(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 269 603**

(51) Int. Cl.:
H04N 7/167 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **02080137 .9**
(86) Fecha de presentación : **04.12.2002**
(87) Número de publicación de la solicitud: **1427210**
(87) Fecha de publicación de la solicitud: **09.06.2004**

(54) Título: **Terminal, sistema de distribución de datos que comprende dicho terminal y método de retransmisión de datos digitales.**

(45) Fecha de publicación de la mención BOPI:
01.04.2007

(45) Fecha de la publicación del folleto de la patente:
01.04.2007

(73) Titular/es: **Irdeto Access B.V.**
Jupiterstraat 42
2132 HD Hoofddorp, NL

(72) Inventor/es: **Ranjan, Karthik**

(74) Agente: **Durán Moya, Carlos**

DESCRIPCIÓN

Terminal, sistema de distribución de datos que comprende dicho terminal y método de retransmisión de datos digitales.

Antecedentes de la invención

La invención se refiere al área de transcontrol en límites de red.

En particular, la invención se refiere a un terminal para recibir y retransmitir información, que comprende un primer adaptador de red para recibir un flujo de datos principal en el que la información ha sido codificada, encriptada según un sistema de claves, desde un transmisor principal a través de una primera red en un primer formato,

una disposición para recibir mensajes de autorización, permitir a un receptor autorizado desencriptar la información del flujo de datos encriptados y, por lo menos, un adaptador de red adicional para conectar a una red secundaria, en la que el terminal está configurado para retransmitir por lo menos parte de la información por lo menos en un flujo de datos secundario en un segundo formato, difiriendo del primer formato, a través de la segunda red por lo menos a un terminal secundario conectado a la red secundaria.

La invención se refiere además a un sistema de distribución de datos digitales, que comprende una red principal, un transmisor de datos principal, conectado a la red principal y dispuesto para transmitir información codificada en un flujo de datos encriptado principal, encriptado según un sistema de claves a través de la red principal en un primer formato, un transmisor de mensajes de autorización, dispuesto para transmitir mensajes de autorización que permiten a un receptor autorizado desencriptar la información en el flujo de datos encriptado,

una red secundaria,

uno o más terminales secundarios, conectados a la red secundaria, y

una terminal principal, conectado a la primera y segunda redes, dispuesto para recibir el flujo de datos encriptados desde el transmisor de datos principal a través de la primera red y para retransmitir por lo menos parte de la información, codificada por lo menos en un flujo de datos secundario en un segundo formato, difiriendo del primer formato, a uno o más terminales secundarios conectados a la red secundaria.

La invención también se refiere a un método de recepción y retransmisión de datos digitales, que comprende:

> recibir información codificada en un flujo de datos encriptado principal, encriptado según un sistema de claves, desde un transmisor principal a través de una red principal en un primer formato, recibir mensajes de autorización, permitir a un receptor autorizado desencriptar la información del flujo de datos encriptado, retransmitir por lo menos parte de la información, codificada por lo menos en un flujo de datos secundario en un segundo formato, difiriendo del primer formato por lo menos a un terminal secundario a través de una red secundaria.

Además, la invención se refiere a un programa de ordenador adecuado para cargar en un terminal para recibir y retransmitir datos digitales, que comprende:

un procesador, memoria, un primer adaptador de red para recibir un flujo de datos desde un transmisor principal a través de una primera red en un primer formato, una disposición para recibir mensajes de autorización, permitir a un receptor autorizado desencriptar un flujo de datos encriptado y, por lo menos, un adaptador de red adicional para la conexión a una red secundaria.

El documento US-A1-2002/0094084 da a conocer un sistema de distribución que proporciona un mecanismo por medio del cual los datos, tales como datos digitales de vídeo, comprimidos desde un proveedor de servicios (SP), se transmiten mediante una red de transmisión de banda ancha para presentar en la unidad de decodificación del cliente (STU). Los paquetes de transporte de los sistemas MPEG-2 deben ser transmitidos a través de una red digital a un Nodo de Acceso de Red (NAN) y posteriormente a la STU del cliente. El aparato al que se hace referencia como Acceso a Servicios y Mapeador Encriptador de Banda Ancha (SABER) y el Administrador de Acceso Condicional (CAM) se disponen entre el SP y la red digital. El SABER recibe los paquetes de transporte MPEG-2 a partir del SP a través de un enlace de datos, encapsulado en el protocolo de red de ese enlace. El SABER extrae los paquetes de transporte MPEG-2, añade el acceso condicional y posteriormente vuelve a encapsular los paquetes en un segundo protocolo. El SABER está compuesto, entre otros, de una o dos tarjetas de entrada. Los programas no encriptados se reciben desde un SP a través de las tarjetas de entrada.

El documento EP-A-1 089 470 da a conocer una caja decodificadora que está conectada a un receptor de televisión a través de un cable de vídeo y un cable IEEE 1394. Un circuito frontal extrae una señal de radiodifusión correspondiente a la selección de estación de un usuario desde una entrada DSS (sistema de satélite directo) desde una antena y la emite a un circuito de descifrado. Un circuito de carga suministra al circuito de descifrado la clave de decodificación utilizada para producir una salida de descifrado. Un circuito de edición múltiplex vuelve a disponer las marcas de tiempo y la longitud del paquete de una señal de radiodifusión HD (que está codificado en MPEG) a partir del circuito de descifrado en la estructura de un flujo de transporte definida en el documento IEEE 1394 y posteriormente la emite a un circuito de encriptación. Cuando la señal de radiodifusión de interés es de pago por visión, el circuito de encriptación encripta el flujo de transporte a partir del circuito de edición múltiplex. Un controlador controla una unidad de accionamiento que lee un programa de control grabado en un disco magnético, un disco óptico, un disco magneto-ótpico o una memoria de semiconductores, y controla cada circuito de la caja decodificadora en base al programa de control leído de esta manera y a una entrada de mando por parte del un usuario o similar. El circuito de carga no está conectado al circuito de encriptación.

Cuando se utiliza el terminal conocido, la entidad que transmite los datos desde el transmisor principal pierde control en el momento en que los datos se desencriptan en el terminal principal. Posteriormente, aunque los datos encriptados se vuelven a encriptar, esta entidad ya no controla el acceso a los datos. El operador del terminal principal que se utiliza para recibir y retransmitir los datos a través de la red secundaria puede determinar a qué receptor secunda-

rio permitirá desencriptar y volver a encriptar el flujo de datos, enviándoles la clave utilizada para volver a encriptar el flujo de datos.

Características de la invención

La invención proporciona un terminal, sistema y método de los tipos mencionados anteriormente, que permiten a un proveedor principal de datos digitales conservar el control sobre la posterior distribución de los datos a través de las redes secundarias.

La invención consigue este objetivo proporcionando un terminal para recibir y retransmitir información, que comprende un primer adaptador de red para recibir un flujo de datos principal en el que la información se ha codificado, encriptado según un sistema de claves a partir de un transmisor principal a través de una primera red en un primer formato,

una disposición para recibir mensajes de autorización, permitiendo a un receptor autorizado desencriptar el flujo de datos encriptado, y

por lo menos un adaptador de red adicional para conectar a una red secundaria, en el que el terminal está configurado para retransmitir por lo menos parte de la información por lo menos en un flujo de datos secundario en un segundo formato, difiriendo del primer formato, a través de la segunda red por lo menos a un terminal secundario conectado a la red secundaria, en el que el terminal está configurado para transmitir el flujo o flujos de datos secundarios encriptados según el mismo sistema de claves y para reenviar los mensajes de autorización que permiten a un receptor autorizado desencriptar el flujo o flujos de datos secundarios al terminal o terminales secundarios.

Debido a que los mensajes de autorización reenviados (es decir, generados por la fuente que proporciona la información al terminal) se utilizan para permitir que los receptores secundarios desencripten el flujo de datos retransmitido, el proveedor de datos principal conserva el control sobre la distribución adicional de los datos.

Preferentemente, el terminal está dispuesto para desencriptar el flujo de datos principal recibido y para encriptar el flujo o flujos de datos secundarios según el sistema de claves.

Así pues, el terminal puede acceder a los datos comprendidos en el flujo de datos recibido, por ejemplo, ciertos flujos elementales en un flujo multiplexado. De esta manera, puede acceder a la información, por ejemplo, tablas de identificadores que identifican flujos elementales, de la que puede valerse para decidir qué partes del flujo de datos recibido reenviar.

Según un aspecto adicional de la invención, se da a conocer un sistema de distribución de datos digitales, que comprende una red principal, un transmisor de datos principal, conectado a la red principal y dispuesto para transmitir información codificada en un flujo de datos encriptado principal, encriptado según un sistema de claves a través de la red principal en un primer formato,

un transmisor de mensajes de autorización, dispuesto para transmitir mensajes de autorización que permiten a un receptor autorizado desencriptar el flujo de datos encriptado,

una red secundaria,

uno o más terminales secundarios, conectados a la red secundaria, y

un terminal principal, conectado a la primera y segunda redes, dispuesto para recibir el flujo de datos encriptados desde el transmisor de datos principal a través de la primera red y para retransmitir por lo menos parte de la información, codificada por lo menos en un flujo de datos secundario en un segundo formato, difiriendo del primer formato, a uno o más terminales secundarios conectados a la red secundaria, en el que el terminal principal está configurado para transmitir el flujo o flujo de datos secundarios encriptados según el mismo sistema de claves y para reenviar los mensajes de autorización recibidos que permiten a un receptor autorizado desencriptar el flujo o flujos de datos secundarios al terminal o terminales secundarios.

El sistema permite que la entidad utilice el transmisor de datos principal para mantener el control de los datos que se están retransmitiendo al terminal o terminales secundarios.

Según otro aspecto de la invención, se da a conocer un método de recepción y retransmisión de datos digitales, que comprende:

recibir la información codificada en un flujo de datos encriptado principal, encriptado según un sistema de claves a partir de un transmisor principal a través de una red principal en un primer formato,

recibir mensajes de autorización, permitiendo a un receptor autorizado desencriptar el flujo de datos encriptado,

retransmitir por lo menos parte de la información, codificada por lo menos en un flujo de datos secundario en un segundo formato, difiriendo del primer formato, a por lo menos un terminal secundario a través de una red secundaria, en la que el flujo o flujos de datos secundarios se transmiten encriptados según el mismo sistema de claves, y los mensajes de autorización recibidos, que permiten a un receptor autorizado desencriptar el flujo o flujos de datos secundarios, se reenvían al terminal o terminales secundarios.

Éste es el método llevado a cabo por el terminal según la invención.

Según un último aspecto de la invención, se da a conocer un programa de ordenador, adecuado para cargar en un terminal para recibir y retransmitir datos digitales, que comprende:

un procesador, memoria, un primer adaptador de red para recibir un flujo de datos de un transmisor principal a través de una primera red en un primer formato, una disposición para recibir mensajes de autorización, permitiendo a un receptor autorizado desencriptar un flujo de datos encriptado, y por lo menos un adaptador de red adicional para la conexión a una red secundaria, de manera que el terminal programado de esta manera se dispone con la funcionalidad de un terminal según la invención.

Así pues, un terminal con el hardware adecuado se adapta fácilmente para funcionar como un terminal según la invención, proporcionando a los proveedores de contenido con mayor certeza de que controlan la distribución del contenido hasta el usuario final.

La invención se explicará a continuación en más detalle con referencia a los dibujos adjuntos.

Breve descripción de los dibujos

La figura 1 da una visión general esquemática de

una arquitectura de emisión digital, en la que se utiliza la invención.

La figura 2 es un diagrama esquemático que muestra la composición de paquetes de flujo de transporte.

La figura 3 es un diagrama esquemático que muestra algunos componentes de un terminal según la invención.

La figura 4 es un diagrama esquemático que muestra la composición de un paquete de datos generado por un terminal según la invención.

Descripción específica

Haciendo referencia a la figura 1, la invención da a conocer un receptor principal (1), que se utiliza como puerta de acceso entre dos redes, específicamente una red de distribución y una red doméstica (2), en este ejemplo. El receptor principal (1) recibe los datos en un primer formato, y los retransmite en un segundo formato. Aunque la invención no está limitada a un único tipo de datos, esta descripción se centrará en un ejemplo en el que los paquetes de flujo de transporte MPEG-2 se emiten al receptor principal (1), que los retransmite a una serie de receptores secundarios a través de la red doméstica (2). Entre los ejemplos de receptores secundarios, mostrados en la figura 1, se incluye una caja decodificadora (3), conectada a un aparato de televisión analógico (4), a un aparato de televisión digital (5) y a un ordenador personal (6), equipado con una tarjeta de red, un lector de "media player" y tarjetas inteligentes (7). La invención no está limitada a su utilización en un entorno de emisión; el receptor principal (1) puede recibir también los datos digitales a partir de una fuente mediante una conexión punto a punto.

La norma de MPEG-2 ISO/IEC 13818 describe el método de codificación y transporte de datos en cierto detalle. Esta descripción se referirá principalmente a aquellos aspectos que son relevantes para la invención. Se debe hacer referencia a la norma para más detalles.

En la figura 1, una fuente de emisión (8) codifica un flujo elemental (9) en un único flujo de transporte de MPEG-2 de programa (10). Un flujo elemental es un único componente de un programa, codificado digitalmente o posiblemente comprimido en MPEG, por ejemplo, vídeo o audio. Los datos de diferentes flujos elementales pertenecientes a un programa se transportan en los paquetes de flujo elemental de programa (PES) (11) (ver la figura 2). Un programa corresponde a un canal en la emisión analógica. El paquete PES (11) comprende una cabecera de paquete PES (12) y una carga útil de paquete PES (13). Los datos de los flujos elementales se multiplexan en los paquetes PES (11), con la cabecera de paquete PES (12) indicando a qué flujo elemental corresponde la carga útil de paquete PES (13).

Los paquetes PES (11) se transportan en paquetes de flujo de transporte MPEG (TS) (4) (figura 2). Un multiplexor MPEG (15) (figura 1) multiplexa flujos de transporte múltiples en un flujo de transporte multiprograma, de manera que se transportan múltiples programas en un flujo. Cada paquete TS (14) (figura 2) comprende una cabecera de paquete TS (16) y una carga útil de paquete TS (17). Además, un campo de adaptación (18) asegura que todos los paquetes TS (14) son de la misma longitud, independientemente de la longitud del paquete PES (11) que están transportando. La cabecera de paquete TS (16) comprende, entre otros, un identificador de paquete (PID) (19). El identificador de paquete (19) es un valor entero único utilizado para asociar flujos elementales de un programa en un flujo de transporte de un único o múltiples programas.

Una tabla de asociación de programas (PAT) en los paquetes TS (14) con un valor PID de 0 comprende una lista de todos los programas disponibles en el flujo de transporte. Cada programa en la PAT está asociado a una tabla de mapas de programa (PMT), que ofrece detalles sobre el programa y los flujos elementales de los que está compuesto.

Haciendo referencia de nuevo a la figura 1, un adaptador de red (20) convierte los paquetes TS (14) en un formato adecuado para la transmisión a través de una red principal (21), a un centro regional (22). El centro regional recibe el flujo de transporte a través de un adaptador de red (23). Un empalmador/multiplexor de flujo de bits (24) se utiliza para unir a otros flujos de transporte, que pueden incluir información de servicios (SI), una guía de programas electrónica (EPG) y teletexto. El empalmador/multiplexor de flujo de bits (24) actualiza los valores de PID y la PMT y PAT, para evitar valores de conflicto. El flujo de transporte MPEG resultante se enlaza posteriormente a un transmisor satélite (25), un transmisor terrestre (26) o un transmisor por cable (27), a través de la red principal (21), utilizando adaptadores de red (28) y (29) adecuados.

La red satélite, terrestre o por cable forma una red de distribución, para distribuir los datos a los hogares de los receptores. Otros tipos adecuados de red son aquellos que utilizan fibra en las conexiones de los hogares, ADSL (línea de abonado digital asíncrona), conexiones ethernet, etc. En el contexto de la presente invención, la red de distribución será referida como la primera red.

Tanto la fuente de emisión (8) como el centro regional (22), o ambos, pueden utilizar un sistema acceso condicional para evitar acceso no autorizado a los contenidos del flujo de datos que están enlazados. Para este propósito, se cifran o bien las cargas útiles de paquete PES (13) o bien las cargas útiles de paquete TS (17) se cifran. Obsérvese que, en un flujo de transporte multiplexado, que, de hecho, comprende flujos de transporte múltiple, transportando cada uno un flujo elemental, únicamente un subconjunto de los flujos de transporte puede ser cifrado. Un campo en la cabecera del paquete PES (12) o la cabecera del paquete TS (16) indica si la carga útil de ese paquete particular está encriptada o no. Para evitar complicar la descripción, se supondrá que el cifrado se lleva a cabo en el nivel de flujo de transporte. Preferentemente, se utiliza un algoritmo de encriptación simétrica, tal como DES, para cifrar las cargas útiles de los paquetes TS (17).

Se observa que es posible cifrar todas las cargas útiles de los paquetes TS (17) con la misma clave y/o algoritmo, independientemente del valor PID, o utilizar una clave y/o algoritmo diferente para cada flujo elemental o para cada conjunto de flujos elementales pertenecientes a un programa. Suponiendo que el centro regional (22) es el administrador de sistema CA, unirá uno o más flujos de transporte que contienen mensajes de control de autorización. Modificará adicionalmente la PMT para el programa cifrado, añadiéndolo a un descriptor CA, detallando el tipo de sistema CA que está siendo utilizado y el PID de los mensajes de autorización. Los mensajes de con-

trol de autorización comprenden la palabra de control, la clave utilizada para cifrar y descifrar. Los mensajes de control de autorización (ECMs) se encriptan ellos mismos, con una clave diferente. Un flujo de datos adicional comprende mensajes de administración de autorización (EMMs), éstos permiten a los abonados o grupos de abonados autorizados desencriptar los ECMs, a partir de los que pueden recuperar la palabra de control.

Haciendo referencia nuevamente a la figura 1, el receptor principal (1) recibe el flujo de transporte MPEG(2 mediante una parabólica (30), a la que está conectada. El flujo de transporte se encuentra en un formato adecuado para la transmisión a través de la red de distribución satélite, por ejemplo, en conformidad al DVB)S (Satélite de emisión de vídeo digital). El receptor principal (1) pone en disposición parte o todos los datos para los dispositivos finales a través de la red doméstica (2), a través de la cual los datos se transmiten en un formato diferente. El receptor principal (1) es, de esta manera, una puerta de acceso de la red de distribución: un dispositivo que está conectado a una o más redes de distribución y uno o más segmentos de red doméstica. Incluye uno o más componentes de conexión de manera que se puede interconectar la red de distribución (es decir, la red satélite) con los segmentos de red doméstica en cualquiera de las capas OSI. Puede funcionar como un puente o router, interconectando tecnologías de capas de enlace diferentes, o puede actuar como una puerta de acceso, proporcionando también funcionalidad en la capa OSI (4) y por encima de la misma. En consecuencia, el término formato representa la manera en la que los datos se adaptan para ajustarse a la pila del protocolo de un cierto tipo de red. Una primera red (la red satélite) tiene una pila del protocolo diferente de la red doméstica (2), significando que difiere en uno o más de los niveles de capa de enlace, el nivel de capa de red o el nivel de capa de transporte. Observe que esto significa que el receptor principal (1) debe, cuando los datos se transmiten en tramas y/o paquetes, añadir, extraer o modificar las cabeceras de paquete, y/o volver a segmentar las cargas útiles de paquete para ajustarlas a la pila del protocolo de la red doméstica (2). El término paquete se refiere a una sección corta de datos que se transmiten como una unidad en una red de comunicaciones. Comprende paquetes en niveles por debajo de la capa de red, que son conocidos comúnmente como tramas, así como los tipos de paquetes conocidos como celdas. Un paquete comprende una cabecera o preámbulo y una carga útil. El formato de paquete se refiere a la composición del paquete en términos del tamaño de la carga útil, y en términos de los diversos campos que se encuentran presentes en la cabecera/preámbulo.

La figura 3 muestra esquemáticamente los componentes del receptor principal (1). Comprende un sintonizador/demodulador (31), que extrae la onda portadora para recuperar la señal de banda base que comprende el flujo de transporte MPEG. El receptor principal (1) utiliza un procesador (32) y una memoria (33) para procesar los paquetes. El procesador (32) está conectado a un bus de sistema (34). En este ejemplo, un lector de tarjetas inteligentes (35), un módem (36) y una tarjeta ethernet (37) se conectan al bus de sistema (34). El módem (36) y la tarjeta ethernet (37) funcionan como adaptadores de red, es decir, en combinación con un software adecuado ejecutándose en el procesador, implementan un interfaz de enlace, permitiendo el intercambio de datos sobre una red según el protocolo correcto para esa red. Una tarjeta inteligente (38) se inserta en el lector de tarjetas inteligentes (35) para proporcionar autorización para recibir uno o más programas. Como alternativa a la tarjeta inteligente (38), se puede utilizar otro tipo de dispositivo de seguridad portátil, por ejemplo, una llave USB o una tarjeta de formato PCMCIA. También es concebible un módulo de seguridad implementado en software para proporcionar autorización. En este ejemplo, la red doméstica (2) es una ethernet, es decir, la caja decodificadora (3), el aparato de televisión digital (5) y el ordenador personal (6) también comprenden tarjetas ethernet. Se debe subrayar, no obstante, que se puede utilizar cualquier otro tipo de red doméstica, por ejemplo, una que utilice conexiones USB, IEEE 1394, IEEE 802.11, etc.

Según la invención, el receptor principal (1) recibe el flujo de transporte en formato DVB(S. Entonces, utilizando los PIDs en la PAT y PMT, determina qué flujos elementales comprenden los EMMs y ECMs, y cuáles comprenden los flujos elementales que comprenden los datos de contenido, los datos EPG, posiblemente datos IP, etc. Algunos o todos los flujos de transporte que comprenden los últimos se descifran, en lo que respecta a que la tarjeta inteligente (38) comprende información autorizando al receptor principal (1) a recuperar las palabras de control adecuadas. Para este propósito, la tarjeta inteligente (38) procesa los ECMs para devolver la palabra de control al procesador (32), que lleva a cabo el descifrado.

Entonces, los flujos de datos desencriptados se vuelven a paquetizar. Esto significa que se dividen en cargas útiles de longitud adecuada, y que se añaden las cabeceras necesarias, definidas en los protocolos utilizados en la red doméstica (2). Entonces, estos paquetes se vuelven a encriptar. Las mismas palabras de control se utilizan para volver a encriptar los paquetes en el formato de paquete de datos de la red doméstica (2). Debido a que se utiliza el mismo sistema de claves, los datos en los flujos de transporte que comprenden los mensajes de autorización simplemente se reenvían. No se forman nuevos mensajes de autorización.

Se observa que el receptor principal (1) no difiere sustancialmente de los receptores secundarios, porque no pueden desencriptar los datos de contenido o descifrar los datos de contenido sin la tarjeta inteligente (38). Tampoco es capaz de formar sus propios mensajes de autorización. Esto tiene la doble ventaja de que el receptor principal (1) es relativamente simple y de que el centro regional se asegura de que su sistema CA permanece en funcionamiento para proteger los datos de contenido ante acceso no autorizado.

El receptor principal (1) vuelve a paquetizar los paquetes TS (14) en el formato para la red doméstica (2). En este ejemplo, la pila del protocolo de la red doméstica utiliza ethernet en el nivel de la capa de enlace, IP al nivel de la capa de red y UDP en el nivel de la capa de transporte. La figura 4 muestra la composición de los paquetes transmitidos a través de la red doméstica (2). Diversos paquetes TS (14), por ejemplo, unos siete, forman la carga útil de un paquete IP (39) (también conocido como un datagrama IP). El paquete IP (39) comprende además una cabecera UDP (40) y una cabecera IP (41). La cabecera IP (41) comprende la dirección IP del receptor secundario para el que

está destinado el paquete IP (39), o puede comprender una dirección múltiple. El paquete IP (39) forma la carga útil de una trama ethernet (42), que comprende un preámbulo (43), una dirección de destino (44), una dirección de fuente (45), un tipo (46) y una suma de control CRC (47). La dirección de destino (44) es una dirección de emisión, múltiple o única, utilizada por los receptores secundarios para recuperar las tramas ethernet destinadas a ellos. Se observa que habría sido posible también encapsular directamente los paquetes TS (14) en la trama ethernet (42), sin añadir cabeceras IP y UDP (41), (40). Utilizando IP sobre ethernet, sin embargo, resulta posible transmitir los datos en un rango más amplio.

Preferentemente, el receptor principal (1) utiliza una forma de encriptado bajo la pila, tal como se describe en más detalle en la solicitud internacional codependiente del solicitante WO 02/07378.

En una realización preferente de la invención, los receptores secundarios son capaces de enviar las instrucciones de selección al receptor principal (1) a través de la red doméstica (2). En respuesta a estas instrucciones de selección, el receptor principal (1) filtra estos flujos elementales en el flujo de transporte multiprograma que no han sido solicitados por ninguno de los receptores secundarios. Así pues, es capaz de transmitir únicamente un subconjunto de flujos de datos elementales a cada uno de los receptores secundarios.

Cada uno de los receptores secundarios comprende también un lector de tarjeta inteligente. Una tarjeta inteligente insertada les permite recuperar los ECMs a partir del flujo de datos recibido del receptor principal (1), y descifrar ciertos flujos elementales.

El receptor principal (1) puede recuperar también los paquetes TS utilizando el módem (36). En este caso, los paquetes TS ya pueden estar encapsulados en paquetes IP. No obstante, en lugar de ser encapsulado en paquetes ethernet, los paquetes IP recibidos se transportan típicamente en paquetes PPP o celdas ATM en el nivel de capa de enlace. El receptor principal (1) debe llevar a cabo, por lo tanto, el método según la invención para retransmitir los datos recibidos en formato de trama ethernet.

Tal como se ha descrito anteriormente, el receptor principal (1) vuelve a paquetizar los flujos de datos desencriptados. Dentro del alcance de la invención, es posible una variante adicional del receptor principal (1). En esta variante, el receptor principal (1) está dispuesto para recibir un flujo de datos principal que comprende información codificada en un primer formato, para volver a codificar la información en un segundo formato, y para incluir datos comprendiendo la información recodificada en por lo menos uno de los flujos de datos secundarios. Esta llamada transcodificación puede suponer la descompresión y recompresión de los datos recibidos. Como ejemplo, el receptor principal (1) puede demultiplexar un flujo de transporte para recuperar un flujo elemental de programa codificado y comprimido según la norma MPEG-4, descomprimir los datos de vídeo codificados y volver a comprimir y codificar los datos de vídeo según la norma MPEG-2. Los datos de vídeo transcodificados se multiplexan posteriormente con los otros flujos elementales de programa asociados que contienen audio y datos en un flujo de transporte que se paquetiza y transmite a uno o más receptores secundarios. Por supuesto, la transcodificación desde MPEG-4 a MPEG-2 es sólo un ejemplo ventajoso. Cuando los datos están siendo retransmitidos, el receptor principal (1) también puede estar dispuesto para transcodificar imágenes fijas, por ejemplo, de JPEG a GIF. Estas realizaciones tienen el efecto ventajoso de que es posible continuar utilizando los receptores de legado como receptores secundarios, si un emisor ha cambiado a un formato diferente no soportado por los receptores secundarios. Entonces únicamente es necesario invertir en el receptor principal (1). Otro efecto, especialmente de la recompresión, es que se deben considerar los diferentes anchos de banda disponibles en la red doméstica (2) y la red de distribución.

Preferentemente, al proveedor del flujo de datos principal se le da un instrumento adicional para controlar la distribución secundaria de información. Una manera de hacer esto es proporcionar una serie de mensajes de autorización diferentes, permitiendo cada uno que un receptor autorizado desencripte un flujo de datos, encriptado según el sistema de claves, en el que cada mensaje de autorización comprende una especificación por lo menos de un terminal. En otras palabras, varios de los ECMs enviados desde la fuente de emisión (8) al receptor principal (1) pueden contener la misma palabra de control, pero una especificación diferente de un receptor (tanto el tipo como una identificación de uno o más dispositivos específicos). El receptor principal recupera los mismos ECMs de especificación, a efectos de desencriptar el flujo de datos recibido. Se reenvían a cada receptor secundario únicamente aquellos ECMs que comprenden una especificación a la que ajusta el receptor secundario.

Un instrumento adicional para controlar la distribución comprende transmitir mensajes autorizando la transmisión por lo menos de uno de los flujos de datos secundarios por lo menos a uno de los terminales secundarios. El mensaje puede ser un simple mensaje especificando únicamente si se permite la redistribución, o si se puede limitar la redistribución a ciertos tipos de receptores secundarios o a cierto número máximo de receptores secundarios. El receptor principal (1) está dispuesto para transmitir únicamente aquellos flujos de datos secundarios a aquellos terminales secundarios para los que se ha recibido autorización. En combinación con ECMs específicos del dispositivo, el receptor principal (1) puede, por ejemplo, filtrar ciertos ECMs, para limitar el número de receptores secundarios que pueden acceder a los datos simultáneamente.

La invención no está limitada a las realizaciones descritas, pero puede variar en una serie de maneras dentro del alcance de las reivindicaciones adjuntas. Por ejemplo, los datos cifrados pueden comprender paquetes IP. En este caso, el receptor principal (1) puede extraer la encapsulación en paquetes TS antes de retransmitir los datos.

REIVINDICACIONES

1. Terminal para recibir y retransmitir información, comprendiendo un primer adaptador de red (31, 36) para recibir un flujo de datos principal en el que la información ha sido codificada, encriptada según un sistema de claves a partir de un transmisor principal (25, 26, 27) a través de una primera red en un primer formato,

una disposición para recibir mensajes de autorización, permitiendo que un receptor autorizado desencripte la información del flujo de datos encriptado, y por lo menos un adaptador de red (37) adicional para conectar a una red secundaria (2), en la que el terminal está configurado para retransmitir por lo menos parte de la información por lo menos en un flujo de datos secundario en un segundo formato, difiriendo del primero, a través de la red secundaria (2) por lo menos a un terminal secundario (3, 5, 6) conectado a la red secundaria (2), **caracterizado** porque el terminal está configurado para transmitir el flujo o flujos de datos secundarios encriptados según el mismo sistema de claves, y para reenviar los mensajes de autorización recibidos que permiten a un receptor autorizado desencriptar el flujo o flujos de datos secundarios en el segundo terminal o terminales (3, 5, 6).

2. Terminal, según la reivindicación 1, en el que el terminal está dispuesto para desencriptar el flujo de datos principal recibido y desencriptar el flujo o flujos de datos secundarios según el sistema de claves.

3. Terminal, según la reivindicación 2, en el que el terminal está dispuesto para demultiplexar un flujo de datos encriptado que comprende múltiples flujos de datos elementales, y para retransmitir la información codificada en un subconjunto de los flujos de datos elementales.

4. Terminal, según la reivindicación 3, en el que el terminal está dispuesto para recibir instrucciones de selección desde los terminales secundarios (3, 5, 6), y para seleccionar los flujos de datos elementales comprendidos en el subconjunto según las instrucciones de selección.

5. Terminal, según cualquiera de las reivindicaciones 1-4, en el que el terminal está dispuesto para recibir el flujo de datos principal encriptado en un primer formato de paquete de datos, y para transmitir por lo menos uno de los flujos secundarios en un segundo formato de paquete de datos.

6. terminal, según cualquiera de las reivindicaciones 1-4 y 5, en el que el terminal está dispuesto para desencriptar la carga útil (13, 17) de un paquete de datos encriptado (14, 39, 42) recibido en el primer formato de paquete de datos, para formar datos sin encriptar a partir de la carga útil encriptada, y para volver a paquetizar, en consecuencia, los datos sin encriptar conforme al segundo formato de paquetes de datos.

7. Terminal, según la reivindicación 2 o reivindicación 2 y reivindicación 5 ó 6, en el que el terminal está dispuesto para demultiplexar un flujo de datos encriptado que comprende múltiples flujos de datos elementales encriptados, y para retransmitir un subconjunto de los flujos de datos elementales.

8. Terminal, según cualquiera de las reivindicaciones 1-7, en el que el terminal está dispuesto para incluir una o más direcciones (44), identificando uno o más terminales secundarios (3, 5, 6), en el flujo o flujos de datos secundarios transmitidos.

9. Terminal, según cualquiera de las reivindicaciones 1-8, en el que el terminal está dispuesto para recibir un flujo de datos principal que comprende información codificada en un primer formato, para volver a codificar la información en un segundo formato, y para incluir datos que comprenden la información recodificada por lo menos en uno de los flujos de datos secundarios.

10. Terminal, según la reivindicación 9, en el que el terminal está dispuesto para recibir un flujo de datos principal comprendiendo datos comprimidos según un primer sistema, para descomprimir los datos, para volver a comprimir los datos según un segundo sistema, y para incluir los datos recomprimidos por lo menos en uno de los flujos de datos secundarios.

11. Terminal, según cualquiera de las reivindicaciones 1-10, dispuesto para recibir mensajes que autorizan la transmisión por lo menos de uno de los flujos de datos secundarios por lo menos a uno de los terminales secundarios (3, 5, 6), cuyo terminal está dispuesto para transmitir únicamente aquellos flujos de datos secundarios a aquellos terminales secundarios (3, 5, 6) para los que se ha recibido una autorización.

12. Terminal, según cualquiera de las reivindicaciones 1-11, que comprende una disposición para recibir una serie de mensajes de autorización diferentes, permitiendo cada uno a un receptor autorizado desencriptar un flujo de datos según el sistema de claves, en el que cada mensaje de autorización comprende una especificación por lo menos de un terminal, en el que el terminal está dispuesto para reenviar a un terminal secundario (3, 5, 6) únicamente aquellos mensajes de autorización que comprenden una especificación a la que se adapta el terminal (3, 5, 6).

13. Sistema de distribución de datos digitales, que comprende una red principal, un transmisor de datos (25, 26, 27), principal, conectado a la red principal y dispuesto para transmitir información codificada en un flujo de datos principal encriptado, encriptado según un sistema de claves, a través de la red principal en un primer formato,

un transmisor de mensajes de autorización (25, 26, 27), dispuesto para transmitir mensajes de autorización que permiten a un receptor autorizado desencriptar la información en el flujo de datos encriptado,

una red secundaria (2),

uno o más terminales secundarios (3, 5, 6), conectados a la red secundaria (2), y

un terminal principal, según cualquiera de las reivindicaciones 1-12.

14. Método para recibir y retransmitir datos digitales, que comprende:

recibir información codificada en un flujo de datos principal encriptado, encriptado según un sistema de claves, a partir de un transmisor principal (25, 26, 27) a través de una red principal en un primer formato,

recibir mensajes de autorización, permitiendo a un receptor autorizado desencriptar la información en el flujo de datos encriptado, retransmitir por lo menos parte de la información, codificada por lo menos en un flujo de datos secundario en un segundo formato, difiriendo del segundo formato, por lo menos a un terminal secundario (3, 5, 6) a través de una red secundaria

(2), en el que el flujo o flujos de datos secundarios se transmiten encriptados según el mismo sistema de claves y los mensajes de autorización recibidos, que permiten a un receptor autorizado desencriptar el flujo o flujos de datos secundarios, se reenvían al terminal o terminales secundarios (3, 5, 6).

15. Programa de ordenador adecuado para cargar en un terminal (1) para recibir y retransmitir datos digitales, que comprende

un procesador (32), memoria (33), un primer adaptador de red (31, 36) para recibir un flujo de datos desde un transmisor principal (25, 26, 27) a través de una primera red en un primer formato, una disposición para recibir mensajes de autorización, permitiendo a un receptor autorizado desencriptar un flujo de datos encriptados, y por lo menos un adaptador de red (37) adicional para conectar a una red secundaria (2), de manera que el terminal (1) programado de esta manera está dotado con la funcionalidad de un terminal según cualquiera de las reivindicaciones 1-12.

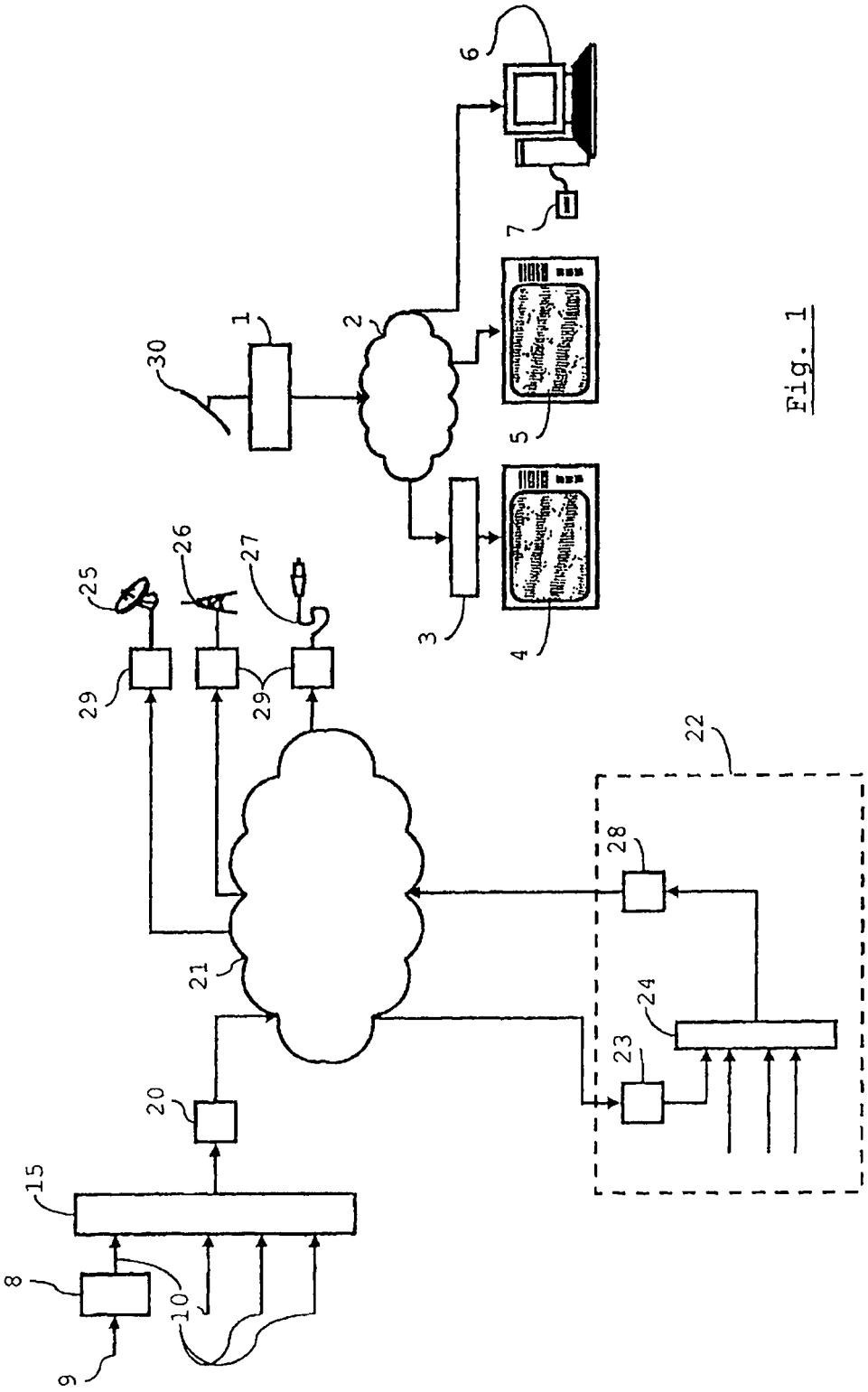

Fig. 1

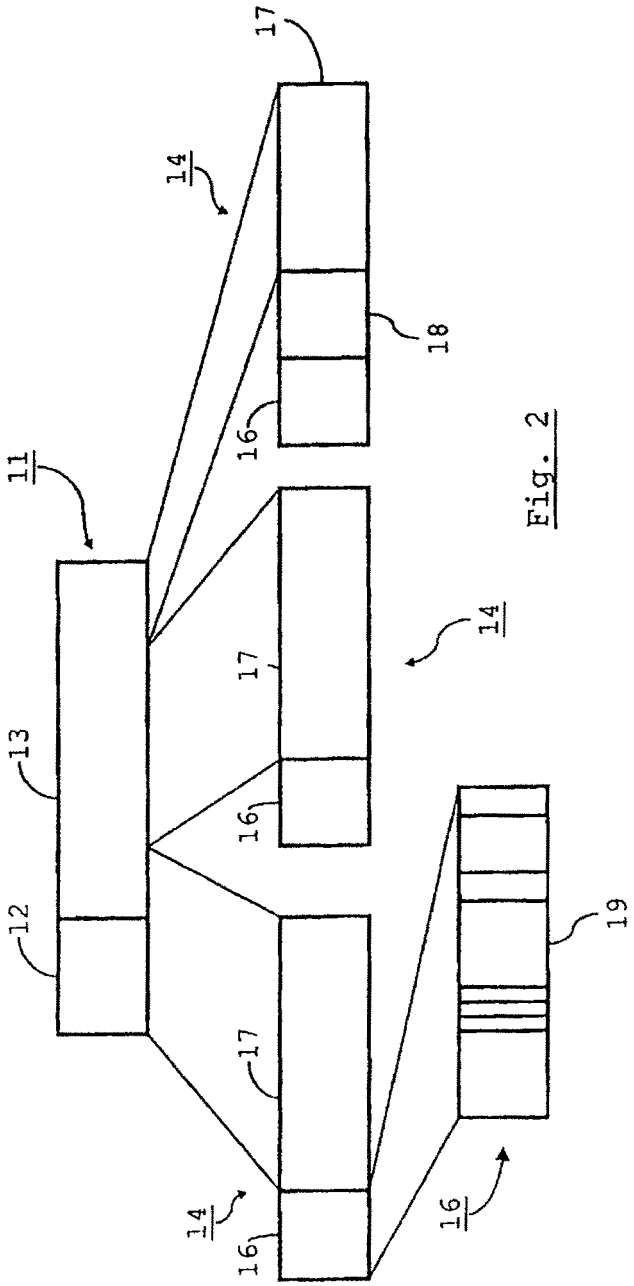

Fig. 2

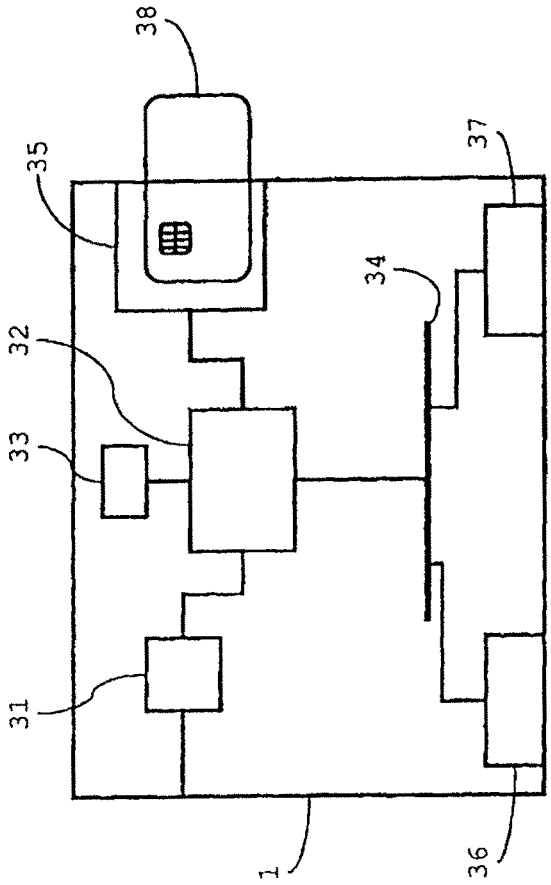

Fig. 3

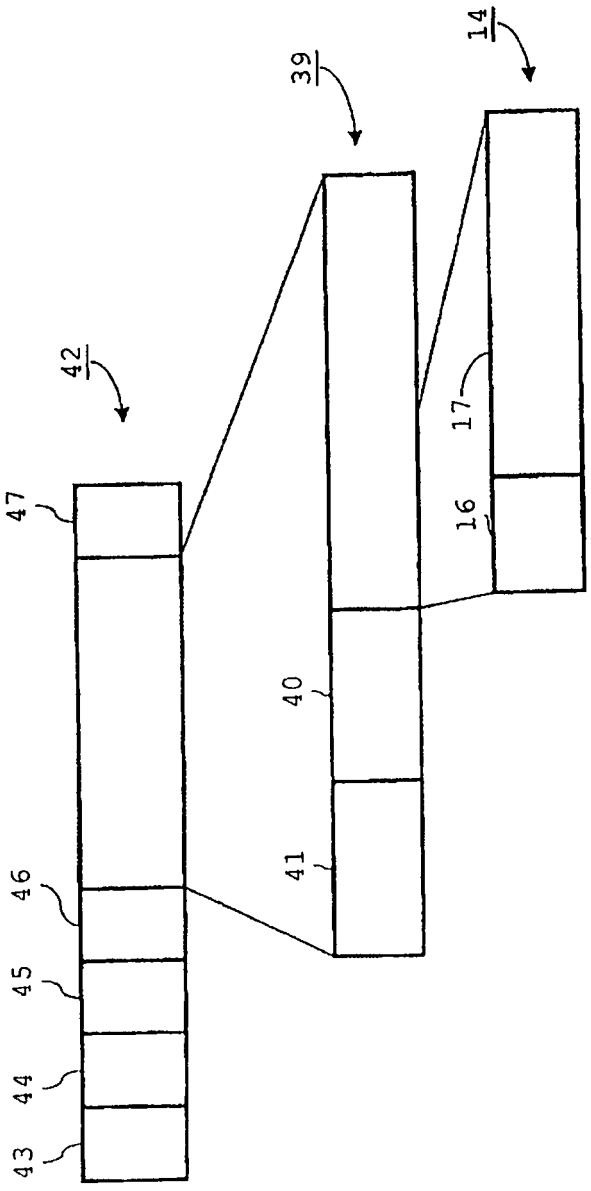

Fig. 4