hace posible evaluar una información de restricción de acceso que se puede utilizar de forma más eficiente que las informaciones de restricción de acceso conocidas.

[0030] En un ejemplo de realización preferido, el analizador de paquete está diseñado para verificar, en respuesta a una localización de una primera tabla que está caracterizada por un primer identificador de tabla predeterminado y que contiene una información de restricción de acceso, e independientemente de una información de longitud de tabla contenida en la primera tabla, si el campo de información adicional del paquete identificado del primer tipo de paquete predeterminado presenta a continuación de la primera tabla otra tabla que contenga una información de restricción de acceso, y para proveer la información de restricción de acceso contenida en la otra tabla. Mediante el uso de varias tablas independientes en un único campo de información adicional y mediante la evaluación

correspondiente de estas tablas se hace posible reaccionar de forma flexible del lado del decodificador a las informaciones de restricción de acceso que estén contenidas en el paquete de flujo de transporte correspondiente del primer tipo de paquete o al volumen de informaciones de restricción de acceso que se transmita en el paquete de flujo de transporte del primer tipo de paquete.

5

[0031] Un ejemplo de realización según la invención crea por lo demás un receptor DAB con un separador de servicios DAB que está diseñado para extraer un flujo de transporte MPEG2 de una señal DAB que comprende adicionalmente al flujo de transporte MPEG2 uno o varios otros servicios DAB. El receptor DAB comprende además un analizador de flujo de transporte, según se ha explicado anteriormente. El analizador de flujo de transporte está diseñado para recibir el flujo de transporte MPEG2 del separador de servicios y proveer, en base al flujo de transporte, la información de restricción de acceso para la descryptación de una información de medios digitales restringida de acceso. El receptor DAB comprende además un descryptador de contenido que está diseñado para descryptar los contenidos de medios encriptados de la información de medios digitales restringida de acceso usando la información de restricción de acceso. El receptor DAB correspondiente trae esencialmente las mismas ventajas que ya se ha descrito con vistas al proveedor de señal DAB.

10

15

[0032] Ejemplos de realización según la presente invención crean por lo demás procedimientos correspondientes y programas informáticos correspondientes.

20

[0033] Otros ejemplos de realización según la invención crean por lo demás una señal de flujo de transporte correspondiente que comprende los paquetes de flujo de transporte arriba descritos, y que por ello trae consigo las ventajas arriba explicadas.

Breve descripción de las figuras

25

[0034] Los ejemplos de realización según la presente invención se explican más en detalle a continuación en referencia a las figuras adjuntas. Muestran:

30

Fig. 1 un diagrama de bloques de un proveedor de flujo de transporte según un ejemplo de realización de la presente invención;

Fig. 2A y 2B diagramas de bloques de proveedores de señal DAB según ejemplos de realización de la presente invención;

35

Fig. 3 un diagrama de bloques de un analizador de flujo de transporte según un ejemplo de la presente invención;

Fig. 4 un diagrama de bloques de un receptor DAB según un ejemplo de la presente invención;

40

Fig. 5A una representación esquemática de paquetes de flujo de transporte de un flujo de transporte MPEG2;

Fig. 5B una representación de la sintaxis de un flujo de transporte MPEG2;

45

Fig. 6 una representación esquemática de los paquetes de flujo de transporte que se usan en la transmisión de un contenido multimedia;

50

Fig. 7 una representación esquemática de un paquete de flujo de transporte que comprende una información de restricción de acceso y una tabla de asociación de programa;

Fig. 8A una descripción de la sintaxis de un paquete de flujo de transporte según ISO/IEC 13818-1;

55

Fig. 8B una descripción de la sintaxis de un campo de adaptación de un paquete de flujo de transporte según ISO/IEC 13818-1 teniendo en cuenta las limitaciones según ETSI TS 102 428 V1.2.1;

Fig. 9A una descripción de la sintaxis de una tabla con informaciones de restricción de acceso según ISO/IEC 13818-1;

60

Fig. 9B una descripción de la sintaxis de los descriptores para el uso en una tabla según la fig. 9A según ISO/IEC 13818-1;

Fig. 10 una descripción de la sintaxis de otra tabla para informaciones de restricción de acceso;

Fig. 11 una descripción de la sintaxis de otra tabla para informaciones de restricción de acceso;

5 Fig. 12 una representación tabulada de posibles combinaciones de bits para la descripción de un estado de restricción de acceso;

Fig. 13 una descripción de la sintaxis de una sección de asociación de programa según ISO-IEC 13818;

10 Fig. 14 un diagrama de bloques de un proveedor de señal DAB convencional;

Fig. 15 un diagrama de bloques de un proveedor de señal DAB comparable; y

Fig. 16 un diagrama de bloques de otro proveedor de señal DAB comparable.

15

Descripción detallada de los ejemplos de realización

[0035] A continuación se describe en primer lugar la estructura base del proveedor de flujo de transporte según la invención del proveedor de señal DAB según la invención, del analizador de flujo de transporte según la invención y del receptor DAB según la invención mediante las fig. 1 – 4. A continuación mediante las fig. 5A – 13 se describe en detalle el flujo de transporte que se proporciona y evalúa según la invención. A continuación mediante las fig. 15 y 16 todavía se describen otros conceptos para la realización de una restricción de acceso que sirven como ejemplos de comparación.

25 1. Proveedor de flujo de transporte según la fig. 1

[0036] La fig. 1 muestra un diagrama de bloques de un proveedor de flujo de transporte 100 para la provisión de una multiplicidad de paquetes de flujo de transporte que describen una información de medios digitales (preferiblemente una información multimedia digital con varios tipos de medios). El proveedor de flujo de transporte 100 está diseñado para recibir la información de medios digitales 100 y proveer en base a ello un flujo de transporte 120. El proveedor de flujo de transporte 100 está diseñado en este caso para proveer un primer paquete de flujo de transporte 124 de un primer tipo de paquete con una tabla de asociación de programa (PAT) y una información de restricción de acceso con una información de clave (ECM) para la descriptación de una información de medios encriptada. La tabla de asociación de programa (PAT) comprende (o describe) en este caso una asociación entre un número de programa y un identificador de tipo de paquete de otro paquete de flujo de transporte de un segundo tipo de paquete. El primer paquete de flujo de transporte 124 puede comprender, por ejemplo, un primer identificador de tipo de paquete PID que señala el primer tipo de paquete. El proveedor de flujo de transporte 100 está diseñado además para proveer un segundo paquete de flujo de transporte que presenta el segundo tipo de paquete, de modo que el paquete de flujo de transporte 128 del segundo tipo de paquete contiene una referencia a los identificadores de tipo de paquete de los paquetes de datos útiles del flujo de transporte que describen los contenidos de diferentes tipos de contenido de la información de medios digitales. El paquete de flujo de transporte 128 puede comprender por consiguiente, por ejemplo, en una tabla de reproducción de programa una multiplicidad de identificadores de tipo de paquete, pudiendo estar definido además por una tabla de reproducción de programa o una información aquí referenciada a qué tipo de medio están asociados los paquetes de flujo de transporte con un identificador de tipo de paquete determinado. El paquete de flujo de transporte 128 del segundo tipo de paquete puede estar caracterizado por lo demás hasta por un identificador de tipo de paquete correspondiente que está indicado en el paquete de flujo de transporte del primer tipo de paquete.

[0037] A continuación todavía se explican más precisamente otros detalles con vistas a que se puede parecer exactamente el flujo de transporte.

2. Proveedor de señal DAB según las fig. 2A y 2B

2.1. Proveedor de señal DAB según la fig. 2A

55

[0038] A continuación en referencia a la fig. 2A se describe una estructura según la invención para una restricción de acceso para la radiodifusión multimedia digital DMB. La restricción de acceso también se designa a veces como acceso condicionado o "Conditional Access" (abreviado: CA). A continuación se describen los distintos aspectos de este concepto y se proporciona en particular una descripción del procedimiento.

2.1.1 Plano de encriptación

[0039] Un aspecto del concepto según la invención consiste en seleccionar un plano de encriptación apropiado. En los ejemplos de realización según la invención se encripta en el plano de flujo de transporte MPEG2. Es decir, en caso de necesidad se encripta la carga útil ("Payload") completa de un paquete de flujo de transporte MPEG2. La cabeza de mensaje del flujo de transporte MPEG2 (también designada como "Header") queda no encriptada e indica si el paquete de flujo de transporte MPEG2 está encriptado. Además, la cabeza de mensaje del flujo de transporte MPEG2 también muestra en este caso (es decir, cuando el paquete de flujo de transporte MPEG2 está encriptado) que clave (de una multiplicidad de claves que se designan, por ejemplo, "claves pares" y "claves impares") es necesaria para la desencriptación. La encriptación verdadera así como la señalización de si se encripta y que clave ("impar" o "par") se usa igualmente se realiza análogamente a la radiodifusión de vídeo digital DVB.

[0040] La fig. 2A muestra un diagrama de bloques de un proveedor de señal DAB 200 que está diseñado para recibir una información de medios digitales 210 y proveer en base a ello una señal DAB 220. La información de medios digitales 210 puede ser preferiblemente una información multimedia que comprende informaciones de varios tipos de medios (por ejemplo información de audio e información de imagen o información de audio e información de video). El proveedor de señal DAB comprende un proveedor de flujo de transporte 230 que está diseñado para proveer, en base a la información de medios digitales 210, un flujo de transporte MPEG2 232 encriptado al menos parcialmente.

[0041] El proveedor de flujo de transporte 230 comprende opcionalmente un codificador DMB 230a (también designado como "DMB-Encoder") que está diseñado para proveer, en base a la información de medios digitales 210, un flujo de transporte MPEG2 230b, que representa la información de medios digitales 210 en un formato de flujo de transporte que se corresponde, por ejemplo, con las especificaciones ETSI TS 102 428, V1.2.1. El proveedor de flujo de transporte 230 comprende además un adicionador de restricción de acceso 230c que está diseñado para recibir el flujo de transporte MPEG2 230b y generar en base a ello el flujo de transporte MPEG2 232 encriptado al menos parcialmente. El adicionador de restricción de acceso está diseñado en este caso para encriptar, por un lado, una parte del flujo de transporte MPEG2 230b, por ejemplo, alguno o todos los paquetes de datos útiles del flujo de transporte del flujo de transporte MPEG2 230b y para añadirle, por otro lado, al flujo de transporte MPEG2 230b una información de restricción de acceso que, a un decodificador que conoce un secreto correspondiente, le permite realizar una desencriptación de las informaciones encriptadas del flujo de transporte MPEG2 232.

[0042] Aquí se alude además a que la funcionalidad del codificador DMB 230a también se puede realizar fuera del proveedor de flujo de transporte 230, de modo que el codificador DMB 230a luego no es parte del proveedor de flujo de transporte 230. Por lo demás también pueden estar combinadas las funcionalidades del codificador DMB 230a y del adicionador de restricción de acceso 230c. Así depende esencialmente de que el proveedor de flujo de transporte 230 proporcione un flujo de transporte MPEG2 232, según se ha explicado brevemente mediante la fig. 1 y según se explica todavía en detalle a continuación.

[0043] El proveedor de señal DAB 200 comprende además una así denominada pasarela DMB 240 que está diseñada para recibir el flujo de transporte MPEG2 232 y proveer en base a ello una señal de subcanal DAB 242 (DAB-Subchannel). El proveedor de señal DAB 200 comprende además un multiplexor DAB 250 que está diseñado para recibir la señal de subcanal DAB 242 y proveer en base a ello una señal DAB 200 que reproduce o describe, por ejemplo, una multiplicidad de servicios DAB en el multiplex.

2.1.2 Transporte de las informaciones de restricción de acceso (Informaciones CA)

[0044] Las informaciones que se refieren a la restricción de acceso (también designadas como informaciones CA), es decir, la indicación de que procedimiento de encriptación se usa, y el mensaje de control de autorización (aquí ECM), se transfieren de otro modo que en DVB. Mientras que la radiodifusión de vídeo digital DVB usa para ello paquetes de flujo de transporte MPEG especiales, las informaciones CA en el concepto de la invención se incluyen en paquetes de flujo de transporte MPEG que se transfieren con frecuencia en la radiodifusión multimedia digital de forma condicionada por el principio DMB, pero sólo se usan en parte y por ello pueden recibir en sí las informaciones CA. En este caso se trata preferiblemente de los paquetes que contienen la tabla de asignación de programa (PAT ("program association table")). Esta tabla PAT se transmite en la radiodifusión multimedia digital DMB de forma estandarizada al menos cada 500 milisegundos (véase ETSI TS 102 428, V1.2.1, apartado 6.2) y ocupa condicionado por el principio un paquete de flujo de transporte MPEG completo, aunque esta misma tabla es realmente pequeña (por ejemplo un tamaño de sólo 28 bytes). Queda inutilizado el resto del paquete, que tiene un

tamaño bruto de, por ejemplo, 188 bytes (véase ISO/IEC 13818-1: 2007 (E), apartado 2.4.3).

[0045] Esta tabla de asociación de programa PAT describe todos los programas contenidos en el flujo de transporte MPEG. Dado que la radiodifusión multimedia digital por definición sólo contiene un programa por flujo de transporte MPEG que se transmite en un subcanal DAB o DAB-Subchannel (al contrario de DVB en el que pueden estar contenidos varios programas en un flujo de transporte MPEG), esta tabla es siempre muy corta. Para los detalles respecto a ello se remite a la referencia [3], capítulo 6.2, donde se aduce que una tabla de asociación de programa PAT siempre debe describir un programa.

[0046] Las informaciones CA se codifican, según es habitual en MPEG, a través de así denominados descriptores CA ("CA descriptors"). Por consiguiente también es posible usar Simulcrypt. Uno o varios descriptores CA, que también pueden contener respectivamente uno o varios mensajes de clave de autorización ECM, se incluye en este caso respectivamente en un paquete PAT (así en un paquete de flujo de transporte que contiene una tabla de asociación de programa PAT) (por ejemplo en una tabla "CA_ECM_section" que todavía se describe abajo más en detalle, o en una tabla "CA_section" que todavía se describe abajo más en detalle). Esto significa entonces que las informaciones CA verdaderamente transmitidas, en algunos ejemplos de realización, son similares o incluso idénticas a las informaciones CA transferidas en DVB. Sin embargo, los datos (por ejemplo los datos de las informaciones CA) se incluyen según la invención en otros puntos y a saber, por ejemplo, igualmente en los paquetes PAT (por ejemplo en las tablas "CA_section" y "CA_ECM_section" y/o en las tablas "CA_data" descritas abajo más en detalle que están contenidas igualmente en los paquetes PAT).

[0047] La inclusión se realiza en este caso conforme a la inclusión prevista en el estándar DMB de así denominados datos PAD. En este caso se usa que en un paquete de flujo de transporte MPEG también se pueden incluir datos (privados) de propiedad, en el presente caso las informaciones CA. Para ello sirve el campo "transport_private_data" (un marcador que indica el transporte de datos privados) dentro del así denominado campo de adaptación "adaptation_field()" en la cabeza de mensaje del paquete de flujo de transporte. El así denominado campo de adaptación "adaptation_field()" representa en este caso un campo de adaptación que hace posible la transmisión de informaciones adicionales en la cabeza de mensaje de un paquete de flujo de transporte, pudiendo comprender las informaciones adicionales entre otros así denominados datos "privados" cuyo contenido no está especificado en los estándares correspondientes.

[0048] Pero la inclusión de las informaciones CA no está restringida a la tabla de asociación de programa PAT (o el paquete de flujo de transporte que contiene la tabla de asociación de programa PAT), sino que las informaciones CA se pueden incluir en principio en cada paquete de flujo de transporte MPEG que contenga suficiente espacio libre. Pero dado que habitualmente un codificador DMB ("DMB-Encoder") llenará todos los paquetes de flujo de transporte MPEG (o al menos paquetes de datos útiles del flujo de transporte MPEG) con datos útiles para usar también todo la tasa de datos, la mayoría de los paquetes de flujo de transporte MPEG (o al menos la mayoría de los paquetes de datos útiles del flujo de transporte MPEG) habitualmente se llenarán completamente con datos de audio / vídeo o datos multimedia o señalización. Por este motivo se prefiere recurrir, para la inclusión de las informaciones CA, esencialmente o incluso exclusivamente a aquellos paquetes de flujo de transporte MPEG que contienen la tabla de asociación de programa (PAT), dado que éstos no son apropiados de todos modos para una inclusión estandarizado de datos de audio codificados y/o datos de vídeo codificados por falta de un campo de datos correspondiente.

[0049] A continuación se describe el concepto para la inclusión de las informaciones CA en la cabeza de mensaje ("Header") de un paquete de flujo de transporte. Dado que la inclusión correspondiente presenta algunas similitudes con las inclusiones de así denominados datos PAD se hace aquí brevemente la comparación. En la inclusión PAD que se describe, por ejemplo, en la referencia [3], capítulo 9, los datos PAD se incluyen en el así denominado campo "transport_private_data" ("campo de datos privados de transporte") de los paquetes PAT (es decir, de los paquetes de flujo de transporte con una tabla de asociación de programa PAT). El primer byte del campo "transport_private_data" que comprende típicamente una multiplicidad de bytes porta en este caso un identificador que describe que datos se incluyen en este campo. En tanto que este valor (o el valor en el primer byte del campo "transport_private_data") para datos PAD es 0, este valor debería tener otro valor para las informaciones CA. El parámetro "transport_privatedata_length" en la cabeza de mensaje del paquete de flujo de transporte señala correspondientemente la longitud del campo con las informaciones CA mas 1 byte (correspondiéndose 1 o el byte adicional de la longitud del campo con el identificador). La inclusión de las informaciones CA se corresponde así, al menos en cierta manera, con la inclusión de los datos PAD. En algunos ejemplos de realización el identificador diferencia (o debería diferenciar) siempre los dos tipos de datos.

[0050] A continuación se entra brevemente de la tasa de datos transmitible. La tabla de asociación de programa PAT se transmite al menos cada 500 milisegundos. Si por paquete PAT, es decir, por paquete de flujo de corriente que contiene una tabla de asociación de programa PAT, se usasen por ejemplo 150 bytes para informaciones CA, de ello se produciría luego una tasa de datos de 300 bytes por segundo o 2400 bits por segundo (bps) para las informaciones CA.

[0051] Esta tasa de datos se aumenta eventualmente si se usasen también otros paquetes. En principio también sería posible como siempre que el codificador DMB ("DMB-Encoder") a veces deje sin usar paquetes de flujo de transporte MPEG completos (es decir, incorpore así denominados "null packets" o "paquetes nulos"). Esto se podría haber determinado en la configuración del codificador DMB o ocurrir cuando un flujo de datos de tasa de datos dinámica (por ejemplo así denominados datos multimedia BIFS) no usa, por ejemplo, brevemente la tasa de datos preconfigurado. Estos (desde el punto del codificador DMB) paquetes "de relleno" (inglés: "padding" o "null") se pueden usar opcionalmente igualmente para informaciones CA y por consiguiente pueden aumentar la tasa de datos para las informaciones CA.

[0052] Pero el procedimiento según la invención de incluir informaciones CA al menos parcialmente, pero alternativamente a ello también exclusivamente, en los paquetes PAT tiene la ventaja de que las mismas informaciones CA se pueden incluir cuando el codificador DMB usa la tasa de datos completa disponible, es decir, no genera paquetes "de relleno" (inglés "Padding" o "Null").

[0053] Para simplificar la inclusión de las informaciones CA, así como la encriptación de los paquetes de flujo de transporte MPEG, se prefiere según la invención (pero no es requerido necesariamente), usar sólo los paquetes PAT para la inclusión de las informaciones CA. Los paquetes PAT son por ello más apropiados ya que se pueden identificar fácilmente mediante su identificador de tipo paquete (PID). Así el identificador de tipo de paquete para los paquetes PAT es siempre igual a 0 (este valor no se define así justo por otros paquetes de flujo de transporte). Los paquetes PAT son más apropiados además para la inclusión de las informaciones CA, ya que se transmiten con suficiente frecuencia, y según la referencia [3] al menos cada 500 milisegundos, típicamente más frecuentemente. Además, los paquetes PAT son muy apropiados para la inclusión de las informaciones CA, ya que presentan de forma fiable capacidades de datos libre, en particular en DMB. Además, los paquetes PAT son muy apropiados para la inclusión de las informaciones CA, ya que la decodificación del flujo de datos MPEG siempre comienza con la tabla de asociación de programa PAT y por consiguiente las informaciones CA también están a disposición ya con la recepción de un paquete PAT. Lo último también garantiza que pese a la encriptación puede quedar no modificado el tiempo de sintonización (también designado como tiempo "Tune-in"), al menos si el decodificador CA (decodificador para las informaciones de restricción de acceso) en el lado de recepción no puede forzar un retardo adicional.

[0054] Opcionalmente sería posible usar paquetes "de relleno" (inglés: "Padding" o "Null") para la inclusión de las informaciones CA, ya que éstos se pueden identificar igualmente fácilmente mediante su identificador de tipo de paquete (PID) (PID == 0x1 FFF). Asimismo se pueden usar opcionalmente paquetes PMT, ya que estos presentan típicamente capacidades de datos libres y típicamente siguen directamente a los paquetes PAT. Lo último garantiza que pese a la encriptación pueda quedar no modificado el tiempo de sintonización (también designado como "Tune-in").

[0055] Sin embargo, naturalmente los paquetes "de relleno" (inglés: "Padding" o "Null") se pueden señalar opcionalmente también directamente como paquete con informaciones CA, es decir los identificadores de tipo de paquete (PID) se adaptan correspondientemente. Sin embargo, esto no es válido típicamente para paquetes con una tabla de reproducción de programa (PMT).

[0056] Cuando siempre están a disposición suficientes paquetes de relleno ("Padding" o "Null"), entonces no sería necesario el procedimiento según la invención y se podría usar directamente la encriptación conforme a DVB. Dado que sin embargo en la mayoría de los casos no se asegura que siempre estén a disposición suficientes paquetes de relleno que se puedan usar para una información CA, el concepto según la invención de incluir informaciones CA en los paquetes PAT traer ventajas muy considerables respecto al concepto mencionado simplificado de la transmisión de la información CA, dado que no se aumenta la tasa de datos del flujo.

[0057] A continuación se describen algunas mejoras opcionales que pueden estar implementadas en algunos ejemplos de realización según la invención.

[0058] Si en un DAB-Esemble se encriptan varios programas DMB, luego es razonable transmitir todos los

mensajes de gestión de autorización EMM en un único canal y transmitir por consiguiente todas las desconexiones de servicios y prolongaciones de servicios para todos los programas encriptados del DAB-Esemble en un canal separado. En este caso sólo se deben transmitir esencialmente mensajes de control de autorización (ECM) dentro del flujo de datos DMB encriptado. Por ello la inclusión en los paquetes PAT ya ofrece una tasa de datos suficiente para las informaciones CA (descripción de los procedimientos usados, así como los mensajes de control de autorización ECM). Los paquetes con la tabla de asociación de programa PAT se pueden identificar muy sencillamente, dado que el parámetro PID (identificación de programa o "program identification") que aquí también se designa como identificador de tipo de paquete, al comienzo de cada paquete de flujo de transporte MPEG tiene el valor fijo 0 (si se trata de un paquete PAT).

[0059] A continuación se explica brevemente como se señala el canal maestro (es decir, un canal separado con informaciones EMM) y se reconoce en el equipo receptor. Un acceso unívoco, sobre un canal fijo predefinido o un canal que se puede identificar de forma unívoca como tal, se puede hacer posible, por ejemplo, de la siguiente manera:

1. Se puede usar un subcanal fijo (por ejemplo subcanal 63) sin otra señalización;
2. Se puede usar una etiqueta de servicio fija, por ejemplo "EMM.CAS". Los receptores buscan luego un servicio con este nombre y lo usan eventualmente (por ejemplo para la recepción de EMM);
3. Un identificador de aplicación de usuario se puede transmitir en el rango de propiedad. Luego el servicio (que hace posible la transmisión del EMM) podría tener una etiqueta cualquiera, pero siempre sería visible en los receptores sin restricción de acceso ("receptores no CA").
4. El canal maestro se "pega" como componente de servicio secundario ("secondary service component") en el servicio DMB y el identificador de aplicación de usuario ("UserApplicationId") dice que son los EMM. Una solución semejante tiene varias ventajas. El receptor busca así la DMB. Esto debe ser los componentes de servicios primarios. Si hay (al menos) un componente de servicio secundario y éste usa el identificador de aplicación de usuario EMM (UserApplicationId) todavía a determinar, luego se pueden encontrar allí los EMM.

[0060] Los detalles con vistas a una codificación a modo de ejemplo de las informaciones CA se explican a continuación todavía más en detalle.

[0061] Por lo demás se alude que el proveedor de flujo de transporte 230 puede estar diseñado para proveer el flujo de transporte MPEG2 232 de manera que éste presente una o todas las propiedades arriba explicadas.

2.2 Proveedor de señal DAB según la fig. 2B

[0062] A continuación todavía se explica brevemente un proveedor de señal DAB 270 según la fig. 2B. El proveedor de señal DAB 270 está diseñado para recibir una información de medios digitales 272 que se puede corresponder, por ejemplo, con la información de medios digitales 210. El receptor de señal DAB 270 está diseñado además para proveer una señal DAB 274 que se puede corresponder, por ejemplo, con la señal DAB 220. El proveedor de señal DAB 270 comprende un proveedor de flujo de transporte 276 que está diseñado para recibir la información de medios digitales 272 y proveer en base a ello un flujo de transporte 280 encriptado al menos parcialmente.

[0063] El proveedor de señal DAB 270 comprende además un combinador de servicios DAB 290 que está diseñado para combinar el flujo de transporte MPEG-2 280 proporcionado por el proveedor de flujo de transporte 276 con uno o varios otros servicios DAB 292 a fin de obtener la señal DAB 274.

[0064] El proveedor de flujo de transporte 276 está diseñado, por ejemplo, para proveer un paquete de flujo de transporte 282 de un primer tipo de paquete que comprende una tabla de asociación de programa PAT y una información de restricción de acceso con informaciones de clave ECM. El proveedor de flujo de transporte 276 está diseñado además para proveer los paquetes de flujo de transporte de un segundo tipo de paquete que contienen una referencia a los identificadores de tipo de paquete de los paquetes de datos útiles del flujo de transporte. El proveedor de flujo de transporte está diseñado además para proveer los paquetes de flujo de transporte 286 de otro primer tipo de paquete (por ejemplo de un tercer tipo de paquete) que describen un contenido de un primer tipo de medio de la información de medios digitales 272 (por ejemplo audio), y para proveer los paquetes de flujo de transporte 288 de otro segundo tipo de paquete (por ejemplo de un cuarto tipo de paquete) que describen un

contenido de un segundo tipo de medio de la información de medios digitales 272 (por ejemplo vídeo). El proveedor de flujo de transporte 276 está diseñado en este caso para proveer el flujo de transporte 280 de modo que está encriptado un contenido de al menos alguno de los paquetes de flujo de transporte del otro primer tipo de paquete (por ejemplo del tercer tipo de paquete), o de modo que está encriptado un contenido de al menos alguno de los paquetes de flujo de transporte del otro segundo tipo de paquete (por ejemplo del cuarto tipo de paquete). Por lo demás, el proveedor de flujo de transporte 276 está diseñado para proveer la información de restricción de acceso, que está contenida en los paquetes de flujo de transporte 282 del primer tipo de paquete, de modo que ésta comprenda una información de clave para la descryptación de los contenidos encriptados de los paquetes de flujo de transporte 286 del otro primer tipo de paquete (por ejemplo del tercer tipo de paquete) o de los contenidos encriptados de los paquetes de flujo de transporte 288 del otro segundo tipo de paquete (por ejemplo del cuarto tipo de paquete). Por consiguiente, al menos algunos contenidos del flujo de transporte MPEG-2 280 están protegidos mediante una encriptación de contenido correspondiente frente a un acceso o entrada no autorizados. La información de clave necesaria para el descryptado se incluye en este caso mediante el proveedor de flujo de transporte 276 en los paquetes de flujo de transporte 282 del primer tipo de paquete. Si el proveedor de flujo de transporte 276 obtiene por lo demás los contenidos encriptados de los paquetes de flujo de transporte del otro primer tipo de paquete (por ejemplo del tercer tipo de paquete) o del otro segundo tipo de paquete (por ejemplo del cuarto tipo de paquete) en sí de forma encriptada o ya una información de medios digitales 272 encriptada al menos parcialmente, tiene en este caso un significado subordinado, pudiéndose utilizar las dos soluciones alternativas.

20 3. Analizador de flujo de transporte según la fig. 3

[0065] A continuación se describe un analizador de flujo de transporte 300 según un ejemplo de realización de la presente invención en referencia a la fig. 3, que muestra un diagrama de bloques de un analizador de flujo de transporte 300 semejante. El analizador de flujo de transporte 300 está diseñado para recibir un flujo de transporte 310 y suministrar en base a ello tanto una información de restricción de acceso 320 como también una información 322 sobre los identificadores de paquete que están asociados a los paquetes de flujo de transporte con contenidos de medios. El analizador de flujo de transporte 300 comprende un identificador de paquete 330 que está diseñado para identificar un paquete 332 de un primer tipo de paquete predeterminado, que presenta un primer identificador de tipo de paquete predeterminado y que contiene una tabla de asociación de programa PAT, como un paquete identificado. El analizador de flujo de transporte 300 comprende además un analizador de paquete que está diseñado para buscar el paquete de flujo de transporte identificado 332 del primer tipo de paquete según una información de restricción de acceso y proveer la información de restricción de acceso 320 encontrada. El analizador de paquete 340 está diseñado además preferiblemente para evaluar la tabla de asociación de programa en el paquete de flujo de transporte identificado 332 del primer tipo de paquete predeterminado y determinar, en base a la tabla de asociación de programa PAT, un segundo identificador de tipo de paquete 342 que está asociado a un paquete de flujo de transporte con una tabla de reproducción de programa. El analizador de flujo de transporte comprende un determinador de asociación de tipo de paquete 350 que está diseñado para identificar, en base al segundo identificador de tipo de paquete 342 determinado, un paquete de flujo de transporte con una tabla de reproducción de programa en el flujo de transporte, y para evaluar la tabla de reproducción de programa a fin de obtener una información 322 sobre que identificadores de tipo de paquete están asociados a los paquetes de flujo de transporte que contienen los contenidos de medios de la información de medios digitales restringida de acceso.

[0066] El analizador de flujo de transporte 300 está diseñado por consiguiente para extraer de un flujo de transporte 120, 232, 280 aquella información que es necesaria para conseguir nuevamente los contenidos de medios codificados y encriptados al menos parcialmente de la información de medios digitales 110, 210, 272. Con esta finalidad el analizador de flujo de transporte 300 analiza de manera eficiente justamente aquellos paquetes de flujo de transporte en los que está incluida la información relevante. Mediante una identificación y análisis de los paquetes de flujo de transporte del primer tipo de paquete, el analizador de flujo de transporte 300 obtiene de manera muy rápida y eficiente la información de restricción de acceso 320, de modo que mediante la nueva consecución de la información de restricción de acceso no se origina un retardo innecesario en la evaluación del flujo de transporte 310. Además, el analizador de flujo de transporte 300 usa el hecho de que en los paquetes de flujo de transporte del primer tipo de paquete está a disposición de todos modos típicamente una capacidad de bits para la inclusión de la información de restricción de acceso 320, que quedó no usado en conceptos alternativos. Además, en el analizador de flujo de transporte 300 la nueva consecución de la información de restricción de acceso es independiente de los paquetes de datos útiles del flujo de transporte, de modo que no se deben buscar estos paquetes de datos útiles del flujo de transporte (de otro tipo de paquete o de otros varios tipos de paquete, por ejemplo, del tercer tipo de paquete o del cuarto tipo de paquete) para la obtención de la información de restricción de acceso 320. En algunos ejemplos de realización sólo hay audio o vídeo como otros tipos de paquete. En otros ejemplos de realización también se usan además todavía otros tipos de paquete, por ejemplo, para la transmisión de

informaciones multimedia.

[0067] Opcionalmente el analizador de flujo de transporte 300 puede presentar por lo demás un descryptador que está diseñado para descryptar los contenidos de medios encriptados que están contenidos en los paquetes de flujo de transporte con los identificadores de tipo de paquete descritos en la tabla de reproducción de programa, usando las informaciones de restricción de acceso contenidas en el paquete de flujo de transporte del primer tipo de paquete predeterminado. En otras palabras, del flujo de transporte 310 se pueden filtrar tales paquetes de flujo de transporte cuyo identificador de tipo de paquete se describe por la información 322. Para la descryptación de estos paquetes filtrados se puede recurrir luego a la información de restricción de acceso 320 que comprende, por ejemplo, una información de clave. La información de clave puede estar presente en este caso, por ejemplo, de forma encriptada de modo que el analizador de flujo de transporte 300 la puede descryptar debido a su conocimiento de un secreto (por ejemplo de una clave secreta).

[0068] En otro ejemplo de realización, el analizador de flujo de transporte 300 puede estar diseñado para examinar el paquete de flujo de transporte 332 identificado del primer tipo de paquete predeterminado en cuanto a si un campo de información adicional presenta una o varias tablas que están caracterizadas por identificadores de tabla predeterminados y contienen una información de restricción de acceso. El analizador de flujo de transporte 300 puede proveer acto seguido las informaciones de restricción de acceso contenidas en las tablas identificadas. La funcionalidad correspondiente se puede percibir, por ejemplo, por el analizador de paquete 340. El analizador de paquete 340 está diseñado preferiblemente para verificar, en respuesta a una localización de una primera tabla que está caracterizada por un primer identificador de tabla predeterminado y que contiene una información de restricción de acceso, e independientemente de una información de longitud de tabla contenida en la primera tabla, si el campo de información adicional del paquete de flujo de transporte identificado 332 del primer tipo de paquete predeterminado presenta a continuación de la primera tabla otra tabla que contiene una información de restricción de acceso. Si se identifica otra tabla semejante, entonces la información de restricción de acceso contenida en la otra tabla se provee por el analizador de paquete 340. Mediante la configuración correspondiente el analizador de paquete 340 es capaz de evaluar una información de restricción de acceso extensa que está dividida en varias tablas, según se explica a continuación todavía más en detalle. En tanto que el analizador de flujo de transporte 300 es capaz de extraer de un campo de información adicional de un único paquete de flujo de transporte distintos tipos de informaciones de restricción de acceso, lo que de nuevo hace posible una codificación de una información de restricción de acceso compleja dentro de un único paquete de flujo de transporte.

4. Receptor DAB según la fig. 4

[0069] A continuación se describe todavía un receptor DAB según la fig. 4. La fig. 4 muestra un diagrama de bloques de un receptor 400 semejante. El receptor DAB está diseñado para recibir una señal DAB 410 que comprende preferiblemente una información de medios digitales encriptada al menos parcialmente (preferiblemente incluso una información multimedia), y para proveer en base a ello una información de medios digitales descryptada (o incluso una información multimedia digital descryptada) 420. El receptor DAB 400 comprende un separador de servicios DAB 430 que está diseñado para recibir la señal DAB 410 y proveer en base a ella una información de servicios DAB 432, que comprende, por ejemplo, una información de audio DAB, así como un flujo de transporte MPEG-2 434. El receptor DAB comprende además un analizador de flujo de transporte 440 que se corresponde, por ejemplo, con el analizador de flujo de transporte 300 descrito mediante la fig. 3. El analizador de flujo de transporte 440 está diseñado para recibir el flujo de transporte MPEG-2 434 del separador de servicios DAB 430 y para proveer, en base al flujo de transporte MPEG-2 434, la información de restricción de acceso 442 para la descryptación de la información de medios digitales restringida de acceso. El receptor DAB 400 comprende además un descryptador de contenido 450 que está diseñado para descryptar los contenidos de medios encriptados de la información de medios digitales restringida de acceso, usando la información de restricción de acceso 442 y para obtener por consiguiente la información de medios digitales 442 descryptada.

[0070] La descryptador de contenido 450 puede estar diseñado, por ejemplo, para seleccionar los paquetes a descryptar en función de una información 444 sobre los identificadores de tipo de paquete que están asociados a los paquetes de flujo de transporte con contenidos de medios, y que se suministra por el analizador de flujo de transporte 440, o bien extraerla del flujo de transporte MPEG-2 434.

[0071] Por consiguiente el receptor 400 puede obtener de manera eficiente una información de medios digitales 420 descryptada a partir de la señal DAB 410, usando el receptor DAB 400 el concepto según la invención para la inclusión de informaciones de restricción de acceso en paquetes de flujo de transporte con una tabla de asociación de programa PAT, a fin de obtener tan rápido como sea posible y las informaciones de restricción de acceso 442 con

baja sobrecarga de recursos.

5. Estructura del flujo de transporte y codificación de las informaciones CA

5 **[0072]** A continuación se explica de forma detallada la estructura del flujo de transporte, así como la codificación de las informaciones CA. Correspondiente a esto se debería tener en cuenta que el proveedor de flujo de transporte 100 o el proveedor de señal DAB 200 está diseñado para proveer un flujo de transporte de la estructura descrita a continuación. Por lo demás el analizador de flujo de transporte según la fig. 3 o el receptor DAB según la fig. 4 está diseñado para evaluar un flujo de transporte correspondiente.

10

5.1. Flujo de transporte según las fig. 5a y 5b

[0073] La fig. 5a muestra una representación esquemática de un flujo de transporte que es, por ejemplo, un flujo de transporte MPEG-2. El flujo de transporte MPEG-2 500 comprende una secuencia de paquetes de flujo de transporte 510, 520, 530 que también se designan abreviadamente como "TS packet" y a los que se asocian diferentes identificadores de tipo de paquete. Sin embargo aquí se alude a que naturalmente siempre aparecen de nuevo típicamente paquetes de flujo de transporte del mismo tipo de paquete o con el mismo identificador de tipo de paquete.

20 **[0074]** La fig. 5b muestra una descripción de la sintaxis de un flujo de transporte MPEG. Una secuencia continua de paquetes de flujo de transporte ("transport_packet") se puede ver en que al comienzo de cada paquete de flujo de transporte aparece una secuencia de bits de sincronización, por ejemplo, en forma de bytes de sincronización. Los detalles con vistas a la sintaxis de un flujo de transporte MPEG están definidos, por ejemplo, en ISO/IEC 13818-1, de modo que para los detalles se remite ello.

25

5.2. Visión de conjunto de diferentes tipos de paquetes de flujo de transporte según la fig. 6

[0075] La fig. 6 muestra una representación esquemática de diferentes tipos de paquete que están contenidos en un flujo de transporte MPEG-2 multimedia según la invención. Los tipos de paquete que se muestran en la fig. 6 son apropiados, por ejemplo, para una transmisión de una información multimedia usando un modo de flujo de datos del concepto de transmisión DAB. Los detalles con vista a los tipos de paquete del flujo de transporte que se muestran en la fig. 6 se describen por lo demás en ETSI TS 102 428 V1.2.1. En este caso se remite en particular a la descripción en el anexo 2 de ETSI TS 102 428 V1.2.1 en la página 30. Sin embargo el flujo de datos descrito en la fig. 6 se modifica en el sentido de que la sección de asociación de programa ("program association section") también comprende adicionalmente a la tabla de asociación de programa PAT todavía la información de restricción de acceso.

[0076] Por consiguiente el flujo de transporte MPEG según la fig. 6 presenta un paquete de flujo de transporte 610 de un primer tipo de paquete que se caracteriza por un identificador de tipo de paquete PID = 0x0000. La tabla de asociación de programa PAT del paquete de flujo de transporte 610 define por lo demás que una tabla de reproducción de programa, que pertenece al programa con el número de programa 0X0001, está contenida en un paquete de flujo de transporte 620 de un segundo tipo de paquete. Con esta finalidad la tabla de asociación de programa PAT del primer paquete de flujo de transporte 610 comprende una referencia al identificador de tipo de paquete 0x0100 del paquete de flujo de transporte 620 del segundo tipo de paquete. La tabla de reproducción de programa en el paquete de flujo de transporte 620 comprende entre otros referencias a otros paquetes de flujo de transporte con los identificadores de tipo de paquete PID = 0x0111, PID = 0x0112, PID = 0x0113 y PID = 0x0114. Por consiguiente la tabla de asociación de programa PMT del paquete de flujo de transporte 620 también remite entre otros a paquetes de flujo de transporte con otro tipo de paquete (por ejemplo un tercer tipo de paquete) a los que se les asigna el identificador de tipo de paquete PID = 0x0113 y que contienen, por ejemplo, una información de imagen codificada. Además, la tabla de asociación de programa PMT del segundo paquete de flujo de transporte 620 remite a los paquetes de flujo de transporte de otro tipo de paquete (por ejemplo de un cuarto tipo de paquete) con identificador de tipo de paquete asociado PID = 0x0114 que describen un contenido de audio de la información multimedia.

50 **[0077]** Además, la tabla de asociación de programa PMT del segundo paquete de flujo de transporte 620 también comprende referencias a paquetes de configuración de flujo de transporte 630, 640 que presentan, por ejemplo, identificadores de paquete PID = 0x0111 y PID = 0x0112. Para los detalles con vista al significado de estos paquetes de configuración 630, 640 se remite a ISO/IEC 13818-1 y ISO/IEC 14496-1. Los detalles correspondientes no tienen importancia aquí. Para informaciones amplias se remite sin embargo a los estándares mencionados que se conocen

adecuadamente por el especialista.

5.3. Estructura y sintaxis del paquete de flujo de transporte del primer tipo de paquete según la fig. 7,8a y 8b

5 **[0078]** A continuación mediante la fig. 7 se describe la estructura exacta de un paquete de flujo de transporte del primer tipo de paquete (PID = 0x0000) que contiene tanto la información de restricción de acceso como también la tabla de asociación de programa PAT. El paquete de flujo de transporte del primer tipo de paquete comprende en una posición predeterminada de una cabeza de mensaje de paquete (también designada como "Header" o "preámbulo") el identificador de tipo de paquete PID = 0x0000, de modo que se puede localizar o identificar sin
10 esfuerzo el paquete de flujo de transporte del primer tipo.

[0079] El paquete de flujo de transporte del primer tipo de paquete comprende además un marcador de 2 bits ("adaptation_field_control") que indica si está presente un así denominado campo de adaptación ("adaptation_field"), y para indicar además si está presente una tabla de asociación de programa ("program association table", PAT) en
15 una sección de asociación de programa ("program_association_section"). A continuación se parte de que están presentes tanto el campo de adaptación que se puede ver como campo de información adicional, como también la tabla de asociación de programa PAT en la sección de asociación de programa.

[0080] El campo de adaptación comprende un marcador de 1 bit "transport_private_data_flag" que indica si el
20 campo de adaptación comprende así denominados "datos privados" que no están sometidos típicamente a la estandarización en el marco del ISO/IEC. Además, el campo de adaptación, al menos en caso de existencia de datos privados, comprende una información "transport_private_data_length" que indica la longitud de los datos privados. El campo de adaptación comprende además los datos privados (también designados como "private_data byte" o bytes de datos privados), que comprenden aquí una información de restricción de acceso o se componen de
25 una información de restricción de acceso. La información de restricción de acceso puede estar depositada en este caso en una o varias tablas que son parte de los datos privados, como se expone a continuación todavía más en detalle.

[0081] A continuación la estructura de un paquete de flujo de transporte se explica brevemente mediante la
30 descripción de la sintaxis según la fig. 8a. Un paquete de flujo de transporte ("transport_packet") que es parte de un flujo de transporte MPEG2 comprende entre otros un byte de sincronización "synch_byte" que está contenido en un prefijo de 4 bytes del paquete de flujo de transporte. El paquete de flujo de transporte comprende además un identificador de tipo de paquete PID que indica el tipo de paquete. El paquete de flujo de transporte comprende además un marcador de 2 bits "transport_scrambling_control" que indica si el contenido de datos del paquete de
35 flujo de transporte está encriptado o con que clave está encriptado el contenido de datos del paquete de flujo de transporte. El paquete de flujo de transporte comprende además un marcador de 2 bits "adaptation_field_control" que indica si está presente un así denominado "campo de adaptación" ("adaptation_field"), y si están presentes bytes de datos (data_byte). El así denominado campo de adaptación precede preferiblemente los otros bytes de datos en el paquete de flujo de transporte. Para detalles con vistas al significado de los elementos individuales de la
40 sintaxis se remite aquí a ISO/IEC 13818-1.

[0082] La fig. 8b muestra por lo demás una representación de la sintaxis de un campo de adaptación de un
paquete de flujo de transporte. El campo de adaptación comprende un valor de longitud del campo de adaptación "adaptation_field_length" que indica la longitud del campo de adaptación. El campo de adaptación comprende por lo
45 demás una multiplicidad de marcadores "discontinuity_indicator", "random_access_indicator", "elementary_stream_priority_indicator", "PCR_flag", "OPCR_flag", "splicing_point_flag", "transport_private_data_flag" y "adaptation_field_extension_flag". El marcador "transport_private_data_flag" indica en este caso si el campo de adaptación comprende así denominados "datos privados" que no están especificados por ISO/IEC, y según la invención se usan para el transporte de una información de restricción de acceso.

[0083] El campo de adaptación comprende, por ejemplo, opcionalmente los parámetros
"program_clock_reference_base" y "program_clock_reference_extension" cuando está puesto el marcador "PCR_flag". Además, el campo de adaptación comprende opcionalmente un parámetro "splice_countdown" cuando
50 está puesto el marcador "splicing_point_flag".

[0084] El campo de adaptación comprende además una sección de datos privados si está puesto el marcador
"transport_private_data_flag". La sección de datos privados comprende, si está presente, una indicación de longitud "transport_private_data_length" que indica la longitud de la sección de datos privados. La sección de datos privados
55 comprende además, si está presente, uno o varios bytes de datos privados "private_data_byte". Los bytes de datos

privados "private_data_byte" se usan en un ejemplo de realización preferido de la invención para codificar la información de restricción de acceso. En otras palabras, la sección de datos privados de un campo de adaptación "adaptation_field" en un paquete de flujo de transporte, que porta la tabla de asociación de programa y está caracterizado por un identificador de tipo de paquete correspondiente PID = 0x000, comprende la información de restricción de acceso, por ejemplo, en forma de una o varias tablas que a continuación se explican todavía más en detalle. Para los detalles con vistas a la sintaxis del campo de adaptación se remite por lo demás a ISO/IEC 13818-1 y a ETSI TS 102 428 V1.2.1.

5.4 Sintaxis de las tablas "CA_section", "CA_ECM_section" y "CA_data"

[0085] A continuación mediante las fig. 9a, 9b, 10 y 11 se describe la sintaxis de diferentes tablas que contienen la información de restricción de acceso. La información de restricción de acceso, que se describe, por ejemplo, por la sección de datos privados del campo de adaptación según la fig. 8, puede presentar, por ejemplo, para la descripción de los mensajes de gestión de autorización una sección de tabla con la sintaxis según las fig. 9a y 9b. La sección de tabla comprende, por ejemplo, un identificador de tabla "table_id" que designa el tipo de la tabla. El identificador de tabla "table_id" se puede seleccionar, por ejemplo, de forma unívoca para diferenciar la tabla según las fig. 9a y 9b de otras tablas con informaciones de restricción de acceso. La sección de tabla según la fig. 9a comprende además un marcador "section_syntax_indicator" que puede estar puesto, por ejemplo, a un valor predeterminado. Además, la sección de tabla comprende una información de longitud "section_length" que describe una longitud de la sección. Además, la sección de tabla comprende un identificador "version_number" que describe un número de versión de la sintaxis. Un marcador "current_next_indicator" indica si las informaciones transmitidas se deben aplicar para un contenido actual o para un contenido de medios transmitido posteriormente. Una información "section_number" indica un número de una sección para hacer posible una división de la información de restricción de acceso en varias secciones. Una información "last_section_number" describe un número de una última sección. Además, la sección según la fig. 9a comprende uno o varios descriptores "descriptor" cuya sintaxis y significado se explica mediante la descripción de la sintaxis de la fig. 9b. Finalmente la sección de tabla también comprende según la fig. 9a todavía una suma de comprobación "CRC_32".

[0086] El descriptor "CA_descriptor", cuya sintaxis se muestra en la fig. 9b y que puede asumir el papel del descriptor "descriptor" mostrado en la fig. 9a, comprende una característica del descriptor "descriptor_tag" y una indicación de longitud del descriptor "descriptor_length". Además, el descriptor descrito en la fig. 9b comprende una característica de sistema "CA_system_ID" que describe el tipo del sistema de restricción de acceso. Además, el descriptor según la figura 9b comprende un indicador de tipo de paquete "CA_PID" que indica el identificador de tipo de paquete PID de los paquetes de flujo de transporte que contienen las informaciones de mensajes de gestión de autorización. En tanto que el descriptor puede presentar una referencia a los paquetes de flujo de transporte determinados con el identificador de tipo de paquete CA_PID. Pero la referencia "CA_PID" también puede verse como referencia a otra tabla que está contenida en la zona de datos privados del mismo paquete de flujo de transporte o de otro paquete de flujo de transporte, y que presenta un identificador que es igual al valor descrito por el descriptor "CA_PID". Por consiguiente se puede establecer una referencia entre una tabla "CA_section()" y una tabla "CA_data()". Pero alternativamente a ello (es decir, alternativamente a una referencia a otro paquete de flujo de transporte o a otra tabla) el descriptor también puede comprender directamente mensajes de gestión de autorización que pueden estar suspendidos, por ejemplo, al final del descriptor correspondiente como bytes de datos privados ("private_data_byte").

[0087] Alternativamente o adicionalmente el descriptor también puede presentar una referencia a un canal determinado en el que se transmiten los mensajes de gestión de autorización EMM.

[0088] A continuación se expone mediante la descripción de sintaxis de la fig. 10 como pueden estar codificadas las referencias a los mensajes de control de autorización. La descripción de la sintaxis de la fig. 10 describe una tabla que puede estar contenida, por ejemplo, alternativamente a la tabla según la fig. 9a o también adicionalmente a la tabla según la fig. 9a en la sección de datos privados del campo de adaptación según la fig. 8b. En este caso se puede ver que la sintaxis de la tabla "CA_ECM_section()" de la fig. 10 se corresponde esencialmente con la sintaxis de la tabla según la fig. 9a. Sin embargo en la tabla según la fig. 10 se pueden usar, por ejemplo, otros descriptores "descriptor" que en la tabla según la fig. 9a. Por ejemplo, los descriptores en la tabla según la fig. 10 pueden constituir directamente los mensajes de control de autorización ECM en lugar de constituir solo referencias.

[0089] Para detalles con vistas al significado de los elementos de sintaxis individuales de la tabla según la fig. 10 se remite por lo demás a la descripción que se refiere a la tabla según la fig. 9a. Pero en las dos tablas no son necesarios todos los marcadores o valores indicados, de modo que opcionalmente se pueden suprimir algunos de

los marcadores o valores que no se refieren directamente a la información de restricción de acceso.

[0090] La fig. 11 muestra una descripción de la sintaxis de otra tabla con informaciones de restricción de acceso que, alternativamente o adicionalmente a las tablas según las figuras 9a y 10, puede estar contenida en la zona de datos privados del campo de adaptación según la fig. 8. La tabla según la fig. 11 comprende un identificador de tabla "table_ID" que adopta típicamente otro valor que los identificadores de tabla según las tablas de las figuras 9a y 10. Además, la tabla según la fig. 11 puede presentar una referencia "CA_PID" (en forma de un identificador de tipo de paquete). La referencia "CA_PID" en la tabla "CA_data()" puede remitir, por ejemplo, a un tipo de paquete que comprende amplias informaciones de restricción de acceso. Alternativamente a ello el valor "CA_PID" en la tabla "CA_data()" también puede indicar que la tabla "CA_data()" porta informaciones que normalmente estarían contenidas en un paquete de flujo de transporte separado del tipo "CA_PID". Por consiguiente, de otra tabla, por ejemplo, la tabla "CA_section()" o la tabla "CA_ECM_section()" se puede remitir a la tabla "CA_data()", identificándose la tabla "CA_data()" por el valor en el campo "CA_PID" como objetivo de referencia. La tabla según la fig. 11 puede contener además informaciones de restricción de acceso de propiedad en un campo "proprietary_CA_información", cuya longitud se puede describir, por ejemplo, mediante una descripción de longitud "CA_info_length".

[0091] A continuación se resumen algunos aspectos con vistas a una codificación a modo de ejemplo de las informaciones CA. La inclusión de las informaciones CA se realiza, por ejemplo, en el campo "transport_private_data" dentro del campo de adaptación "adaptation_field()" en la cabeza de mensaje del paquete de flujo de transporte. Esta inclusión se realiza, por ejemplo, análogamente a lo descrito en la referencia [3]. En una inclusión, según se describen en la referencia [3], el primer byte (dentro de la secuencia de valores de datos "private_data_byte") indica que datos están incluidos en el campo "transport_private_data" (también designado como zona de datos privados). La referencia [3] describe en la tabla 12 los identificadores permitidos siguientes para un transporte de datos privados:

Identificador	Carga útil ("payload")
0	PAD
1 a 255	Reservado

[0092] La codificación a modo de ejemplo descrita a continuación complementa esta codificación y garantiza que el primer byte en el campo "transport_private_data" (según la descripción de longitud "transport_private_data_length") sea respectivamente diferente del valor 0 (que ya está previsto para PAD).

[0093] Correspondiente a esto se advierte que los datos PAD sólo están permitidos para radio DMB (así no para televisión DMB). Pero la codificación propuesta a continuación garantiza, incluso en el caso de radio DMB, que un receptor de radio DMB existente no interpretaría como datos PAD los datos del campo "transport_private_data", que se refieren a una restricción de acceso.

[0094] Mientras que la codificación PAD, que se usa cuando el primer byte (según la descripción de longitud "transport_private_data_length") tiene el valor 0, parte de que todos los otros datos del campo "transport_private_data" son ahora datos PAD, la codificación siguiente se ocupa de que se puedan disponer varios campos de datos de distinto tipo en un campo "transport_private_data" (y se puedan extraer de él mediante un analizador de flujo de transporte).

[0095] En las informaciones de restricción de acceso se deben diferenciar:

- Referencias a mensajes de gestión de autorización EMM; éstas pueden estar codificadas, por ejemplo, según la sección de restricción de acceso "CA_section()" según la referencia [6], con una referencia a un PID de los paquetes de gestión de autorización (paquetes EMM) en el mismo flujo de transporte MPEG (eventualmente también codificado conforme a los mensajes de control de autorización ECM de propiedad) o otro flujo de transporte MPEG.
- Referencias a mensajes de control de autorización ECM; éstas pueden estar codificadas, por ejemplo, según se describe abajo con vistas a la tabla "CA_ECM_section()" (eventualmente en conexión con la tabla "CA_data()").
- Estructuras de datos para los mensajes de control de autorización ECM de propiedad y otros datos CA; éstas pueden estar codificadas, por ejemplo, según se describe abajo.

• Referencias a mensajes de control de autorización ECM pueden estar codificadas, por ejemplo, según se describe mediante la descripción de la sintaxis de la fig. 10. La codificación según la descripción de sintaxis en la fig. 10 es esencialmente idéntica a la codificación de la sección de restricción de acceso "CA-section()" según la referencia [6], siendo sólo el identificador de tabla "table_ID" otro dado que ésta tabla sirve para la localización de los mensajes de control de autorización ECM, mientras que la tabla "CA_section()" sirve para la localización de mensajes de gestión de autorización EMM. El identificador de tabla "table_ID" podría ser igual, por ejemplo, a 0x2 para la tabla "CA_ECM_section()", a fin de poder diferenciar esta información de los datos PAD en el caso de radio DMB (identificador de tabla 0x0) y de los datos de una tabla "CA_section()" (identificador de tabla 0x1).

[0096] Los identificadores contenidos en descriptor "CA_descriptor" de las tablas según las figuras 9a y 10 ("CA_ECM_section()" o "CA_section()" o identificadores de tipo de paquete ("valores CA_PID") identifican habitualmente los tipos de paquete PID de los paquetes de flujo de transporte que contienen informaciones ECM (tabla "CA_ECM_section()" según la fig. 10) o informaciones EMM (tabla "CA_section()" según la fig. 9a). Según la presente invención, los identificadores "CA-PID" se pueden usar como identificadores para identificar la información CA de propiedad ("proprietary_CA_information()") contenida en una tabla "CA_data()". En otras palabras, en lugar de usar paquetes de flujo de transporte separados con un tipo de paquete específico asociado para la transmisión de la información ECM o la información EMM, la información ECM o información EMM puede estar contenida en subtablas "CA_data()" según la fig.11. Estas subtablas "CA_data()" pueden estar contenidas, así como las tablas "CA_section()" y "CA_ECM_section()", en el campo de adaptación o en la zona de datos privados ("private_data_byte") del campo de adaptación ("adaptation_field"). Las tablas CA_section(), CA_ECM_section() están preferiblemente en los paquetes de flujo de transporte que contienen la tabla de asociación de programa, dado que en estos paquetes todavía hay suficiente espacio típicamente independientemente de la tasa de bits de codificación de los datos útiles (datos de audio o datos de video).

[0097] La estructura de datos para informaciones ECM, que se puede usar en principio también para informaciones EMM y otros datos CA (es decir, datos para la restricción de acceso), puede estar codificada, por ejemplo, según se muestra en la descripción de la sintaxis de la fig. 11. Si es necesario, es decir, por ejemplo, en caso de gran necesidad de datos, la información CA de propiedad ("proprietary_CA_information()") también se podría entregar fragmentada. La codificación exacta se le entrega al sistema de restricción de acceso correspondiente o sistema CA. Una tabla con informaciones CA, que está designada con "CA_data()", comprende, por ejemplo, un identificador de tabla "table_ID" así como un identificador "CA_PID". El identificador CA_PID se corresponde en este caso con un identificador que está contenido, por ejemplo, por el valor "CA_PID" en un descriptor "CA_descriptor()" de una tabla "CA_section()". Por consiguiente, por ejemplo, la tabla "CA_section()" comprende a través del valor CA_PID del descriptor "CA_descriptor" una referencia a una tabla determinada "CA_data()". En otras palabras, el valor CA_PID de la tabla "CA_data()" indica a que tabla subordinada "CA_section()" o "CA_ECM_section()" se le asocia la información CA de propiedad "proprietary_CA_information()" contenida en la tabla "CA_data()". La tabla "CA_data" comprende por lo demás una indicación de longitud "CA_info_length" que indica una longitud de la información CA de propiedad "proprietary_CA_information()" contenida en la tabla "CA_data()".

[0098] El identificador de tabla "table_ID" de la tabla "CA_data()" puede ser, por ejemplo, 0x3 para poder diferenciar estas informaciones de los datos PAD en el caso de radio DMB, de "CA_section()" y/o "CA_ECM_section()".

[0099] Una secuencia de las tablas "CA_section()", "CA_ECM_section()" y/o "CA_data()" se transmite preferiblemente en el campo "transport_private_data" de los paquetes PAT y opcionalmente también de los paquetes "de relleno" (también designados como paquetes "Padding" o "Null"). Dado que cada elemento individual (o cada tabla individual) porta una indicación de tipo (el identificador de tabla "table_ID") así como un identificador de longitud (por ejemplo el indicador de longitud "section_length") o la indicación de longitud "CA_info_length", esta secuencia (de tablas) se puede dividir fácilmente de nuevo en los elementos individuales (tablas individuales).

[0100] La verdadera encriptación se puede realizar, por ejemplo, en el plano de flujo de transporte MPEG. En este caso se le entrega al encriptador o "scrambler" si se encriptan todos los paquetes, salvo paquetes con la tabla de asociación de programa PAT o paquetes "de relleno" (así denominados paquetes "padding" o paquetes "null"), o si se encriptan de forma selectiva, de modo que, por ejemplo, la tabla de reproducción de programa PMT y un componente de audio se dejan no encriptados. En el caso de una encriptación parcial se debería adaptar la tabla de asociación de programa PAT a fin de señalar a los receptor que se encripta. El parámetro

"transport_scrambling_control_values" en la cabeza de mensaje del paquete de flujo de transporte puede indicar en este caso si un paquete de flujo de transporte MPEG contiene datos encriptados. Por ejemplo, con vistas al parámetro "transport_scrambling_control" se puede usar la asociación según la tabla en la fig. 12.

5 5.5. Sintaxis de la tabla de asociación de programa PAT ("program_association_section")

[0101] A continuación se describe todavía brevemente la tabla de asociación de programa PAT o la sección de asociación de programa que se puede representar, por ejemplo, mediante los datos "data-byte" de un paquete de flujo de transporte con el identificador de paquete PID = 0x0000.

10

[0102] Una representación de la sintaxis de la sección de asociación de programa "program-association-section()" se muestra en la fig. 13. La sección de asociación de programa comprende un identificador de tabla "table_ID" así como un marcador de la sintaxis "section_syntax_indicator". Además, la sección de asociación de programa comprende una indicación de longitud "section_length". Junto a ello la sección de asociación de programa comprende un identificador de flujo de transporte "transport_stream_ID", así como una indicación de número de versión "version_number". Por lo demás la sección de asociación de programa comprende un marcador "current_next_indicator" que muestra si la sección de asociación de programa debe ser efectiva para contenidos de medios actuales o para contenidos de medios transferidos posteriormente. Junto a ello la sección de asociación de programa comprende una indicación de número de sección "section_number", así como una indicación "last_section_number" que designa una última sección de una secuencia de secciones. Los números de sección mencionados hacen posible dividir una sección de asociación de programa en varios paquetes.

15

20

[0103] Además, la sección de asociación de programa comprende un identificador de número de programa "program_number" así como un identificador de tipo de paquete "program_map_PID" que muestra un tipo de paquete de un paquete de flujo de transporte que comprende una tabla de asociación de programa.

25

[0104] Finalmente la sección de asociación de programa también comprende una suma de comprobación "CRC_32".

30 6. Comportamiento del receptor

[0105] A continuación se describe brevemente el comportamiento de un receptor que recibe el flujo de transporte explicado arriba. Un receptor DMB-CA, es decir un receptor para una radiodifusión multimedia digital con restricción de acceso, se comporta según la selección de un flujo de datos DMB, como sigue:

35

[0106] En una primera etapa el receptor espera a la tabla de asociación de programa PAT. Ésta se puede reconocer fácilmente en el identificador de tipo de paquete o la identificación de programa PID en la cabeza de mensaje del flujo de transporte MPEG, dado que este identificador de tipo de paquete debe ser 0 (o presentar otro valor predeterminado). En este paquete de flujo de transporte MPEG se reconoce ahora mediante los descriptores de restricción de acceso incluidos en las tablas "CA_ECM_section()" o "CA_section()" dentro de la zona de datos privados "transport_private_data", si se usa una restricción de acceso CA, y si apoya al sistema de restricción de acceso (CA-System) usado. En caso afirmativo debe evaluar el descriptor de restricción de acceso del procedimiento apoyado por él. Eventualmente el receptor debe esperar así también a otros paquetes PAT (o paquetes "de relleno" o paquetes "Padding" o paquetes "Null") y/o a los "restantes" paquetes de restricción de acceso o paquetes CA, hasta que se recogen todas las informaciones necesarias. A continuación se puede reconocer ahora en cada otro paquete de flujo de transporte MPEG (así paquetes con un identificador de tipo de paquete PID ≠ 0) mediante los valores de la información "transport_scrambling_control" si el paquete está encriptado y que clave se necesita eventualmente.

40

45

[0107] Un comportamiento de recepción correspondiente se puede obtener, por ejemplo, al menos parcialmente por el analizador de flujo de transporte 300 o por el receptor DAB 400.

50

7. Conceptos alternativos

[0108] A continuación se describen todavía algunos conceptos alternativos y posibles actualmente referidos a la estructura base de los procedimientos de restricción de acceso para la radiodifusión multimedia digital DMB.

55

7.1 Encriptación según la referencia [6]

[0109] Para una realización de una restricción de acceso se puede realizar, por ejemplo, una encriptación de flujos de transporte MPEG (por ejemplo de paquetes de flujo de transporte MPEG-2 a respectivamente 188 bytes) o de programas completos codificados en MPEG-4 o partes de programas (como por ejemplo, flujos de programa elementales PES). Esta encriptación se corresponde con la encriptación usada en el DVB-T.

5

[0110] A continuación se describe brevemente este procedimiento de encriptación. La fig. 15 muestra un diagrama de bloques de un proveedor de señal. El proveedor de señal 1500 según la fig. 15 comprende un codificador DMB 1520 que está diseñado para recibir una información de medios, por ejemplo, una información de audio y/o una información de video 1510, y proveer en base a ello un flujo de transporte MPEG-2 1522. Un restrictor de acceso o

10

adicionador de restricción de acceso 1530 recibe el flujo de transporte MPEG-2 1522 y proporciona en base a ello un flujo de transporte MPEG-2 1532 encriptado al menos parcialmente. Una pasarela DMB 1540 recibe el flujo de transporte MPEG-2 1532 encriptado al menos parcialmente y proporciona en base a ello una señal de subcanal DAB 1542. Un multiplexor DAB 1550 recibe la señal de subcanal DAB 1542 y provee en base a ello la señal DAB.

15

[0111] El codificador DMB (DMB-Encoder) 1520 describe el programa codificado y su elemento de programa (por ejemplo audio y vídeo) dentro de la tabla de reproducción de programa PMT. En el caso de un flujo de datos encriptado esta señalización también debe describir lo que se encripta (programa completo o sólo parte de un programa) y con qué procedimientos. Además, para la desencriptación también se deben incluir informaciones de restricción de acceso necesarias (por ejemplo informaciones ECM) en el flujo de datos del flujo de transporte MPEG-

20

2. **[0112]** Ahora el codificador DMB 1520 añade la señalización necesaria (aunque el mismo ya no encripta necesariamente), o el módulo de restricción de acceso (módulo CA 1530) adapta la información de señalización y añade las informaciones de restricción de acceso necesarias. Dado que está prevista la tasa de datos de un subcanal DAB 1542 esto significa que el codificador DMB 1520 no debe usar toda la tasa de datos del subcanal, sino que no usa una parte de la tasa de datos (es decir, un número determinado de paquetes de flujo de transporte MPEG) y éste está a disposición por consiguiente del módulo de restricción de acceso 1530. La transmisión de un paquete de flujo de transporte MPEG por segundo se corresponde en este caso con una tasa de datos de 1632 bit/s (incluso de la protección adicional frente a error).

30

[0113] El procedimiento recién descrito conlleva sin embargo algunas desventajas del procedimiento que se describen a continuación. El codificador DMB 1520 no debe realizar por sí mismo una encriptación, pero debe ser capaz de dejar sin usar al menos un número determinado de paquetes de flujo de transporte MPEG, para que éste esté a disposición para la transmisión de las informaciones de restricción de acceso (y una tabla de reproducción de programa PMT alargada eventualmente por una señalización de restricción de acceso). Esto significa una adaptación necesaria de estos codificadores 1520. Un codificador que se ha desarrollado para la DMB no encriptada se debe modificar para que sea posible la DMB encriptada.

35

7.2. Encriptación de los subcanales DAB según la referencia [5]

40

[0114] A continuación se describe una encriptación de subcanales DAB (también designados como "subchannels") que también se designa de forma abreviada como "DAB subchannel CA".

45

[0115] Un subcanal DAB es un canal de tasa de datos fija. Cada 24 ms un receptor DAB obtiene en cada subcanal DAB un número fijo de bytes, denominado marco DAB o "DAB Frame". El número de bytes depende de la tasa de bits (fija) del canal.

50

[0116] En la restricción de acceso del subcanal DAB (DAB subchannel CA) existe un marco DAB de dos partes. La primera parte del marco contiene datos CA (por ejemplo ECMs, EMMs) y la segunda y a distancia mayor parte del marco contiene los datos útiles encriptados.

55

[0117] La fig. 16 muestra con la referencia 1610 la representación esquemática de los marcos DAB con una longitud de, por ejemplo, 24 ms. Un primer mensaje está designado con 1612, y un segundo mensaje está designado con 1614. El primer mensaje 1612 contiene datos CA 1612a y datos útiles encriptados 1612b. De manera similar el segundo mensaje 1614 contiene datos CA 1614a y datos útiles encriptados 1614b.

[0118] La fig. 16 muestra además con la referencia 1620 un diagrama de bloques de un proveedor de señal DAB que hace realidad el concepto correspondiente. El proveedor DAB 1620 comprende un codificador DAB 1630 que está diseñado para recibir datos de audio y/o datos de video 1628 y proveer en base a ello un flujo de transporte

MPEG-2 1632. El proveedor de señal DAB 1620 comprende además una pasarela DMB 1640 que está diseñada para recibir el flujo de transporte MPEG-2 1632 y proveer en base a ello un subcanal DAB 1642. El proveedor de señal DAB 1620 comprende además un adicionador de autorización de acceso que está diseñado para recibir el subcanal DAB 1642 y proveer en base a ello un subcanal DAB 1652 encriptado al menos parcialmente que se le suministra al multiplexor DAB 1660 como señal de entrada. El multiplexor 1660 provee en base a ello la señal DAB.

[0119] A continuación se describe brevemente el procedimiento correspondiente. En el procedimiento se incluyen los paquetes de flujo de transporte MPEG en primer lugar en los subcanales DAB y los marcos DAB resultantes (es decir bytes del subcanal transmitidos cada 24 ms) se encriptan luego. El módulo CA reúne luego informaciones CA y datos encriptados y genera un marco DAB que es correspondientemente mayor (es decir, necesita más tasa de bits) que el proporcionado por la pasarela DMB 1640. Para ello al comienzo de cada marco se juntan las informaciones CA 1612a, 1614a necesarias. El resto del marco resultante contiene los datos DMB encriptados 1612b, 1614b (es decir, partes del flujo de datos del flujo de transporte MPEG-2).

[0120] Con el CA del subcanal DAB sólo es posible condicionada por el principio la encriptación de un programa DMB. No es posible, por ejemplo, encriptar sólo el audio (o la parte de audio), pero dejar no encriptado el vídeo (o la parte de vídeo).

[0121] Dado que los subcanales DAB siempre deben ser un múltiplo de 8 kbps, la sobrecarga ("overhead") por CA del subcanal DAB siempre es al menos 8 bps o un múltiplo de 8 kbps.

[0122] A continuación se explican algunas desventajas del procedimiento del concepto recién descrito. En primer lugar se debe mantener que el marco DAB encriptado esté dividido en dos, conteniendo la primera parte los datos CA 1612a, 1614a, y conteniendo la segunda parte los datos DMB encriptados 1612b, 1614b. Los datos DMB están protegidos, según es habitual en los flujos de transporte MPEG, por un anidamiento ("interleaver") y un código Reed-Solomon frente a fallos de transmisión. Pero el tipo de la encriptación significa ahora que en primer lugar calcula la protección frente a errores y luego se encriptan los paquetes de flujo de transporte MPEG protegidos frente a errores. Pero esto también significa que en el lado de recepción primero se debe desencriptar y luego aplicar la protección frente a errores. Pero esto contradice la estructura habitual de un receptor, en el que en primer lugar se aplica la protección frente a errores y a continuación se pasan los datos corregidos de errores. La restricción de acceso se debería montar así en capas de protocolo muy profundas del receptor.

[0123] Los datos DMB están protegidos adicionalmente frente a errores de transmisión. Así parece recomendable requerir también lo mismo para las informaciones CA, dado que si éstas no se reciben correctamente no es posible una desencriptación del flujo DMB. Pero para ello el CA del subcanal DAB no toma precauciones. Entonces esto sólo se debería extender (de propiedad).

[0124] El CA de subcanal DAB también requiere siempre al menos 8 kbps en la sobrecarga, y debido a la granularidad de un subcanal DAB.

7.3. Encriptación de unidades de acceso conforme a MPEG-4 IPMP

[0125] MPEG-4 IPMP ofrece una encriptación de final a final que es muy segura, pero debe estar integrada en el codificador (Encoder) y por ello no es apropiada cuando se debe encriptar posteriormente un flujo de datos presente. MPEG-4 IPMP no está muy difundido.

8. Conclusiones

[0126] Los ejemplos de realización según la invención hacen posible mantener tan bajo como sea posible la sobrecarga que se origina por la emisión de las informaciones CA. Esto puede ocurrir, por un lado, por informaciones CA cortas pero, por otro lado, por una inclusión habilidosa de las informaciones CA.

[0127] La longitud de las informaciones CA difiere según el sistema CA utilizado. Para la inclusión habilidosa de las informaciones CA se define según la invención una estructura CA. Esta estructura CA es independiente del sistema CA utilizado. Define,

1. en que plano de transporte se debe encriptar;
2. como se señala la encriptación; y

3. donde están incluidas las informaciones CA (EMM y ECM).

[0128] La televisión de pago (Pay-TV) usando la tecnología DMB es una aplicación relativamente nueva. Al contrario del DVB-T, que también usa flujos de transporte MPEG-2, y DAB todavía no hay una estructura definida para una restricción de acceso para DMB. Arriba se ha descrito porque es posible, pero no óptima, una encriptación análogamente a la estructura de restricción de acceso para DVB-T o de la estructura de restricción de acceso DAB. Aquí se describe por lo demás una estructura de restricción de acceso según la invención especialmente para DMB que usa los siguientes requisitos:

1. Definición de una estructura de restricción de acceso que se pueda aplicar para cada sistema de restricción de acceso y cada procedimiento de encriptación.
2. Definición de los planos de encriptación e inclusión de las informaciones de restricción de acceso para DMB;
3. Definición de la señalización;
4. Transmisión que ahora tasa de bits de las informaciones CA;
5. Transporte de las claves de contenido (ECMs) en el mismo canal que el contenido mismo;
6. Transporte de todos los EMM es posible en un "canal maestro" separado;
7. Capacidad de integración sencilla en sistemas emisores existentes;
8. La descripción del procedimiento es posible de forma sencilla, es decir, uso a ser posible de muchos mecanismos existentes. En este caso se encuentra una cantidad parcial sencilla de tipos de encriptaciones posibles en conjunto para DMB (así, por ejemplo, sólo un plano en el que se encripta, por ejemplo, sólo encriptación de flujo de transporte MPEG), a fin de mantener baja la complejidad del receptor.

[0129] Los ejemplos de realización según la invención satisfacen los requisitos mencionados y crean por consiguiente un concepto especialmente ventajoso de la limitación de acceso.

[0130] A continuación se resumen otra vez algunos aspectos y ventajas importantes del concepto de la invención.

[0131] En ejemplos de realización según la invención, la inclusión de informaciones CA se realiza en campos de datos existentes, pero no usados hasta ahora. Según la invención se propone el uso del campo "transport_private_data" dentro del campo de adaptación "adaptation_field()" en la cabeza de mensaje del paquete de flujo de transporte. Por ejemplo, está disponible una tasa de datos utilizable suficiente dentro de los paquetes con una tabla de asociación de programa (paquetes PAT). La inclusión de informaciones CA se realiza análogamente a la inclusión de datos PAD en la referencia [3] en la PAT. Una codificación posible de estas informaciones CA se describe arriba a modo de ejemplo. La verdadera encriptación se realiza en el plano de transporte o plano de flujo de transporte o plano de flujo de programa elemental (véase referencia [6]). Por ejemplo, es posible enviar dos flujos de audio de los que sólo uno está encriptado.

[0132] Opcionalmente es posible el uso adicional de paquetes "de relleno" (paquetes "padding" o paquetes "null") u otros paquetes de flujo de transporte MPEG con informaciones CA incluidas.

[0133] Ejemplos de realización según la invención presentan ventajas del procedimiento considerables respecto a otros procedimientos de encriptación. Respecto a una encriptación dentro de los paquetes de flujo de transporte MPEG, los ejemplos de realización según la invención presentan, por ejemplo, una o varias de las ventajas siguiente:

- Se usa la tasa de datos no usada actualmente, es decir, no se debe prever una tasa de datos para informaciones CA;
- El codificador DMB puede usar toda la tasa de datos, y no se origina una sobrecarga para las informaciones CA (así no están reservados paquetes de flujo de transporte MPEG para la información CA); y

• Dado que las informaciones CA están contenidas en el mismo paquete de flujo de transporte MPEG que la tabla de asociación de programa PAT están a disposición muy rápidamente en la sintonización o cambio de canal ("tune-in"). Una restricción de acceso conforme a esta propuesta no aumenta así, comparado a un flujo de datos no encriptado, el tiempo de sintonización o tiempo de cambio de canal.

5

[0134] Respecto a una encriptación de los subcanales DAB (designada también como "DAB-Subchannel-CA") se producen una o varias de las ventajas siguientes:

• ninguna sobrecarga de al menos 8 kbps;

10

• la información CA está protegida frente a errores;

• el subcanal completo está codificado de forma unitaria (todo es flujo de transporte MPEG) y no hay bipartición; y

15 • la encriptación se realiza antes de la aplicación de la protección frente a errores, lo que se corresponde entonces al modelo de capas del receptor.

[0135] En los ejemplos de realización según la invención se incluye por consiguiente la estructura de datos "CA-Descriptor" arriba descrita en el paquete de flujo de transporte MPEG con la tabla de asociación de programa PAT, y se usa la verdadera encriptación en el plano de flujo de transporte MPEG. Según la invención se incluyen los datos con baja necesidad de tasa de bits, a saber las informaciones CA, en los paquetes de flujo de transporte MPEG transmitidos regularmente, pero ciertamente vacíos, con la tabla de asociación de programa.

20

[0136] La inclusión de las informaciones CA se parece o corresponde en este caso con el tipo de inclusión ya usado en el estándar DMB para datos PAD.

25

9. Alternativas de implementación

[0137] Aunque se han descrito algunos aspectos en relación con un dispositivo, se entiende que estos aspectos también representan una descripción del procedimiento correspondiente, de modo que un bloque o un módulo de un dispositivo también se debe entender como una etapa del procedimiento correspondiente o como una característica de una etapa del procedimiento. Análogamente a ello los aspectos, que se han descrito en relación con una o como una etapa del procedimiento, también representan una descripción de un bloque o detalle o característica correspondiente de un dispositivo. Algunas o todas las etapas del procedimiento se pueden realizar por un aparato de hardware (o usando un aparato de hardware), como por ejemplo, un microprocesador, un ordenador programable o un circuito electrónico. En algunos ejemplos de realización se pueden realizar algunas o varias de las etapas del procedimiento más importantes por un aparato semejante.

30

[0138] Una señal codificada según la invención, como por ejemplo, una señal de audio o una señal de vídeo o una señal de flujo de transporte o una señal DAB, puede estar almacenada en un medio de almacenamiento digital o se puede transmitir en un medio de transmisión, como por ejemplo, un medio de transmisión inalámbrico o un medio de transmisión por cable, por ejemplo internet.

40

[0139] La señal de audio codificada según la invención puede estar almacenada en un medio de almacenamiento digital, o se puede transmitir en un medio de transmisión, como por ejemplo, un medio de transmisión inalámbrico o un medio de transmisión por cable, como por ejemplo internet.

45

[0140] Según los requisitos de implementación determinados, los ejemplos de realización de la invención pueden estar implementados en el hardware o en el software. La implementación se puede realizar usando un medio de almacenamiento digital, por ejemplo, un disquete, un DVD, un disco Blu-ray, un CD, una ROM, una PROM, una EPROM, una EEPROM o una memoria FLASH, un disco duro u otra memoria magnética u óptica, sobre la que se puedan almacenar las señales de control legibles electrónicamente, que pueden cooperar o cooperan con un sistema informático programable de manera que se realiza el procedimiento correspondiente. Por ello el medio de almacenamiento digital puede ser legible por ordenador.

50

55

[0141] Aquellos ejemplos de realización según la invención comprenden así un soporte de datos que presenta señales de control legibles electrónicamente que son capaces de cooperar con un sistema informático programable, de manera que se realiza uno de los procedimientos aquí descritos.

[0142] En general los ejemplos de realización de la presente invención pueden estar implementados como producto de programa informático con un código de programa, siendo eficaz el código de programa en el sentido de que se realiza uno de los procedimientos cuando el producto de programa informático se ejecuta en un ordenador.

5 **[0143]** El código de programa también puede estar almacenado, por ejemplo, en un soporte legible a máquina.

[0144] Otros ejemplos de realización comprenden el programa informático para la realización de uno de los procedimientos aquí descritos, estando almacenado el programa informático en un soporte legible a máquina.

10 **[0145]** Con otras palabras, un ejemplo de realización del procedimiento según la invención es por consiguiente un programa informático que presenta un código de programa para la realización de uno de los procedimientos aquí descritos cuando se ejecuta el programa informático en un ordenador.

15 **[0146]** Otro ejemplo de realización de los procedimientos según la invención es por consiguiente un soporte de datos (o un medio de almacenamiento digital o un medio legible por ordenador) en el que está registrado el programa informático para la realización de uno de los procedimientos aquí descritos.

20 **[0147]** Otro ejemplo de realización del procedimiento según la invención es por consiguiente un flujo de datos o una secuencia de señales, que representa o representan el programa informático para la realización de uno de los procedimientos aquí descritos. El flujo de datos o la secuencia de las señales puede o pueden estar configurados, por ejemplo, en el sentido de que se transfieren a través de una conexión de comunicación de datos, por ejemplo a través de Internet.

25 **[0148]** Otro ejemplo de realización comprende un dispositivo de procesamiento, por ejemplo, un ordenador o un módulo lógico programable que esté configurado o adaptado en el sentido de realizar uno de los procedimientos aquí descritos.

[0149] Otro ejemplo de realización comprende un ordenador en el que está instalado el programa informático para la realización de uno de los procedimientos aquí descritos.

30 **[0150]** En algunos ejemplos de realización se puede usar un módulo lógico programable (por ejemplo una matriz de puertas programable, una FPGA) para realizar algunas o todas las funcionalidades de los procedimientos aquí descritos. En algunos ejemplos de realización una matriz de puertas programable de campo puede cooperar con un microprocesador para realizar uno de los procedimientos aquí descritos. En general los procedimientos se realizan en algunos ejemplos de realización por parte de un dispositivo de hardware cualesquiera. Éste puede ser un hardware utilizable de forma universal, como un procesador de ordenador (CPU) o hardware específicos para el procedimiento, como por ejemplo un ASIC.

40 **[0151]** Los ejemplos de realización arriba descritos sólo representan una clarificación de los principios de la presente invención. Se entiende que modificaciones y variaciones de las disposiciones y detalles serán obvias para otros especialistas. Por ello se pretende que la invención sólo esté limitada por el alcance de protección de las siguientes reivindicaciones y no por los detalles específicos que se han presentado aquí mediante la descripción y explicación de los ejemplos de realización.

45 10. Referencias

[0152]

50 [1] ETSI, ETR 289 (1996-10), Digital Video Broadcasting (DVB); Support for use of scrambling and Conditional Access (CA) within digital broadcast systems

[2] ETSI TS 102 428 v1.1.1 (2005-06): "Digital Audio Broadcasting (DAB); DMB video services; User application specification", 06/2005.

55 [3] ETSI TS 102 428 v1.2.1 (2009-06): "Digital Audio Broadcasting (DAB); DMB video services; User application specification", 06/2009.

[4] ETSI EN 300 401 V1.4.1 (2006-06): "Digital Audio Broadcasting (DAB) to mobile, portable and fixed receivers, 06/2006

[5] ETSI TS 102 367 V1.2.1 (2006-01): "Digital Audio Broadcasting (DAB); Conditional access), 01/2006

[6] ITU-T H.222.0 (2006-05): "Series H: Audiovisual and multimedia system, Infrastructure of audiovisual services -
5 Transmission multiplexing and synchronization", "Information technology - Generic coding of moving pictures and associated audio information: Systems"

11. Leyenda

10 [0153]

elementary_PID	PID elemental
DMB Encoder	Codificador DMB
TS packet	Paquete de flujo de transporte
MPEG transport stream	Flujo de transporte MPEG
do	Hace
transport_packet	Paquete de transporte
while	Mientras
nextbits	Bits siguientes
sync_byte	Byte de sincronización
program_number	Número de programa
program_map_PID	PID de reproducción de programa
Object Descriptor	Descriptor de objeto
ES_Descriptor	Descriptor ES
stream Type	Tipo de flujo
specific Info	Información específica
Image	Imagen
Audio	Audio
SD-Stream	Flujo SD
OD-Stream	Flujo OD
program_stream_info_length	Longitud de la información de flujo de programa
1st_descriptor_loop	Primer bucle de descriptor
IOD-Descriptor	Descriptor IOD
stream_type	Tipo de flujo
elementary_PID	PID elemental
2nd_descriptor_loop	Segundo bucle de descriptor
SL_Descriptor	Descriptor SL
PES-packet	Paquete PES
adaptation_field_control	Control de campo de adaptación
adaptation_field	Campo de adaptación
transport_private_data_flag	Marcador de datos privados de transporte
transport_private_data_length	Longitud de datos privados de transporte
program_association_section	Sección de asociación de programa
sync_byte	Byte de sincronización
transport_error_indicator	Indicador de error de transporte
Payload_unit_start_indicator	Indicador de inicio de unidad de carga útil
transport_priority	Prioridad de transporte
transport_scrambling_control	Control de encriptación de transporte
adaptation_field_control	Control de campo de adaptación
continuity_counter	Contador de continuidad
If	Si
adaptation_field	Campo de adaptación
data_byte	Byte de datos
adaptation_field_length	Longitud de campo de adaptación
discontinuity_indicator	Indicador de discontinuidad
random_access_indicator	Indicador para acceso aleatorio
elementary_stream_priority_indicator	Indicador de prioridad de flujo elemental

PCR-Flag	Marcador PCR
OPCR_flag	Marcador OPCR
splicing_point_flag	Marcador de punto de unión
transport_private_data_flag	Marcador de datos privados de transporte
adaptation_field_extension_flag	Marcador de extensión del campo de adaptación
program_clock_reference_base	Base de referencia del reloj de programa
reserved	Reservado
program_clock_reference_extension	Extensión de referencia del reloj de programa
splice_countdown	Cuenta atrás de unión
transport_private_data_length	Longitud de datos privados de transporte
for	Para
Private_data_byte	Byte de datos privados
stuffing_byte	Byte de relleno
CA_section	Sección CA
table_id	ID de tabla
section_syntax_indicator	Indicador de la sintaxis de sección
reserved	Reservado
section_length	Longitud de sección
reserved	Reservado
version_number	Número de versión
current_next_indicator	Indicador actual siguiente
section_number	Número de sección
last_section_number	Número de última sección
descriptor	Descriptor
CA_descriptor	Descriptor CA
descriptor_tag	Marcador de descriptor
descriptor_length	Longitud de descriptor
CA_system_ID	ID de sistema CA
private_data_byte	Byte de datos privados
CA_ECM_section	Sección ECM CA
CA_data	Datos CA
CA_info_length	Longitud de información CA
proprietary_CA-Information	Información CA de propiedad
program_association_section	Sección de asociación de programa
transport_stream_id	Identificación de flujo de transporte
version_number	Número de versión
current_next_indicator	Indicador actual siguiente
section_number	Número de sección
last_section_number	Número de última sección
program_number	Número de programa
network_PID	PID de red
program_map_PID	PID de reproducción de programa

REIVINDICACIONES

1. Un proveedor de flujo de transporte (100) para la provisión de una multiplicidad de paquetes de flujo de transporte (124, 128; 282, 284, 286, 288; 610, 620) que describen una información de medios digitales (110),
 5 en el que el proveedor de flujo de transporte está diseñado para proveer un paquete de flujo de transporte (124; 282; 610; 700) de un primer tipo de paquete con una tabla de asociación de programa (720; 1300) y una información de restricción de acceso (730) con una información de clave (CA_section, CA_ECM_section, CA_data) para la descriptación de una información de medios encriptada, en el que la tabla de asociación de programa (720; 1300) contiene una asociación entre un número de programa y un identificador de tipo de paquete de otro paquete de flujo
 10 de transporte (128; 284; 620) de un segundo tipo de paquete; y
 en el que el proveedor de flujo de transporte está diseñado para proveer un paquete de flujo de transporte (128; 284; 620) del segundo tipo de paquete, de modo que el paquete de flujo de transporte del segundo tipo de paquete contiene una referencia a los identificadores de tipo de paquete de los paquetes de datos útiles del flujo de transporte (286, 288; PES_packet) que describen los contenidos de diferentes tipos de contenido de la información
 15 de medios digitales (110).
2. El proveedor de flujo de transporte (100) según la reivindicación 1, en el que el proveedor de flujo de transporte está diseñado para proveer paquetes de flujo de transporte con el primer tipo de paquete, que comprenden tanto la tabla de asociación de programa (720; 1300) como también la información de restricción de
 20 acceso (730) con la información de clave (CA_section; CA_ECM_section),
 para proveer paquetes de transporte de flujo (128; 284) con el segundo tipo de paquete, y
 para proveer paquetes de datos útiles del flujo de transporte (286) con un tercer tipo de paquete que se diferencia
 25 del primer tipo de paquete y el segundo tipo de paquete; y
 en el que el proveedor de flujo de transporte está diseñado para proveer los paquetes de flujo de transporte con el primer tipo de paquete, los paquetes de flujo de transporte con el segundo tipo de paquete y los paquetes de flujo de transporte con el tercer tipo de paquete, de modo que los paquetes de flujo de transporte con el primer tipo de
 30 paquete, los paquetes de flujo de transporte con el segundo tipo de paquete y los paquetes de flujo de transporte con el tercer tipo de paquete presentan las mismas longitudes de paquete predeterminadas a fin de obtener un flujo de transporte con paquetes de flujo de transporte de la misma longitud.
3. El proveedor de flujo de transporte según la reivindicación 1 o reivindicación 2, en el que el proveedor
 35 de flujo de transporte está diseñado para añadir la información de restricción de acceso en un campo de información adicional (adaptation_field) del paquete de flujo de transporte (124; 282; 610; 700) del primer tipo de paquete, y en el que el proveedor de flujo de transporte está diseñado para señalar una presencia del campo de información adicional por un marcador (adaptation_field_control).
4. El proveedor de flujo de transporte según cualquiera de las reivindicaciones 1 a 3, en el que el
 40 proveedor de flujo de transporte está diseñado para proveer los paquetes de flujo de transporte de modo que cada uno de los paquetes de flujo de transporte presenta, en una posición predeterminada de un preámbulo del paquete de flujo de transporte, un identificador de tipo de paquete (PID) que identifica un tipo de paquete del paquete de flujo de transporte correspondiente,
 45 en el que el proveedor de flujo de transporte está diseñado para proveer los paquetes de flujo de transporte de modo que un paquete de flujo de transporte (124; 282; 610; 700) con la tabla de asociación de programa (720; 1300) y la información de restricción de acceso (730) presenta una referencia a un identificador de tipo de paquete de un paquete de flujo de transporte (128; 284; 620) con una tabla de reproducción de programa que comprende los
 50 identificadores de tipo de paquete para uno o varios tipos de flujos de datos, sin que el mismo paquete de flujo de transporte (124; 282; 610; 700) con la tabla de asociación de programa y la información de restricción de acceso describa el contenido útil de la información de medios digitales.
5. El proveedor de flujo de transporte según cualquiera de las reivindicaciones 1 a 4, en el que el
 proveedor de flujo de transporte está diseñado para proveer el paquete de flujo de transporte (124; 282; 610; 700)
 55 con la tabla de asociación de programa y la información de restricción de acceso de modo que el paquete de flujo de transporte con la tabla de asociación de programa y la información de restricción de acceso presenta una secuencia de secciones (CA_section, CA_ECM_section, CA_data) de informaciones de restricción de acceso diferentes, en el que una de las secciones presenta un mensaje de gestión de autorización (EMM) o una referencia a un mensaje de gestión de autorización, y

en el que otra de las secciones presenta un mensaje de clave de autorización (ECM) o una referencia a un mensaje de clave de autorización; y

en el que las secciones de la información de restricción de acceso comprenden respectivamente un identificador de tabla (table_id) que describe el tipo de la información de restricción de acceso contenida en la sección, y una información de longitud (section_length, CA_info_length) que describe una longitud de las informaciones contenidas en la sección.

6. El proveedor de flujo de transporte según cualquiera de las reivindicaciones 1 a 5, en el que el proveedor de flujo de transporte está diseñado para añadir informaciones de clave de contenido (ECM) para la descryptación de una información de medios encriptada exclusivamente en los paquetes de flujo de transporte (124; 282; 610; 700) con una tabla de asociación de programa, de modo que los paquetes de flujo de transporte (286, 288), que describen el contenido de la información de medios digitales en forma de una información de audio codificada o en forma de una información de imagen codificada o en forma de una información de video codificada, están exentos de informaciones de clave de contenido (ECM) para la descryptación de la información de medios encriptada.

7. El proveedor de flujo de transporte según cualquiera de las reivindicaciones 1 a 6, en el que el proveedor de flujo de transporte está diseñado para proveer el flujo de transporte de modo que el flujo de transporte comprende una referencia a un canal separado en el que se transmiten los mensajes de gestión de autorización (EMM).

8. El proveedor de flujo de transporte según cualquiera de las reivindicaciones 1 a 7, en el que el proveedor de flujo de transporte está diseñado para añadir la información de restricción de acceso en un zona de datos privados (private_data_byte) de un paquete de flujo de transporte (124; 282; 610; 700) según ETSI TS 102 428, que comprende la tabla de asociación de programa (720; 1300) según ISO-IEC 13818-1.

9. El proveedor de flujo de transporte según cualquiera de las reivindicaciones 1 a 8, en el que el proveedor de flujo de transporte está diseñado para proveer en un flujo de transporte al menos una vez por segundo paquetes de flujo de transporte (124; 282; 610; 700) con una tabla de asociación de programa y una información de restricción de acceso.

10. El proveedor de flujo de transporte según cualquiera de las reivindicaciones 1 a 9, en el que el proveedor de flujo de transporte está diseñado para ocupar por la tabla de asociación de programa menos del 30% de un paquete de flujo de transporte (124; 282; 610; 700) con una tabla de asociación de programa y una información de restricción de acceso.

11. Un proveedor de señal DAB (200; 270) para proveer de una señal DAB (220; 274) que comprende una información de medios restringida de acceso, con las características siguientes:

un proveedor de flujo de transporte (100; 230; 276) según cualquiera de las reivindicaciones 1 a 10, que está diseñado para proveer paquetes de flujo de transporte (124; 282; 610; 700) de un primer tipo de paquete que comprenden una tabla de asociación de programa y una información de restricción de acceso, y para proveer un paquete de flujo de transporte (128; 284; 620) del segundo tipo de paquete de modo que el paquete de flujo de transporte del segundo tipo de paquete contiene una referencia a los identificadores de tipo de paquete de los paquetes de datos útiles del flujo de transporte (286, 288), y para proporcionar paquetes de datos útiles del flujo de transporte (286) de un tercer tipo de paquete que describen un contenido de un primer tipo de medio restringido de acceso, y para proveer paquetes de datos útiles del flujo de transporte (288) de un cuarto tipo de paquete que describen un contenido de un segundo tipo de medio de la información de medios restringida de acceso,

en el que un contenido de al menos algunos de los paquetes de datos útiles del flujo de transporte del tercer tipo de paquete está encriptado o un contenido de al menos algunos de los paquetes de datos útiles del flujo de transporte del cuarto tipo de paquete está encriptado,

en el que los paquetes de flujo de transporte del primer tipo de paquete, los paquetes de flujo de transporte del segundo tipo de paquete, los paquetes de flujo de transporte del tercer tipo de paquete y los paquetes de flujo de transporte del cuarto tipo de paquete son parte de un flujo de transporte MPEG2, y

en el que la información de restricción de acceso que está contenida en los paquetes de flujo de transporte del

primer tipo de paquete comprende una información de clave de contenido (ECM) para la descriptación de los contenidos encriptados de los paquetes de flujo de transporte del tercer tipo de paquete o de los contenidos encriptados de los paquetes de flujo de transporte del cuarto tipo de paquete; y

5 un combinador de servicios DAB (290) que está diseñado para combinar el flujo de transporte MPEG2 con uno o varios otros servicios DAB (292) a fin de obtener la señal DAB (274).

12. Un analizador de flujo de transporte (300) para la provisión de una información de restricción de acceso (320) para la descriptación de una información de medios digitales restringida de acceso a base de un
10 flujo de transporte (310) con las características siguientes:

un identificador de tipo de paquete (330) que está diseñado para identificar un paquete (124; 282; 610; 700) de un primer tipo de paquete predeterminado, que presenta un primer identificador de tipo de paquete predeterminado y que contiene una tabla de asociación de programa, como un paquete identificado (332); y

15 un analizador de paquete que está diseñado para buscar el paquete identificado (332) según una información de restricción de acceso y proveer una información de restricción de acceso (320) encontrada en él.

13. El analizador de flujo de transporte (300) según la reivindicación 12, en el que el analizador de flujo de transporte está diseñado además para evaluar la tabla de asociación de programa (720; 1300) en el paquete de flujo de transporte (124; 282; 610; 700) del primer tipo de paquete predeterminado y determinar, en base a la tabla de asociación de programa, un segundo identificador de tipo de paquete que está asociado a un paquete de flujo de transporte (128; 284; 620) con una tabla de reproducción de programa;

25 en el que el analizador de flujo de transporte presenta un determinador de asociación de tipo de paquete (350) que está diseñado para identificar, en base al segundo identificador de tipo de paquete determinado, un paquete de flujo de transporte (128; 284; 620) con una tabla de reproducción de programa en el flujo de transporte (310) y evaluar la tabla de reproducción de programa a fin de obtener una información sobre qué identificadores de tipo de paquete están asociados a los paquetes de datos útiles del flujo de transporte (286, 288) que contienen los contenidos de
30 medios de la información de medios digitales restringida de acceso.

14. El analizador de flujo de transporte según la reivindicación 12 o reivindicación 13, en el que el analizador de flujo de transporte presenta además un descriptador que está diseñado para descriptar los contenidos de medios encriptados que están contenidos en los paquetes de flujo de transporte (286, 288) con los
35 identificadores de tipo de paquete descritos en la tabla de reproducción de programa, usando la información de restricción de acceso contenida en el paquete de flujo de transporte del primer tipo de paquete predeterminado.

15. El analizador de flujo de transporte según cualquiera de las reivindicaciones 12 a 14, en el que el analizador de paquete está configurado para examinar el paquete identificado (332) del primer tipo de paquete
40 predeterminado en cuanto a si un campo de información adicional (adaptation_field) presenta una o varias tablas (CA_section, CA_ECM_section, CA_data) que están caracterizadas por identificadores de tabla predeterminados y contienen una información de restricción de acceso, y para proveer la información de restricción de acceso contenida en las tablas identificadas.

16. El analizador de flujo de transporte según la reivindicación 15, en el que el analizador de paquete está diseñado para verificar, en respuesta a una localización de una primera tabla (CA_section, CA_ECM_section, CA_data) que está caracterizada por un primer identificador de tabla predeterminado y que contiene una información de restricción de acceso, y usando una información de longitud de tabla (section_length, CA_info_length) contenida en la primera tabla, si el campo de información adicional del paquete identificado (332) del primer tipo de paquete
50 predeterminado presenta a continuación de la primera tabla otra tabla (CA_section, CA_ECM_section, CA_data) que contiene una información de restricción de acceso, y para proveer la información de restricción de acceso contenida en la otra tabla.

17. Receptor DAB (400) con las características siguientes:

55 un separador de servicios DAB (430) que está diseñado para extraer un flujo de transporte MPEG2 (434) de una señal DAB (410) que comprende uno o varios otros servicios DAB adicionalmente al flujo de transporte MPEG2; y

un analizador de flujo de transporte (300; 440) según cualquiera de las reivindicaciones 12 a 16 que está diseñado

para recibir el flujo de transporte MPEG2 del separador de servicios DAB y proveer la información de restricción de acceso (442) para la descryptación de una información de medios digitales restringida de acceso en base al flujo de transporte; y

- 5 un descryptador de contenido (450) que está diseñado para descryptar los contenidos de medios encriptados de la información de medios digitales restringida de acceso usando la información de restricción de acceso (442).

18. Procedimiento para proveer una multiplicidad de paquetes de flujo de transporte que describen una información de medios digitales con las etapas siguientes:

- 10 proveer un paquete de flujo de transporte de un primer tipo de paquete con una tabla de asociación de programa y una información de restricción de acceso con una información de clave para la descryptación de una información de medios encriptada, en el que la tabla de asociación de programa contiene una asociación entre un número de programa y un identificador de tipo de paquete de otro paquete de flujo de transporte (128; 284; 620) de un segundo tipo de paquete; y

- 15 proveer un paquete de flujo de transporte (124; 282; 610; 700) del segundo tipo de paquete de modo que el paquete de flujo de transporte del segundo tipo de paquete contiene una referencia a los identificadores de tipo de paquete de los paquetes de datos útiles del flujo de transporte (286, 288) que describen los contenidos de diferentes tipos de contenido de la información de medios digitales.

19. Procedimiento para proveer una información de restricción de acceso para la descryptación de una información de medios digitales restringida de acceso en base a un flujo de transporte con las etapas siguientes:

- 25 identificación de un paquete de flujo de transporte (124; 282; 610; 700) de un primer tipo de paquete predeterminado, que presenta un primer identificador de tipo de paquete predeterminado y que contiene una tabla de asociación de programa, como un paquete identificado;

buscar el paquete identificado según una información de restricción de acceso; y

- 30 proveer una información de restricción de acceso encontrada en el paquete identificado.

20. Programa informático para la realización de un procedimiento según la reivindicación 18 o reivindicación 19 cuando el programa informático se ejecuta en un ordenador.

- 35 21. Señal de flujo de transporte con las características siguientes:

- 40 un paquete de flujo de transporte (124; 282; 610; 700) de un primer tipo de paquete con una tabla de asociación de programa e información de restricción de acceso con una información de clave para la descryptación de una información de medios encriptada, en el que la tabla de asociación de programa contiene una asociación entre un número de programa y un identificador de tipo de paquete de otro paquete de flujo de transporte (128; 284) de un segundo tipo de paquete; y

- 45 un paquete de flujo de transporte (128; 284) del segundo tipo de paquete, en el que el paquete de flujo de transporte del segundo tipo de paquete contiene una referencia a los identificadores de tipo de paquete de los paquetes de datos útiles del flujo de transporte (286, 288) que describen los contenidos de diferentes tipos de contenido de la información de medios digitales.

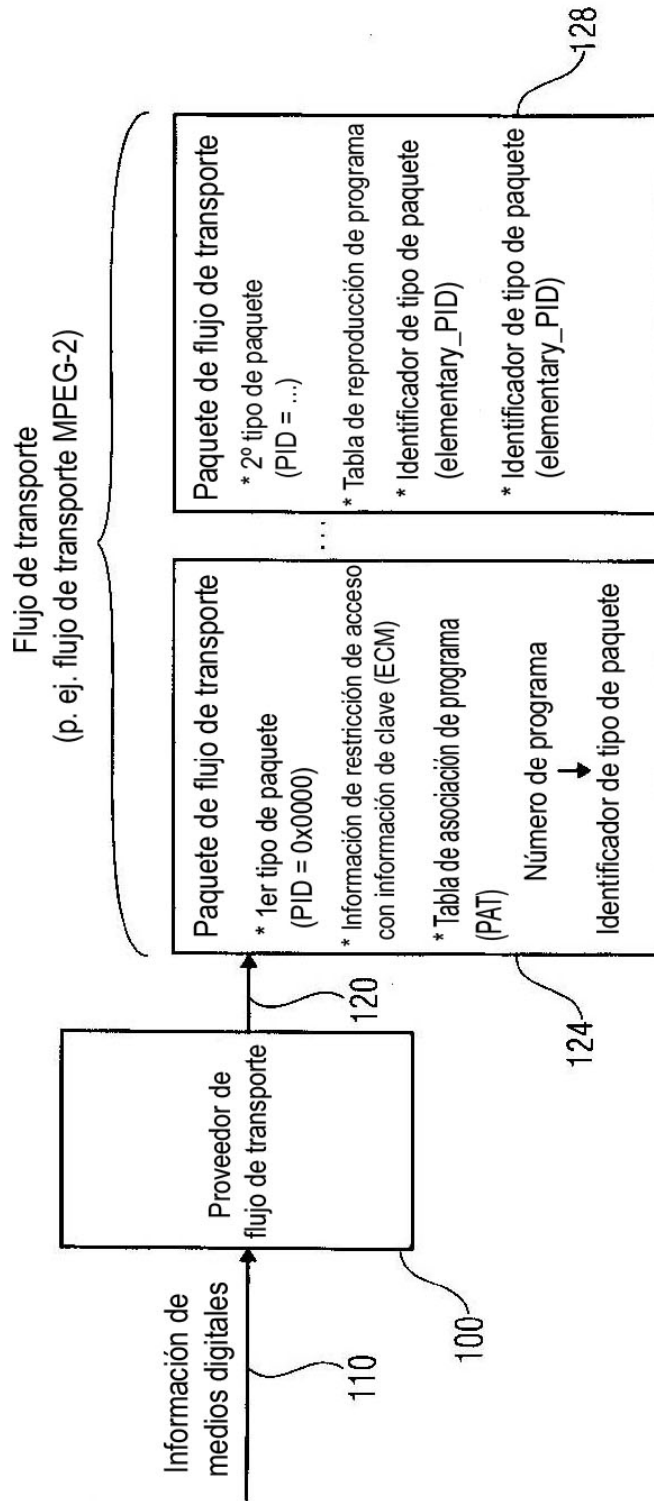


FIG 1

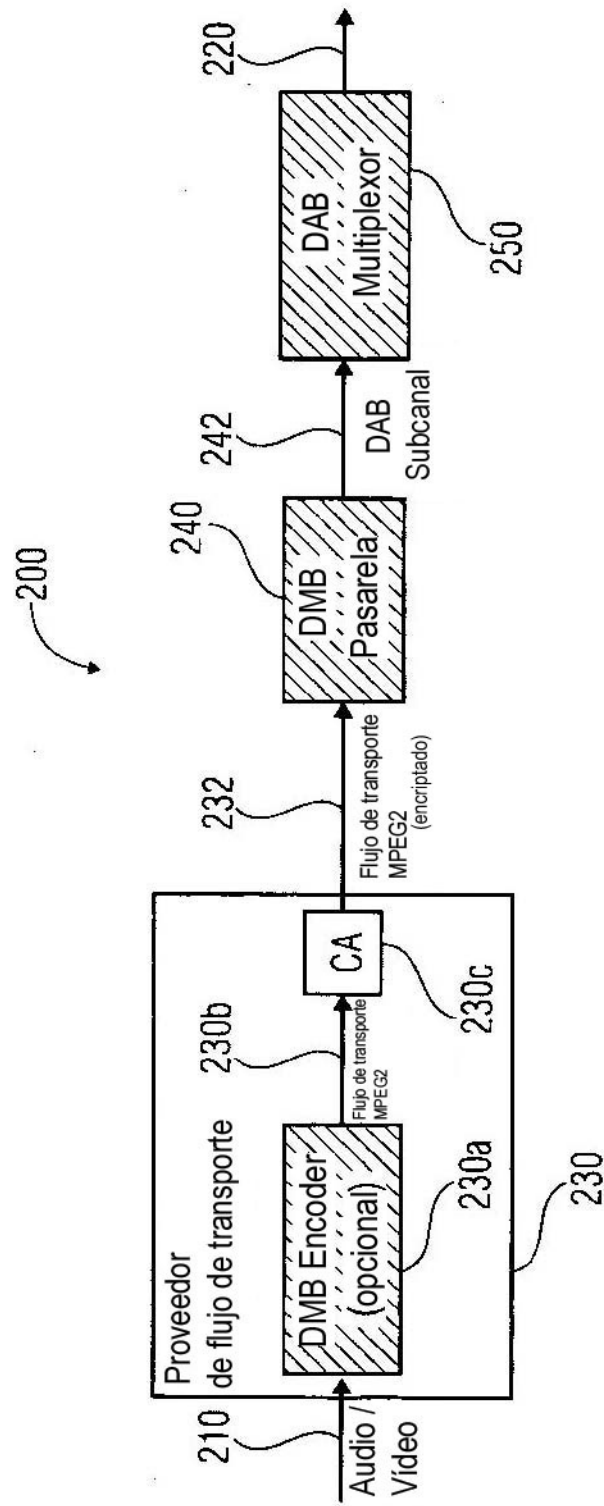


FIG 2A

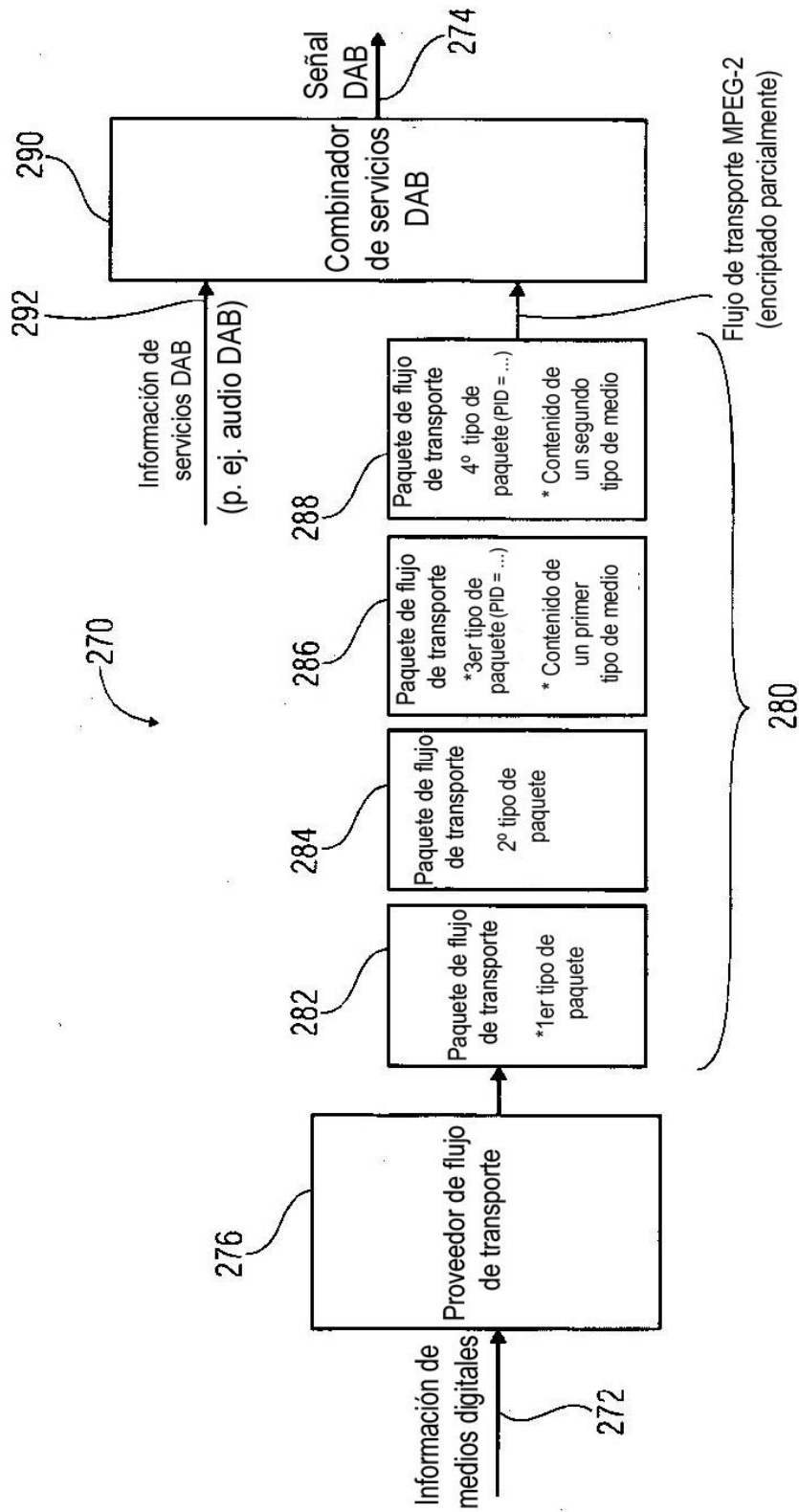


FIG 2B

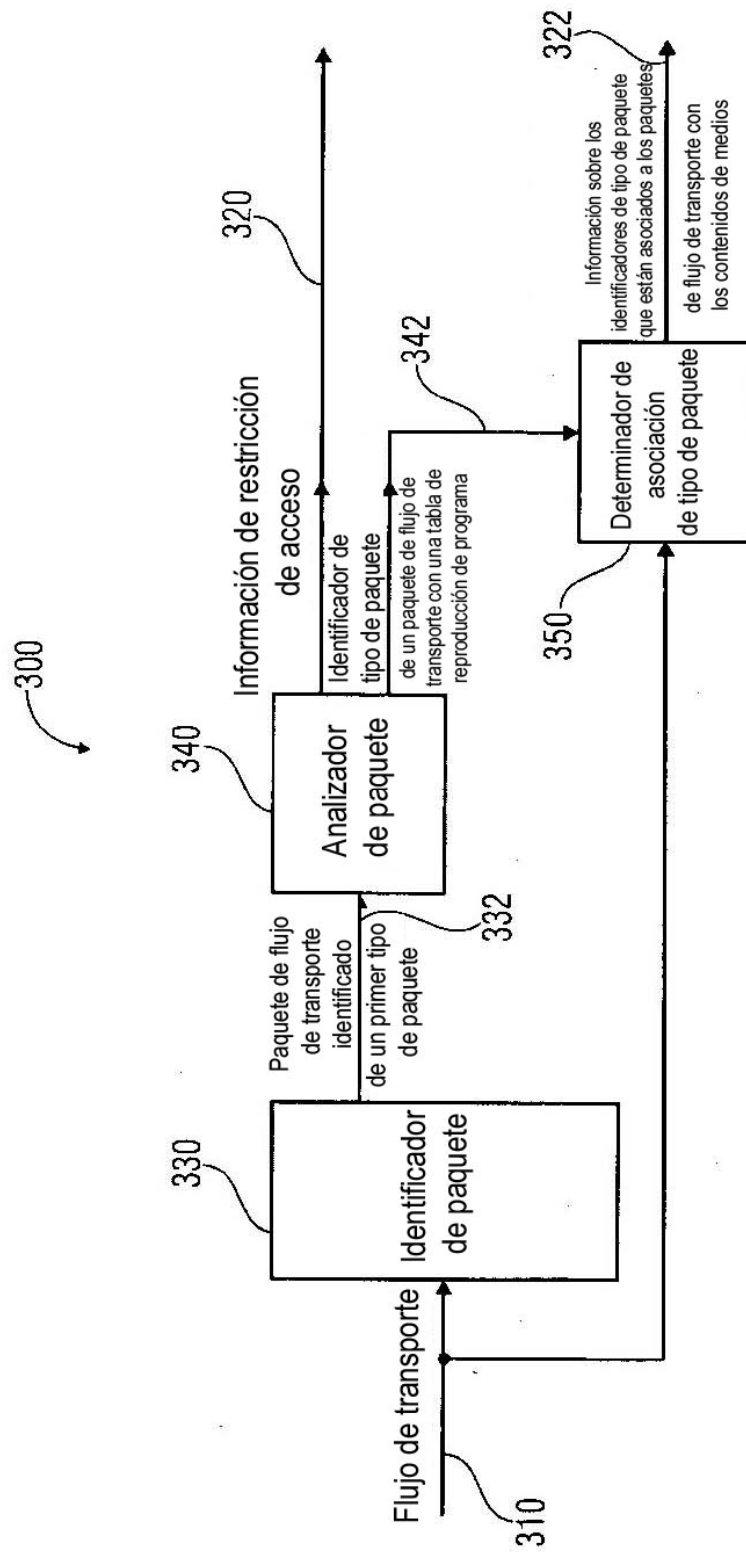


FIG 3

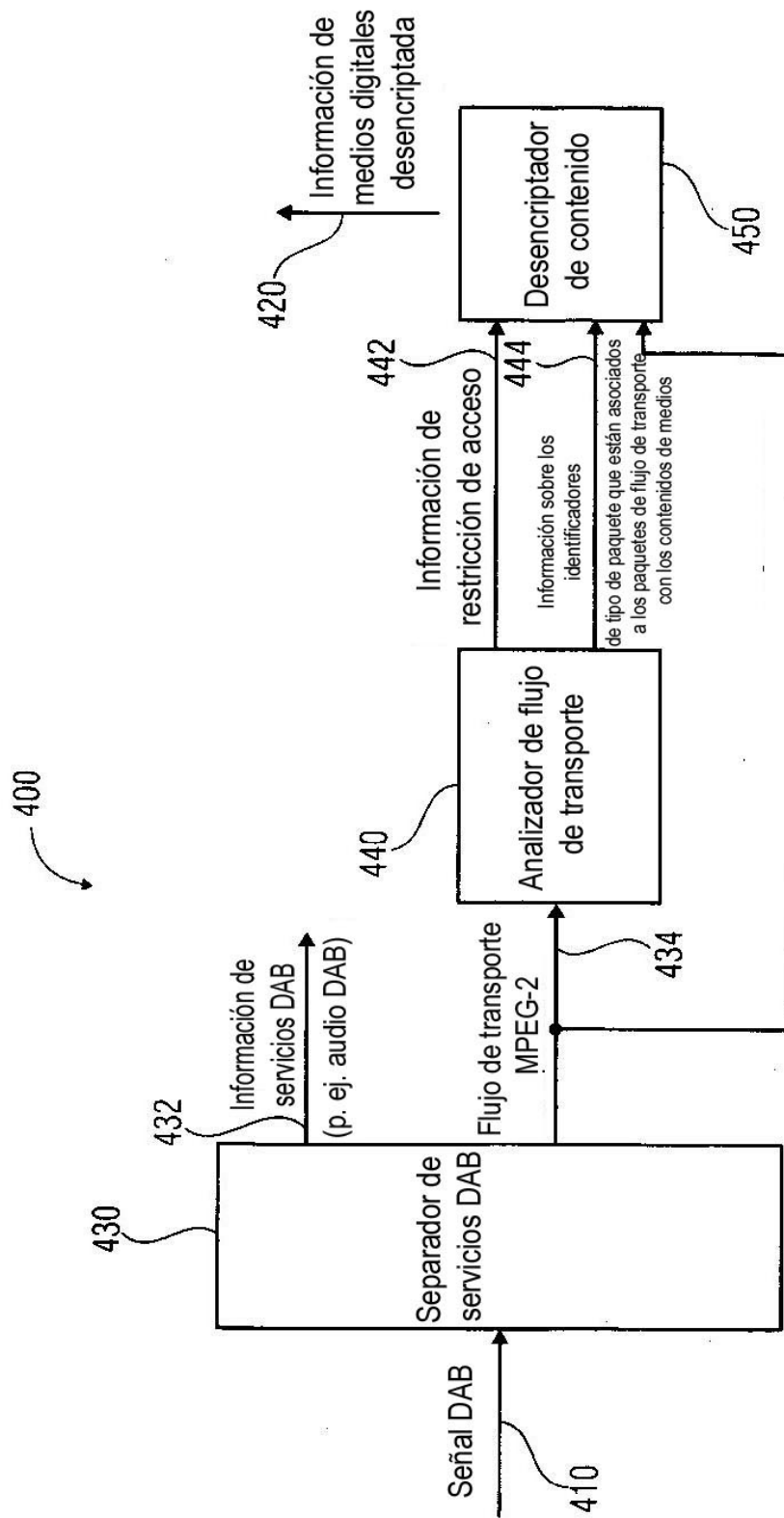


FIG 4

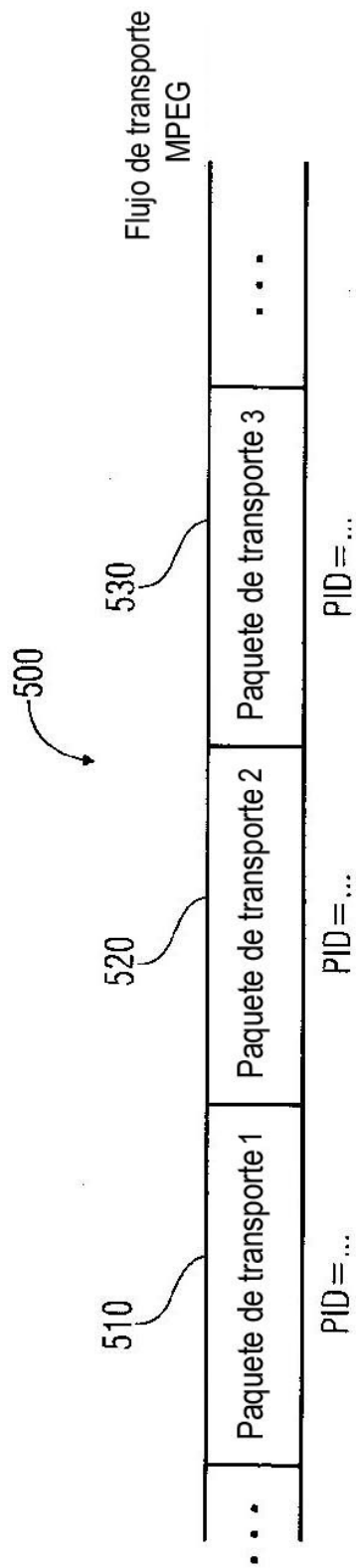


FIG 5A

Flujo de transporte MPEG

Sintaxis
<pre>MPEG_transport_stream() { do { transport_packet() } while (nextbits() == sync_byte) }</pre>

FIG 5B

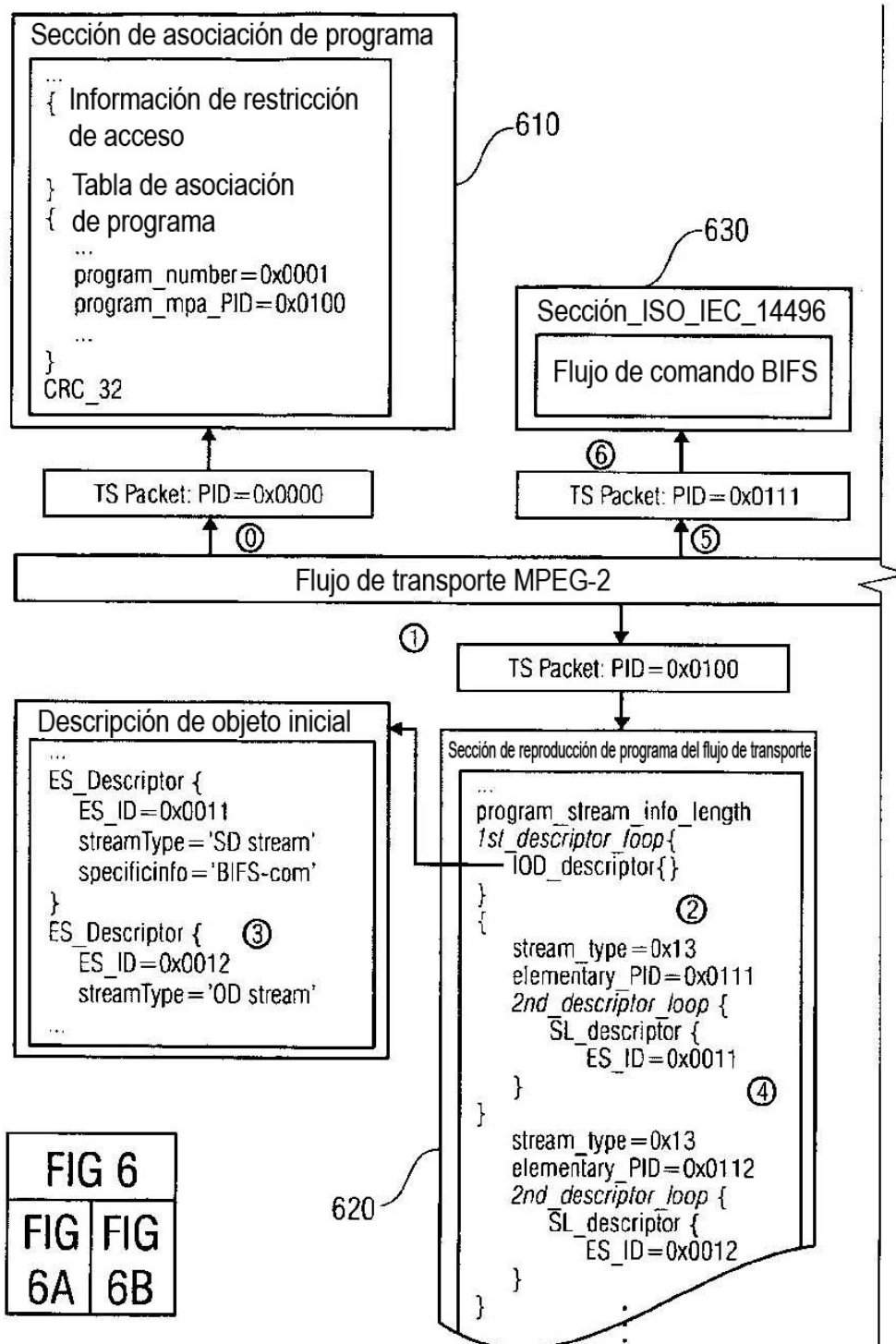


FIG 6
FIG 6A FIG 6B

FIG 6A

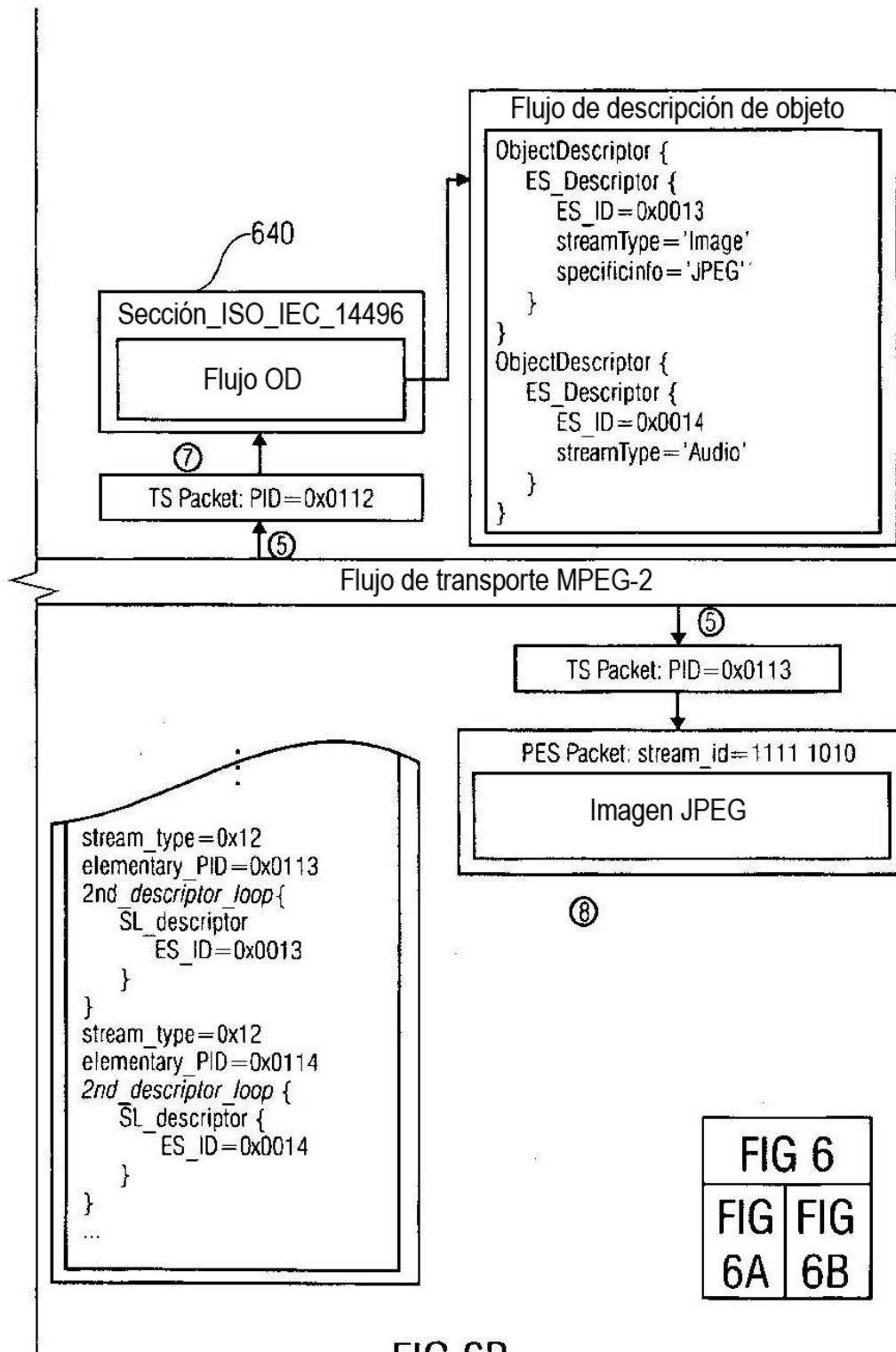


FIG 6B

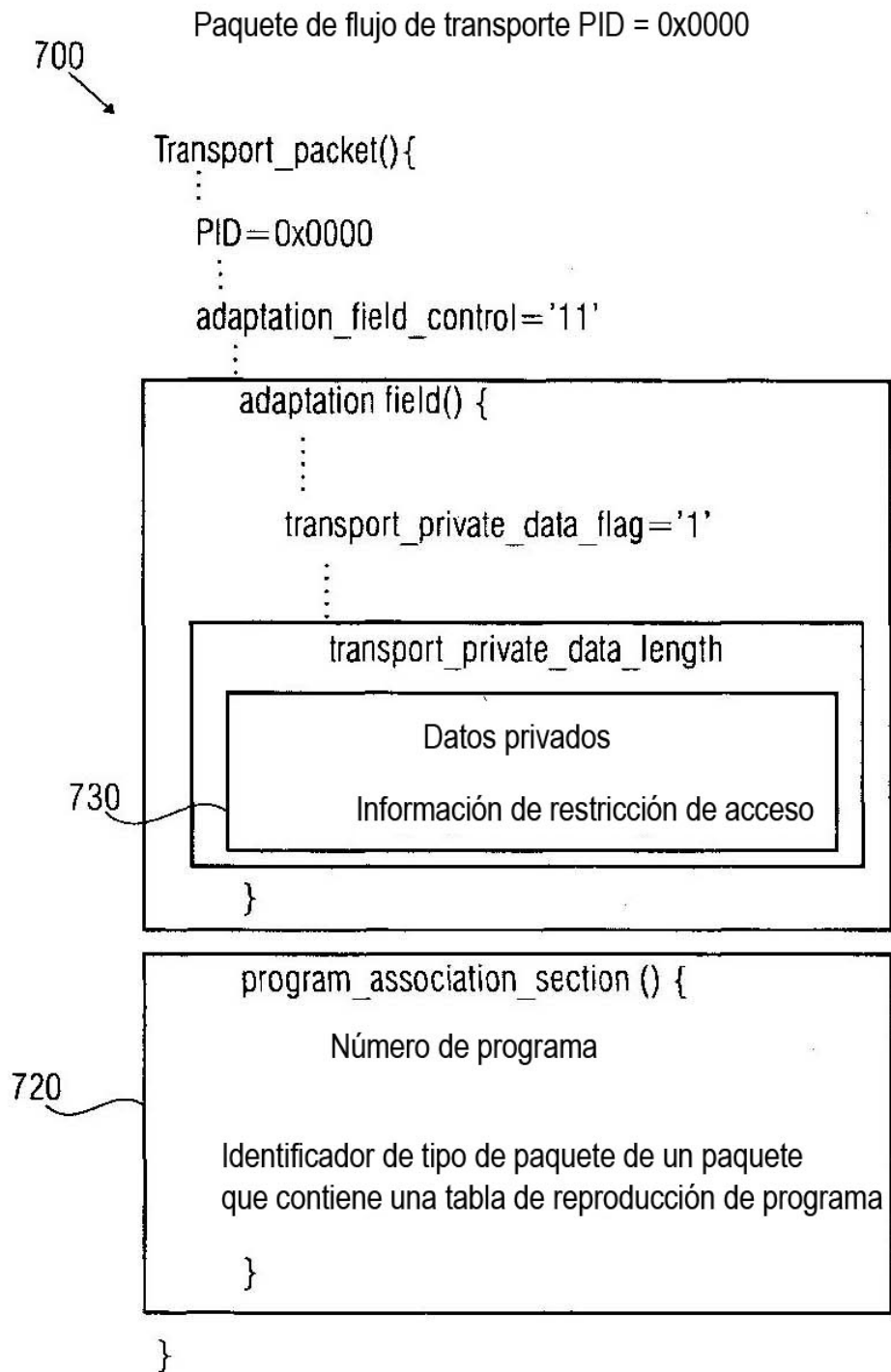


FIG 7

Estructura de un paquete de flujo de transporte (general)

Sintaxis	Número de bits	Limitaciones
<pre>Transport_packet(){ sync_byte transport_error_indicator payload_unit_start_indicator transport_priority PID transport_scrambling_control adaptation_filed_control continuity_counter if(adaptation_field_control=='10' adaptation_field_control=='11'){ adaptation_field() } if(adaptation_field_control=='01' adaptation_field_control=='11'){ for(i=0; <N; i++){ Data_byte } } }</pre>	8 1 1 1 13 2 2 4 8	"00" Prefijo de 4 bytes

FIG 8A

Estructura de un paquete de flujo de transporte (general)

Sintaxis	Número de bits	Limitaciones
<pre> adaptation_field(){ adaptation_field_length if (adaptation_field_length>0){ Discontinuity_indicator random_access_indicator elementary_stream_priority_indicator PCR_flag OPCR_flag splicing_point_flag transport_private_data_flag adaptation_field_extension_flag if (PCR_flag=='1'){ program_clock_reference_base Reserved program_clock_reference_extension } if (OPCR_flag=='1'){ } if (splicing_point_flag=='1'){ splice_countdown } if (transport_private_data_flag=='1'){ transport_private_data_length for (i=0; i<transport_private_data_length; i++){ Private_data_byte } } if (adaptation_field_extension_flag=='1'){ } for (i=0; i<N; i++){ stuffing_byte } } } </pre>	8 1 1 1 1 1 1 1 1 33 6 9 8 8 8 8	"0" "0" No utilizado No utilizado

FIG 8B

Sintaxis	Número de bits	Mnemotécnico
CA_section(){ table_id section_syntax_indicator '0' reserved section_length reserved version_number current_next_indicator section_number last_section_number for(i=0; i<N; i++){ descriptor() } CRC_32 }	 8 1 1 2 12 18 5 1 8 8 32	 uimsbf bslbf bslbf bslbf uimsbf bslbf uimsbf bslbf uimsbf uimsbf rpchof

FIG 9A

Sintaxis	Número de bits	Mnemotécnico
CA_descriptor(){ descriptor_tag descriptor_length CA_system_ID reserved CA_PID for(i=0; i<N; i++){ private_data_byte } }	 8 8 16 3 13 8	 uimsbf uimsbf uimsbf bslbf uimsbf uimsbf

FIG 9B

Sintaxis	Número de bits	Mnemotécnico
CA_ECM_section(){		
table_id	8	uimsbf
section_syntax_indicator	1	bslbf
'0'	1	bslbf
reserved	2	<u>bslbf</u>
section_length	12	uimsbf
reserved	18	bslbf
version_number	5	uimsbf
current_next_indicator	1	bslbf
section_number	8	uimsbf
last_section_number	8	uimsbf
for(i=0; i<N; i++){		
descriptor()		
}		
CRC_32	32	rpchof
}		

FIG 10

Sintaxis	Número de bits	Mnemotécnico
CA_data(){		
table_id	8	uimsbf
reserved	3	bslbf
CA_PID	13	uimsbf
CA_info_length	8	uimsbf
proprietary_CA_Information();		
CRC_32	32	rpchbf
}		

FIG 11

Valores de bits	Descripción
00	Sin encriptación de la carga útil del paquete de flujo de transporte MPEG
01	Reservado
10	Paquete de flujo de transporte encriptado con clave par
11	Paquete de flujo de transporte encriptado con clave impar

FIG 12

1300



Sección de asociación de programa

Sintaxis	Número de bits	Mnemotécnico
program_association_section(){		
table_id	8	uimsbf
section_syntax_indicator	1	bslbf
'0'	1	bslbf
reserved	2	bslbf
section_length	12	uimsbf
transport_stream_id	16	uimsbf
reserved	2	bslbf
version_number	5	uimsbf
current_next_indicator	1	bslbf
section_number	8	uimsbf
last_section_number	8	uimsbf
for(i=0; i<N; i++){		
program_number	16	uimsbf
reserved	3	bslbf
if (program_number=='0'){		
network_PID	13	uimsbf
}		
else {		
program_map_PID	13	uimsbf
}		
}		
CRC_32	32	rpchbf
}		

FIG 13

FIG 14

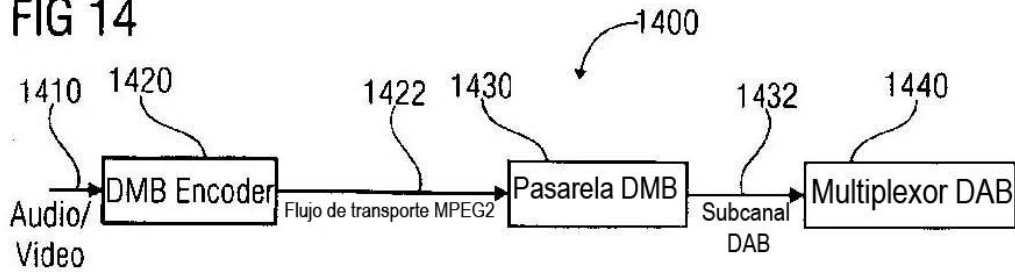


FIG 15

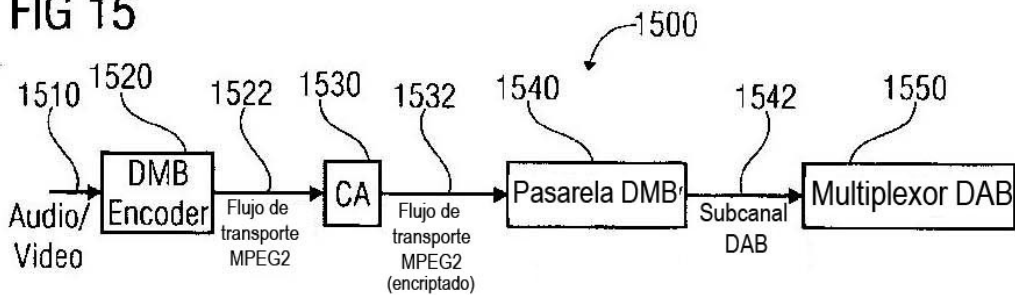


FIG 16A

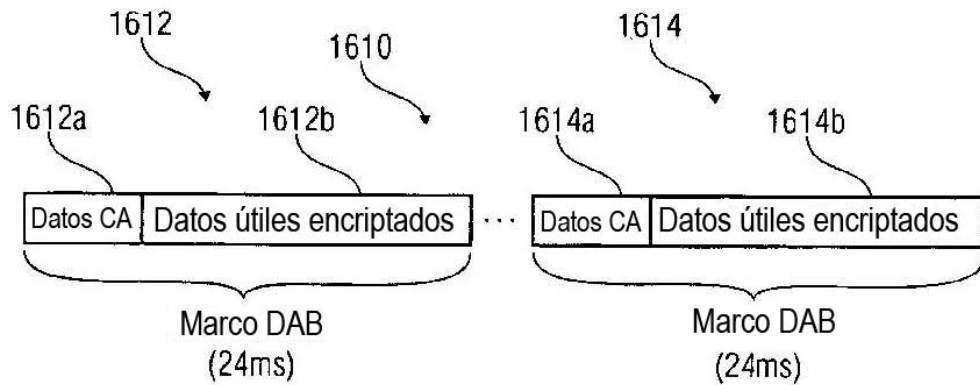


FIG 16B

