(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 287 872**

(51) Int. Cl.:
H04L 9/32 (2006.01)
H04N 7/167 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **05110162 .4**
(86) Fecha de presentación : **25.03.1999**
(87) Número de publicación de la solicitud: **1619826**
(87) Fecha de publicación de la solicitud: **25.01.2006**

(54) Título: **Autenticación de datos en un sistema de transmisión digital.**

(30) Prioridad: **25.03.1998 EP 98400686**

(45) Fecha de publicación de la mención BOPI:
16.12.2007

(45) Fecha de la publicación del folleto de la patente:
16.12.2007

(73) Titular/es: **Thomson Licensing**
46, quai Alphonse Le Gallo
92100 Boulogne-Billancourt, FR

(72) Inventor/es: **Beuque, Jean-Bernard**

(74) Agente: **Arpe Fernández, Manuel**

DESCRIPCIÓN

Autenticación de datos en un sistema de transmisión digital.

La presente invención se refiere a un método para autenticar datos enviados en un sistema de transmisión digital.

La transmisión de datos digitales mediante radiodifusión es muy conocida en el ámbito de los sistemas de TV de pago, en los que se envía información audiovisual codificada, normalmente vía satélite o mediante un enlace vía satélite/cable, a diversos abonados y cada uno de los cuales posee un decodificador capaz de decodificar el programa transmitido para verlo posteriormente. También se conocen los sistemas de radiodifusión digital terrestre. Los sistemas más recientes también han utilizado el enlace de radiodifusión para transmitir otro tipo de datos, además de datos audiovisuales, tales como programas informáticos o aplicaciones interactivas, al decodificador o a un PC conectado a este.

Un problema específico de la transmisión de datos de aplicaciones radica en la necesidad de verificar la integridad y el origen de dichos datos. Dado que se pueden utilizar datos de este tipo para reconfigurar el decodificador, así como para ejecutar cualquier número de aplicaciones interactivas, es esencial que los datos recibidos sean completos y se les haya identificado como procedentes de una fuente conocida. De lo contrario, pueden surgir problemas operativos relacionados con la descarga de datos incompletos, además de darse el riesgo de que el decodificador quede abierto a ataques de terceros o similares.

Los intentos anteriores de autentificar dichos datos se han concentrado en la verificación a nivel de encapsulado o formateo de los datos en un flujo de paquetes. Por ejemplo, la solicitud de patente europea EP0752786 describe un sistema, en el cual los datos se encapsulan en una serie de módulos o, utilizando la terminología asociada a la norma MPEG, a una serie de tablas o secciones, encapsulándose entonces las tablas o secciones en paquetes en un flujo de transporte MPEG.

Las operaciones de autenticación se llevan a cabo en relación con los datos tabulados, conteniendo por ejemplo una tabla de directorio, una lista de todas las tablas que contienen datos para dicha aplicación, junto con una lista de los valores flash asociados a cada tabla para permitir la posterior verificación de los datos de la tabla. La propia tabla de directorio puede ir firmada con anterioridad a la transmisión, de forma que la información de la tabla del directorio y de las tablas asociadas no pueda modificarse sin alterar los valores de troceo y de firma.

El problema con estos sistemas conocidos radica en su falta de idoneidad para la gestión de estructuras organizativas con unos datos más complejos. Concretamente, el uso de una sola tabla de directorio que contenga una lista completa de valores de troceo para cada tabla asociada significa que dichos sistemas no pueden adaptarse fácilmente para gestionar un gran número o un número variable de tablas.

El sistema también está deficientemente adaptado para permitir la autenticación del software facilitado por diversos operadores de radiodifusión, debido a que una sola tabla de directorio MPEG enlaza todas las tablas y debido a que las operaciones de autenticación se llevan a cabo durante la fase de formateo de los datos en tablas para el encapsulado y la radiodifusión de paquetes. Esta operación suele llevarse a cabo bajo el control de un solo operador.

De acuerdo con un primer aspecto de la presente invención, se propone un método de autenticación de datos enviados en un sistema de transmisión digital caracterizado por la organización de los datos con anterioridad a la transmisión en una jerarquía con al menos una unidad de directorio raíz, una unidad de subdirectorio y una unidad de archivo, actuándose sobre los datos de un archivo mediante un algoritmo de autenticación y un valor de autenticación del archivo asociado almacenado en el subdirectorio de referencia, actuándose a su vez sobre este valor de autenticación del archivo mediante un algoritmo de autenticación y un valor de autenticación del subdirectorio asociado, almacenado en el directorio raíz de referencia.

A diferencia de los sistemas conocidos, cuando un directorio de una sola tabla hace referencia a todas las tablas asociadas, la utilización de una estructura de jerarquía múltiple junto con la aplicación de un algoritmo de autenticación en cada fase de la jerarquía proporciona una estructura de datos segura y modular. Dado que el valor de autenticación de un archivo en un subdirectorio es autentificado a su vez a un nivel superior mediante un valor correspondiente en el directorio raíz, no es posible cambiar un elemento situado en un nivel inferior sin modificar los valores de autenticación que se encuentran en un nivel superior (y viceversa).

Preferiblemente, la autenticación de los datos del archivo se lleva a cabo aplicando un algoritmo de troceo a una parte o a todos los datos del archivo, almacenándose el valor de troceo resultante como valor de autenticación del archivo en el subdirectorio de referencia. Igualmente, la autenticación de un subdirectorio puede llevarse a cabo aplicando un algoritmo de troceo al valor de autenticación del archivo (y a otros datos si así se desea), almacenándose el valor de troceo resultante como valor de autenticación del subdirectorio en el directorio raíz de referencia.

Pueden preverse otras realizaciones, por ejemplo cuando los datos del archivo se han cifrado de acuerdo con un algoritmo de codificación y la clave de codificación (o su número clave de identificación) utilizada como valor de autenticación se encuentra almacenada en el subdirectorio. Esta clave de archivo puede a su vez cifrarse y la clave de cifrado almacenarse en el directorio raíz como valor de autenticación, etc. Aunque posible, esta realización resulta bastante más complicada de poner en práctica debido a la mayor complejidad de las operaciones necesarias para la generación de los valores de la clave de cifrado.

Por el contrario, la utilización de un algoritmo de troceo para llevar a cabo la autenticación de cada módulo permite llevar a cabo una comprobación especialmente sencilla y rápida de la integridad de cada módulo. En una realización, puede utilizarse un sencillo algoritmo de troceo, tal como un cálculo de la suma de control. No obstante, esto no permitiría detectar una falsificación debido a que resulta relativamente sencillo determinar la forma en que cualquier cambio en un mensaje afecta al valor de troceo.

Preferiblemente, el algoritmo de troceo se corresponde con un algoritmo criptográficamente seguro que genera un valor flash 15 sustancialmente único a partir de un conjunto dado de datos. Entre los al-

goritmos de troceo adecuados que pueden utilizarse con este fin se encuentran por ejemplo el algoritmo Message Digest versión 5 (MD5) o el Algoritmo de Troceo Seguro (SHA).

Ventajosamente, la autenticación de los datos del archivo para una pluralidad de archivos se lleva a cabo mediante la aplicación de un algoritmo de troceo a una acumulación de datos procedentes de una pluralidad de archivos para generar un único valor de troceo. Igualmente, la autenticación de varios subdirectorios puede llevarse a cabo aplicando un algoritmo de troceo a una serie de valores de autenticación de archivo procedentes de diversos subdirectorios (y otros datos, si se desea) para generar un valor de troceo único.

La utilización de un proceso de troceo acumulativo que cubra diversos módulos de datos (archivos, subdirectorios, etc.) en una capa de nivel inferior simplifica aún más el sistema si se compara, por ejemplo, con sistemas que almacenan listas individuales de valores de troceo para cada módulo. Esto permite nuevamente que el sistema reduzca las fases de cálculo necesarias en cada nivel y reduce el tamaño de los datos de autenticación almacenados en un nivel superior.

En el caso de las realizaciones que utilizan un algoritmo de troceo para autentificar cada capa, el sistema estará "abierto", es decir todos los valores de troceo podrán leerse hasta el directorio raíz. Dado que los algoritmos de troceo están disponibles públicamente, en teoría un tercero podría cambiar los datos almacenados, por ejemplo a nivel de archivo, sin detectar sí los valores de troceo correspondientes a nivel de subdirectorio y de directorio raíz se han cambiado también al mismo tiempo.

A fin de evitar esto, se actúa al menos sobre una parte de los datos almacenados en el directorio raíz mediante una clave secreta de un algoritmo de cifrado y el valor cifrado resultante se almacena en el directorio raíz. Preferiblemente, el valor cifrado corresponde a una firma digital. Entre los algoritmos de clave privada/pública adecuados para este propósito puede citarse, por ejemplo, el algoritmo RSA.

Ventajosamente, los datos cifrados mediante la clave secreta para generar una firma almacenada en el directorio raíz incluyen al menos uno o más valores de autenticación del subdirectorio. No obstante, es posible prever en el directorio raíz unos datos diferentes de los valores de autenticación del subdirectorio que se firman a fin de "cerrar" el sistema.

Como alternativa a la generación de una firma, puede simplemente cifrarse o codificarse la totalidad o una parte del directorio raíz cuando el receptor posee una clave equivalente para descifrar los datos cifrados del directorio raíz. En este caso, puede utilizarse un algoritmo de clave simétrica como DES.

Como se comprenderá, aunque el proceso de autenticación se ha descrito anteriormente haciendo referencia a dos niveles jerárquicos, pueden efectuarse fases similares de autenticación hasta el infinito para archivos, subdirectorios, directorios raíz, etc. adicionales de referencia.

Igualmente, aunque la estructura se ha definido como de directorio raíz/subdirectorio/archivo por motivos de claridad, no se asume ninguna característica específica de cada una de las unidades de una capa, salvo que hace referencia a una unidad de nivel inferior mediante dos unidades de nivel superior. Como se comprenderá, la estructura de datos puede ser igualmente directorio raíz/subdirectorio/segundo directorio raíz o cualquier otra combinación.

Las realizaciones que se describen a continuación se centran en una unidad situada en una capa inferior, es decir a la que se hace referencia mediante un directorio o subdirectorio. Como es evidente, aunque se hace referencia a ella desde una capa superior, esta unidad puede ser, no obstante, una unidad de directorio, una unidad de subdirectorio, etc.

En una realización, una unidad a la que se ha hecho referencia incluye un valor cifrado generado mediante una clave secreta, calculándose un valor de autenticación para esta unidad en función de los resultados de la aplicación de un algoritmo de autenticación al valor cifrado que se encuentra almacenado en la unidad a la que se hace referencia. Particularmente, como en la realización equivalente de directorio raíz que se ha descrito anteriormente, una unidad a la que se haga referencia puede ir firmada, calculándose el valor de autenticación correspondiente a dicha unidad como resultado de una función de troceo sobre dicha firma.

La unidad a la que se hace referencia puede corresponder, por ejemplo, a un archivo o subdirectorio. No obstante, esta realización resulta especialmente adecuada a la situación en la cual la unidad a la que se hace referencia es un directorio raíz para un conjunto adicional de datos, por ejemplo datos con un origen diferente y en el que la unidad raíz a la que se hace referencia también incluye una firma. En este caso, un primer operador puede reunir y firmar datos hasta el nivel del directorio raíz.

Posteriormente, un segundo operador puede hacer referencia a estos datos sin conocer la clave de cifrado, limitándose a autentificar cualquier enlace en la unidad de referencia mediante el valor de troceo de la firma que se encuentra en el directorio raíz al que se hace referencia. La autenticación de ambos conjuntos de datos tan sólo le será posible, por supuesto, a un receptor que posea las claves necesarias para verificar las firmas en ambos directorios raíz.

Como se ha descrito anteriormente, la presente invención puede aplicarse a cualquier conjunto de unidades de datos con múltiples jerarquías. Incluso puede aplicarse a la organización de tablas o paquetes en un flujo de transporte, cuando en dicho flujo de paquetes pueden facilitarse múltiples niveles de directorio raíz, subdirectorio, archivo, etc. No obstante, esta invención resulta especialmente aplicable al caso en el que las unidades correspondientes a un conjunto de archivos de datos encapsulados en tablas o secciones de datos, encapsulándose posteriormente dichas tablas en paquetes de datos para generar un flujo de transporte.

A diferencia de la autenticación a nivel de paquete o tabla, esta realización permita una completa independencia entre el conjunto de datos autentificados y su encapsulado en un flujo de transporte y, una vez más, facilita el suministro de software procedente de diversas fuentes en el flujo de transporte controlado por un único emisor de radiodifusión. Los datos autentificados de acuerdo con esta realización pueden incluso transmitirse a través de diferentes rutas de transmisión (pro ejemplo, un enlace de telecomunicaciones bidireccional o un enlace vía satélite), utilizando formatos alternativos de encapsulado para transmitir los datos.

Como se ha mencionado anteriormente, la utilización de un proceso de autenticación aplicado con an-

terioridad a la preparación de los datos para la transmisión tiene como efecto que los datos pueden enviarse posteriormente a un receptor mediante cualquier número de canales, tal como un canal de radiodifusión o un canal de telecomunicaciones, sin cambiar el proceso de autenticación. Igualmente, una vez que un receptor o decodificador ha reconstituido los archivos de datos a partir del formato asociado a la ruta de transmisión, puede llevarse a cabo una verificación de estos datos, independientemente del modo de transmisión seleccionado.

Cualquiera o todas las características del primer aspecto de la invención y sus realizaciones preferidas pueden, por supuesto, combinarse con el segundo y tercer aspecto de la invención.

La presente invención se ha descrito anteriormente en relación con las etapas de generación de datos de autenticación con anterioridad a la transmisión. La invención, en sus realizaciones más amplias y preferidas, también se aplica a las fases inversas llevadas a cabo en un receptor para verificar estos datos.

En sus aspectos más amplios, la presente invención puede aplicarse a cualquier sistema de transmisión digital. No obstante, la invención se aplica preferiblemente a un sistema de televisión digital y, concretamente, a módulos de datos que transporten software de aplicaciones para su uso en un receptor/decodificador del sistema de televisión digital.

Tal y como se usa en el presente documento, el término "sistema de transmisión digital" incluye cualquier sistema de transmisión para la transmisión o radiodifusión, por ejemplo básicamente de datos digitales audiovisuales o multimedia. Aunque la presente invención resulta especialmente aplicable a un sistema de televisión digital por radiodifusión, la invención también puede aplicarse a una red fija de telecomunicaciones para aplicaciones de Internet multimedia, a un circuito cerrado de televisión, etc. Como se comprenderá, el término "sistema digital de televisión" incluye, por ejemplo, cualquier sistema vía satélite, terrestre, por cable y otros sistemas.

El término "receptor/decodificador" o "decodificador" utilizado en la presente solicitud puede referirse a un receptor para la recepción de señales codificadas o no codificadas, por ejemplo señales de televisión y/o radio que pueden ser emitidas o transmitidas por cualquier otro medio. El término también puede referirse a un decodificador para la decodificación de las señales recibidas. Entre las realizaciones de dichos receptores/decodificadores pueden incluirse un decodificador integrado con el receptor para la decodificación de las señales recibidas, por ejemplo en un "decodificador de sobremesa", tal como un decodificador que funcione en combinación con un receptor físicamente independiente o un decodificador que incluye funciones adicionales, tal como un navegador web y/o que se encuentre integrado con otros dispositivos como una grabadora de vídeo o una televisión.

El término MPEG se refiere a las normas de transmisión de datos desarrolladas por el grupo de trabajo "Motion Pictures Expert Group [grupo de expertos de imágenes en movimiento]" de la Organización Internacional de Normalización y en particular, pero no exclusivamente, a la norma MPEG-2 desarrollada para aplicaciones de televisión digital y recogida en los documentos ISO 13818-1, ISO 13818-2, ISO 13818-3 e ISO 13818-4. En el contexto de la presente solicitud de patente, el término MPEG incluye todas las variantes y modificaciones de los formatos MPEG aplicables al ámbito de la transmisión de datos digitales.

El término DSMCC hace referencia a las normas de formato de archivo de datos descritas en los documentos MPEG y en el actual documento ISO 13818-6.

A continuación se describirá, únicamente a modo de ejemplo, una realización preferida de la invención, haciendo referencia a las figuras adjuntas en las cuales:

La figura 1 muestra un diagrama esquemático de un sistema de televisión digital para ser utilizado con la presente invención.

La figura 2 muestra la estructura de un decodificador del sistema de la figura 1.

La figura 3 muestra la estructura de diversos componentes incluidos en el flujo de transporte de radiodifusión MPEG.

La figura 4 muestra la división de una aplicación de software en diversas tablas MPEG.

La figura 5 muestra la relación entre los archivos de datos DSMCC y las tablas MPEG finalmente generadas.

La figura 6 muestra la relación entre el cliente, el servidor y el gestor de la red, según se define en el contexto de DSMCC.

La figura 7 muestra el directorio autentificado, el subdirectorio y los objetos de archivo en esta realización de la invención.

En la figura 1 se muestra un resumen de un sistema de televisión digital 1. La realización incluye un sistema de televisión digital 2 completamente convencional que utiliza el conocido sistema de compresión MPEG-2 para transmitir señales digitales comprimidas. En más detalle, el compresor MPEG-2 3 situado en un centro de radiodifusión recibe un flujo de señales digitales (normalmente un flujo de señales de vídeo). El compresor 3 está conectado a un multiplexor y codificador 4 mediante una conexión 5.

El multiplexor 4 recibe una pluralidad de señales de entrada adicionales, ensambla el flujo de transporte y transmite las señales digitales comprimidas a un transmisor 6 del centro de radiodifusión a través de una conexión 7 que por supuesto puede adoptar diversas formas, comprendiendo enlaces de telecomunicaciones. El transmisor 6 transmite señales electromagnéticas a través de un enlace de subida 8 hacia un transmisor-receptor de satélite 9 donde se procesan electrónicamente y se emiten a través de un enlace descendente nacional 10 al receptor de tierra 12, que normalmente consiste en una antena parabólica propiedad de o alquilada por el usuario final. Las señales recibidas por el receptor 12 se transmiten a un receptor/decodificador integrado 13 comprado o alquilado por el usuario final y que se encuentra conectado al televisor 14 del usuario final. El receptor/decodificador 13 decodifica la señal comprimida MPEG-2 en una señal de televisión para el televisor 14.

Por supuesto son posibles otros canales de transporte para la transmisión de los datos, como la radiodifusión terrestre, la transmisión por cable, enlaces combinados satélite/cable, redes telefónicas, etc.

En un sistema de canales múltiples, el multiplexor 4 gestiona la información de audio y vídeo recibida desde diversas fuentes paralelas e interactúa con el transmisor 6 para transmitir la información a través de un número similar de canales. Además de la infor-

mación audiovisual, pueden introducirse mensajes o aplicaciones o cualquier otro tipo de datos digitales en algunos o en todos estos canales, entrelazados con la información de audio y vídeo digital transmitida. En este caso, un flujo de datos digitales, por ejemplo en forma de archivos de software y mensajes de acuerdo con el formato DSM-CC se comprimirá y empaquetará en el formato MPEG a través del compresor 3. La descarga de los módulos de software se describirá más adelante en mayor detalle.

Un sistema de acceso condicional 15 se encuentra conectado al multiplexor 4 y al receptor/decodificador 13, y se encuentra parcialmente situado en el centro emisor y en el decodificador. Permite al usuario final acceder a emisiones de televisión digital procedentes de uno o más proveedores de emisiones. Una tarjeta inteligente capaz de descifrar mensajes relativos a ofertas comerciales (es decir, uno o varios programas de televisión vendidos por el proveedor de emisiones) se inserta en el receptor/decodificador 13. Usando el decodificador 13 y la tarjeta inteligente, el usuario final puede adquirir ofertas comerciales mediante suscripción o pago por visión. En la práctica, el decodificador puede configurarse para gestionar sistemas de control de acceso múltiple, por ejemplo del tipo Simulcrypt o Multicrypt.

Como se ha mencionado anteriormente, los programas transmitidos por el sistema se codifican en el multiplexor 4, estando determinadas las condiciones y claves de cifrado aplicadas a una transmisión dada por el sistema de control de acceso 15. La transmisión de datos codificados de esta forma es bien conocida en el ámbito de los sistemas de TV de pago. Normalmente, los datos codificados se transmiten junto con una palabra de control para el descifrado de los datos, estando la propia palabra de control cifrada mediante la denominada clave de explotación, transmitiéndose en formato cifrado.

Los datos codificados y la palabra de control cifrada son recibidos entonces por el decodificador 13 que puede acceder a un equivalente de la clave de explotación almacenada en una tarjeta inteligente insertada en el decodificador para descifrar la palabra de control cifrada y descodificar posteriormente los datos transmitidos. Un abonado que se encuentre al corriente de pago recibirá, por ejemplo, en un EMM (Mensaje de Gestión de Derechos) transmitido mensualmente la clave de explotación necesaria para descifrar la palabra de control cifrada y para permitir ver la transmisión. Además de su uso para descifrar programas audiovisuales de televisión, pueden generarse y transmitirse claves de explotación similares para ser utilizadas en la verificación de otros datos, como módulos de software según se describirá más adelante.

Un sistema interactivo 16, que también se encuentra conectado al multiplexor 4 y al receptor/decodificador 13, y que se encuentra una vez más situado parcialmente en el centro emisor y parcialmente en el decodificador permite que el usuario final interactúe con diversas aplicaciones a través de un canal de retorno de módem 17. El canal de retorno de módem también puede utilizarse para las comunicaciones usadas en el sistema de acceso condicional 15. Un sistema interactivo puede utilizarse, por ejemplo, para permitir que el espectador se comunique inmediatamente con el centro transmisor para solicitar la autorización para ver un evento concreto, descargar una aplicación etc.

Haciendo referencia a la figura 2, se describirán brevemente a continuación los elementos físicos del receptor/decodificador 13 o el decodificador de sobremesa adaptados para ser utilizados en la presente invención. Los elementos mostrados en esta figura se describirán en términos de bloques funcionales.

El decodificador 13 incluye un procesador central 20 que comprende elementos de memoria asociados y que está adaptado para recibir datos de entrada procedentes de un interfaz serie 21, un interfaz paralelo 22 y un módem 23 (conectado al canal de retorno de módem 17 de la figura 1).

El decodificador está adaptado adicionalmente para recibir entradas de un mando a distancia por infrarrojos 25 a través de una unidad de control 26 y de unos contactos 24 situados en el panel frontal del decodificador. El decodificador también posee dos lectoras de tarjeta inteligente 27, 28 adaptadas para leer tarjetas inteligentes bancarias o de abono 29, 30 respectivamente. Las entradas también pueden recibirse a través de un teclado por infrarrojos (no mostrado). El lector de tarjetas inteligentes de abono 28 se acopla con una tarjeta de abono insertada y con una unidad de acceso condicional 29 para suministrar la palabra de control necesaria a un demultiplexor/descodificador 30 para permitir la descodificación de la señal de transmisión cifrada. El decodificador también incluye un sintonizador convencional 31 y un demodulador 32 para recibir y demodular la transmisión vía satélite antes de ser filtrada y demultiplexada por la unidad 30.

El procesamiento de los datos en el decodificador suele estar gestionado por el procesador central 20. La arquitectura de software 15 del procesador central corresponde a una máquina virtual que interactúa con un sistema operativo de nivel inferior ejecutado en los componentes de hardware del decodificador.

A continuación se describirá, haciendo referencia a las figuras 3 y 4, la estructura de paquetes de los datos incluidos en el flujo de transporte MPEG transmitido que se ha enviado desde el transmisor al decodificador. Como puede apreciarse, aunque la descripción se centrará en el formato de tabulación utilizado en la norma MPEG, los mismos principios se aplican igualmente a otros formatos de flujo de datos por paquetes.

Haciendo referencia concretamente a la figura 3, un flujo de bits MPEG incluye una tabla de acceso al programa ("PAT") 40 con un identificador de paquete ("PID") de 0. La PAT contiene referencias a los PIDs de las tablas de correspondencia de programas ("PMTs") 41 de diversos programas. Cada PMT incluye una referencia a los PIDs de los flujos de las tablas MPEG de audio 42 y las tablas MPEG de vídeo 43 correspondientes a dicho programa. Un paquete que tenga un PID de cero, es decir la tabla de acceso al programa 40, facilita el punto de entrada para todo el acceso MPEG.

Para que se puedan descargar aplicaciones y datos para ellos, se definen dos nuevos tipos de flujo y la PMT correspondiente también contiene referencias a los PIDs de los flujos de tablas MPEG de aplicación 44 (o secciones de ellas) y de tablas MPEG de datos 45 (o secciones de ellas). De hecho, aunque en algunos casos puede ser conveniente definir tipos de flujo independientes para el software de aplicación ejecutable y datos para su procesamiento por dicho software, ello no es esencial. En otras realizaciones, los datos y

el código ejecutable pueden ensamblarse en un solo flujo al que se accede a través de la PMT como ya se ha descrito.

Haciendo referencia a la figura 4, para poder descargar, por ejemplo, una aplicación incluida en un flujo 44, la aplicación 46 se divide en módulos 47, cada uno de ellos formado por una tabla MPEG. Algunas de estas tablas tienen una sola sección, mientras que otras pueden estar compuestas por una pluralidad de secciones 48. Una sección típica 48 tiene una cabecera que incluye una identificación de tabla de un octeto ("TID") 50, el número de sección 51 de dicha sección en la tabla, el número total 52 de secciones de dicha tabla y una referencia de extensión 54 de dos octetos 110. Cada sección incluye también un componente de datos 54 y un CRC 55. Para una tabla específica 47, todas las secciones 48 que constituyen dicha tabla 47 tienen la misma TID 50 y la misma extensión TID 53. Para una aplicación específica 46, todas las tablas 47 que constituyen dicha aplicación 46 tienen la misma TID 50, pero sus extensiones TID respectivas son diferentes.

Para cada aplicación 46, se utiliza una sola tabla MPEG como tabla de directorio 56. La tabla de directorio 56 tiene en su encabezamiento la misma TID que el resto de las tablas 47 que constituyen la aplicación. No obstante, la tabla de directorio tiene una extensión TID predeterminada de cero con fines de identificación y debido al hecho de que tan sólo se necesita una sola tabla para la información del directorio. El resto de las tablas 47 tendrán normalmente extensiones TID distintas de cero y estarán compuestas por varias secciones asociadas 48. La cabecera de la tabla de directorio también incluye un número de versión de la aplicación que va a descargarse.

Haciendo de nuevo referencia a la figura 3, las PMTs 40, las PMTs 41 y los componentes del flujo de aplicación y datos 44, 45 se transmiten cíclicamente. Cada una de las aplicaciones que se transmiten tiene un TID respectivo predeterminado. Para descargar una aplicación, la tabla MPEG con el TID adecuado y una extensión TID de cero se descarga al receptor/decodificador. Esta es la tabla de directorio correspondiente a la aplicación requerida. A continuación el decodificador procesa los datos del directorio para determinar la extensión TID de las tablas que constituyen la aplicación requerida. Posteriormente podrá descargarse cualquier tabla requerida que tenga el mismo TID que la tabla del directorio y una extensión TID determinada a partir del directorio.

El decodificador está configurado para comprobar cualquier actualización de la tabla del directorio. Esto puede llevarse a cabo descargando de nuevo periódicamente la tabla del directorio, por ejemplo cada 30 segundos, o cada minuto o cada cinco minutos, y comparando el número de versión de la tabla de directorio anteriormente descargada. Si el número de versión de la que se acaba de descargar corresponde a una versión posterior se borrarán las tablas asociadas al directorio anterior y se descargarán y ensamblarán las tablas asociadas a la nueva versión.

En una configuración alternativa, el flujo de binario entrante se filtra utilizando una máscara correspondiente al TID, a la extensión TID y al número de versión, con unos valores fijados para el TID de la aplicación, una extensión TID de cero y un número de versión superior en una unidad al número de versión del directorio actualmente descargado. De este modo puede detectarse un aumento del número de versión y una vez detectado se descarga el directorio y se actualiza la aplicación como se ha descrito anteriormente. Si debe finalizarse una aplicación, se transmite un directorio vacío con el siguiente número de versión pero sin que ninguno de los módulos esté listado en el directorio. En respuesta a la recepción de dicho directorio vacío, el decodificador 2020 está programado para borrar la aplicación.

En la práctica, el software y los programas para ejecución de aplicaciones en el decodificador pueden introducirse mediante cualquiera de los componentes del decodificador, concretamente en el flujo de datos recibido a través de la conexión vía satélite como se ha descrito anteriormente, pero también a través del puerto serie, la conexión de la tarjeta inteligente, etc. Dicho software puede incluir aplicaciones de alto nivel utilizadas para ejecutar aplicaciones interactivas en el decodificador, tales como navegadores, aplicaciones de concursos, guías de programas, etc. También puede descargarse software para modificar la configuración de funcionamiento del software del decodificador, por ejemplo mediante parches o similares.

También pueden descargarse aplicaciones a través del decodificador y enviarse a un PC o similar conectado al decodificador. En dicho caso, el decodificador actúa como un dispositivo de encaminado (router) de comunicaciones para el software, que se ejecuta en el dispositivo conectado. Además de esta función de encaminado, el decodificador también puede funcionar convirtiendo los datos por paquetes MPEG antes de su envío al PC en software de archivos informáticos organizado, por ejemplo, de acuerdo con el protocolo DSMCC (véase más abajo).

Anteriormente, las medidas ejecutadas para verificar el origen y el grado de finalización de los datos de la aplicación se han centrado en la verificación de las tablas del flujo de paquetes MPEG. Concretamente, en sistemas convencionales se aplica una función troceo a cada una de las secciones individuales 48 con anterioridad a la transmisión y el valor de comprobación resultante o firma correspondiente a cada sección se almacena en una lista en la tabla de directorio 56 enviada al decodificador. Mediante la comparación del valor de troceo posteriormente calculado por el decodificador con el valor de comprobación almacenado en el directorio para una sección recibida se puede verificar la integridad de la sección recibida. Los datos del directorio 40 pueden también estar sometidos a un proceso de troceo para generar un valor de comprobación adicional o firma para la tabla del directorio 40. Además, este valor de comprobación puede codificarse mediante una clave privada y almacenarse en la tabla del directorio. Tan sólo los decodificadores que posean la clave pública correspondiente podrá autentificar la firma.

En contraste con dichos sistemas convencionales, la presente realización se refiere a un medio para garantizar y verificar los datos de aplicación organizados en torno a una jerarquía múltiple de archivos u objetos de datos a nivel de la aplicación. Esto se comprenderá más claramente mediante la figura 5, que muestra la relación entre los datos organizados en un conjunto de archivos de datos DSMCC U-U 60, en una aplicación ensamblada 46 y encapsulados en una serie de tablas MPEG 47.

Con anterioridad a la transmisión, los archivos de

datos se ensamblan en la aplicación 46 y posteriormente son formateados por un compresor MPEG obteniendo tablas MPEG o módulos 47 como se ha descrito anteriormente, comprendiendo una cabecera 49 específica para el flujo de paquetes MPEG y que incluya la ID de la tabla, el número de versión, etc. Posteriormente estas tablas son encapsuladas por el compresor MPEG en paquetes MPEG. Como se apreciará, puede no existir una relación fija entre los datos organizados en los archivos de datos 61 y las eventuales tablas MPEG 47. Tras la recepción y filtrado por parte del decodificador, se descartan las cabeceras de paquetes y se reconstituyen las series de tablas a partir de los datos útiles de los paquetes transmitidos. Más adelante, los descartan las cabeceras de tabla 49 y se reconstituye la aplicación 46 a partir de los datos útiles de las tablas 47.

El formato DSMCC para archivos de datos es una norma adaptada en particular para su uso en redes multimedia y que define una serie de formatos de mensaje y de comandos de sesión para la comunicación entre un usuario cliente 70, un usuario servidor 71 y un gestor de recursos de red 72. Véase la figura 6. El gestor de recursos de red 72 puede considerarse como una entidad lógica que actúa gestionando la atribución de recursos en el seno de una red. A pesar de haberse concebido inicialmente para su uso en el contexto de comunicaciones de red bidireccionales, las recientes puestas en práctica de la norma DSM-CC se han centrado en su uso con fines de radiodifusión unidireccional.

La comunicación entre un cliente y un servidor se configura mediante una serie de sesiones, intercambiándose una primera serie de mensajes entre un usuario (cliente 70 o servidor 71) y el gestor de la red 72 para configurar el cliente y/o el servidor para las comunicaciones. Dichos mensajes están formateados de acuerdo con el denominado protocolo DSMCC U-N (usuario a red). Se ha definido concretamente un subconjunto de este protocolo para la descarga de datos mediante radiodifusión.

Una vez establecido un enlace de comunicaciones, los mensajes son intercambiados posteriormente entre el cliente 70 y el servidor 71 de acuerdo con DSMCC U-U (protocolo usuario a usuario). Una secuencia de mensajes de este tipo corresponde a los archivos de datos 60 de la figura 5. En el caso de mensajes DSMCC U-U, los datos se organizan en una serie de mensajes 61 agrupados de acuerdo con el Protocolo BIOP o Broadcast InterOrb Protocol [protocolo interorb de difusión].

Cada mensaje u objeto 61 incluye una cabecera 62, una sub-cabecera 63 y unos datos útiles 64 que contienen los propios datos. De acuerdo con el protocolo BIOP, la cabecera 62 contiene, entre otras cosas, una indicación del tipo de mensaje y de la versión BIOP, mientras que la sub-cabecera indica el tipo de objeto y otras informaciones que han de ser definidas por el arquitecto del sistema.

Los objetos de datos 64 incluidos en los datos útiles de los archivos DSMCC U-U pueden generalmente definirse como pertenecientes a uno de los tres tipos siguientes: objetos de directorio, objetos de archivo y objetos de flujo. Los objetos de directorio definen directorios raíz o subdirectorios utilizados para referirse a una serie de objetos de archivo asociados que contienen los datos reales de la aplicación.

Los objetos de flujo pueden utilizarse para permitir el establecimiento de una relación temporal entre los datos contenidos en los archivos de datos y el propio flujo de paquetes MPEG. Esto se puede utilizar, por ejemplo, en el caso de aplicaciones interactivas incluidas en los archivos de datos y diseñadas para su sincronización con los flujos elementales de vídeo o audio recibidos y procesados por el decodificador. Como se ha mencionado anteriormente, en otros casos puede no existir una correlación directa entre los datos por paquetes MPEG y los archivos de datos.

A diferencia de las tablas MPEG, cuando un único directorio hace referencia a un conjunto de tablas con tan sólo un único nivel de jerarquía, los archivos de datos 60 pueden organizarse de una forma jerárquica bastante más compleja. Como en el caso de los archivos almacenados en un PC o servidor, un directorio principal o raíz puede hacer referencia a uno o más subdirectorios que, a su vez, hacen referencia a un segundo nivel de archivos de datos. Incluso puede hacerse referencia a un segundo directorio raíz asociado a otro conjunto de datos de aplicación.

Haciendo referencia a la figura 7, se muestra un ejemplo de la estructura de archivo para un conjunto de archivos de datos o unidades. Un directorio raíz DIR A0 indicado como 75 hace referencia a un grupo de subdirectorios A1 a A4 indicado como 76. Cada subdirectorio 76 hace referencia a uno o más conjuntos de archivos de objeto asociados 77. Con fines de aclaración, tan sólo se muestra un único grupo de archivos de objeto F1, F2, etc. asociado al subdirectorio A4. En la práctica, cada uno de los subdirectorios A1 a A4 puede hacer referencia a varios grupos de archivos de objeto.

Dentro de cada directorio y subdirectorio se introduce un conjunto de fases de autenticación para los archivos vinculados 20 a dicho directorio. Haciendo referencia al directorio raíz 75, la sub-cabecera 63 incluye un valor de troceo obtenido mediante la aplicación de un algoritmo de troceo a una parte o a la totalidad de los datos almacenados en los archivos de subdirectorio A1 a A4 indicados como 76. El algoritmo de troceo utilizado puede ser de cualquier tipo conocido, como por ejemplo el algoritmo Message Digest MD5.

En una realización, el algoritmo puede aplicarse individualmente a cada archivo o subdirectorio asociado, almacenándose una lista de los valores de troceo para cada subdirectorio 76 en el directorio raíz 75 con anterioridad a la transmisión. Sin embargo, aunque dicha solución permite un mayor nivel de resolución de comprobación en lo tocante a la verificación de cada subdirectorio, esta solución puede resultar bastante ineficaz en términos del tiempo de procesamiento necesario para que el decodificador calcule las correspondientes firmas.

Por ello, la sub-cabecera 63 del directorio 79 incluye preferiblemente un valor flash acumulativo 79, calculado mediante la aplicación del algoritmo de troceo MD5 a las secciones combinadas de sub-cabecera y datos útiles 63, 64 de los subdirectorios 76, es decir sin la cabecera 62. Concretamente, los valores flash 82 contenidos en los subdirectorios 76 y que hacen referencia a la capa de objetos de archivo 77 están incluidos en este cálculo de troceo.

En el caso del subdirectorio A4 mostrado en la figura 7, este subdirectorio hace referencia a una serie de archivos de objeto F1-Fn indicados como 77. En este caso, se genera un valor flash acumulativo 82 pa-

ra los contenidos combinados de los archivos de objeto 77. Este valor se incluye en el proceso de troceo que da lugar al valor flash 79. Por lo tanto, no es posible cambiar ninguno de los archivos de objeto 77 sin cambiar el valor flash 82 del subdirectorio 76 que, a su vez, cambiará el valor flash 79 del directorio 75.

En el caso actual, se calcula un valor de troceo combinado para todos los subdirectorios A1-A4 a los que se hace referencia en el directorio. Este valor de troceo se almacena junto con un identificador del grupo de subdirectorios a partir del cual se han tomado los datos. En otras realizaciones, puede almacenarse una serie de valores de troceo combinados o individuales así como sus correspondientes identificadores en la sub-cabecera del directorio.

Por ejemplo, un segundo conjunto de subdirectorios asociado también al directorio raíz pero relativo a un conjunto de datos o código ejecutable diferente puede ser también agrupado conjuntamente, calculándose un valor de troceo acumulativo calculado para este subdirectorio y almacenándose en el directorio raíz de l sub-cabecera. Un único valor de troceo asociado a un único directorio puede también almacenarse en la sub-cabecera del directorio raíz.

La autorización de grupos o archivos de datos individuales no impide, por supuesto, que el directorio raíz (o 25, por supuesto, cualquier otro archivo) haga también referencia a archivos de datos no validados o sin troceo, pero deberá tenerse en cuenta la ausencia de validación de dicho archivo a la hora de efectuar cualquier operación con este archivo. A este respecto, podría no ser necesario, por ejemplo, autentificar los objetos de flujo.

La utilización en este caso de una función de troceo permite, en primer lugar, que el decodificador verifique la integridad o el grado de finalización de la descarga de los archivos de datos. En el caso, por ejemplo, de fallo o corte de la transmisión, la utilización de un algoritmo de troceo acumulativo con los archivos dependientes recibidos no dará el mismo resultado que el valor de troceo correspondiente a estos archivos almacenado en el directorio raíz. El decodificador será alertado entonces de la presencia de posibles errores en los datos descargados y volverá a cargar los archivos de datos defectuosos.

Como puede apreciarse, en el caso de un algoritmo de troceo, el cálculo del valor de troceo se lleva a cabo de acuerdo con una serie públicamente conocida de fases de cálculo y, como tal, cualquiera puede generar el valor de troceo correspondiente a un conjunto de archivos de datos determinado. Por lo tanto, normalmente, no es posible verificar el origen de dichos archivos de datos mediante una simple comprobación de los valores de troceo.

Para superar este problema, se calcula un valor de firma correspondiente al directorio raíz 75 utilizando un valor de clave secreta conocido únicamente por el operador. Esta clave puede corresponderse con una clave obtenida mediante un algoritmo de clave simétrica, como el algoritmo Data Encryption Standard [Norma de cifrado de datos] o DES. No obstante, preferiblemente se utiliza un algoritmo de clave privada/pública como el algoritmo de Rivest, Shamir y Adelman o RSA, estando el operador responsable de generar los archivos de datos en posesión del valor de la clave privada y de los valores de clave pública de los decodificadores.

Como se muestra en la figura 7, el directorio raíz 75 incluye un identificador de clave o número mágico 80 que identificará para el decodificador la clave pública a utilizar en la fase de verificación junto con el valor de la firma calculado 81 generado mediante la utilización de la clave privada del operador. En este caso, el valor de la firma 81 se genera aplicando la clave privada del operador a una parte o a todos los datos del directorio 75, comprendiendo preferiblemente los datos útiles 64 y/o el valor o valores de troceo acumulativos 79. El decodificador puede entonces verificar este valor de firma 81 utilizando la clave pública correspondiente identificada por el número de clave 80.

En este ejemplo, los datos del directorio 75 están sin cifrar y la clave privada se utiliza simplemente para proporcionar un valor de firma que pueda ser verificado por la clave pública. En realizaciones alternativas pueden cifrarse mediante la clave privada una parte o la totalidad de los contenidos del directorio, descifrándose posteriormente mediante una clave correspondiente.

En cualquiera de los casos, la generación de un valor de firma o bloque de código cifrado mediante el uso de una clave secreta permite que un decodificador verifique la integridad del origen del directorio 75 y, por implicación, la integridad y el origen de los archivos a los que hace referencia este directorio raíz. Dado que los valores de troceo acumulativos para los archivos de referencia están incluidos en el cálculo de la firma 81, no es posible alterar estos valores sin detectarlo en la fase de verificación. Debido a que por lo general cada valor de troceo es único para un conjunto dado de datos, no sería por tanto posible modificar el contenido de cualquier archivo dependiente al que se le haya aplicado el troceo sin cambiar su valor de troceo característico y, por tanto, el valor de firma resultante de un directorio.

El directorio raíz 75, los subdirectorios 76 y los archivos de objetos 77 son generados por un operador de radiodifusión del sistema, indicado aquí como operador A. En este caso, estos archivos tendrán un origen común conocido y verificable.

No obstante, dependiendo de la aplicación a implementar, también puede hacerse referencia a una serie de archivos de datos asociados a un segundo operador B. En este caso, el subdirectorio 76 incluye una referencia al directorio raíz DIR B0 de un segundo conjunto de archivos de datos, indicado como 78. También es posible prever conexiones entre archivos de datos procedentes de distintas fuentes a otros niveles, por ejemplo una jerarquía de archivos en la que un primer subdirectorio en un conjunto de archivos hace referencia a un subdirectorio de un segundo conjunto de archivos de datos, etc.

Al igual que con el directorio raíz DIR A0 para el operador A, el directorio raíz DIR B0 indicado como 78 incluye uno o más valores de código flash acumulativo 84 asociados a sus subdirectorios asociados (no mostrados), identificando un número de clave 85 la clave pública del operador B a utilizar durante la fase de verificación, generando la clave privada correspondiente del operador un valor de firma 86.

Se calcula un valor de troceo para este directorio utilizando el valor flash 84 y la firma 86 en la sub-cabecera del directorio, así como los datos útiles 64 del directorio 78. Este valor de troceo se almacena entonces en el subdirectorio A4, lo que permite verificar la

integridad de los datos en la tabla de directorio que debe construirse.

Debido al hecho de que la firma 86 y los valores de troceo 84 están incluidos en el cálculo del valor de troceo 83, también puede asumirse la integridad del resto de los archivos de datos a los que ha hecho referencia el directorio raíz 78, ya que ninguno de estos archivos dependientes puede modificarse sin modificar el valor de troceo 84 y, lo que es más importante, el valor de firma 86. Dado que el valor de firma 86 sólo puede ser calculado por una persona que posea la clave privada del operador, puede asumirse la integridad de todos los archivos a los que hace referencia el directorio 78, suponiendo que se calculen los valores de troceo correspondientes de los subdirectorios y archivos de objetos dependientes adicionales.

De este modo, los datos de aplicación relativos a programas ejecutables o similares generados por un segundo operador pueden estar vinculados a aplicaciones asociadas a un primer operador de una forma segura y fiable.

Como se observará, pueden darse diversas variaciones, especialmente para reducir la cantidad de datos sometidos a troceo o a firma en cada fase. Concretamente, en el caso de una firma o valor de troceo en un subdirectorio o subdirectorios utilizados para verificar un archivo de datos de nivel inferior, la firma o el valor de troceo del directorio pueden generarse utilizando solamente el valor de troceo de nivel inferior y no otros datos.

Por ejemplo, el valor de troceo combinado 79 del directorio A0 75 puede ser generado utilizando los valores de troceo combinados 82, 83 de cada uno de los subdirectorios A1-A4 indicados como 76. Dado que estos valores son únicos, al igual que los datos útiles del subdirectorio, el valor de troceo combinado 79 seguirá siendo único para los subdirectores en cuestión. Además, puede seguir asumiéndose la integridad del nivel inferior de archivos de objeto y directorio 77, 78 dado que los valores de troceo 82 se utilizan todavía para el cálculo.

Igualmente, el valor de troceo 82 calculado para verificar el directorio B0 indicado como 78 puede calcularse simplemente utilizando el valor de firma 86. Dado que esto depende de, y está asociado únicamente a los valores de troceo 84, y siendo a su vez dichos valores de troceo dependientes del siguiente nivel de archivos, puede seguir asumiéndose la integridad de todos los conjuntos de archivos de datos a los que hace referencia el directorio 78.

REIVINDICACIONES

1. Método de verificación de los datos recibidos en una red de transmisión digital, estando organizados los datos en una jerarquía compuesta al menos por una unidad de directorio raíz (75), una unidad de subdirectorio (76) y una unidad de archivo (77), actuando un valor de autenticación de archivo (82, 83) resultante de un primer algoritmo de autenticación sobre un archivo de datos almacenado en el subdirectorio de referencia y actuando un valor de autenticación del subdirectorio (63) resultante de un segundo algoritmo de autenticación sobre el valor de autenticación del archivo almacenado en la unidad del directorio raíz de referencia, comprendiendo dicho método, en un aparato receptor, las siguientes etapas:

actuar sobre los datos de un archivo con un primer algoritmo de autenticación para obtener un primer valor resultante,

comparar el primer valor resultante con el valor de autenticación almacenado en el subdirectorio de referencia,

actuar sobre, al menos, el valor de autenticación del archivo almacenado en el subdirectorio de referencia mediante un segundo algoritmo de autenticación para obtener un segundo valor resultante, y

comparar el segundo valor resultante con el valor de autenticación del subdirectorio asociado almacenado en el directorio raíz de referencia.

2. Aparato para verificar datos recibidos en una red de transmisión digital, estando organizados los datos en una jerarquía compuesta, al menos, por una unidad de directorio raíz (75), una unidad de subdirectorio (76) y una unidad de archivos (77), actuando un valor de autenticación de archivo (82, 83) resultante de un primer algoritmo de autenticación sobre un archivo de datos almacenado en el subdirectorio de referencia y actuando un valor de autenticación del subdirectorio (63) resultante de un segundo algoritmo de autenticación sobre el valor de autenticación del archivo almacenado en la unidad del directorio raíz de referencia, comprendiendo dicho aparato:

medios para actuar sobre los datos de un archivo con un primer algoritmo de autenticación para obtener un primer valor resultante,

medios para comparar el primer valor resultante con el valor de autenticación almacenado en el subdirectorio de referencia,

medios para actuar sobre al menos el valor de autenticación del archivo almacenado en el subdirectorio de referencia mediante un segundo algoritmo de autenticación para obtener un segundo valor resultante, y

medios para comparar el segundo valor resultante con el valor de autenticación del subdirectorio asociado almacenado en el directorio raíz de referencia.

3. Aparato de acuerdo con la reivindicación 2 en el que la red es una red de televisión por cable.

4. Aparato de acuerdo con la reivindicación 2 en el que la red es una red de televisión vía satélite.

5. Aparato de acuerdo con la reivindicación 2 en el que la red es una red de televisión terrestre.

6. Aparato de acuerdo con cualquiera de las reivindicaciones 2 a 5 en el que el aparato es una televisión digital.

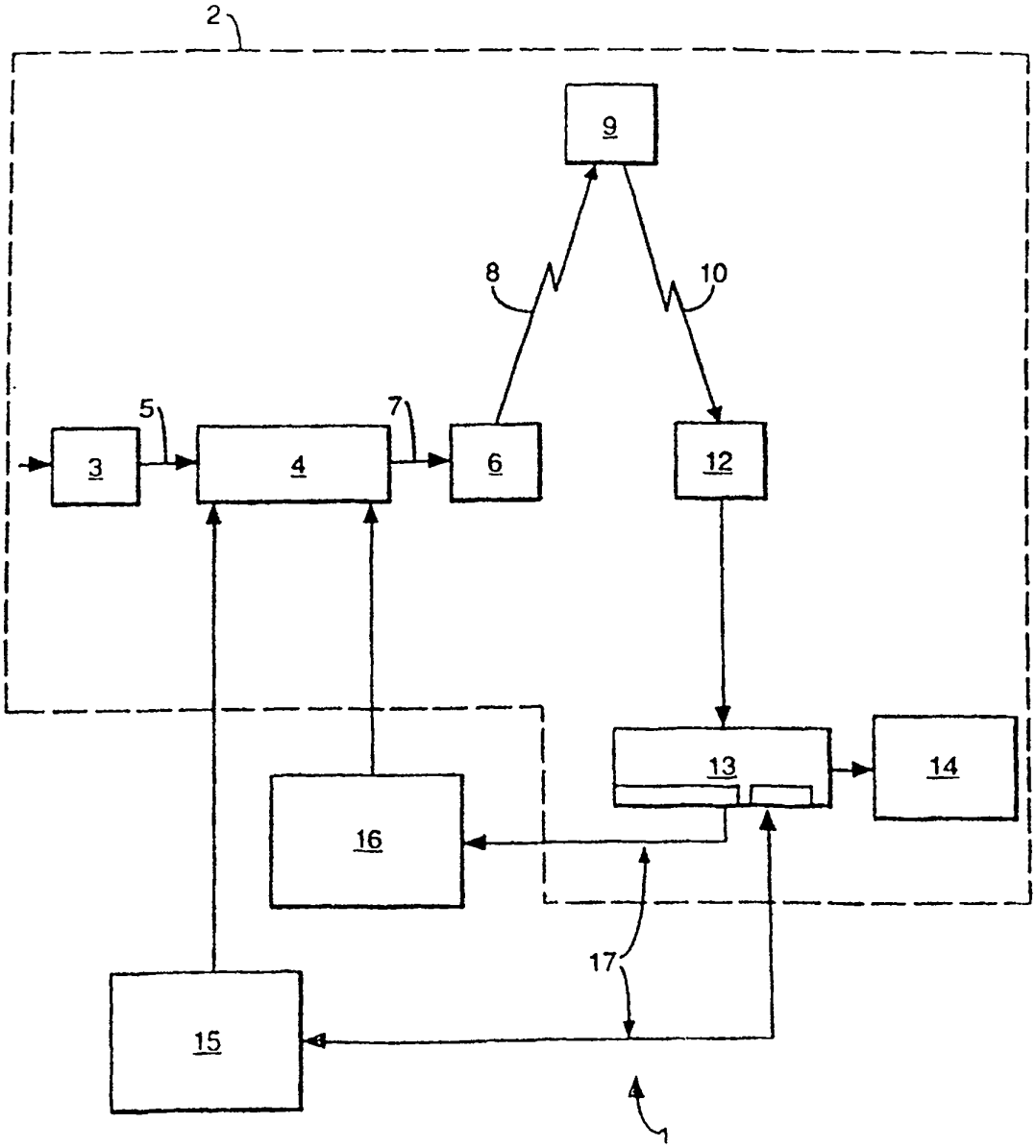
7. Aparato de acuerdo con cualquiera de las reivindicaciones 2 a 5 en el que el aparato es un decodificador.

8. Aparato de acuerdo con cualquiera de las reivindicaciones 2 a 5 en el que el aparato incluye igualmente dos lectoras de tarjetas inteligentes.

9. Aparato de acuerdo con cualquiera de las reivindicaciones 2 a 5 en el que el aparato es una grabadora de vídeo.

10. Aparato de acuerdo con cualquiera de las reivindicaciones 2 a 5 en el que el aparato es un decodificador con un navegador web.

Fig.1.



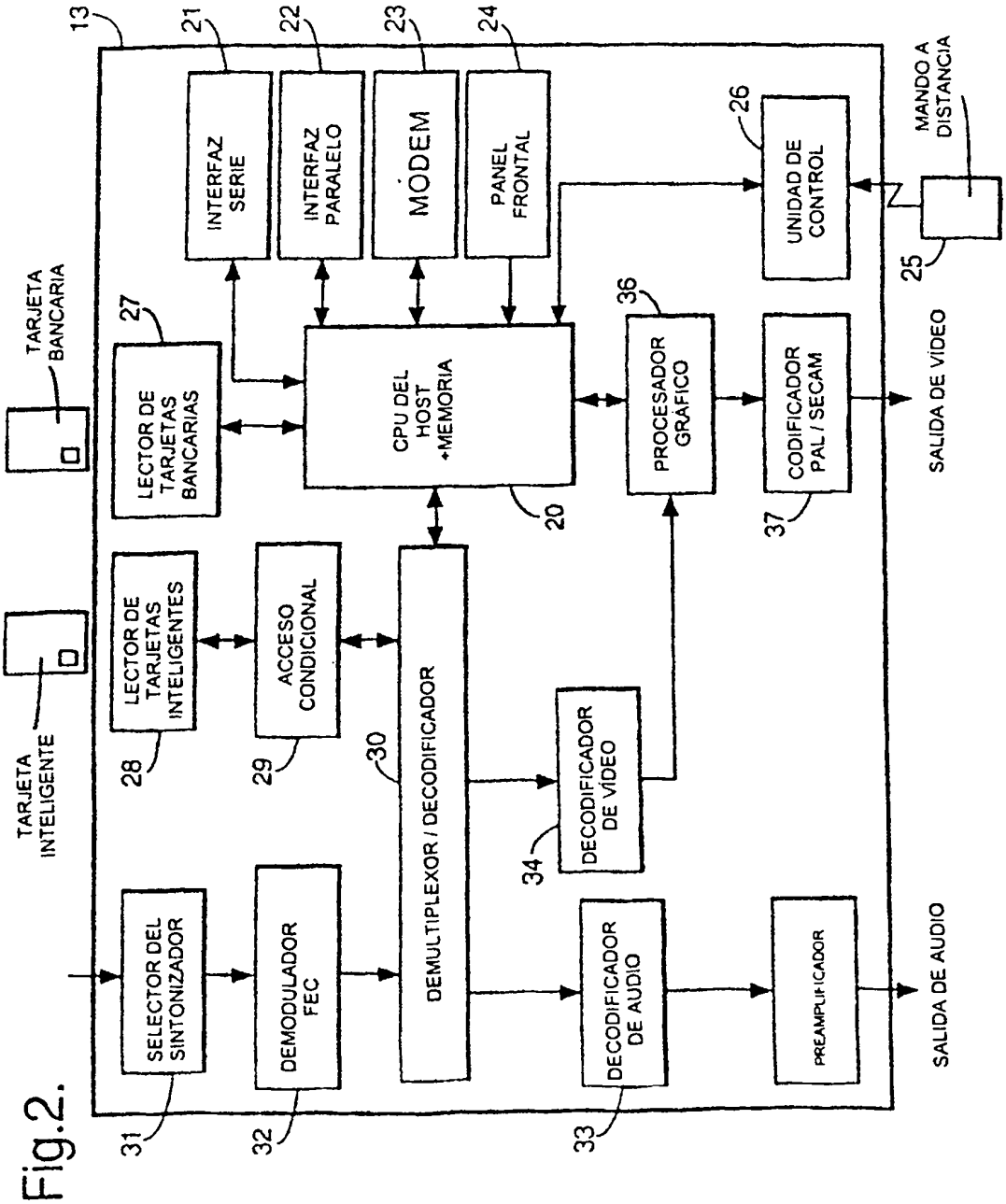

13
21
22
23
24
INTERFAZ SERIE
INTERFAZ PARALELO
MÓDEM
PANEL FRONTAL
26
UNIDAD DE CONTROL
MANDO A DISTANCIA
25
TARJETA BANCARIA
27
LECTOR DE TARJETAS BANCARIAS
CPU DEL HOST +MEMORIA
20
36
PROCESADOR GRÁFICO
CODIFICADOR PAL / SECAM
37
SALIDA DE VÍDEO
TARJETA INTELIGENTE
LECTOR DE TARJETAS INTELIGENTES
28
ACCESO CONDICIONAL
29
30
DEMULTIPLEXOR / DECODIFICADOR
DECODIFICADOR DE VÍDEO
34
SELECTOR DEL SINTONIZADOR
31
DEMODULADOR FEC
32
DECODIFICADOR DE AUDIO
33
PREAMPLIFICADOR
SALIDA DE AUDIO

Fig.2.

Fig.3.

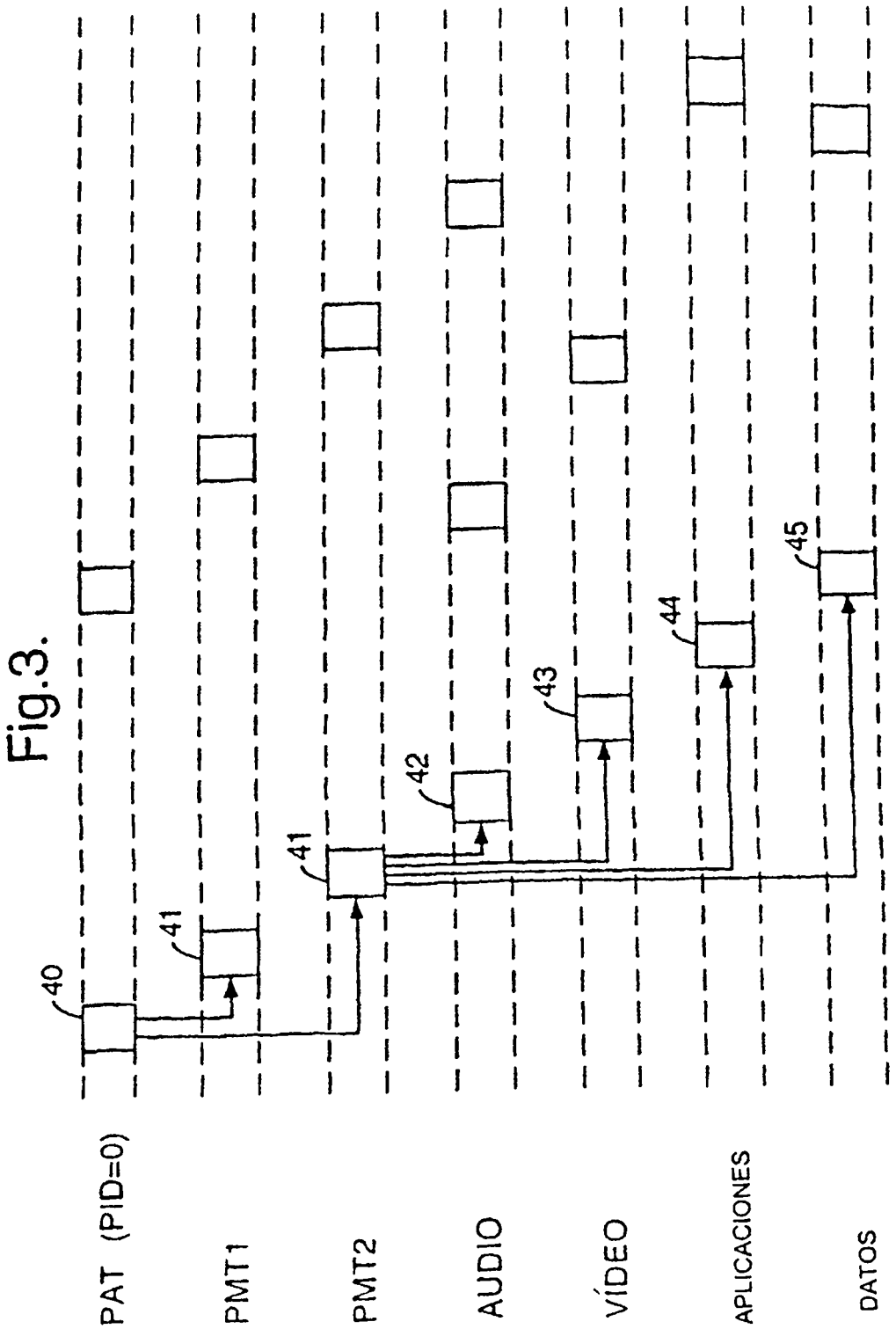

PAT (PID=0)
PMT1
PMT2
AUDIO
VÍDEO
APLICACIONES
DATOS
40
41
41
42
43
44
45

Fig.4.

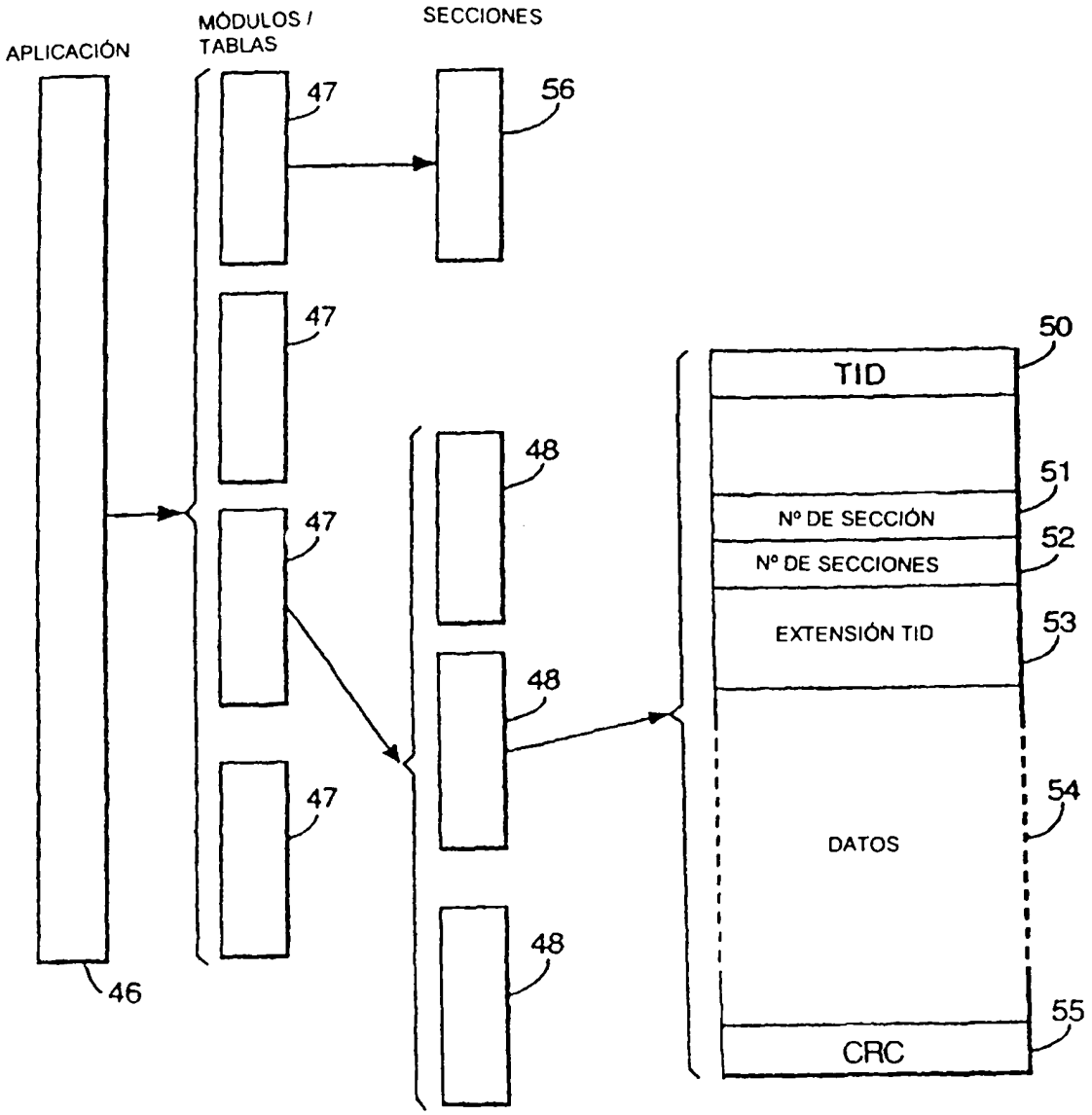
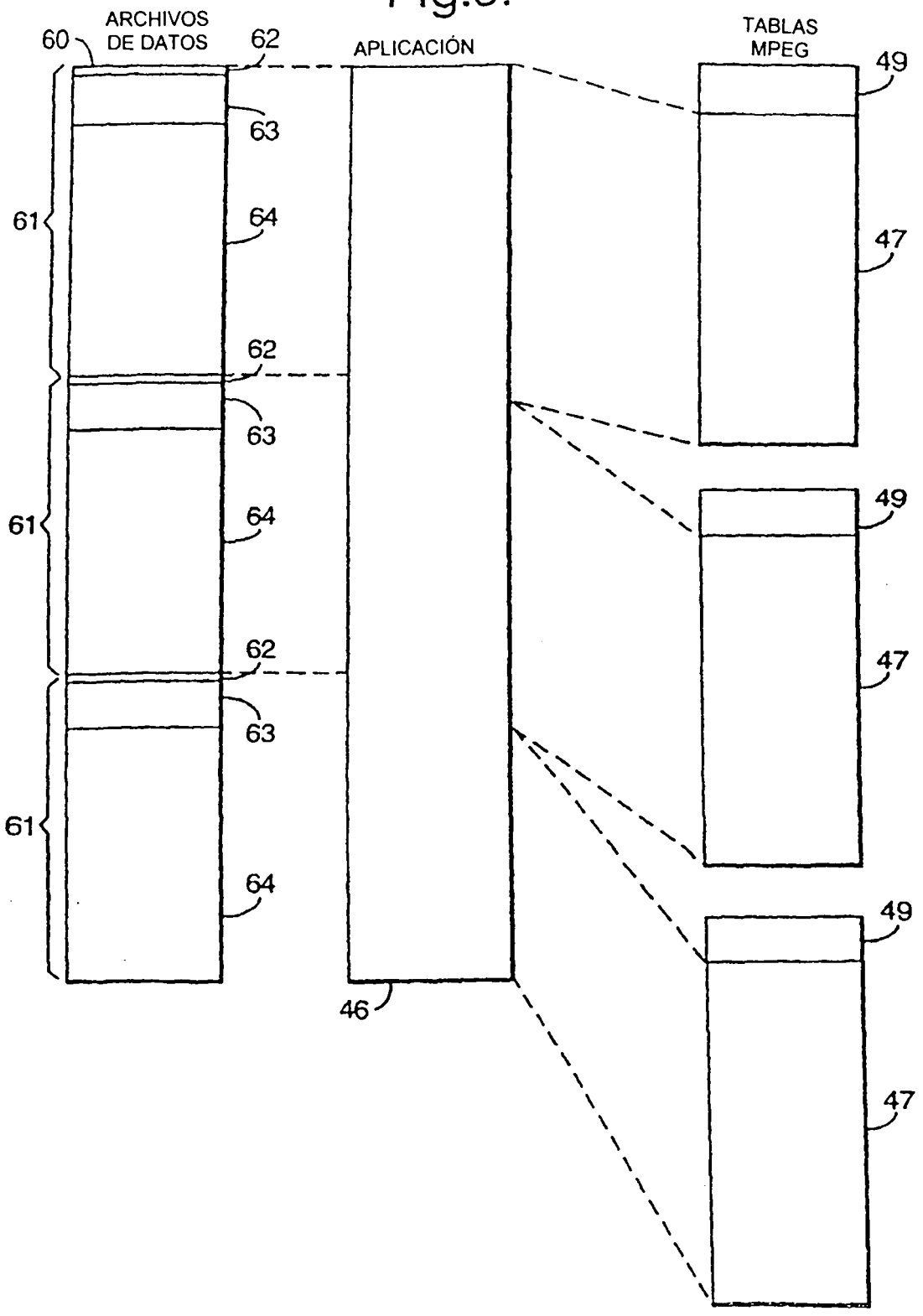

APLICACIÓN
MÓDULOS / TABLAS
SECCIONES
47
47
47
47
56
48
48
48
46
50
TID
51
Nº DE SECCIÓN
52
Nº DE SECCIONES
53
EXTENSIÓN TID
54
DATOS
55
CRC

Fig.5.


ARCHIVOS DE DATOS
60
62
63
64
61
62
63
64
61
62
63
64
61
APLICACIÓN
46
TABLAS MPEG
49
47
49
47
49
47

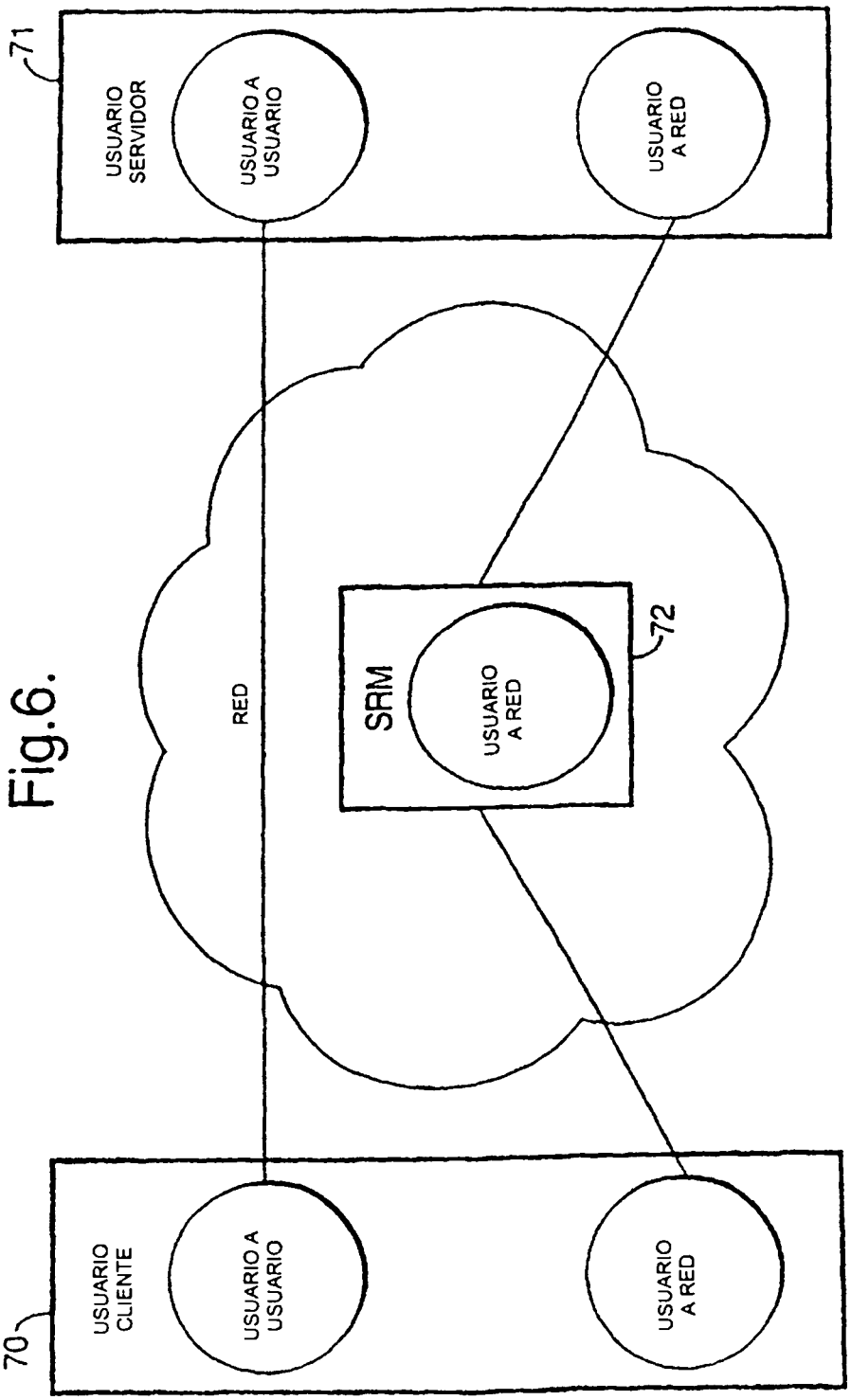

71
USUARIO SERVIDOR
USUARIO A USUARIO
USUARIO A RED
RED
SRM
USUARIO A RED
72
70
USUARIO CLIENTE
USUARIO A USUARIO
USUARIO A RED

Fig.6.

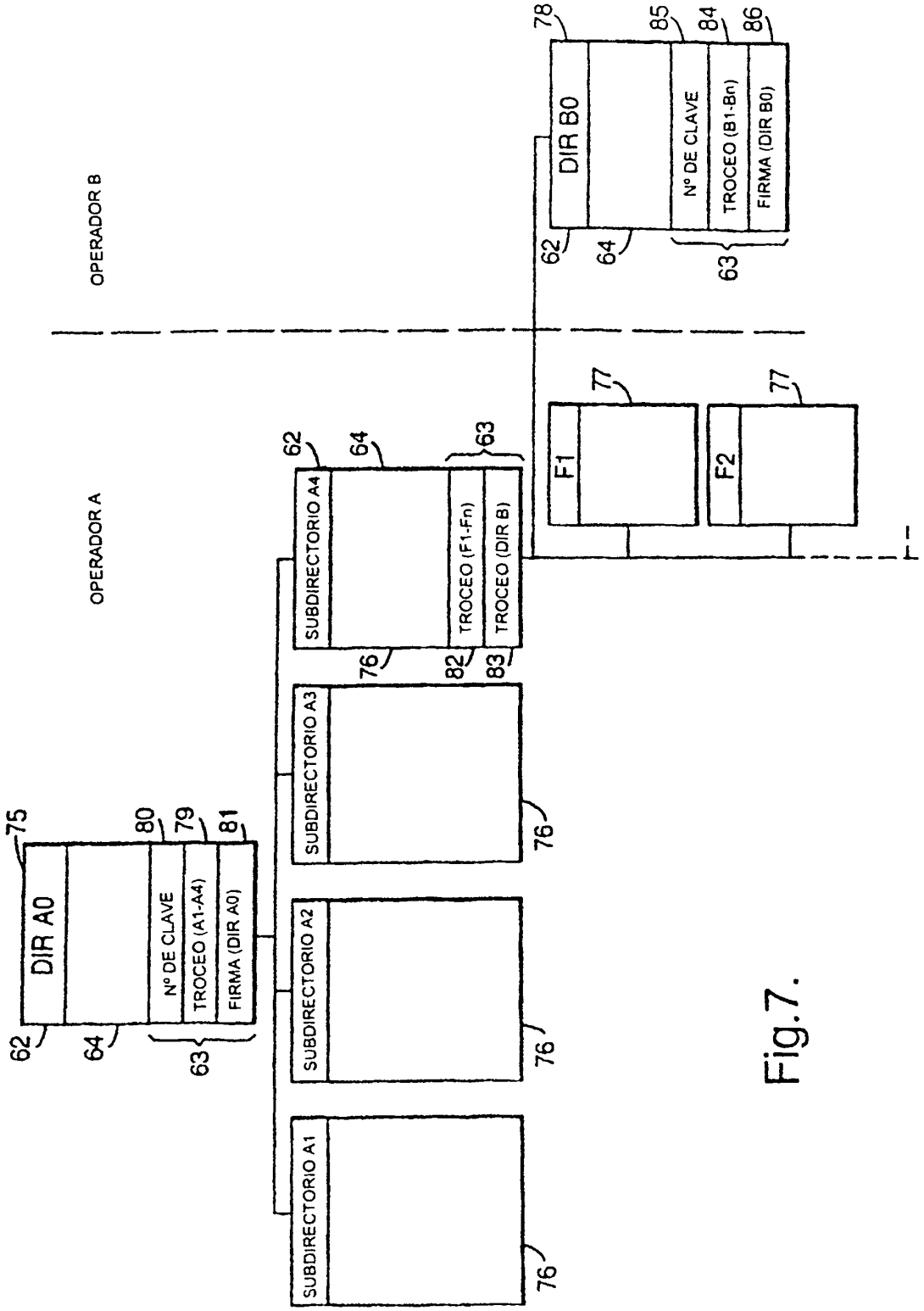

OPERADOR B
OPERADOR A
DIR B0
Nº DE CLAVE
TROCEO (B1-Bn)
FIRMA (DIR B0)
F1
F2
SUBDIRECTORIO A4
TROCEO (F1-Fn)
TROCEO (DIR B)
SUBDIRECTORIO A3
SUBDIRECTORIO A2
SUBDIRECTORIO A1
DIR A0
Nº DE CLAVE
TROCEO (A1-A4)
FIRMA (DIR A0)
62
63
64
75
76
77
78
79
80
81
82
83
84
85
86

Fig.7.