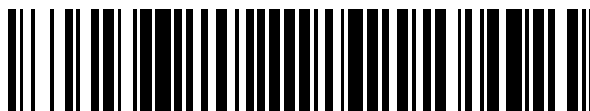


19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 653 246**

51 Int. Cl.:

H04N 21/418 (2011.01)

H04N 21/4367 (2011.01)

H04N 21/462 (2011.01)

H04N 21/482 (2011.01)

H04N 21/434 (2011.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **25.03.2013 PCT/GB2013/050772**

87 Fecha y número de publicación internacional: **07.11.2013 WO13164566**

96 Fecha de presentación y número de la solicitud europea: **25.03.2013 E 13726252 (3)**

97 Fecha y número de publicación de la concesión europea: **22.11.2017 EP 2845385**

54 Título: **Recepción de contenido de audio / video**

30 Prioridad:

04.05.2012 GB 201207854

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

06.02.2018

73 Titular/es:

SATURN LICENSING LLC (100.0%)

25 Madison Avenue

New York, NY , US

72 Inventor/es:

HILL-JOWETT, DAVID

74 Agente/Representante:

ELZABURU, S.L.P

ES 2 653 246 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

Recepción de contenido de audio / video

Antecedentes

Campo de la divulgación

- 5 La presente divulgación se refiere a la recepción de contenido de audio / video.

Descripción de la técnica relacionada

10 La descripción "antecedente" proporcionada en el presente documento tiene el propósito de presentar en general el contexto de la divulgación. El trabajo de los inventores actualmente nombrados, en la medida en que sea descrito en esta sección de antecedentes, así como los aspectos de la descripción que pueden no calificar de otra manera como estado de la técnica en el momento de la presentación, no se admiten ni expresamente ni implícitamente como técnica anterior contra la presente divulgación.

15 Como tecnología antecedente, la especificación de la Interfaz Común ("CI" – Common Interface, en inglés) de DVB permitía a un receptor de televisión o a un decodificador (un "hospedador") interactuar con un módulo de hardware seguro (un módulo de acceso condicional o "CAM" (Conditional Access Module, en inglés)) para permitir al hospedador descryptar el contenido de audio / video de acceso controlado (audio, video o audio y video). La especificación CI define una interfaz entre el hospedador y el CAM, para que los dos trabajen juntos si ambos cumplen con la especificación CI. Esta interoperabilidad proporcionaba un beneficio significativo del sistema CI, ya que, en principio, permitía a los consumidores elegir productos compatibles de diferentes fabricantes.

20 En la especificación CI, el CAM interactúa con una tarjeta inteligente y/o un número de identificación personal ("PIN" – Personal Identification Number, en inglés) del usuario de para proporcionar la autenticación de usuario.

25 Sin embargo, un inconveniente de la especificación CI original es que daba la posibilidad de copiar el contenido descryptado. Este problema surge de la forma en que el hospedador y el CAM interactúan. En uso, el hospedador envía datos encryptados al CAM. El CAM verifica la autenticación del usuario y, suponiendo que el usuario esté autenticado, descrypta el contenido de acceso controlado. A continuación, el CAM envía el contenido descryptado de vuelta al hospedador a través de la interfaz de hospedador del CAM, que generalmente es una PCMCIA (Asociación internacional de tarjetas de memoria para ordenadores personales - Personal Computer Memory Card International, en inglés), aunque no se limita a esta interfaz - por ejemplo, se podría utilizar una interfaz USB. Esta conexión desde el CAM al hospedador representa una debilidad en la seguridad, dado que el contenido digital descryptado puede, en principio, ser interceptado y copiado ilegalmente. Esta debilidad en la seguridad significaba que algunos proveedores de contenido preferían dispositivos integrados, que tienen el hospedador y el CAM como una sola unidad, porque esto les permitía una mejor seguridad sobre la transferencia de datos no encryptados desde el CAM al hospedador. Sin embargo, esto, por supuesto, actuaba en contra de la ventaja asociada con la CI, en relación con la interoperabilidad potencial de diferentes CAM y hospedadores.

35 La especificación CI Plus se redactó para abordar estos problemas, por dos rutas principales. CI Plus proporciona una interfaz segura entre el CAM y el hospedador, de modo que los datos del contenido descryptado no se envían de forma clara entre los dos dispositivos. Asimismo, CI Plus proporciona la autenticación tanto del hospedador como del CAM, en lugar de la técnica de IC de autenticación solamente del CAM.

El sistema de autenticación utiliza una jerarquía de certificados para que tanto el hospedador como el CAM tengan certificados emitidos por una autoridad (tal como CI Plus LLP).

40 La interfaz PCMCIA entre un hospedador y un CAM se protege encryptando los datos de contenido descryptado antes de su envío desde el CAM al hospedador y, descryptándolos a continuación en el hospedador. Esta encryptación está separada de la encryptación-descryptación de control de acceso establecida por el proveedor de contenido, y es específica para cada par CAM-hospedador particular. Las claves se intercambian entre el CAM y el hospedador mediante la técnica de intercambio de claves Diffie-Hellman. Las teclas también se ciclan de vez en cuando, de modo que incluso si una clave resultase comprometida, sería cambiada en cualquier caso unos segundos más tarde.

La versión 1.3 de la especificación CI Plus incluye una denominada disposición de perfil de operador. Los perfiles de operador permiten la selección de una tabla de información de la red (NIT – Network Information Table, en inglés) de una selección de diferentes fuentes. A continuación, se describirá la naturaleza de la NIT.

50 La NIT contiene información específica de la red, y puede relacionarse con una red que abarca más de un canal de radiofrecuencia (RF) y más de un flujo de transporte (TS – Transport Stream, en inglés). La información transmitida por la NIT puede incluir frecuencias de radio o números de canales de RF aplicables a esa red, y un mapeo entre los números de los canales lógicos (LCN – Logical Channel Numbers, en inglés) y los identificadores de programa difundidos por la red. Los números de los canales lógicos se relacionan con el orden en el que los canales de

5 televisión son presentados al usuario para su selección en un hospedador individual (mediante un selector de canales o una guía electrónica de programación (EPG – Electronic Programme Guide, en inglés)) y son en general independientes del mecanismo real mediante el cual son transmitidos los canales de televisión. Por ejemplo, en el Reino Unido, el canal de emisión BBC1 está asignado a LCN 1 (en un sistema terrestre) o a 101 (en un sistema por satélite). Esta asignación es completamente independiente de la frecuencia de radio real por la que se transmite el canal BBC1, y también es completamente independiente de a qué identificadores de paquetes (PID – Packet Identifiers, en inglés) está asignado el flujo de transporte de BBC1 para su transmisión. La NIT proporciona un mapeo entre el LCN y la información de transmisión, tal como el canal de RF o TS. Para sintonizar un canal particular, tal como el BBC1, un receptor puede consultar la NIT para establecer qué TS transporta el BBC1, luego sintoniza la frecuencia de RF que transporta ese TS, a continuación filtra los paquetes de ese TS con PID = 0 para obtener la tabla de asignación de programa (PAT – Programme Allocation Table, en inglés), a continuación (una vez que se ha realizado una selección de canal) utiliza la información de PAT para filtrar paquetes de la tabla de mapa de programas (PMT – Programme Map Table, en inglés) para obtener los PID de los denominados flujos elementales correspondientes al canal deseado (BBC1), y luego filtra los paquetes para obtener los PID requeridos para permitir la descodificación de dichos flujos elementales.

Anteriormente, la NIT fue proporcionada como parte de la señal de emisión. La disposición del perfil de operador de CI Plus 1.3 permite dos opciones de entrega de la NIT y, en particular, permite la entrega potencial de una NIT a través del CAM en lugar de la recepción como entrega por el aire (OTA – Over The Air, en inglés).

Existen dos configuraciones de perfil de operador de CI Plus 1.3:

20 tipo_de_perfil (tipo de perfil) = 0: en este modo, la NIT se determina a partir de la información de emisión; and
profile type = 1: en este modo, el CAM entrega una NIT al hospedador, y el hospedador genera una lista de LCN que depende de la NIT entregada por el CAM.

25 El CAM puede generar la NIT a partir de diversas fuentes. En principio, la NIT puede ser preprogramada en el CAM. O bien, el CAM puede recibir la NIT como una señal OTA dirigida a ese CAM o a esos CAM proporcionada por una red concreta. O bien, la red puede transmitir la NIT al CAM mediante el mecanismo de comunicaciones de baja velocidad (LSC – Low Speed Communications, en inglés) proporcionado por la especificación CI Plus, utilizando una conexión segura separada, como una conexión a internet. El CAM también puede proporcionar la configuración de perfil de operador en función de los datos del operador procedentes de cualquiera de dichas fuentes.

30 En funcionamiento, el hospedador consulta al CAM para preguntar qué perfil de operador es aplicable. Si el perfil del operador es de tipo 0, entonces el hospedador desmultiplexa la NIT de la señal de emisión. Si el perfil del operador es de tipo 1, entonces el CAM proporciona la NIT al hospedador.

En los documentos US 2010/186043 A1, se da a conocer una disposición propuesta previamente.

Compendio

La presente divulgación proporciona una disposición tal como la definida en la reivindicación 1.

35 Otros aspectos y características respectivos están definidos en las reivindicaciones adjuntas.

Se debe entender que tanto la descripción general anterior como la descripción detallada siguiente son ilustrativas, pero no restrictivas, de la presente tecnología.

Breve descripción de los dibujos

40 Una apreciación más completa de la divulgación y muchas de las sus ventajas esperadas se obtendrán fácilmente, ya que la misma se comprende mejor haciendo referencia a la siguiente descripción detallada de realizaciones a modo de ejemplo cuando se considera en conexión con los dibujos adjuntos, en los que:

la figura 1 es un diagrama esquemático de un dispositivo hospedador con un CAM y una tarjeta inteligente;

la figura 2 es un diagrama esquemático de un sistema de acceso condicional (CA – Conditional Access, en inglés) que incorpora el dispositivo hospedador de la figura 1;

45 la figura 3 es un diagrama esquemático que ilustra aspectos del funcionamiento del sistema de la figura 2;

la figura 4 ilustra esquemáticamente el funcionamiento de un sistema de CA de acuerdo con una realización;

la figura 5 ilustra esquemáticamente un proceso de consulta de perfil;

la figura 6 ilustra esquemáticamente un proceso de un CAM obteniendo una NIT; y

la figura 7 ilustra esquemáticamente la combinación de varias NIT procedentes de un CAM y de una señal de emisión.

Para establecer el contexto técnico de las presentes realizaciones, se describirá primero un sistema de emisión que tiene un sintonizador y una disposición de descodificador haciendo referencia a las figuras 1 a 3.

5 A continuación, haciendo referencia a la figura 1, un dispositivo hospedador 10 se muestra en el presente documento como un televisor, pero podría ser, por ejemplo, un descodificador (observándose que la expresión "descodificador" (dispositivo para encima del televisor - set top, en inglés) no implica, para el experto, ningún requisito de una posición física particular del dispositivo durante la utilización). El dispositivo hospedador 10 recibe una señal de televisión de acceso controlado 15 a través de una ruta de datos de emisión. Esta podría ser, por ejemplo, una señal de televisión por satélite recibida por una antena parabólica (no mostrada), una señal de televisión terrestre, una señal de televisión por cable o similar, aunque otros tipos de señal de televisión incluyen una señal de televisión difundida o transmitida por un< señal en paquetes de protocolo de internet (IP). Una técnica consiste en codificar una secuencia de transporte (TS) MPEG en paquetes IP, para que un paquete IP transmita varios (por ejemplo 7 u 8) paquetes TS. Otra técnica codifica la señal de televisión como una disposición llamada BMFF (Formato de archivo de medios de base - Base Media File Format, en inglés) de ISO (Organización Internacional de Estándares – International Standards Organisation, en inglés) descrita en la referencia:

10 http://en.wikipedia.org/wiki/ISO_base_media_file_format. En tales disposiciones, la interfaz IP en un dispositivo hospedador en general se considera en la técnica como un "sintonizador", aunque puede no tener circuitos o funcionalidades de radiofrecuencia. Sin embargo, actúa de manera similar a un sintonizador de radiofrecuencia, ya que selecciona un flujo IP de entre una multitud de posibles flujos IP. También puede proporcionar almacenamiento en memoria temporal del flujo IP recibido.

El dispositivo hospedador 10 tiene una ranura de PCMCIA 20 que incluye conexiones eléctricas y un espacio físico para un módulo enchufable, ambos según el estándar PCMCIA. En otras realizaciones, se puede utilizar un bus serie universal (USB – Universal Serial Bus, en inglés) u otra interfaz eléctrica en lugar de la interfaz PCMCIA.

25 Un módulo de acceso condicional CI Plus, denominado CICAM 30, es un módulo PCMCIA que se puede insertar en la ranura de PCMCIA 20. Cuando el CICAM 30 está completamente enchufado en la ranura 20, se realizan conexiones eléctricas entre los conectores del CICAM 30 y los conectores cooperantes en la ranura 20.

El propio CICAM puede ser un módulo sin tarjeta o puede tener una ranura 40 en la que se puede insertar una denominada tarjeta inteligente 50. La tarjeta inteligente es extraíble y transporta información que define un usuario actual del receptor de contenido en una forma inviolable, segura y no volátil. Cuando la tarjeta inteligente está completamente insertada en la ranura 40, se forma una conexión de datos entre la tarjeta inteligente 50 y el CICAM 30, ya sea utilizando conectores eléctricos cooperantes en la tarjeta inteligente 50 y en la ranura 40, o utilizando una técnica de conexión sin contacto conocida en la que los datos se transfieren de manera inalámbrica en un rango muy corto, como 1-2 cm.

35 Un enlace de datos 68, denominado enlace de comunicaciones de baja velocidad (LSC – Low Speed Communications, en inglés), proporciona comunicaciones de datos entre el extremo de cabecera y el CICAM, a través del puerto de IP (Protocolo de Internet, en inglés) del hospedador – o, en otras palabras, la conexión a internet del hospedador. Por lo tanto, el enlace LSC puede proporcionarse, por ejemplo, mediante un enlace de datos de internet encriptados entre el hospedador y el extremo de cabecera. El término "Baja velocidad" se refiere en un sentido general a una comparación entre la velocidad del LSC y la velocidad de datos de la ruta de datos de emisión, que (en el caso de una ruta de datos por satélite o terrestre) en general sería mucho mayor. Pero no está implicado ningún valor absoluto de velocidad o de velocidad de datos. De esta forma, el CAM y la fuente de contenido están configurados para establecer un enlace de comunicaciones seguro a través de una conexión de datos de internet.

45 En consecuencia, el dispositivo hospedador y el CICAM cooperan para proporcionar un receptor de contenido de audio / video configurado para recibir contenido multimedia de una fuente de contenido mediante una ruta de datos de emisión, estando dispuesto el contenido multimedia como una pluralidad de canales de medios, comprendiendo el receptor de contenidos: un módulo hospedador (tal como el dispositivo hospedador 10) que tiene un sintonizador configurado para asignar índices a los canales lógicos para permitir su selección, en el módulo hospedador, de uno o más de los canales de medios para reproducción mediante la selección del índice del canal lógico correspondiente, almacenando el módulo de hospedador los datos de asociación de canales que asocian los índices de canales lógicos con los canales de medios recibidos; y un módulo de acceso condicional (CAM) extraíble (tal como el CICAM 30), teniendo el CAM una unidad de control de acceso para descodificar contenido de emisión codificado de acceso controlado, estando dispuesto el módulo hospedador y el CAM extraíble para proporcionar un enlace de comunicación encriptado para establecer un enlace de comunicaciones seguro a través de una conexión de datos de internet.

Dicho receptor puede ser configurado para mostrar una lista de selección de canales para permitir la selección por parte del usuario de un canal de acuerdo con el índice de canal lógico asociado con ese canal.

La figura 2 ilustra esquemáticamente el dispositivo hospedador 10 en el contexto de un sistema de acceso condicional. Un denominado extremo de cabecera 60 representa la fuente de la señal de televisión de acceso controlado 15. El extremo de cabecera puede representar, por ejemplo, una estación de enlace ascendente de un emisor por satélite o un centro de distribución de señal de un emisor por cable o terrestre. El sistema de CA codifica el contenido en el extremo de cabecera utilizando una encriptación de sistema de CA. El extremo de cabecera puede introducir asimismo otra información relacionada con el CA en el flujo de datos encriptados que permite al CICAM descodificar el contenido y gestionar el acceso y derechos del abonado (del usuario).

El extremo de cabecera 60 envía la señal de televisión 15 al hospedador 10 que a su vez pasa la señal al CICAM 30 para la descodificación de la encriptación del control de acceso. A continuación, el CICAM 30 vuelve a encriptar la señal mediante una encriptación local y envía la señal nuevamente encriptada de vuelta al hospedador 10 a través de la conexión PCMCIA. El hospedador descodifica la señal recibida del CICAM 30 para ser mostrada en una pantalla de visualización o para ser suministrada a otro dispositivo 70 como un grabador de video basado en disco duro.

La figura 3 es un diagrama esquemático que ilustra el funcionamiento del sistema de la figura 2. El funcionamiento detallado del sistema de la figura 3 se describe en la especificación CI Plus 1.3 (2010-01), disponible (en el momento de la presentación) en http://www.ci-plus.com/data/ci-plus_specification_v1.3.pdf. La presente descripción de la figura 3 simplemente proporciona una visión general de esa operación detallada, con el propósito de colocar la siguiente descripción en el contexto técnico apropiado.

Como antes, la figura 3 muestra el extremo de cabecera 60 (que recibe una señal de contenido de un proveedor de contenido 90), el dispositivo hospedador 10, el CICAM 30 y la tarjeta inteligente 50. La señal 15 se muestra pasando desde el extremo de cabecera 60 al dispositivo hospedador 10. La interfaz segura 80 entre el dispositivo hospedador 10 y el CICAM 30 se denomina interfaz común.

Acceso Condicional

Los sistemas de CA conocidos proporcionan técnicas mediante las cuales se puede denegar o permitir el acceso de un usuario a un flujo de televisión digital. El acceso se proporciona solo a aquellos suscriptores o usuarios con cuentas de pago válidas. En términos prácticos, se proporciona a un usuario una tarjeta inteligente 50 que identifica a ese usuario en (de manera ideal) una forma sin alteraciones, y el sistema está configurado de modo que solo los usuarios con tarjetas inteligentes válidas puedan obtener acceso al contenido de acceso controlado.

El control de acceso se proporciona mediante la utilización de codificación y encriptación. La señal de contenido es codificada con una palabra de control de 8 bytes, que se cambia frecuentemente (hasta varias veces por minuto) para evitar que el sistema de CA se vea comprometido por el conocimiento externo de la palabra de control. Las palabras de control se transmiten al CICAM del receptor, para descodificar el contenido codificado, en forma encriptada como un mensaje de control de derechos (ECM – Entitlement Management Message, en inglés). El CICAM descodifica la palabra de control para permitir la descodificación del contenido de acceso controlado solo cuando está autorizado para hacerlo mediante la recepción de un mensaje de gestión de derechos (EMM). Los EMM son específicos para cada usuario o grupo de usuarios; el CICAM confirma los derechos que proporciona un EMM comparando la identificación del usuario proporcionada en el EMM con la información del usuario proporcionada en la tarjeta inteligente 50. Los EMM pueden ser enviados con menos frecuencia que los ECM, variando los intervalos entre EMM sucesivos en los sistemas comerciales actuales entre 12 minutos y seis semanas.

Los propios ECM y los EMM son tipos de mensajes bien conocidos en los sistemas de distribución de televisión MPEG. El formato de sus cargas útiles puede ser específico para el sistema de CA en uso, siendo las diferencias entre los formatos a menudo semánticas en lugar de tener un significado técnico.

Extremo de cabecera

El extremo de cabecera 60 comprende un encriptador de CA 61, un generador de clave 62, una unidad de control de derechos 63 y un multiplexor y modulador 64.

El proveedor de contenido 90 suministra contenido (como señales de televisión) al extremo de cabecera 60. El extremo de cabecera 60 aplica codificación y encriptación de acceso condicional (CA) al contenido.

Más específicamente, el encriptador de CA 61 encripta o codifica el contenido utilizando una clave de CA como palabra de control. La clave de CA es generada por el generador de claves de CA 62. El contenido codificado generado por el encriptador de CA es suministrado al multiplexor y modulador 64.

La clave de CA es proporcionada asimismo a la unidad de control de derechos 63, que genera ECM basados en las claves de CA y EMM basados en datos del suscriptor que definen qué suscriptores tienen derecho a descodificar qué flujos de contenido. Los ECM y EMM son suministrados al multiplexor y modulador 64. Uno o más flujos de contenido codificado del encriptador de CA 61, uno o más flujos de contenido no codificado (acceso abierto o "en abierto") y los mensajes de control de derechos se multiplexan juntos para formar un flujo de transporte tal como un flujo de transporte MPEG2. Se utilizan formatos conocidos para transportar los datos de contenido, los ECM y los

EMM. Los ECM, EMM y los datos que definen el tipo de codificación utilizado en cada flujo elemental (correspondiente a flujos de contenido codificados individuales) se proporcionan en un formato conocido y se referencian utilizando técnicas conocidas en una tabla de mapa de programas (PMT y/o en una tabla de acceso condicional (CAT – Conditional Access Table, en inglés) que tiene un identificador de programa (PID) predeterminado de 0x001, de modo que la CAT puede ser reconocida en el CICAM.

A continuación, el flujo de transporte multiplexado es modulado por el multiplexor y modulador 64 para su transmisión como una señal de emisión 15 por cable, por satélite o terrestre.

Dispositivo hospedador

El dispositivo hospedador 10 comprende un sintonizador 11, un demodulador y demultiplexor 12, un demultiplexor ("demux") 14 y un descryptador de CC (control de contenido – Content Control, en inglés) 13. Téngase en cuenta que el dispositivo hospedador puede tener otras funciones adicionales; por ejemplo, un dispositivo hospedador puede proporcionar dos o más de recepción de emisión por satélite, recepción de emisión por cable, recepción de emisión terrestre y recepción de televisión por red (IPTV). Por consiguiente, la fuente de contenido puede ser configurada para enviar datos al módulo hospedador como uno o más de: datos de protocolo de internet (IP), datos de emisión por satélite, datos de emisión de televisión terrestre y datos de transmisión por cable.

Dependiendo del tipo de señal de emisión 15, el sintonizador actúa para transformar la señal recibida de nuevo en banda base, de modo que el demodulador y demultiplexor 12 pueda seleccionar y demultiplexar un único flujo de contenido elemental y los datos de la CAT asociados de la señal recibida. El flujo de contenido y los datos del ECM / EMM son pasados a través de la interfaz común 80 al CICAM 30.

En el caso de datos de contenido de acceso controlado, en esta etapa los datos de contenido todavía se codifican cuando pasan a través de la interfaz común 80 al CICAM 30. Esta parte de la transmisión a través de la interfaz común 80 es, por lo tanto, segura, en virtud de la encriptación de CA.

Suponiendo que los ECM y EMM lo permiten, el CICAM 30 descrypta los datos de contenido y los vuelve a encriptar mediante una encriptación mediante control de contenido (CC). La forma en que se realiza esto se describirá a continuación. Los datos encriptados mediante CC son devueltos al dispositivo hospedador 10 donde se demultiplexan mediante el demultiplexor 14 y se descryptan mediante el descryptador de CC 13, de modo que pueden ser visualizados o pasados a otro dispositivo 70 como contenido sin codificar.

Por lo tanto, el dispositivo hospedador funciona para recibir contenido de audio / video y tiene un descodificador de contenido (el módulo CAM, por ejemplo) capaz de descodificar un programa de audio / video a partir de un flujo de datos en paquetes (tal como un TS) utilizando paquetes de datos (tales como EMM / ECM) definiendo información de descryptación. El TS recibido puede comprender uno o más programas que tienen paquetes de datos identificados por conjuntos respectivos de identificadores de paquetes (tales como los PID) y que comprenden programas de mapeo de datos de identificación (PAT, PMT, CAT y similares) a conjuntos respectivos de los PID.

El dispositivo hospedador está configurado asimismo para obtener datos de asociación de canales a través de la ruta de datos de emisión o, en otras palabras, para recibir una NIT de emisión. Esta característica se describirá con más detalle a continuación.

CICAM

El CICAM 30 puede ser un CAM de acuerdo con el estándar de interfaz común plus y comprende un descryptador de CA 31, un generador de claves de CA 32, un encriptador de CC 33 y un generador de claves de CC 34.

El descryptador de CA 31 y el generador de claves de CA 32 pueden considerarse como una unidad de control de acceso para descodificar contenido de emisión de acceso controlado u otros datos. El generador de claves de CC 34 y el encriptador de CC 33 del CICAM 30, y el demultiplexor 14 y el descryptador de CC 13 del dispositivo hospedador 10 cooperan para proporcionar un enlace de comunicación encriptado (la interfaz común 80) para contenido de emisión transmisión codificada mediante acceso controlado descodificado, entre el CICAM y el dispositivo hospedador.

El descryptador de CA 31 utiliza claves generadas a partir de los ECM y EMM recibidos por el generador de claves CA 32, utilizando comprobaciones de la identidad del usuario desde la tarjeta inteligente 50, para descodificar el contenido de acceso controlado recibido. Esta parte de la operación del CICAM utiliza técnicas de CA conocidas para recuperar y aplicar las claves de CA.

Los datos de contenido sin codificar son pasados del descryptador de CA 31 al encriptador de CC 33. Sin embargo, dado que esta transferencia de datos es completamente interna a CICAM, puede hacerse segura e inviolable mediante técnicas conocidas tales como proporcionar el descryptador CA 31, el encriptador de CC 33 y la interfaz de contenido sin codificar dentro de un solo dispositivo de circuito integrado.

5 El encriptador de CC 33 encripta el contenido descodificado utilizando una clave de CC suministrada por el generador de claves de CC 34. Esta clave se establece mediante un intercambio seguro entre el CICAM 30 y el dispositivo hospedador 10, y es específica para ese par de dispositivos CICAM - hospedador. El contenido encriptado de CC es pasado a través de la interfaz común 80 al dispositivo hospedador 10. Por lo tanto, esta parte de la interfaz común también es segura, ya que los datos de contenido son encriptados mediante CC a medida que pasan al dispositivo hospedador.

En consecuencia, el módulo hospedador y el CAM pueden estar dispuestos para proporcionar un enlace de comunicación encriptado para el contenido de emisión codificado mediante acceso controlado descodificado entre el CAM y el módulo hospedador.

10 Intercambio de claves

El CICAM 30 y el dispositivo hospedador 10 contienen lógica, firmware o software que proporcionan algoritmos para intercambio de claves seguro de Diffie-Hellman (DH), comprobación aleatoria y encriptación utilizando los algoritmos conocidos SHA-256, DES y AES, certificados respectivos emitidos por una autoridad de certificación como CI Plus LLP, y claves privadas con las claves públicas correspondientes.

15 Cuando el CICAM 30 se asocia primero con el dispositivo hospedador 10, el CICAM 30 inicia un proceso de autenticación con el dispositivo hospedador 10. En este proceso, cada dispositivo verifica el certificado del otro, y el intercambio de claves de DH se lleva a cabo para compartir claves de manera segura entre los dos dispositivos. En particular, el CICAM primero solicita que el dispositivo hospedador proporcione sus datos de certificado. El CICAM verifica la firma en el certificado del dispositivo hospedador. El mismo proceso es llevado a cabo a continuación por el hospedador que solicita y verifica el certificado de CICAM. Por lo tanto, el CICAM y el hospedador demuestran que poseen la clave privada correspondiente a la clave pública en el certificado firmando una clave pública de DH y enviándola al otro dispositivo para su validación. A continuación, el CICAM obtiene y verifica una clave de autenticación de AKH del hospedador. El CICAM y el hospedador comienzan a calcular e intercambiar datos clave para el encriptado y la autenticación de los datos enviados a través de la interfaz común 80. De esta forma, la clave, el par de claves u otra información de la clave establecida por el CICAM y el hospedador para la comunicación sobre la interfaz común 80 es específica para ese par CICAM-hospedador.

Después de la autenticación, el CICAM también comienza a calcular la clave de CC. El CICAM también puede indicar al dispositivo hospedador que calcule la clave de CC. La clave de CC se utiliza por lo tanto tal como se ha descrito anteriormente para encriptar los datos de contenido pasados desde el CICAM 30 al dispositivo hospedador 10, de acuerdo con el algoritmo de AES. Por lo tanto, se comprenderá que las claves utilizadas para la interfaz común 80 segura son específicos para un par CICAM-hospedador particular.

El dispositivo hospedador de la figura 3 puede funcionar bajo el control de una unidad de procesamiento central que a su vez puede ser un dispositivo procesador programable que funciona según el software o el firmware almacenados en una memoria (que a su vez puede ser una memoria legible por máquina no transitoria tal como un almacenamiento de disco magnético u óptico o una memoria de semiconductor no volátil).

La figura 4 ilustra esquemáticamente el funcionamiento de un sistema de CA de acuerdo con una realización.

En particular, la figura 4 ilustra esquemáticamente aspectos de la comunicación entre el CICAM 30 y el hospedador 10. No todas las características de la figura 3 se muestran en la figura 4, en aras de la claridad del diagrama, pero su presencia se supone en la siguiente explicación.

40 El CICAM 30 recibe un flujo de transporte desde el sintonizador 11 y el demodulador y demultiplexor 12 del hospedador. Una caja 110 ilustra esquemáticamente el proceso llevado a cabo por el descryptador de CA 31, el generador de claves de CA 32, el generador de claves de CC 34 y el encriptador de CC 33, para llevar a cabo la descryptación de la red (CA) y la encriptación del CICAM de un canal deseado en el flujo de transporte recibido. A este respecto, la función de los artículos representados por la caja 110 es la descrita con referencia a la figura 3 anterior. Obsérvese que todas las comunicaciones entre el CICAM 30 y el hospedador 10 se realizan a través de la interfaz común 80. La ruta de datos que implica la caja 110 representa el flujo de datos durante el funcionamiento normal (recepción del canal de televisión) del sistema.

Para detectar una NIT, el CICAM 30 emplea un demultiplexor 120, un generador de NIT 130 y un almacén de NIT 140. El demultiplexor 120 también recibe el flujo de transporte y el demultiplexor es de sus datos proporcionados por el operador del servicio u otra fuente, tal como la NIT de emisión, una tabla de prestación de servicios (SDT – Service Delivery Table, en inglés), datos privados y otros. Estos datos son pasados al generador de NIT 130. Aquí, los datos se ensamblan en una NIT que se almacena en el almacén de NIT 140. Se pueden incluir otros componentes de datos dentro de la NIT generada, tal como los datos de la tarjeta inteligente 50, o los datos recibidos a través del enlace de LSC 68. La NIT que se genera es una estructura de datos cuasi-estática, lo que quiere decir que no cambia muy a menudo. Por lo tanto, es apropiado almacenar la NIT generada en el almacén de NIT 140 para su utilización futura.

En el hospedador, el descifrador de CC 13 y el demultiplexor 14 reciben los datos del programa encriptados mediante CC de la caja 110, los descifran y demultiplexan. Los datos del programa demultiplexados son pasados a un generador o cargador de NIT 150. El generador o cargador de NIT 150 puede obtener una NIT a partir de los datos del programa recibidos o puede cargar una NIT del almacén de NIT 140 del CICAM 30.

- 5 En otro modo de operación, que se describirá a continuación, el generador o cargador de NIT 150 puede combinar una NIT recibida de la señal de emisión y una NIT proporcionada por el CICAM 30 para formar una NIT compuesta. Este modo de operación se denominará tipo_de_perfil = 2.

10 En base a la NIT recibida (en tipo_de_perfil = 0), la NIT proporcionada por el CICAM 30 (en tipo_de_perfil = 1) o la NIT compuesta (en tipo_de_perfil = 2), el generador o cargador de NIT 150 almacena una lista de LCN en un almacén de listas de LCN 160.

15 Un componente final del hospedador 10 que se describirá es un controlador 170 de receptor de hospedador. El controlador 170 controla las operaciones del hospedador, incluidas aquellas operaciones representadas por las características funcionales ilustradas en la figura 3 y controla la interacción con el CICAM 30. Con respecto a la funcionalidad que se describe en la presente memoria, el controlador 170 se comunica con el generador de NIT 130 del CICAM 30 de modo que el generador de NIT 130 pueda dar instrucciones al hospedador para que sintonice un canal de la frecuencia de radio requerida para que un flujo de transporte a partir del cual se puede obtener una NIT esté disponible para el CICAM 30. El controlador 170 también puede consultar al CICAM para establecer el tipo_de_perfil actual y puede dar instrucciones al generador de NIT 132 para proporcionar la última versión de la NIT de CICAM al hospedador.

20 Una vez que el almacén de listas de LCN 160 ha sido rellenado por el generador o cargador de NIT 150, el controlador 170 puede controlar las operaciones de recepción de canales del hospedador de acuerdo con el mapeo entre flujos de transporte, los PID y LCN proporcionados por los datos en el almacén de listas de LCN 160.

25 Los aspectos del funcionamiento del sistema de CA descritos anteriormente se analizarán ahora haciendo referencia a las figuras 5 a 7, en las cuales las operaciones de procesamiento llevadas a cabo por el CICAM 30 se representan como la columna de la izquierda tal como la dibujada, y las operaciones de procesamiento llevadas a cabo por el hospedador 10 están representadas por una columna de la derecha tal como la dibujada.

30 La figura 5 ilustra esquemáticamente un proceso de consulta de perfil. En una etapa 200, el CICAM 30 informa del estado del perfil actual al hospedador al abrir una "sesión", es decir, tras iniciar una interacción entre el CICAM y el hospedador. El estado del perfil simplemente indica si se establece un perfil para el operador y la red actuales y si el CICAM 30 contiene una NIT de CICAM actualmente válida con respecto al operador y la red actuales.

35 En una etapa 210, el hospedador 10 consulta al CICAM 30 para encontrar el perfil real para el operador actual y la red. El CICAM 30 envía una respuesta en una etapa 220. En particular, la etapa 200 implica que el CICAM 30 informe al hospedador 10 cuál de los valores disponibles de tipo_de_perfil es aplicable, es decir, tipo_de_perfil = {0,1,2}, más cualquier otro dato que el hospedador puede requerir o solicitar con respecto al operador y la red actuales. Si tipo_de_perfil = 1 o 2 y el CICAM 30 ya tienen una NIT de CICAM válida con respecto al operador y la red actuales, el CICAM puede transmitir la NIT de CICAM al hospedador en la etapa 220.

Si la indicación en la etapa 200 era que actualmente no hay establecido un perfil válido, se pueden omitir las etapas 210 y 220.

40 La figura 6 ilustra esquemáticamente un proceso del CICAM que obtiene una NIT y la pasa al hospedador (es decir, proporciona más datos de asociación de canales al hospedador) teniendo lugar este proceso cuando lo requiera el hospedador y en circunstancias que el CICAM haya indicado, en la etapa 200, que el CICAM 30 no posea un perfil actualmente válido para el operador y la red actuales.

45 En algunas realizaciones, la búsqueda de una NIT de CICAM es iniciada por el hospedador. Tal disposición se ilustra en la figura 6, en la que, en una etapa 230, el hospedador inicia una nueva búsqueda enviando una instrucción al CICAM 30 (por ejemplo, el controlador 170 envía tal instrucción al generador de NIT 130). En otras realizaciones, la etapa 230 puede omitirse y el CICAM 30 puede iniciar el proceso de búsqueda comenzando con la etapa 240 que se describirá.

50 En la etapa 240, el generador de NIT 130 del CICAM 30 da instrucciones al hospedador para sintonizar un canal de radiofrecuencia requerido para que el flujo de transporte apropiado pueda ser recibido y procesado por el CICAM 30 para obtener la NIT de CICAM. Esto implica que el generador de NIT 130 envía una instrucción de este tipo al controlador 170 que a su vez (en una etapa 250) controla el funcionamiento del sintonizador 11 para sintonizar el canal de radiofrecuencia correcto.

55 Una vez que el CICAM 30 recibe el flujo de transporte apropiado, el generador de NIT 130 obtiene una NIT del CICAM tal como se describió anteriormente, la almacena en el almacén de NIT 140 y devuelve un informe de estado (en una etapa 260) al controlador 170 para indicar que está disponible una NIT del CICAM.

En una etapa 270, el controlador 170 envía una solicitud al generador de NIT 132 para proporcionar la NIT del CICAM al hospedador. En respuesta, en una etapa 280, el generador de NIT 130 hace que la NIT del CICAM sea leída del almacén de NIT 140 y proporcionado al generador de NIT o cargador 150, que a su vez almacena datos derivados de la NIT (tal como una planificación de los LCN) en el almacén de listas de LCN 160.

5 El proceso descrito haciendo referencia a la figura 6 se refiere al CICAM que obtiene la NIT del CICAM a partir de la información de emisión. Tal como se ha explicado anteriormente, sin embargo, este no es el único medio por el cual el CICAM 30 puede generar la NIT del CICAM. Por ejemplo, el generador de NIT 130 puede comunicarse directamente con el proveedor de contenido 90 utilizando, por ejemplo, el enlace de LSC 68. El CICAM 30 también puede comunicarse con la tarjeta inteligente 50 para obtener información de la tarjeta inteligente 50. Para preparar la NIT del CICAM, el CICAM puede combinar una o más de estas fuentes de información según un algoritmo de combinación establecido por el proveedor de contenido. En realizaciones, el CAM puede ser configurado para obtener los datos de asociación de canales del CAM, al menos en parte, de la fuente de contenido utilizando el enlace de comunicaciones (el LSC). En otras realizaciones, el CAM puede ser configurado para obtener los datos de asociación del canal del CAM, al menos en parte, a partir de datos de emisión dirigidos a un subconjunto de varios CAM del que el CAM es miembro.

El proceso descrito anteriormente conduce a que el CICAM 30 proporciona una NIT de CICAM al hospedador 10 a petición del hospedador 10.

Para recapitular, en la presente memoria se explican tres configuraciones de perfil de operador. Estas son:

tipo_de_perfil = 0: en este modo, la NIT se determina a partir de la información de emisión;

20 tipo_de_perfil = 1: en este modo, el CAM proporciona una NIT al hospedador, y el hospedador genera una lista de LCN que depende de la NIT proporcionada por el CAM; y

tipo_de_perfil = 2: en este modo, el CAM proporciona una NIT al hospedador, y el hospedador genera una lista de LCN dependiendo de una NIT compuesta obtenida a partir de una combinación de la NIT de emisión y la NIT del CICAM.

25 Sin embargo, se apreciará que las realizaciones pueden funcionar solo en el modo referido anteriormente como tipo_de_perfil = 2. Es decir, la opción de operar en tipo_de_perfil = {0,1} no es esencial para la presente tecnología; en cambio, el sistema siempre podría funcionar de una manera que combine cualquier información de la NIT proporcionada por el CICAM con cualquier información de la NIT obtenida de la señal de emisión. En este caso, no sería necesario que el hospedador consultara el tipo de perfil actual, y de hecho la variable tipo_de_perfil no sería necesaria en absoluto. Entonces, las disposiciones para combinar las dos NIT en una NIT compuesta (que se describirá a continuación haciendo referencia a la figura 7) son aplicables tanto si este es el único modo de funcionamiento del sistema como si el sistema puede funcionar de acuerdo con los diferentes valores de tipo_de_perfil explicados anteriormente.

35 La figura 7 ilustra esquemáticamente la combinación de varias NIT de un CICAM y de una señal de emisión. El proceso comienza desde el final de la figura 6, en el que el CICAM 30 ha proporcionado una NIT de CICAM al hospedador. Se supone asimismo que el hospedador 10 ha obtenido una NIT de emisión por sí mismo, y también tiene disponibles dos versiones de NIT, para ser combinadas en la NIT compuesta. En términos generales, las etapas llevadas a cabo por el hospedador en la figura 7 pueden ser realizadas por el controlador 170, y las etapas llevadas a cabo por el CICAM en la figura 7 pueden ser realizadas por el generador de NIT 130.

40 Cada NIT puede contener diversos tipos de información, pero, a los efectos de la presente explicación, los campos de información importantes son: LCN, nombre del canal y ubicación del canal (señalando que, como mínimo, solo se debe especificar el flujo de transporte respectivo, porque los PID para cada canal dentro de un flujo de transporte se definen mediante las PAT / PMT de ese flujo de transporte). Meramente como ejemplos para su utilización en la siguiente explicación, y omitiendo cualquier información adicional que no sean los tres campos identificados anteriormente, la NIT de CICAM y la NIT de emisión se muestran a continuación. El símbolo "..." indica filas de datos adicionales que se omiten para mayor claridad de la siguiente discusión, y el símbolo "-----" indica que un campo de datos está vacío o indefinido. Los ejemplos se refieren a los canales de emisión en utilización actual (en la fecha de presentación de la presente solicitud) en el Reino Unido, pero resultará evidente que las técnicas son aplicables en general a otros canales de emisión.

50 (a) NIT de emisión:

LCN	Nombre del canal	Ubicación del canal
1	BBC1	TS-A
2	BBC2	TS-A
...

LCN	Nombre del canal	Ubicación del canal
7	-----	-----
8	Canal 4	TS-B
9	Canal 5	TS-B
...
23	-----	-----
24	-----	-----
...

(b) NIT de CICAM:

LCN	Nombre del canal	Ubicación del canal
1	BBC1	TS-A
2	BBC2	TS-A
...
7	-----	-----
8	Servicio de operador 1	TS-C
9	Canal 5	TS-D
...
23	Servicio de operador 2	TS-C
24	-----	-----
...

5 Haciendo referencia de nuevo a la figura 7, en una etapa 300 el hospedador combina, o intenta combinar, las dos NIT. En el primer caso, el hospedador, en la etapa 300, forma una combinación aditiva simple de las dos NIT, de modo que la información asociada con cada valor disponible de LCN está incluida en ambas NIT a combinar.

Por lo tanto, haciendo referencia a los ejemplos proporcionados anteriormente, el primer intento de un NIT compuesto generado por la etapa 300 incluiría la siguiente información:

(c) NIT compuesta en la etapa 300:

LCN	Nombre del canal	Ubicación del canal
1	BBC1	TS-A
2	BBC2	TS-A
...
7	-----	-----
8	Canal 4, Servicio de operador 1	TS-B, TS-C
9	Canal 5	TS-B, TS-D
...
23	Servicio de operador 2	TS-C
24	-----	-----
...

Donde la información es idéntica entre las dos NIT, esa información es enviada a la NIT compuesta. Donde la información está incluida solo en una NIT, pero no existen conflictos de LCN, por ejemplo, con respecto al LCN 23 donde solo una de los NIT define un canal en ese LCN, se utiliza la información de una de los NIT que define un canal en ese LCN. En el caso en que las dos NIT definan información diferente con respecto a un LCN particular, ambos conjuntos de información están incluidos mediante la etapa 300 y el conflicto por colisión se trata mediante las etapas 310 en adelante. Un ejemplo de tal colisión ocurre con respecto al LCN 8, donde las dos NIT definen diferentes servicios respectivos en ese LCN.

En el ejemplo anterior, el LCN 9 tiene el mismo nombre de canal en las dos NIT, pero dos TS asociados. En casos como este, el asunto puede decidirse por convención. En el presente ejemplo, la convención es que la NIT de emisión prevalezca sobre la NIT del CICAM.

Como variante adicional, el hospedador podría informar al CAM de las ubicaciones del nombre del canal, donde el nombre del canal es el mismo pero el TS es diferente. Esto permitiría al CAM cambiar el nombre de un canal en la NIT del CICAM a un nombre diferente, tal vez como una variante del nombre original, por ejemplo, al agregar un sufijo de una sola letra. Por ejemplo, el canal BBC2 podría renombrarse como BBC2W (W por Gales – Wales, en inglés).

En la etapa 310, el hospedador detecta colisiones (tal como se definió anteriormente, donde los diferentes servicios están definidos por las dos NIT con respecto al mismo LCN), y el hospedador notifica al CICAM la colisión, otorgándole al CICAM al menos el LCN (que puede denominarse índice de canal lógico) en (o en, o con respecto a) la colisión que ha ocurrido. En otras palabras, el módulo hospedador comprende un detector configurado para detectar un conflicto de índice de canal lógico entre los datos de asociación de canales obtenidos por el hospedador a partir de la ruta de datos de emisión y los datos de asociación de canales proporcionados por el CAM y, en el caso de un conflicto, para detectar uno o más índices de canales lógicos no utilizados. Si no se detecta ninguna colisión en la etapa 310, entonces el control se puede pasar directamente a una etapa 380 para controlar la recepción.

En una etapa 320, el CICAM solicita una nueva ubicación desde el hospedador. En otras palabras, el CICAM solicita un LCN diferente para el servicio asignado originalmente al LCN en conflicto. Se debe observar que esto puede ocurrir varias veces dentro de las NIT, de modo que en cada caso la colisión se notifica al CICAM en esta etapa 310 y, de nuevo en cada caso, el CICAM solicita una nueva ubicación para ese canal en la etapa 320. cuando existen múltiples colisiones, las notificaciones y solicitudes pueden ser tratadas en paralelo o como una serie de interacciones entre el hospedador y el CICAM. En otras palabras, el CAM está configurado para seleccionar uno de los índices de canal lógico no utilizados para su utilización por un canal de medios para el cual el índice de canal lógico definido en los datos de asociación del CAM entra en conflicto con un índice de canal lógico definido en los datos de asociación de canales del hospedador.

En una etapa 330, el hospedador consulta el NIT compuesto inicial generado en la etapa 300, y detecta los valores LCN actualmente no utilizados. En realizaciones, el hospedador también detecta cuáles de esos valores de LCN actualmente no utilizados están numéricamente más cercanos al (o a cada) valor de LCN en el que se ha producido una colisión. En una etapa 340, el hospedador comunica al CICAM el (los) LCN que representan las ubicaciones disponibles.

En una realización alternativa, en lugar de realizar la etapa 320, el hospedador puede combinar las etapas 310 y 330, de modo que, en efecto, el hospedador recibe la NIT del CAM, combina las NIT en la etapa 300, detecta colisiones e informa al CAM de las ubicaciones disponibles. El CAM puede seleccionar una de las ubicaciones ofrecidas o responder con una solicitud de LCN diferente, o simplemente establecer un LCN diferente.

De hecho, es estrictamente necesario notificar al CICAM una ubicación disponible con respecto a cada colisión, porque la forma en que se detectan las ubicaciones disponibles, desde el intento inicial (c) en la NIT compuesta, significa que una ubicación detectada por el hospedador como disponible, por definición, no se utilizará dentro de la NIT del CICAM. Sin embargo, para proporcionar flexibilidad al CICAM, y en particular al operador o proveedor de NIT del CICAM, se puede notificar al CICAM más de una ubicación disponible con respecto a cada colisión, en la etapa 340.

En una etapa 350, el CICAM selecciona una de las ubicaciones disponibles notificadas con respecto a cada LCN para el cual existe una colisión. La selección puede ser arbitraria (por ejemplo, LCN numéricamente más bajo que los ofrecidos con respecto a cada colisión), o puede realizarse consultando al operador (por ejemplo, mediante interacción sobre el enlace LSC 68), o puede realizarse de acuerdo con un algoritmo o tabla de consulta predeterminados proporcionados durante la fabricación o mediante una comunicación de datos previa del operador. Por ejemplo, cuando los índices lógicos de canal o LCN son índices numéricos, y el CAM puede configurarse para seleccionar el número más bajo de los índices de canal lógico no utilizados proporcionados por el hospedador. El CAM puede estar configurado para comunicar a la fuente de contenido que un índice de canal lógico de un canal definido por los datos de asociación de canales del CAM ha sido cambiado en respuesta a un conflicto con los datos de asociación de canales del hospedador.

Desde la etapa 350, el control pasa a ambos a una etapa opcional 360, en la cual el CICAM puede notificar al operador el conflicto y su resolución (por ejemplo, mediante interacción sobre el enlace LSC 68), y a una etapa 370 en la que el hospedador establece una versión final de la NIT compuesta utilizando las ubicaciones seleccionadas por el CICAM en la etapa 350 para superar cualquier colisión. Después de la etapa 370 el control puede pasarse a la etapa 380 para controlar la recepción, o el control puede pasarse de nuevo a la etapa 300 para detectar de nuevo cualquier colisión.

En el presente ejemplo, supóngase que el hospedador ofreció al CICAM los LCN 7 y 24 como ubicaciones disponibles alternativas con respecto al "Servicio de operador 1" conflictivo en LCN 8. Supóngase también que en la etapa 350, el CICAM seleccionó el LCN 7 para ese servicio, por ejemplo, sobre la base de que el LCN 7 era numéricamente el más bajo de las ubicaciones disponibles ofrecidas por el hospedador. Por lo tanto, en la etapa 370 el hospedador configura la NIT compuesta final de la siguiente manera:

(d) NIT compuesta final en la etapa 370:

LCN	Nombre del canal	Ubicación del canal
1	BBC1	TS-A
2	BBC2	TS-A
...
7	Servicio de operador 1	TS-C
8	Canal 4	TS-B
9	Canal 5	TS-B
...
23	Servicio de operador 2	TS-C
24	-----	-----
...

El hospedador controla la recepción del material del programa de acuerdo con la NIT compuesta final en una etapa 380. Esto puede implicar la visualización de datos tales como la transmisión de los datos de la guía electrónica de programas de emisión, con LCN asociados, para permitir la selección de un canal por parte del usuario para su reproducción sobre la base del LCN.

Tal como se explicó anteriormente, si solo se comunica una ubicación potencial disponible al CICAM en la etapa 340, entonces la etapa 350 simplemente se convierte en una etapa de aceptación del cambio al LCN en conflicto. Alternativamente, el CAM puede afirmar un LCN diferente por completo para ese servicio.

La etapa 320 puede omitirse, o combinarse de manera más precisa con la etapa 340, de modo que al CICAM se le notifica la colisión y la ubicación alternativa disponible en una sola etapa.

Se debe observar que las técnicas no están restringidas a la combinación de solo dos NIT; si existen diferentes fuentes de NIT disponibles, pueden combinarse en una NIT compuesta utilizando estas técnicas, de modo que cualquier conflicto de LCN se trate tal como se describió anteriormente.

Aunque las realizaciones se han descrito en el contexto de transmisión por canales de frecuencia de radio como canales satelitales o terrestres, se apreciará que las técnicas son igualmente adecuadas para la transmisión de datos por otros medios, tales como un sistema de emisión de protocolo de internet (IP) o a través de un sistema de distribución por cable. En cada caso, el término "sintonizador" se aplica a una parte del sistema que selecciona un flujo de transporte en lugar de otro, incluso si ese proceso de selección no implica una operación de sintonización de la frecuencia de radio.

Si el hospedador es de hecho capaz de manejar dos servicios en el mismo LCN, no necesita informar al CAM de una colisión y, en cambio, puede solicitar al usuario que seleccione una de las dos variantes del servicio para un LCN particular.

Las realizaciones incluyen asimismo una señal de datos, que es una señal dentro del aparato tal como se describe, en particular (aunque no exclusivamente) una señal transmitida desde el hospedador al CAM o al conjunto de varios CAM, o la señal de retorno. Un medio de almacenamiento tal como una memoria mediante la cual se almacena dicha señal también se considera como una realización de la presente descripción. El medio de almacenamiento puede ser, por ejemplo, un medio de almacenamiento no transitorio legible por máquina.

Las realizaciones de la divulgación también incluyen: un receptor de contenido de audio / video configurado para recibir contenido multimedia de una fuente de contenido a través de una ruta de datos de emisión, estando el contenido de los medios dispuesto como una pluralidad de canales de medios, comprendiendo el receptor de contenido:

5 un módulo hospedador que tiene un sintonizador configurado para asignar índices de canales lógicos a los canales de medios para permitir la selección, en el módulo hospedador, de uno o más de los canales de medios para su reproducción seleccionando el índice de canal lógico correspondiente, almacenando el módulo de hospedador datos de asociación de canales que asocian los índices de canales lógicos con los canales de medios recibidos;

10 un módulo de acceso condicional (CAM) extraíble que tiene una unidad de control de acceso para descodificar contenido de emisión codificada de acceso controlado, estando el módulo hospedador y el CAM extraíble dispuestos para proporcionar un enlace de comunicación encriptado para el contenido de emisión codificado de acceso controlado descodificado entre el módulo de acceso condicional y el módulo hospedador;

en el que:

15 el módulo hospedador está configurado para obtener datos de asociación de canales a través de la ruta de datos de emisión;

el CAM está configurado para proporcionar más datos de asociación de canales al módulo hospedador;

20 el módulo hospedador comprende un detector configurado para detectar un conflicto de índice de canal lógico entre los datos de asociación de canales obtenidos por el hospedador de la ruta de datos de emisión y los datos de asociación de canales proporcionados por el CAM y, en el caso de un conflicto, proporcionar al CAM la información que representa el índice de canal lógico en el que se ha producido el conflicto.

Las realizaciones de la divulgación también proporcionan un CAM que funciona para recibir información que representa el índice de canal lógico en el que se ha producido el conflicto.

25 Las realizaciones de la divulgación también incluyen un receptor de contenido de audio / video configurado para recibir contenido multimedia de una fuente de contenido mediante una ruta de datos de emisión, estando dispuesto el contenido multimedia como una pluralidad de canales de medios, comprendiendo el receptor de contenido:

un módulo hospedador que tiene un sintonizador configurado para asignar índices de canales lógicos a los canales de medios para permitir la selección, en el módulo hospedador, de uno o más de los canales de medios para reproducción seleccionando el índice de canal lógico correspondiente, almacenando el módulo hospedador los datos de asociación de canales que asocian los índices de canal lógico con los canales de medios recibidos;

30 un módulo de acceso condicional (CAM) extraíble, teniendo el CAM una unidad de control de acceso para descodificar contenidos de emisión codificados de acceso controlado, estando el módulo hospedador y el CAM extraíble dispuestos para proporcionar un enlace de comunicación encriptado para el contenido de emisión codificado de acceso controlado descodificado entre el módulo de acceso condicional y el módulo hospedador;

en el que:

35 el módulo hospedador está configurado para obtener datos de asociación de canales a través de la ruta de datos de emisión;

el CAM está configurado para proporcionar más datos de asociación de canales al módulo hospedador;

40 el módulo hospedador comprende un detector configurado para detectar un conflicto de índice de canal lógico entre los datos de asociación de asociación de canales obtenidos por el hospedador de la ruta de datos de emisión y los datos de asociación de canales proporcionados por el CAM y, en el caso de un conflicto, para detectar uno o más índices de canales lógicos no utilizados que están numéricamente más cercanos al índice del canal lógico en el que ha ocurrido un conflicto.

45 Las realizaciones de la divulgación proporcionan un CAM configurado para recibir uno o más índices de canales lógicos no utilizados que están numéricamente más cercanos al índice del canal lógico en el que se ha producido el conflicto.

De manera más general, se apreciará que cuando en la presente memoria se describe una característica técnica de una realización con respecto a un elemento que comunica ciertos datos a otro elemento, tanto el envío de datos como los elementos de recepción de datos en esta comunicación se consideran como respectivas realizaciones de la presente divulgación.

50 En la medida en que las realizaciones se hayan implementado, al menos en parte, utilizando el aparato de procesamiento de datos controlado por software, se apreciará que dicho software, y un medio por el cual se proporciona el software (tal como un medio de almacenamiento no transitorio legible por máquina, por ejemplo, un

disco magnético u óptico o una memoria no volátil) también se consideran como realizaciones de la presente descripción.

5 Será evidente que son posibles numerosas modificaciones y variaciones de la presente descripción a la luz de las enseñanzas anteriores. Por lo tanto, debe entenderse que, dentro del alcance de las reivindicaciones adjuntas, la tecnología puede ponerse en práctica de otra manera distinta de la específicamente descrita en el presente documento.

REIVINDICACIONES

- 5 1. Un receptor de contenido de audio / video configurado para recibir contenido multimedia de una fuente de contenido a través de una ruta de datos de emisión, estando dispuesto el contenido multimedia como una pluralidad de medios de comunicación, comprendiendo el receptor de contenido:
- 10 un módulo hospedador (10) que tiene un sintonizador configurado para asignar índices de canales lógicos a los canales de medios para permitir la selección, en el módulo hospedador, de uno o más de los canales de medios para su reproducción seleccionando el índice de canal lógico correspondiente, almacenando el módulo de hospedador datos de asociación de canales que asocian los índices de canales lógicos con los canales de medios recibidos;
- 15 un módulo de acceso condicional CAM (30, 50) extraíble, teniendo el CAM una unidad de control de acceso para descodificar contenido de emisión codificado de acceso controlado, estando el módulo hospedador y el CAM dispuestos para proporcionar un enlace de comunicación encriptado para contenido de emisión codificado de acceso controlado descodificado entre el CAM y el módulo hospedador;
- en el que:
- el módulo hospedador está configurado para obtener datos de asociación de canales a través de la ruta de datos de emisión;
- el CAM está configurado para proporcionar más datos de asociación de canales al módulo hospedador;
- 20 el módulo hospedador comprende un detector configurado para detectar un conflicto de índice de canal lógico entre los datos de asociación de canales obtenidos por el hospedador de la ruta de datos de emisión y los datos de asociación de canales proporcionados por el CAM (310) y, en el caso de un conflicto, detectar uno o más índices de canales lógicos no utilizados; y
- 25 el CAM está configurado para seleccionar uno de los índices de canal lógico no utilizados para su utilización por un canal de medios para el cual el índice de canal lógico definido en los datos de asociación de canal del CAM entra en conflicto con un índice de canal lógico definido en los datos de asociación de canales del hospedador.
2. Receptor según la reivindicación 1, en el que los índices de canales lógicos son valores numéricos, y el CAM está configurado para seleccionar el número más bajo de los índices de canales lógicos no utilizados proporcionados por el hospedador.
- 30 3. Receptor según la reivindicación 1 o la reivindicación 2, en el que el CAM y la fuente de contenido están configurados para establecer un enlace de comunicaciones seguro a través de una conexión de datos de internet.
4. Receptor según la reivindicación 3, en el que el CAM está configurado para comunicar a la fuente de contenido que un índice de canal lógico de un canal definido por los datos de asociación de canales del CAM ha sido cambiado en respuesta a un conflicto con los datos de asociación de canales del hospedador.
- 35 5. Receptor según la reivindicación 3 o la reivindicación 4, en el que el CAM está configurado para obtener los datos de asociación de canales del CAM, al menos en parte, de la fuente de contenido que utiliza el enlace de comunicaciones.
6. Receptor según una cualquiera de las reivindicaciones anteriores, en el que es CAM está configurado para obtener los datos de asociación de canales del CAM, al menos en parte, a partir de los datos de emisión dirigidos a un subconjunto de varios CAM de los cuales el CAM es miembro.
- 40 7. Receptor según una cualquiera de las reivindicaciones anteriores, en el que el módulo hospedador y el CAM están dispuestos para proporcionar un enlace de comunicación encriptado para el contenido de emisión codificado de acceso controlado descodificado entre el CAM y el módulo hospedador.
8. Receptor según una cualquiera de las reivindicaciones anteriores, en el que la fuente de contenido está configurada para enviar datos al módulo hospedador como uno o más de: datos de protocolo de internet (IP), datos de emisión por satélite, datos de emisión de televisión terrestre y datos de emisión por cable.
- 45 9. Receptor según una cualquiera de las reivindicaciones anteriores, en el cual el CAM es un CAM de acuerdo con la interfaz común más estándar.
- 50 10. Método de recepción de contenido de audio / video para recibir contenido multimedia de una fuente de contenido a través de una ruta de datos de emisión por parte de un receptor que tiene un módulo hospedador (10) y un módulo de acceso condicional CAM (30, 50) extraíble, teniendo el CAM una unidad de control de acceso para descodificar

contenido de emisión codificado de acceso controlado, estando dispuesto el módulo hospedador y el CAM para proporcionar un enlace de comunicación encriptado para el contenido de emisión codificado de acceso controlado descodificado entre el CAM y el módulo hospedador, estando el contenido multimedia dispuesto como una pluralidad de canales de medios, comprendiendo el método:

5 el módulo hospedador asigna índices de canales lógicos a los canales de medios para permitir la selección, en el módulo de hospedador, de uno o más de los canales de medios para su reproducción mediante la selección del índice de canal lógico correspondiente;

el módulo hospedador almacena los datos de asociación de canales que asocian los índices de canales lógicos con los canales de medios recibidos;

10 el módulo hospedador obtiene datos de asociación de canales a través de la ruta de datos de emisión;

el CAM proporciona datos de asociación de canales adicionales al módulo hospedador;

15 el módulo hospedador detecta un conflicto de índice de canal lógico entre los datos de asociación de canales obtenidos por el hospedador a través de la ruta de datos de emisión y los datos de asociación de canales proporcionados por el CAM (310) y, en el caso de un conflicto, detecta uno o más índices de canales lógicos no utilizados; y

el CAM seleccionan uno de los índices de canales lógicos no utilizados para ser utilizado por un canal de medios para el cual el índice de canal lógico definido en los datos de asociación de canales del CAM entra en conflicto con un índice de canal lógico definido en los datos de asociación de canales del hospedador.

20 11. Módulo de acceso condicional CAM (30, 50) extraíble para utilización en un receptor de contenido de audio / video configurado para recibir contenido multimedia de una fuente de contenido a través de una ruta de datos de emisión, estando el contenido multimedia dispuesto como una pluralidad de canales de medios, comprendiendo el receptor de contenido un módulo hospedador (10) que tiene un sintonizador configurado para asignar índices de canales lógicos a los canales de medios para permitir la selección, en el módulo hospedador, de uno o más de los canales de medios para su reproducción mediante la selección del índice de canal lógico correspondiente, almacenando el módulo hospedador datos de asociación de canales que asocian los índices de canales lógicos con los canales de medios recibidos, estando el módulo de hospedador configurado para obtener datos de asociación de canales a través de la ruta de datos de emisión;

30 teniendo el CAM una unidad de control de acceso para descodificar contenidos de emisión codificados de acceso controlado, estando el CAM dispuesto para tener un enlace de comunicación encriptado con el módulo hospedador;

en el cual:

el CAM está configurado para proporcionar más datos de asociación de canales al módulo hospedador;

35 en respuesta a la detección de un conflicto de índice de canal lógico entre los datos de asociación de canales obtenidos por el hospedador de la ruta de datos de emisión y los datos de asociación de canales proporcionados por el CAM (310) y una detección, por parte del hospedador, de uno o más índices de canales lógicos no utilizados, el CAM está configurado para seleccionar uno de los índices de canales lógicos no utilizados para su utilización por un canal de medios para el cual el índice de canal lógico definido en los datos de asociación de canales del CAM entra en conflicto con un índice de canal lógico definido en los datos de asociación de canales del hospedador.

40 12. Método de accionamiento de un módulo de acceso condicional CAM (30, 50) extraíble para utilizar en un receptor de contenido de audio / video configurado para recibir contenido multimedia de una fuente de contenido a través de una ruta de datos de emisión, estando el contenido multimedia dispuesto como una pluralidad de canales de medios, comprendiendo el receptor de contenido un módulo hospedador (10) que tiene un sintonizador configurado para asignar índices de canales lógicos a los canales de medios para permitir la selección, en el módulo hospedador, de uno o más de los canales de medios para su reproducción mediante la selección del índice de canal lógico correspondiente el módulo hospedador que almacena datos de asociación de canales asociando los índices de canales lógicos con los canales de medios recibidos, estando el módulo hospedador configurado para obtener datos de asociación de canales a través de la ruta de datos de emisión;

50 teniendo el CAM una unidad de control de acceso para descodificar contenido de emisión codificado de acceso controlado, estando el CAM dispuesto para tener un enlace de comunicación encriptado con el módulo hospedador;

comprendiendo el método:

proporcionar más datos de asociación de canal al módulo hospedador; y

5 en respuesta a la detección de un conflicto de índice de canal lógico entre los datos de asociación del canal obtenidos por el hospedador a partir de la ruta de datos de emisión y los datos de asociación de canales proporcionados por el CAM (310) y una detección, por el hospedador, de uno o más índices de canales lógicos no utilizados, seleccionando uno de los índices de canales lógicos no utilizados para su utilización por un canal de medios para el cual el índice de canal lógico definido en los datos de asociación de canales del CAM entra en conflicto con un índice de canal lógico definido en los datos de asociación de canales del hospedador.

10 13. Módulo hospedador (10) para utilización en un receptor de contenido de audio / video configurado para recibir contenido multimedia de una fuente de contenido a través de una ruta de datos de emisión, estando el contenido multimedia dispuesto como una pluralidad de canales de medios,

15 teniendo el módulo de hospedador un sintonizador configurado para asignar índices de canales lógicos a los canales de medios para permitir la selección, en el módulo hospedador, de uno o más de los canales de medios para reproducción seleccionando el índice de canal lógico correspondiente, almacenando el módulo hospedador los datos de asociación de canales que asocian los índices de canales lógicos con los canales de medios recibidos y que se pueden conectar a un módulo de acceso condicional CAM (30, 50) extraíble, estando el módulo hospedador dispuesto para tener un enlace de comunicación encriptado con el CAM;

en el que:

20 el módulo hospedador está configurado para obtener datos de asociación de canales a través de la ruta de datos de emisión y para recibir datos de asociación de canales adicionales desde el CAM; y

25 el módulo hospedador comprende un detector configurado para detectar un conflicto de índice de canal lógico entre los datos de asociación de canales obtenidos por el hospedador a partir de la ruta de datos de emisión y los datos de asociación de canales proporcionados por el CAM (310) y, en el caso de un conflicto, detectar uno o más índices de canales lógicos no utilizados para su selección por un canal multimedia para el cual el índice de canal lógico definido en los datos de asociación de canales del CAM entra en conflicto con un índice de canal lógico definido en los datos de asociación de canales del hospedador.

14. Módulo de hospedador según la reivindicación 13, configurado para ser conectado al CAM a través de una interfaz común que cumple con el estándar interfaz común Plus.

15. Un televisor que comprende un módulo hospedador según la reivindicación 13 o la reivindicación 14.

30 16. Método de accionamiento de un módulo hospedador (10) en un receptor de contenido de audio / video configurado para recibir contenido multimedia de una fuente de contenido a través de una ruta de datos de emisión, estando dispuesto el contenido multimedia como una pluralidad de canales de medios,

35 teniendo el módulo hospedador un sintonizador configurado para asignar índices de canales lógicos a los canales de medios para permitir la selección, en el módulo hospedador, de uno o más de los canales de medios para su reproducción mediante la selección del índice de canal lógico correspondiente, almacenando el módulo hospedador datos de asociación de canales asociando los índices de canales lógicos con los canales de medios recibidos y que pueden conectarse a un módulo de acceso condicional CAM (30, 50) extraíble, estando dispuesto el módulo hospedador para tener un enlace de comunicación encriptado con el CAM;

comprendiendo el método:

40 obtener datos de asociación de canales a través de la ruta de datos de emisión y recibir datos de asociación de canal adicionales del CAM; y

45 detectar un conflicto de índice de canal lógico entre los datos de asociación de canal obtenidos por el hospedador de la ruta de datos de emisión y los datos de asociación de canal proporcionados por el CAM (310) y, en el caso de un conflicto, detectar uno o más índices de canal lógico no utilizados para selección por la CAM para utilización por parte de un canal de medios para el cual el índice de canal lógico definido en los datos de asociación de canales del CAM entra en conflicto con un índice de canal lógico definido en los datos de asociación de canales del hospedador.

17. Programas informáticos que, cuando son ejecutados por un ordenador hacen que el ordenador implemente un método según cualquiera de las reivindicaciones 10, 12 y 16.

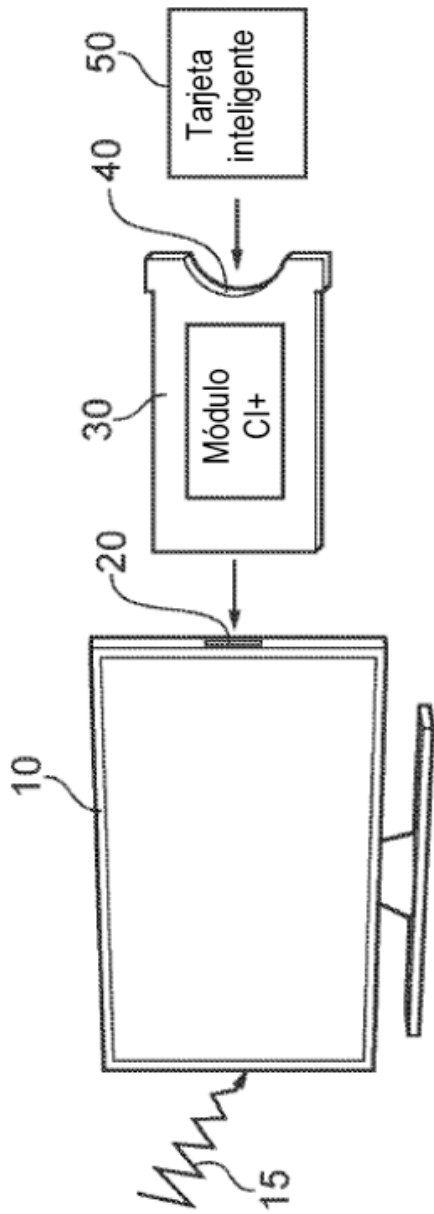


FIG. 1

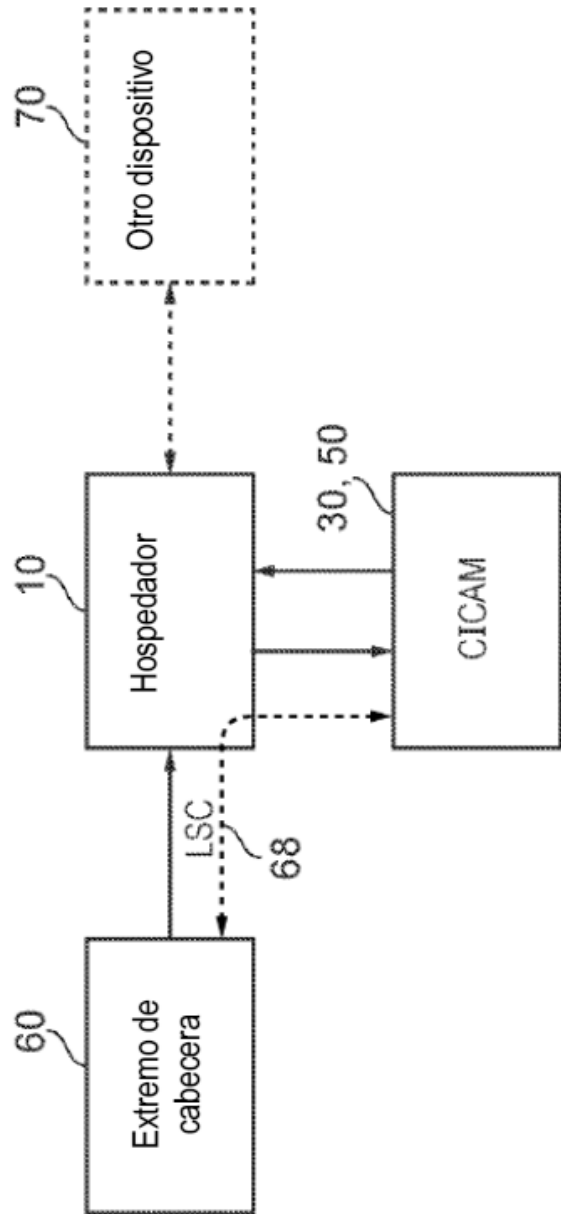


FIG. 2

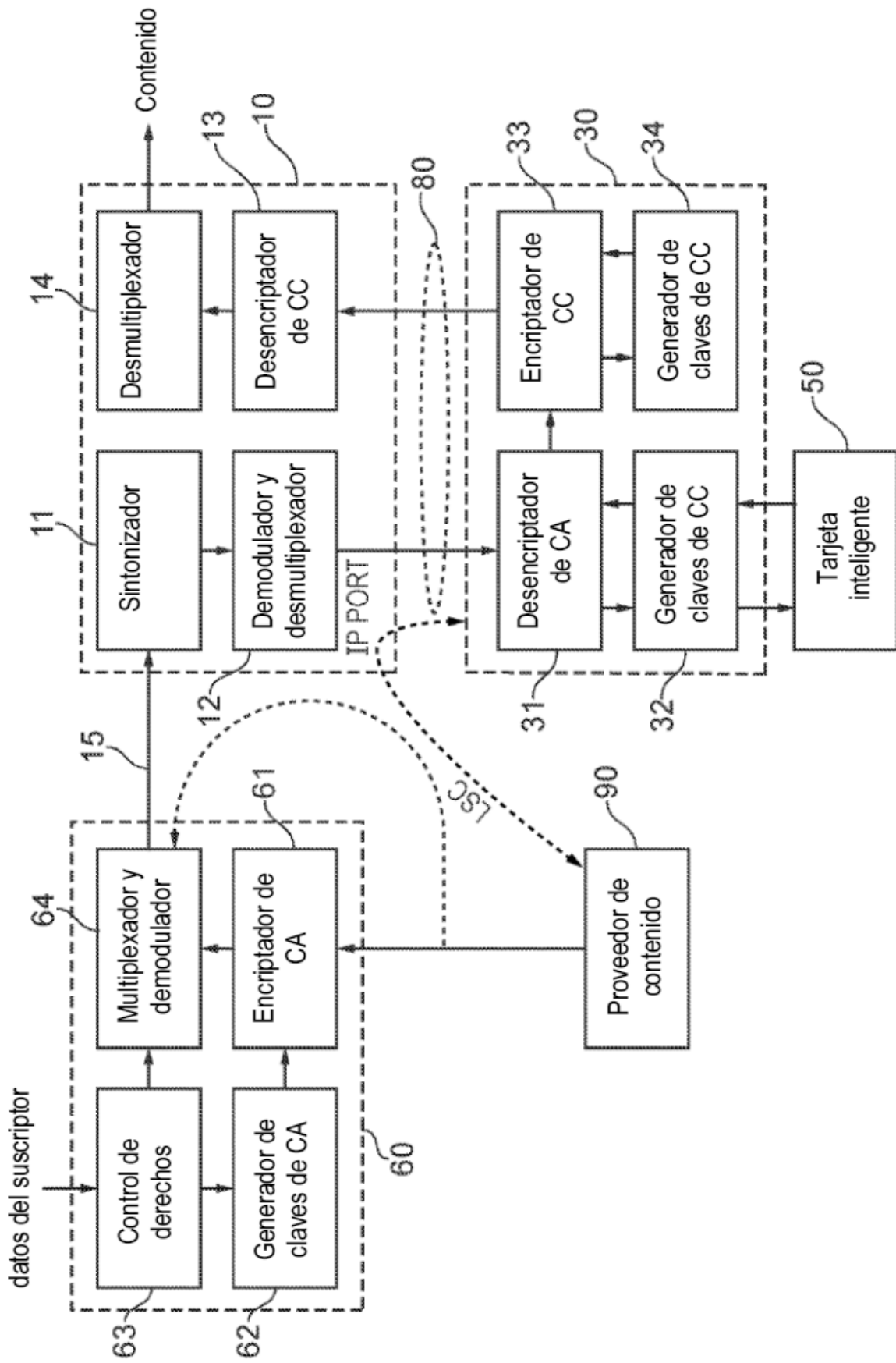


FIG. 3

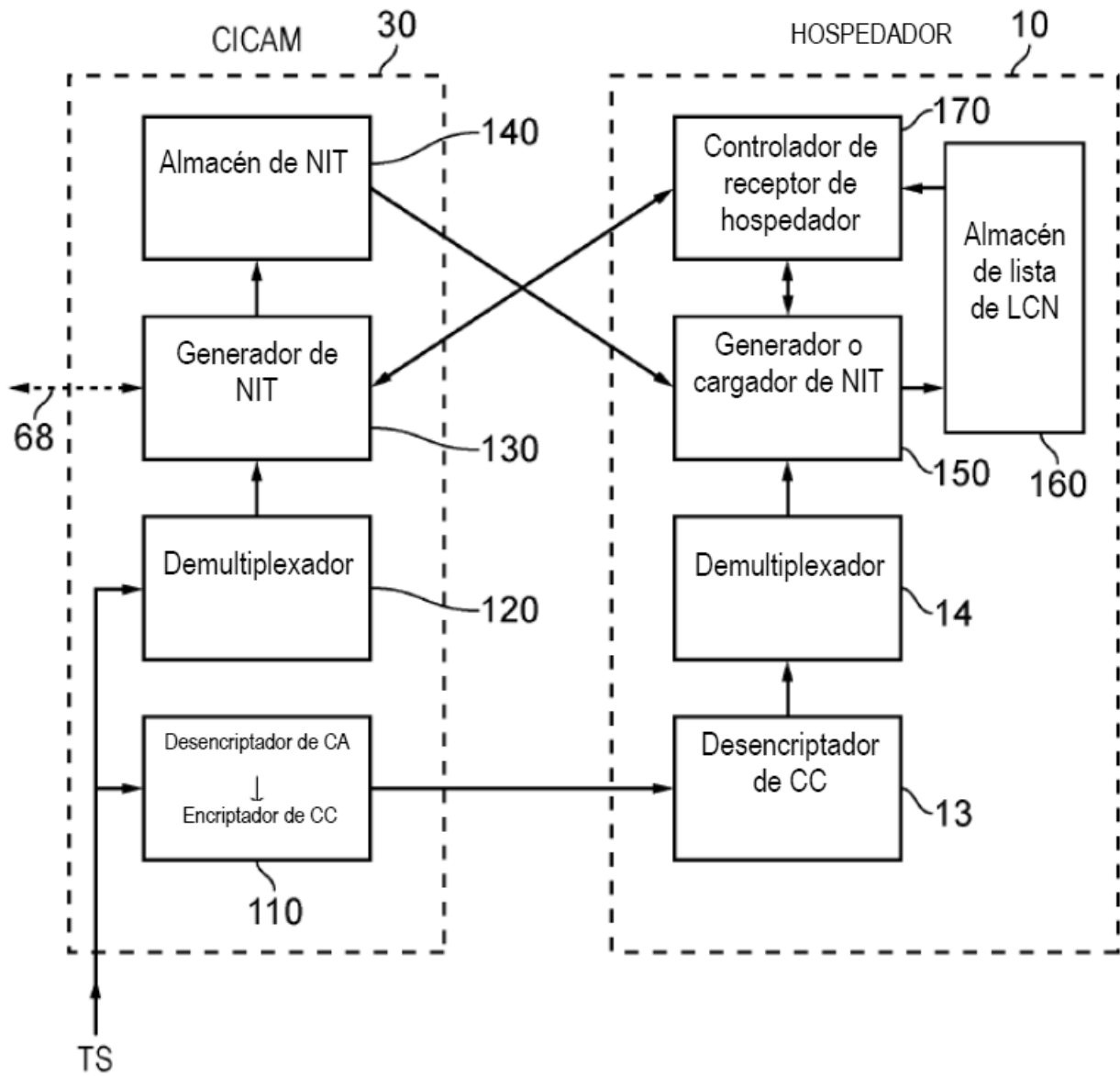


FIG. 4

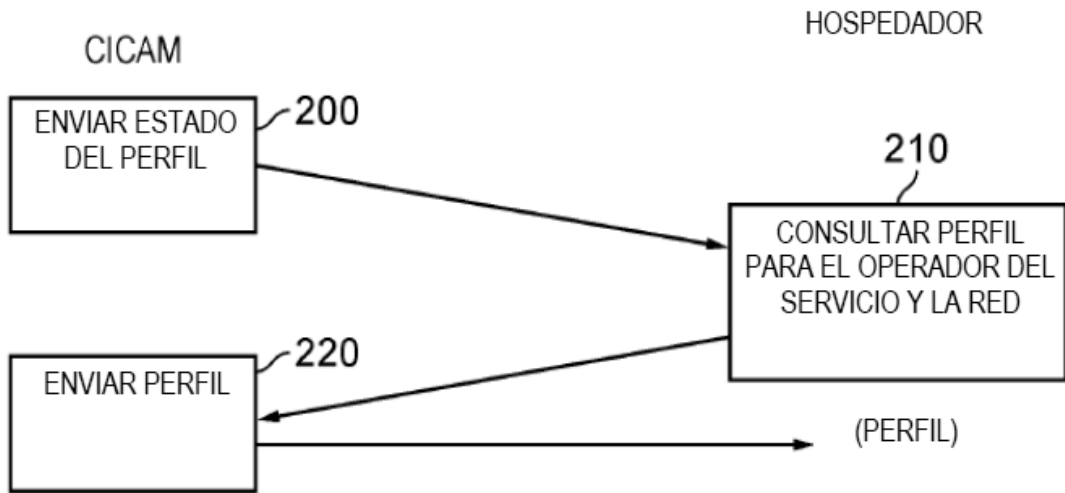


FIG. 5

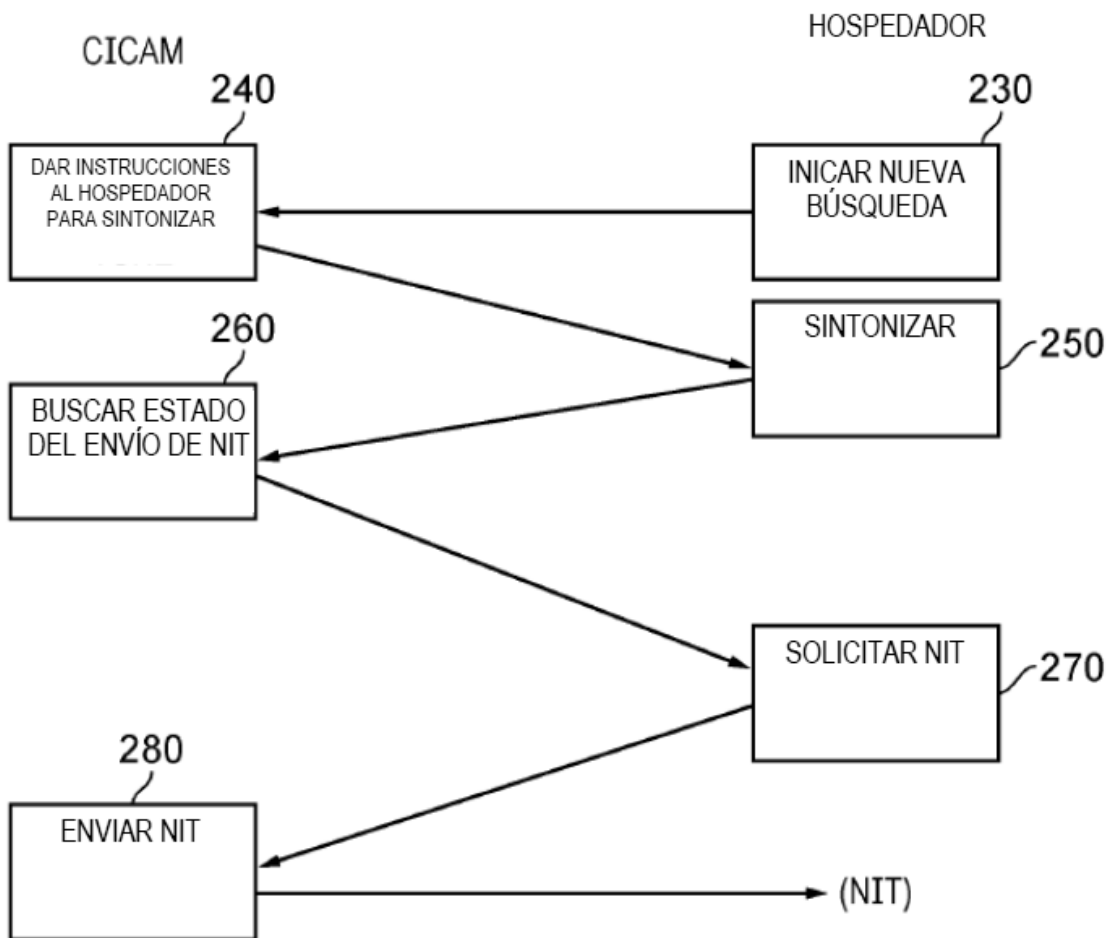


FIG. 6

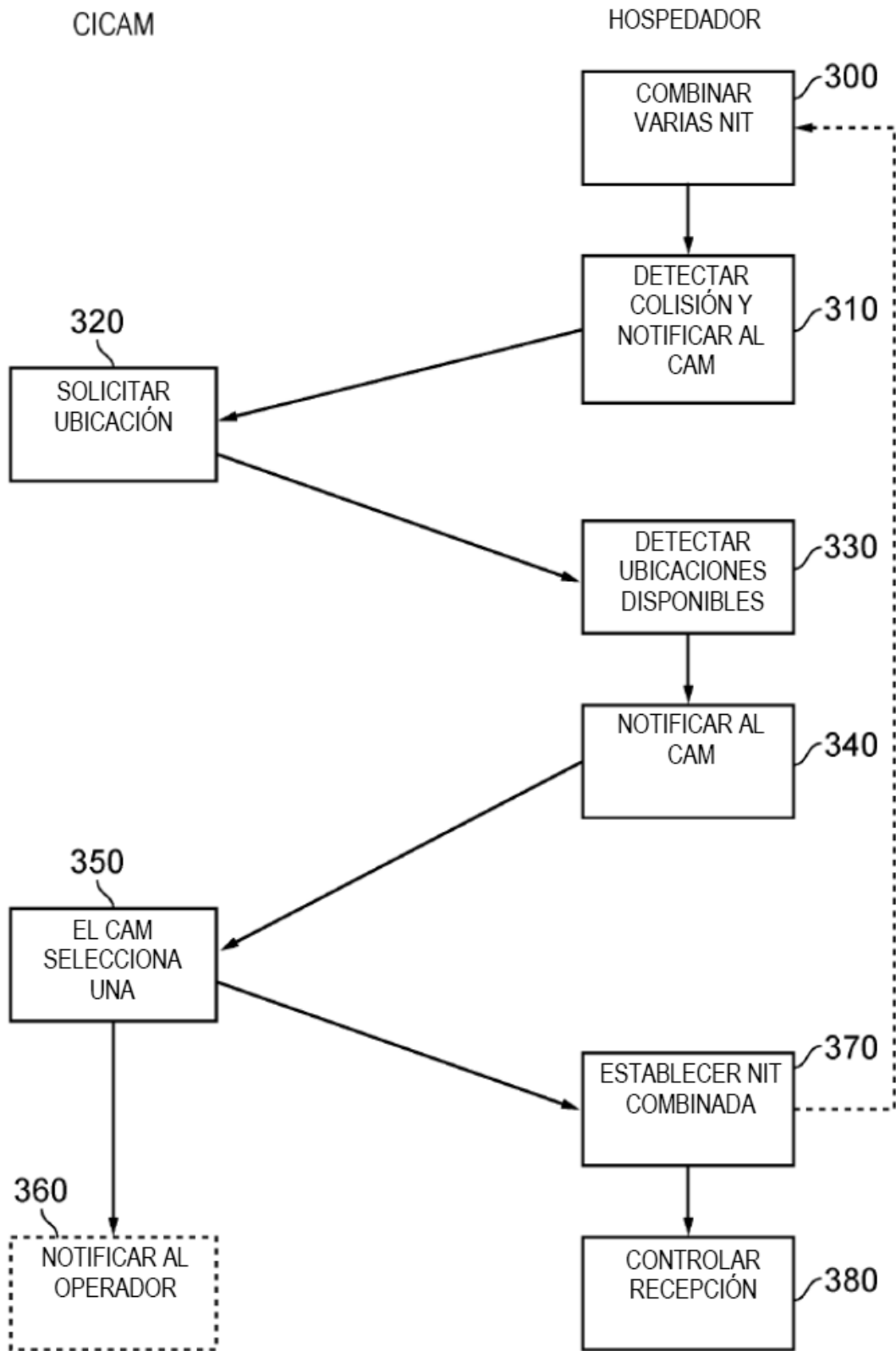


FIG. 7