

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 625 896**

51 Int. Cl.:

H04N 21/258 (2011.01) **H04N 7/173** (2011.01)
H04N 21/266 (2011.01)
H04N 21/414 (2011.01)
H04N 21/418 (2011.01)
H04N 21/426 (2011.01)
H04N 21/4623 (2011.01)
H04N 21/61 (2011.01)
H04N 21/658 (2011.01)
H04N 21/6583 (2011.01)
H04N 7/16 (2011.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

- 86 Fecha de presentación y número de la solicitud internacional: **21.11.2003 PCT/EP2003/050866**
- 87 Fecha y número de publicación internacional: **17.06.2004 WO 2004/052004**
- 96 Fecha de presentación y número de la solicitud europea: **21.11.2003 E 03796037 (4)**
- 97 Fecha y número de publicación de la concesión europea: **08.03.2017 EP 1568226**

54 Título: **Mensajería a través de una red de telefonía móvil para una red multimedia digital**

30 Prioridad:

02.12.2002 EP 02292960

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

20.07.2017

73 Titular/es:

**NAGRA FRANCE SAS (100.0%)
86, rue Henri Farman
92130 Issy-les-Moulineaux, FR**

72 Inventor/es:

WENDLING, BERTRAND

74 Agente/Representante:

TOMAS GIL, Tesifonte Enrique

ES 2 625 896 T3

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

DESCRIPCIÓN

Mensajería a través de una red de telefonía móvil para una red multimedia digital

5 Campo de la invención

[0001] La invención se refiere a la gestión de derechos de acceso en una red multimedia digital.

Antecedentes de la invención

10

[0002] La Fig. 1 ilustra esquemáticamente un ejemplo de una red multimedia digital. Una red 1 se utiliza para intercambiar información entre uno o muchos operadores de difusión, representado(s) en los recuadros 2 y 3, y abonados representados en los recuadros 4 a 6. La red puede ser, por ejemplo, una red de difusión de televisión terrestre donde los operadores de difusión emiten señales que son recibidas mediante una antena de televisión por el abonado. Otro ejemplo de red puede ser una red por cable, o una red de transmisión por satélite.

15

[0003] Cada operador de difusión puede emitir varios servicios multimedia digitales a los abonados. Los servicios multimedia pueden incluir, por ejemplo, programas de televisión, programas radiofónicos y aplicaciones interactivas.

20

[0004] Cada abonado tiene un decodificador receptor que se usa para recibir los servicios multimedia y, en algunos casos, para procesar los servicios multimedia recibidos para reproducir los servicios multimedia en un dispositivo de reproducción según sea apropiado. Un programa de televisión puede, por ejemplo, ser reproducido en un televisor, y una aplicación interactiva puede precisar ser ejecutada por un sistema de procesamiento del decodificador receptor y generar una interactividad con el abonado.

25

[0005] Típicamente, todos los servicios multimedia digitales son recibidos por todos los abonados. Más generalmente, toda la información difundida por los operadores de difusión a través de la red puede ser potencialmente recibida por todos los abonados.

30

[0006] Se conoce limitar el acceso a los servicios multimedia atribuyendo derechos de acceso a los abonados. Por lo tanto, un abonado sólo puede acceder a los servicios multimedia para los que posee los derechos de acceso correspondientes.

35

Un grado más alto de acceso restringido a los servicios multimedia se puede conseguir mediante la aleatorización de un servicio utilizando una palabra de control. En este caso, el abonado sólo puede acceder y desaleatorizar el servicio aleatorizado si posee la palabra de control.

40

[0007] La información de derechos de acceso se puede enviar a los abonados 4-6 a través de la red 1. Típicamente, la palabra de control se envía a todos los abonados utilizando un mensaje de control de derechos o "Entitlement Control Message" (ECM). Sin embargo, la palabra de control sólo se puede extraer del ECM si el abonado tiene acceso a una clave de explotación que se emite periódicamente a través de la red en un mensaje de gestión de derechos (EMM).

45

[0008] La publicación de la solicitud internacional WO01/17249A1 de DEUTSCHE TELECOM AG trata sobre un método para emitir autorizaciones específicas para el cliente utilizando módulos de seguridad en sistemas de acceso condicional para dispositivos cargables. WO01/17249A1 describe la transmisión de EMM a los abonados. Una primera posibilidad permite la transmisión de un EMM utilizando una red telefónica pública conmutada (RTPC), una red de telefonía móvil tal como una red GSM, o cualquier otra forma de difusión para transmitir el EMM a un dispositivo de control de un vendedor. El vendedor usa a su vez el dispositivo de control para transmitir el EMM a un dispositivo de abonado para activar una suscripción. Se dice que la primera posibilidad es indirecta porque requiere una intervención de un intermediario entre un proveedor y el abonado, en este caso el vendedor. Una segunda posibilidad permite la transmisión del EMM directamente por difusión al dispositivo de abonado. Una localización geográfica del dispositivo del abonado se puede efectuar mediante la explotación de los datos de localización con respecto a un dispositivo GSM de abonado. Un proveedor de red GSM tiene la posibilidad de determinar una localización geográfica de un dispositivo GSM del abonado si este dispositivo está encendido. El conocimiento de la localización geográfica del dispositivo del abonado puede permitir limitar la difusión del EMM a una localización geográfica restringida, si es posible. La segunda posibilidad también menciona una forma de realización según la cual el abonado primero llama al proveedor EMM usando su teléfono GSM y obtiene posteriormente el EMM por difusión.

50

55

60

[0009] WO01/17249A1 describe la posibilidad de usar la red de telefonía GSM para transmitir un EMM a un abonado. Sin embargo WO01/17249A1 aconseja no usar la red de telefonía GSM para este propósito.

65

[0010] La publicación *Functional model of a conditional access system*, EBU Technical review, Winter 1995 describe en el párrafo 7.2.1 que sería posible establecer una vía de retorno entre el decodificador de un abonado y un sistema de administración de abonados (SMS) usando la RTPC o una red por cable, y usar esta vía de

retorno para transmitir EMM. Una razón para utilizar una vía de retorno sería reducir el ancho de banda de difusión consumido por la difusión de EMM.

Resumen de la invención

5

[0011] En un primer aspecto, la invención proporciona un método para distribuir un mensaje a partir de un servicio de administración de mensajes a un decodificador receptor de abonado de una red multimedia digital. Un mensaje determinado para un decodificador receptor determinado se transfiere desde el servicio de administración de mensajes hasta un sistema de comunicación de punto a punto distinto de la red multimedia.

10

Se determina un punto de destino de un receptor en el sistema de comunicación de punto a punto que corresponde con el decodificador receptor determinado. El mensaje determinado se almacena temporalmente en el sistema de comunicación de punto a punto, y el mensaje determinado recuperado en el decodificador receptor determinado desde el receptor.

15

[0012] Preferiblemente, el mensaje determinado se almacena temporalmente en un punto emisor en el sistema de comunicación de punto a punto, que corresponde con el servicio de administración de mensajes. Una señal de disponibilidad se genera en el receptor. Tras la recepción de la señal de disponibilidad, se activa una emisión del mensaje determinado, y el mensaje determinado se emite al receptor.

20

[0013] En un segundo aspecto, la invención proporciona un método para recibir un mensaje de gestión de derechos (EMM) determinado a un decodificador receptor de abonado determinado en una red multimedia digital. El decodificador receptor de abonado determinado está habilitado para recibir información a través de una red de comunicación de telefonía móvil diferente de la red multimedia digital. Un mensaje que contiene al menos el EMM determinado se recibe en un módem de telefonía móvil del decodificador receptor, el mensaje estando dirigido específicamente al módem de telefonía móvil del decodificador receptor determinado. Al menos el EMM se almacena en un almacenamiento del módem de telefonía móvil.

25

30

[0014] En un tercer aspecto, la invención proporciona un decodificador receptor para una red multimedia digital, que comprende un módem de telefonía móvil conectado operativamente al decodificador receptor, y una dirección de punto de destino atribuida únicamente al módem de telefonía móvil. El receptor comprende además un espacio de almacenamiento en el módem de telefonía móvil para memorizar al menos un mensaje de gestión de derechos (EMM).

Breve descripción de las figuras

35

[0015] La invención se describirá con mayor detalle a continuación en referencia a los dibujos anexos, en los cuales

40

la Fig. 1 contiene una representación esquemática de una red multimedia digital,

la Fig. 2 ilustra un sistema de difusión y receptor para una red multimedia digital,

45

la Fig. 3 contiene una representación esquemática de un sistema de acceso condicional aplicado a un sistema de recepción de difusión,

la Fig. 4 ilustra un ejemplo de un mensaje de gestión de derechos,

la Fig. 5 contiene un diagrama de bloques que representa un ejemplo de un decodificador receptor,

45

la Fig. 6 contiene una representación esquemática de un ejemplo de forma de realización de la invención,

la Fig. 7 contiene un organigrama que ilustra un ejemplo de forma de realización de la invención

Descripción de las formas de realización preferidas

Resumen del sistema

50

[0016] Se usarán las mismas referencias para hacer referencia a los mismos elementos de las figuras a lo largo de toda la descripción.

55

[0017] La Fig. 2 contiene una ilustración esquemática de un sistema de televisión digital. En un lado de un emisor, un sistema de compresión de señal 100 comprende un flujo de señal digital (no mostrado) y emite un flujo comprimido a un multiplexor 101. Un ejemplo de compresión es el ampliamente conocido estándar MPEG-2, que es de uso extendido en el campo de servicios de televisión digital. El multiplexor 101 produce un flujo de transporte de señales comprimidas que se transmite a un abonado que tiene un decodificador receptor 102.

60

El flujo de transporte se emite utilizando una antena a un satélite 104 y, posteriormente, es enviado a una antena de recepción 105 que está conectada a una entrada del decodificador receptor 102. La Fig. 2 ilustra un sistema de transmisión por satélite, pero se puede utilizar cualquier otra forma de transmitir el flujo de transporte del lado del locutor al abonado.

65

[0018] El decodificador receptor 102 procesa el flujo de transporte recibido para extraer datos, como por ejemplo un servicio audio/visual o una aplicación, y emite las señales de vídeo y audio resultantes a un dispositivo de

reproducción, como por ejemplo un televisor 106. En el presente ejemplo, el decodificador receptor 102 puede descodificar el flujo MPEG-2 comprimido en una señal de televisión emitida al televisor 106.

5 [0019] Aunque se muestra un decodificador receptor separado 102, el decodificador receptor también puede ser una parte integral de un televisor digital.

10 [0020] En un sistema multicanal, el multiplexor 101 puede administrar información de audio y de vídeo proporcionada simultáneamente por una pluralidad de fuentes. Además de información de audio y vídeo, cualquier otro tipo de información, por ejemplo, mensajes o aplicaciones, se pueden introducir en uno o más de los canales, entrelazados con la información de audio y de vídeo.

15 [0021] La Fig. 3 ilustra el sistema de televisión digital de la Fig. 2 mejorado con varios dispositivos de seguridad. Para una mayor legibilidad, los elementos de transmisión de difusión de la Fig. 2 se han sustituido por una flecha punteada 200 en la Fig. 3. Un sistema de acceso condicional 201 está conectado al multiplexor 101. Otro componente de acceso condicional 202 está conectado al decodificador receptor 102. El sistema de acceso condicional 201 y el otro componente de acceso condicional 202 permiten un acceso protegido en el decodificador receptor 102 a servicios de televisión digital emitidos por uno o muchos proveedores de difusión. El otro componente de acceso condicional 202 está completado por una tarjeta inteligente hija 203 que se inserta en una ubicación apropiada del decodificador receptor 102. La tarjeta inteligente hija 203 lleva información requerida para desaleatorizar mensajes aleatorizados relacionados con ofertas comerciales disponibles. La información puede comprender derechos de suscripción, una o más claves de explotación extraídas de EMM recibidos y una o más palabras de control extraídas de ECM. Al utilizar la tarjeta inteligente hija 203, es posible comprar ofertas comerciales por medio de suscripción o pago por visión.

25 [0022] Los servicios digitales incluidos en el flujo de datos digital son aleatorizados en un nivel del multiplexor 101, bajo el control del sistema de acceso condicional 201. Típicamente, la aleatorización se hace utilizando una palabra de control, está última siendo transmitida junto con los servicios digitales aleatorizados para una futura desaleatorización. La propia palabra de control se encripta para la transmisión, y dicha encriptación se hace con una clave de explotación.

30 [0023] El sistema de acceso condicional 201 comprende un sistema de autorización de abonado (SAS) 204, que está conectado con un sistema o sistemas de gestión de abonado (SMS) 205. El SMS 205 y el SAS 204 pueden estar conectados, por ejemplo usando un enlace TCP/IP. Típicamente, hay un SMS 205 por operador de difusión, pero puede suceder que el SMS 205 sea compartido por más de un operador de difusión.

35 [0024] El sistema de acceso condicional 201 comprende además una primera unidad de cifrado 206 que hace uso de una primera tarjeta inteligente madre 207, y está conectado al SAS 204. La primera tarjeta inteligente madre 207 almacena información confidencial que se usa para encriptar datos.

40 [0025] Una segunda unidad de cifrado 208 que usa una segunda tarjeta inteligente madre 209 está conectada al multiplexor 101.

Sistema de administración de abonados

45 [0026] El SMS 205 incluye una base de datos que administra, entre otros, ficheros de abonado, datos de ofertas comerciales incluyendo tarifas y ofertas especiales, detalles de pago por visión, autorización y datos de consumo.

50 [0027] El SMS 205 puede ser remoto respecto al SAS 204.

[0028] El SMS 205 transmite mensajes al SAS 204 relacionados, por ejemplo, con unas autorizaciones del abonado para ver un servicio digital cuando tal servicio digital es solicitado por el abonado, o a las tarifas de un servicio digital adquirido y que ha de ser pagado por el abonado.

55 [0029] Por otro lado, el SAS 204 puede enviar mensajes al SMS 205 relacionados, por ejemplo, con solicitudes acerca de una identificación de contacto del abonado.

Mensaje de gestión de derechos (EMM)

60 [0030] El EMM es un mensaje destinado a un abonado individual, o un grupo de abonados. Esto contrasta con el ECM, que generalmente está destinado a uno o a un número determinado de servicio(s) digital(es) aleatorizado(s) en lugar de estar destinado a uno o muchos abonados.

65 [0031] Varios tipos específicos de EMM son posibles. A continuación, se describen 4 ejemplos de tipos de EMM, a saber EMM individuales, grupales, de público y únicos.

[0032] Un EMM individual está destinado a un abonado individual, y típicamente se puede usar cuando se suministra un servicio de pago por visión. El EMM individual comprende un identificador de grupo y una posición del abonado individual en el grupo.

5 [0033] Un EMM grupal está destinado a un grupo de abonados, por ejemplo 256 abonados individuales, y típicamente se usa para administrar servicios de suscripción.

[0034] Un EMM de público está destinado a un público entero de abonados individuales. El público comprende todos los abonados individuales que tienen una tarjeta inteligente que lleva un mismo identificador de operador.

10 [0035] Un EMM único está destinado ser direccionado a un identificador único de una tarjeta inteligente.

[0036] La Fig. 4 ilustra un ejemplo de una forma general de un EMM. El EMM se implementa como una serie de bits de datos digitales y comprende un encabezado 400, un EMM completo 401 y una firma 402. El encabezado 400 comprende a su vez un identificador de tipo 403 que identifica el mensaje como un EMM y también indica el tipo de EMM, un identificador de longitud 404 que da una longitud del EMM, una dirección opcional 405 para el EMM, un identificador de operador 406, y un identificador de clave 407. La firma 402 es opcional y proporciona un número de verificaciones contra la corrupción de los bits de datos en el EMM.

15 [0037] El EMM completo comprende datos acerca de la autorización del abonado y de una o muchas claves de explotación.

Sistema de autorización de abonado (SAS)

20 [0038] En referencia nuevamente a la Fig. 3, el SAS 204 recibe y procesa mensajes procedentes del SMS 205. El SAS 204 genera mensajes que acusan recibo de los mensajes generados por el SMS 205 y pasa estos mensajes de acuse de recibo al SMS 205.

25 [0039] Los mensajes recibidos del SMS 205 tratan sobre, por ejemplo, una suspensión de unos derechos del abonado en el caso de que el abonado no haya pagado su cuota de suscripción, una modificación de derechos del abonado para añadir o eliminar una oferta comercial, o una adición de derechos que se requieren para acceder un servicio digital de pago por visión específico.

30 [0040] El SAS 204 administra una base de datos que almacena un estado para cada abonado declarado previamente por el SMS 205. Según el estado y otras informaciones recibidas desde el SMS 205, el SAS 204 genera uno o más EMM para la tarjeta inteligente del abonado 203. Los EMM son cifrados utilizando la primera unidad de cifrado 206.

35 [0041] En los sistemas de red conocidos del estado de la técnica, el SAS 204 asegura que los EMM sean recibidos por el abonado enviando los EMM cíclicamente al multiplexor 101 para difundirlos al abonado. Una frecuencia del ciclo depende del tipo de EMM, y típicamente puede tener un valor de entre 30 segundos y 30 minutos.

40 [0042] Los EMM se envían al multiplexor 101 a través de un dispositivo comúnmente conocido como inyector (no mostrado en la fig. 3). El inyector es ampliamente conocido en la técnica y no se describirá más en este documento.

Mensaje de control de derechos (ECM)

45 [0043] En referencia nuevamente a la Fig. 3, el multiplexor 101 contiene típicamente un aleatorizador que se usa para aleatorizar servicios digitales que se van a difundir. El aleatorizador genera una palabra de control que se usará en el proceso de aleatorización y se transmitirá con el servicio digital aleatorizado al abonado.

50 [0044] Un servicio digital también puede estar sometido a criterios de acceso que, por ejemplo, asocian el servicio digital a una oferta comercial determinada. Los criterios de acceso deberían corresponder con una suscripción del abonado a la oferta comercial determinada para que el servicio digital se vuelva accesible al abonado.

55 [0045] Tanto la palabra de control como el criterio de acceso se insertan en un ECM que se difunde junto con el servicio digital aleatorizado. La inserción se hace mediante la transmisión de la palabra de control y del criterio de acceso a la segunda unidad de cifrado 208 donde el ECM es generado, aleatorizado utilizando una clave de explotación almacenada en la segunda tarjeta inteligente madre 209 y transmitido de nuevo al multiplexor 101.

60 [0046] El servicio digital es aleatorizado por el aleatorizador utilizando la palabra de control. Posteriormente, el servicio digital aleatorizado y el ECM aleatorizado son difundidos al abonado.

65

Decodificador receptor

[0047] En referencia a la Fig. 5, se proporciona una visión de conjunto para varios elementos en una forma de realización del decodificador receptor 102, mostrados aquí como bloques funcionales.

[0048] El decodificador receptor 102 también se denomina a veces Set Top Box (STB). El decodificador receptor 102 comprende un procesador central 500 que incluye elementos de memoria asociados. El procesador central 500 está adaptado para recibir datos de entrada a partir de una interfaz en serie 501, una interfaz paralela 502, un módem 503 y contactos de conmutación 504 situados en un panel del decodificador receptor 102.

[0049] El decodificador receptor también está adaptado para recibir entradas a partir de un control remoto infrarrojo 505 a través de una unidad de control 506, y comprende uno o muchos lectores de tarjeta inteligente 507 y 508 que permiten leer una tarjeta bancaria inteligente 509 o la tarjeta inteligente hija 203.

La tarjeta inteligente hija 203 interactúa con el lector de tarjeta inteligente 507 y el otro componente de acceso condicional 202 para suministrar la palabra de control necesaria a un demultiplexor / desaleatorizador 510 y, por lo tanto, permitir que la señal de difusión encriptada sea desaleatorizada.

[0050] El decodificador receptor 102 comprende además un sintonizador convencional 511 y un desmodulador 512 para recibir y desmodular la señal difundida antes de su procesamiento por el demultiplexor / desaleatorizador 510.

[0051] La señal desenscriptada en una emisión del demultiplexor / desaleatorizador 511 se procesa como apropiada por un decodificador 513 y preamplificador 514 de audio antes de ser hecha disponible en una emisión de audio 515, y por un decodificador de vídeo 516, antes de ser transmitida a un procesador gráfico 517 y codificador en un codificador PAL/SECAM 518 y hecha disponible en una emisión de vídeo 519.

Transmisión cíclica de EMM

[0052] Tal y como se ha mencionado anteriormente en esta especificación, los EMM de sistemas del estado de la técnica son permanentemente difundidos a los abonados en modo de carrusel, es decir, son transmitidos cíclicamente, en todos los medios de difusión. Esto se hace para asegurar que, independientemente de un estado de un decodificador receptor y de una ubicación geográfica del decodificador receptor, tan pronto como el decodificador receptor se enciende, éste sea capaz de recibir el EMM relativo para un periodo de suscripción futuro.

[0053] El uso de la transmisión cíclica usa una cantidad relativamente grande de ancho de banda de difusión. Además, resulta imposible saber si o cuándo un decodificador receptor determinado ha recibido un EMM.

[0054] Un periodo de ciclo de la difusión de EMM ha de ser razonablemente corto para evitar que haya un plazo de espera largo hasta la recepción del EMM por un decodificador receptor que ha estado apagado durante un periodo de tiempo extendido.

[0055] Se conoce la reducción del ancho de banda de difusión requerido para la difusión de EMM usando EMM de grupo que pueden llegar a más de un usuario.

[0056] En el estándar de difusión ampliamente conocido DVB, un EMM se difunde típicamente como un mensaje con un número de identificación determinado específico. Ya que el EMM puede ser recibido por cualquiera que reciba la difusión, es potencialmente posible analizar los mensajes recibidos que tengan el número de identificación determinado específico para reunir información acerca de los EMM y un esquema de seguridad relacionado. Esto, en algunos casos, puede debilitar el nivel de seguridad del sistema de difusión.

Transmisión de EMM a través de una red de telefonía móvil

[0057] Según la presente invención, los EMM se transmiten a los abonados utilizando una red de telefonía móvil en lugar de la red de difusión. La red de telefonía móvil permite una comunicación de punto a punto, es decir, se puede transmitir un mensaje de un punto emisor a una única dirección de punto de destino.

[0058] En referencia a la Fig. 6, se muestra un sistema en el que los EMM se transmiten a través de una red de telefonía móvil 600. El sistema de la Fig. 6 se basa en el sistema mostrado en la Fig. 3, y el decodificador receptor 202 se basa en el decodificador receptor mostrado en la Fig. 3 y Fig. 5. Para una mayor legibilidad, varios elementos mostrados en las figuras 3 y 5 no han sido representados en la Fig. 6.

[0059] El SAS 204 transmite los EMM a una base de datos de telefonía móvil 601 en lugar de transmitir los EMM a través de un inyector de EMM al multiplexor 101. Cada EMM está destinado a al menos un decodificador receptor determinado. El decodificador receptor determinado está relacionado con una dirección de la red de telefonía móvil, es decir, la dirección del punto de destino, que está almacenada en la base de datos de telefonía

móvil 601. Por consiguiente, la base de datos de telefonía móvil permite recuperar la dirección para el decodificador receptor determinado cuando recibe el EMM desde el SAS. La dirección se usará para enviar el EMM al decodificador receptor determinado.

5 [0060] El EMM y la dirección correspondiente del decodificador receptor determinado son posteriormente reenviados a la red de telefonía móvil 600, es decir, al punto emisor de la red de telefonía móvil, donde un sistema de gestión de red y un transmisor celular local (no mostrado) manda el EMM a un módem receptor de telefonía móvil 602 conectado a o integrado en el decodificador receptor 202, y que tiene la dirección correspondiente recibida con el EMM.

10 [0061] El EMM permanece almacenado temporalmente en la red de telefonía móvil o el módem receptor de telefonía móvil hasta que es recuperado por el decodificador receptor. Más precisamente, el EMM puede permanecer almacenado en el nivel de la red de telefonía móvil 600 si el módem receptor de telefonía móvil 602 no está disponible para recibir mensajes. Una vez el módem receptor de telefonía móvil 602 se vuelve disponible, es decir, el módem receptor de telefonía móvil 602 genera una señal que indica que está disponible, el EMM es transmitido. El EMM permanece almacenado en el módem receptor de telefonía móvil 602 hasta que es recuperado por el decodificador receptor. Este en particular es el caso cuando el decodificador receptor está desconectado o apagado por otros motivos.

15 [0062] Opcionalmente, el decodificador receptor 202 comprende un lector de tarjetas SIM 603 adaptado para leer una tarjeta SIM 604. La tarjeta SIM 604 contiene información requerida para administrar derechos de acceso para la red de telefonía móvil, derechos de acceso que son usados por el módem receptor de telefonía móvil 602.

20 [0063] Ventajosamente, los derechos de acceso para la red de telefonía móvil pueden estar incluidos en la tarjeta inteligente hija (no mostrada) en vez de en la tarjeta SIM 604.

25 [0064] El EMM específico es enviado sólo una vez desde el SAS 204 a la base de datos de telefonía móvil 601 y red de telefonía móvil 600. El EMM específico permanece en el sistema de telefonía móvil y sólo se transmite al módem 602 cuando este último está preparado recibir el EMM específico. Si para entonces el EMM específico se ha convertido en obsoleto, preferiblemente éste puede ser eliminado y/o sustituido sin haber sido previamente enviado al decodificador receptor 202.

30 [0065] Opcionalmente, el módem 602 puede devolver un mensaje de confirmación a la red de telefonía móvil después de la recepción del EMM específico. El mensaje de confirmación puede comprender datos adicionales tales como datos de decodificador receptor específicos o datos relacionados con la tarjeta inteligente hija en uso con el decodificador receptor 202. Un ejemplo de información comprendida en los datos adicionales se puede obtener utilizando uno o una pluralidad de elementos de la lista siguiente: estado del decodificador receptor, estado de la tarjeta inteligente hija, número(s) de identificación, versión de elementos contenidos en el decodificador receptor. La transmisión del mensaje de confirmación que comprende datos adicionales puede proporcionar un método que permite al locutor verificar parámetros del decodificador receptor y detectar un estado legal del decodificador receptor, es decir, un posible uso ilegal del decodificador receptor o de la tarjeta inteligente hija.

35 [0066] El EMM específico se puede transmitir al módem 602 introducido en un pequeño mensaje comúnmente conocido como SMS (servicio de mensajes cortos o Short Message Service, que no debe confundirse con el sistema de administración de abonados o Subscriber Management System) en las redes de telefonía móvil GSM. El SMS puede permanecer almacenado en un servidor de SMS de la red de telefonía móvil GSM si el módem receptor de telefonía móvil no está preparado o disponible para recibir mensajes.

40 [0067] Como resultado de la invención, el inyector de EMM conocido por estado de la técnica, que es usado por el SAS para inyectar EMM al multiplexor, puede ser omitido.

45 [0068] Opcionalmente, el módem GSM 602 también se puede usar junto con el decodificador receptor 202 para la comunicación a través de la red de telefonía móvil 600 mediante la emisión de llamadas de teléfono o el establecimiento de conexiones de datos. Para este propósito, el adaptador receptor 202 puede comprender dispositivos de entrada y salida de audio 605, incluyendo un micrófono.

50 [0069] Se ha hecho aparente que cada EMM se envía únicamente a su decodificador receptor asociado utilizando una red diferente de la red de difusión. Por consiguiente, la invención no usa un ancho de banda de difusión como en la técnica anterior. El EMM se puede enviar a través de la red de telefonía móvil en momentos convenientes cuando la capacidad de red es menos usada por los servicios de telefonía móvil convencionales. Como se sabe, en las redes de telefonía móvil, la información enviada al módem de telefonía móvil sólo se transmitirá dentro de un área geográfica que corresponde con una célula de transmisión en la que el módem telefónico está situado.

[0070] Ventajosamente, el decodificador receptor 202 no necesita explícitamente iniciar una conexión con el CAS 201 para recibir un EMM.

5 [0071] Opcionalmente el módem de telefonía móvil 602 se puede configurar para permanecer siempre en recepción no sólo de un EMM, sino también de cualquier otro tipo de información o servicio de telefonía móvil entrante si es necesario.

10 [0072] El sistema según la invención mejora la seguridad en que el EMM específico se envía sólo a un decodificador receptor. Se vuelve más difícil recibir y escuchar más de un EMM, como era el caso en la técnica anterior.

[0073] Los mensajes de confirmación opcionales mejoran la seguridad en el sistema en que el uso del EMM por un decodificador receptor determinado puede ser verificado.

15 [0074] El módem de telefonía móvil 602 se ha descrito como un módem GSM. Por supuesto, es posible usar cualquier otro tipo de módem dependiendo del estándar de la red de telefonía móvil, por ejemplo, GSM GPRS UMTS ...

[0075] La Fig. 7 muestra un diagrama de flujo que ilustra una forma de realización de la invención.

20 Un mensaje de gestión de derechos EMM_{D1} destinado a un decodificador receptor D1 se transfiere del SAS a la red de telefonía móvil (MPN) en una etapa 700. En una etapa siguiente 701, se determina una dirección de un receptor de telefonía móvil (receptor D1) para el decodificador receptor. En una etapa de decisión 702, la MPN verifica si el receptor D1 está preparado para recibir el EMM_{D1} . Si el receptor D1 no está preparado, entonces el EMM_{D1} se almacena temporalmente en el punto emisor de la MPN en la etapa 703. Posteriormente una etapa de
25 decisión 704 comprueba si el EMM_{D1} sigue siendo válido, por ejemplo, si una fecha de validez para el EMM_{D1} puede haber caducado. En el caso de que el EMM_{D1} no sea válido, se obtiene un nuevo EMM_{D1} en la etapa 705 y la etapa 700 se lleva a cabo nuevamente. En el caso de que el EMM_{D1} sea válido, la etapa de decisión 702 se realiza nuevamente.

30 [0076] Si en un lanzamiento de la etapa 702 se descubre que el receptor D1 está preparado, el EMM_{D1} se transmite al receptor D1 a través de la MPN en una etapa 706, y se almacena temporalmente en el receptor D1 en la etapa 707. En una etapa de decisión 708 se controla si el decodificador receptor D1 está preparado para recuperar el EMM_{D1} del receptor D1. Si este no es el caso, el EMM_{D1} permanece en almacenamiento temporal con el receptor D1. En caso afirmativo, el EMM_{D1} es recuperado del receptor D1 por el decodificador receptor D1
35 en una etapa 709. Posteriormente, un acuse de recibo para el EMM_{D1} se devuelve al punto emisor en la etapa 710, por ejemplo utilizando la MPN.

REIVINDICACIONES

1. Método para distribuir un mensaje desde un servicio de administración de mensajes (204) a un decodificador receptor de abonado (202) de una red multimedia digital, donde dicho método comprende:
- transferencia de un mensaje determinado para un decodificador receptor determinado desde el servicio de administración de mensajes a un sistema de comunicación de punto a punto (601, 600, 700) diferente de la red multimedia, donde el mensaje determinado incluye un mensaje de gestión de derechos (EMM) de la red multimedia digital,
 - determinación de una dirección de punto de destino de un receptor en el sistema de comunicación de punto a punto (701), que corresponde con el decodificador receptor determinado,
 - recepción (709) por el decodificador receptor del mensaje determinado desde el sistema de comunicación de punto a punto,
 - **caracterizado por el hecho de que** el sistema de comunicación de punto a punto es un sistema de comunicación de punto a punto móvil, y el método comprende además las etapas de:
 - almacenamiento temporal (703, 707) del mensaje determinado en el sistema de comunicación de punto a punto,
 - generación y transmisión, por el receptor, de una señal de disponibilidad al sistema de comunicación de punto a punto y, tras la recepción de dicha señal,
 - emisión del mensaje determinado al receptor,
 - generación de un acuse de recibo (710) en el receptor,
 - emisión del acuse de recibo (710) al sistema de comunicación de punto a punto móvil (601, 600, 700).
2. Método según la reivindicación 1, que comprende además
- recepción en el receptor del mensaje determinado,
 - almacenamiento temporal (707) en el receptor del mensaje determinado.
3. Método según la reivindicación 1, donde el acuse de recibo comprende uno o una pluralidad de elementos de información adicional del grupo siguiente: un estado del decodificador receptor, un estado de una tarjeta inteligente hija utilizada con el decodificador receptor, un número de versión de un elemento del decodificador receptor.
4. Método según la reivindicación 3, que comprende además
- extracción de un elemento de información adicional del acuse de recibo,
 - evaluación del elemento de información adicional para determinar un estado legal del decodificador receptor.
5. Método según cualquiera de las reivindicaciones 1 a 4, donde el sistema de comunicación de punto a punto es una red de telefonía móvil.
6. Método según cualquiera de las reivindicaciones 1 a 5, donde el servicio de administración de mensajes está comprendido en un sistema de autorización de abonado.
7. Método para recibir un mensaje de gestión de derechos (EMM) determinado en un decodificador receptor de abonado determinado en una red multimedia digital, donde dicho mensaje de gestión de derechos concede autorización a la red multimedia digital, donde el decodificador receptor de abonado determinado está habilitado para recibir información a través de una red de comunicación telefónica diferente de la red multimedia digital, donde el método comprende:
- recepción (706, 707) en un módem del decodificador receptor de un mensaje que contiene al menos el EMM determinado, donde el mensaje está dirigido específicamente al módem del decodificador receptor determinado,
 - almacenamiento (707) de al menos el EMM en un almacenamiento del módem.
 - recuperación (709) del EMM del almacenamiento en el receptor determinado y
 - actualización de la autorización relacionada con la red multimedia digital basándose en los datos relacionados con la autorización de abonado contenida en el EMM
- caracterizado por el hecho de que** el sistema de comunicación de punto a punto es un sistema de comunicación de punto a punto móvil, y el módem es un módem de telefonía móvil, donde el método comprende además las etapas de:
- antes de la recepción del mensaje, generación y transmisión de una señal de disponibilidad al sistema de comunicación de punto a punto móvil y, una vez se ha recibido el mensaje,
 - generación de un acuse de recibo (710) en el receptor,
 - emisión del acuse de recibo (710) al sistema de comunicación de telefonía móvil.
8. Decodificador receptor para una red multimedia digital, donde el decodificador receptor comprende:
- un módem operativamente conectado al decodificador receptor,
 - una dirección de punto de destino únicamente atribuida al módem,

- un espacio de almacenamiento en el módem de telefonía móvil para almacenar al menos un mensaje de gestión de derechos (EMM) y
- medios para actualizar la autorización a la red multimedia digital basándose en los datos relacionados con la autorización de abonado contenida en el mensaje de gestión de derechos (EMM),

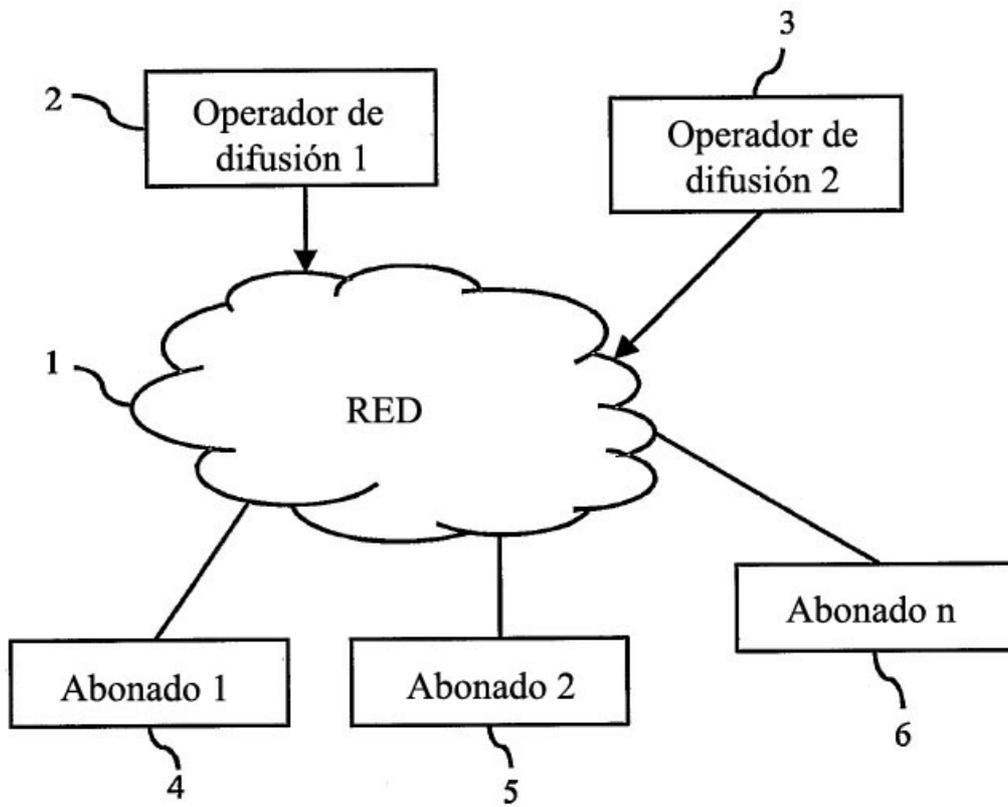
5 **caracterizado por el hecho de que** el módem es un módem de telefonía móvil y el decodificador receptor comprende además:

- medios para generar y transmitir una señal de disponibilidad a un sistema de comunicación de punto a punto móvil,
- medios para generar un acuse de recibo (710)
- medios para transmitir el acuse de recibo (710) al sistema de comunicación de punto a punto móvil.

10

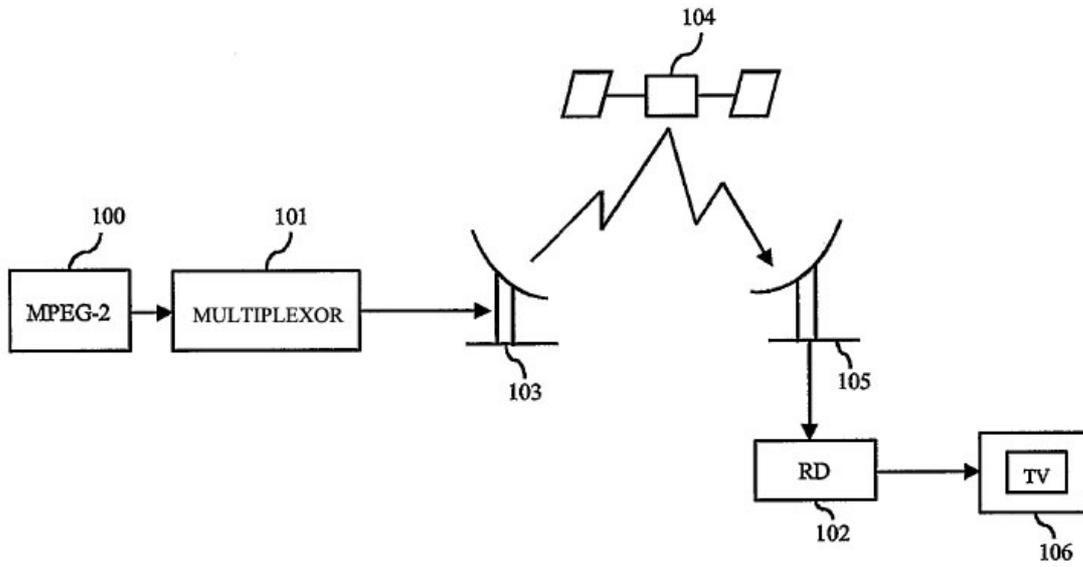
9. Decodificador receptor según la reivindicación 8, donde el módem de telefonía móvil recibe el EMM desde el sistema de comunicación de punto a punto móvil y almacena el EMM independientemente de un estado del decodificador receptor.

15



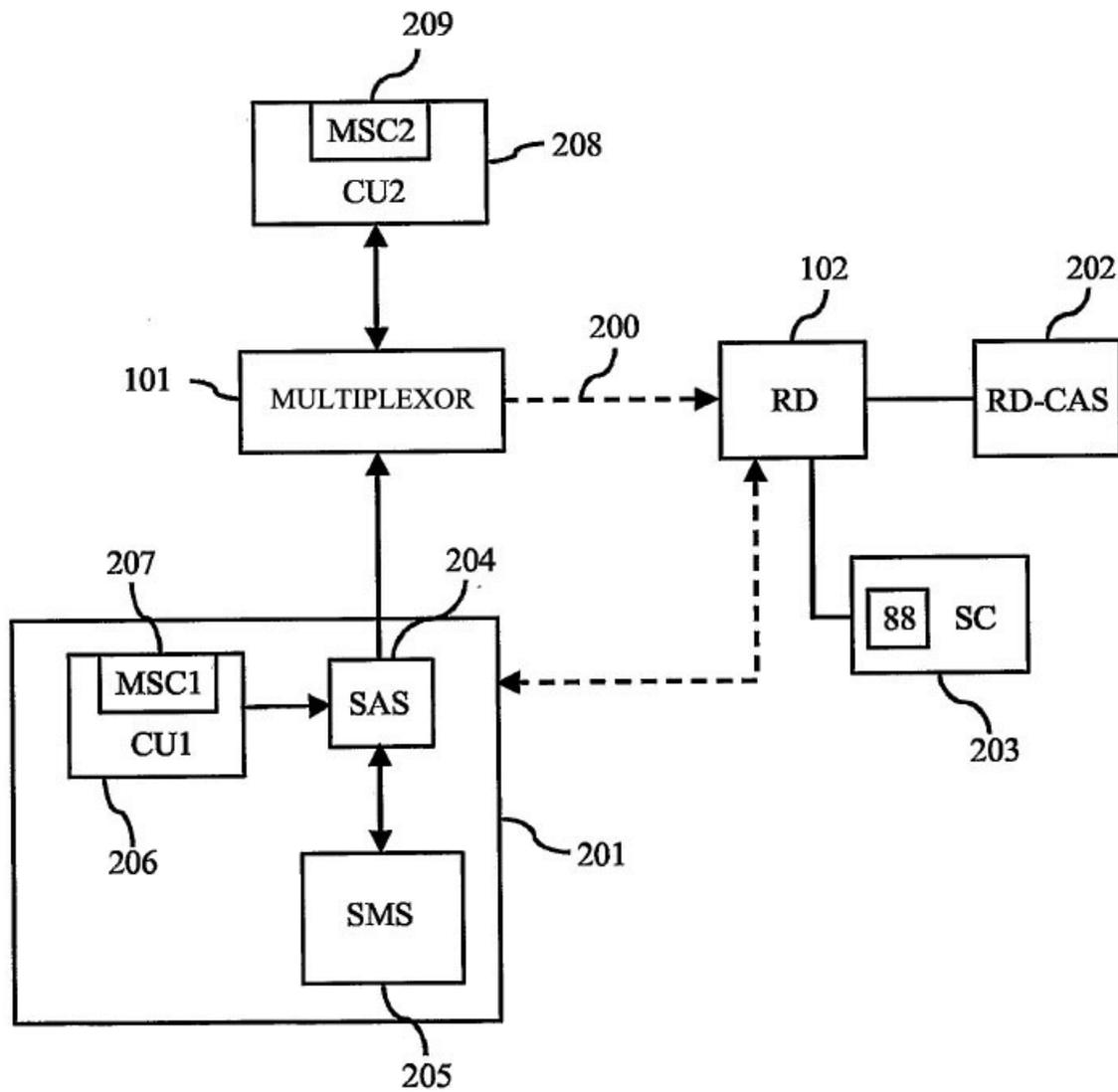
ESTADO DE LA TÉCNICA

FIG. 1



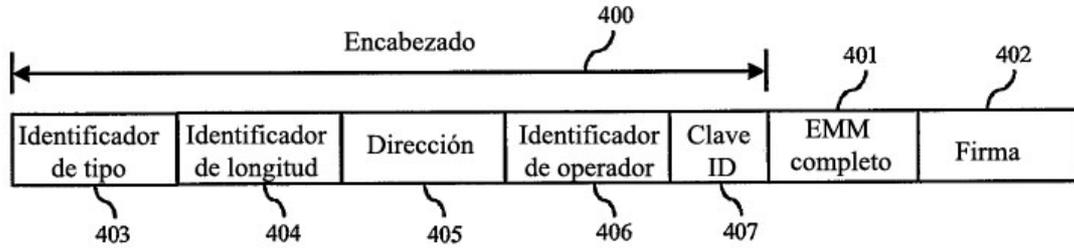
ESTADO DE LA TÉCNICA

FIG. 2



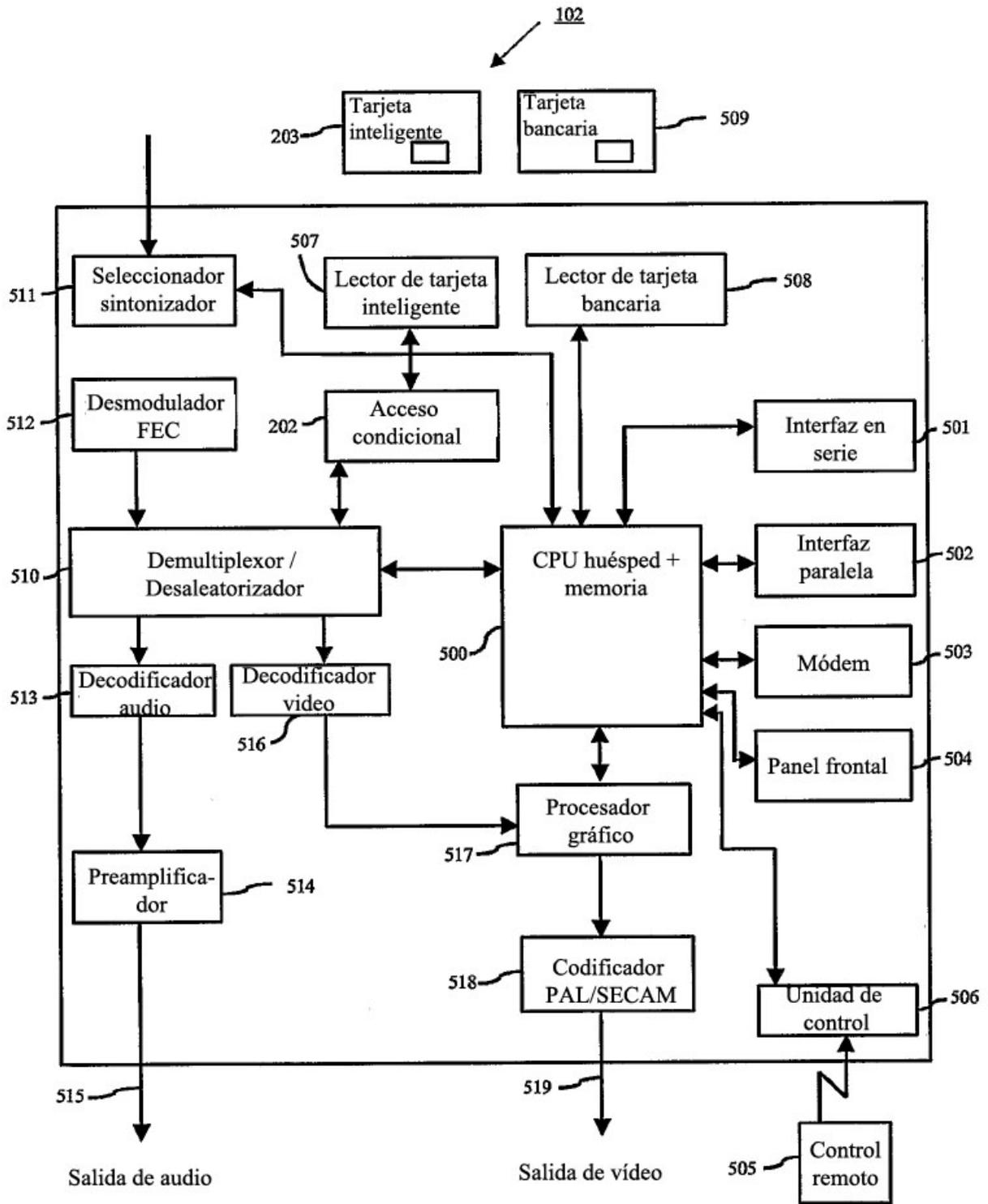
ESTADO DE LA TÉCNICA

FIG. 3



ESTADO DE LA TÉCNICA

FIG. 4



ESTADO DE LA TÉCNICA

FIG. 5

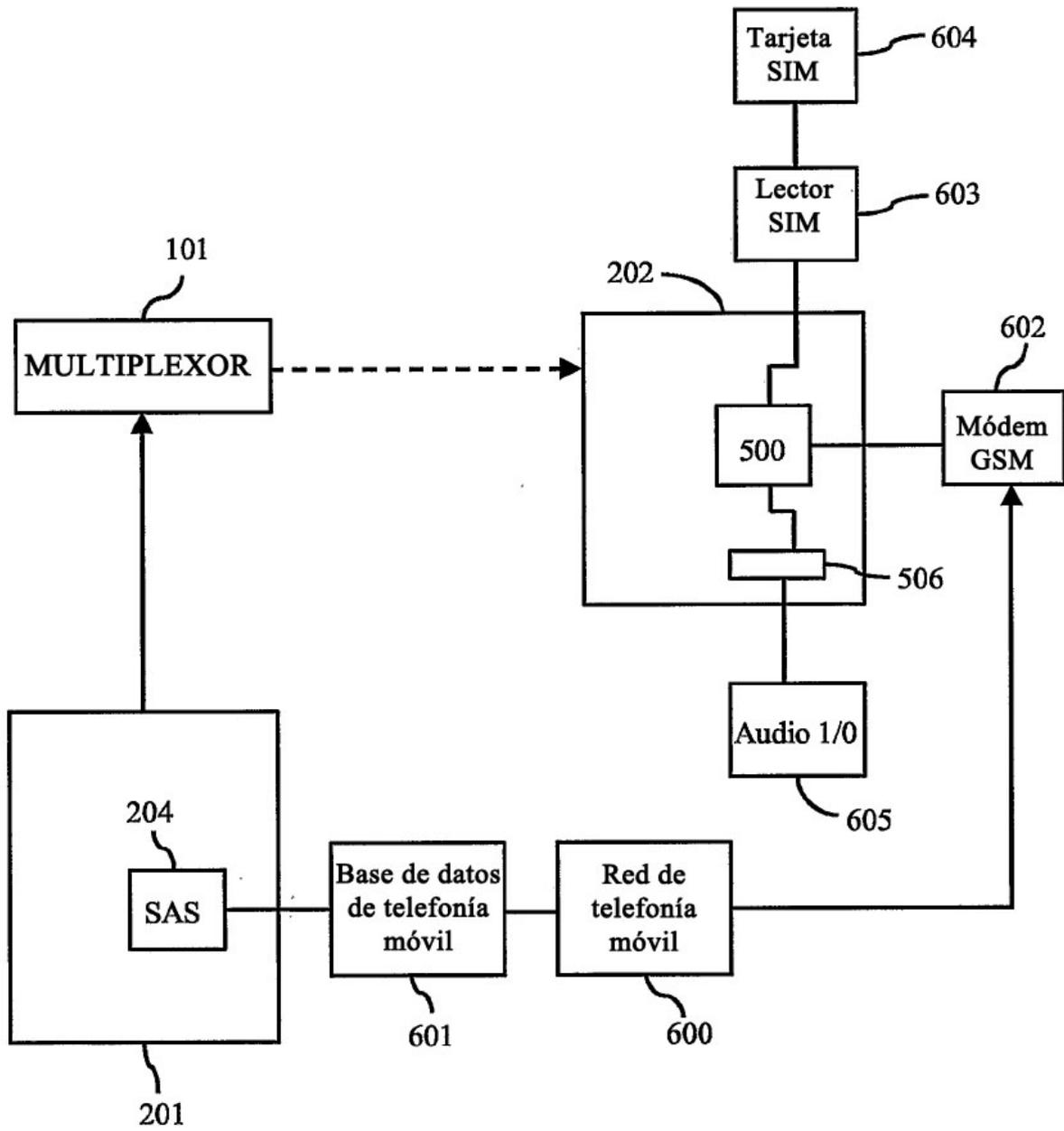


FIG. 6

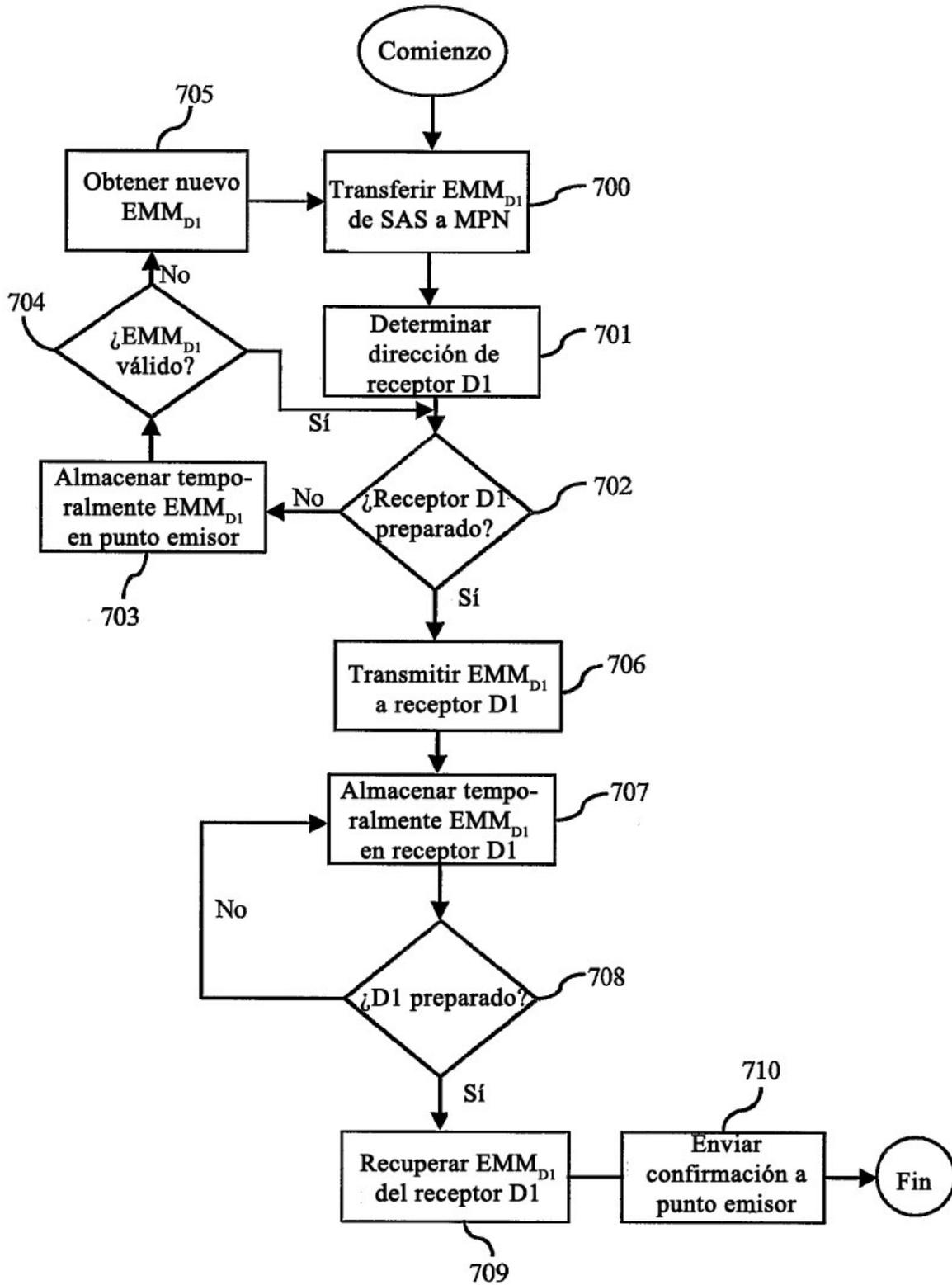


FIG. 7