



19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA

11 Número de publicación: **2 319 287**

51 Int. Cl.:
H04N 7/16 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Número de solicitud europea: **04100932 .5**

96 Fecha de presentación : **08.03.2004**

97 Número de publicación de la solicitud: **1463319**

97 Fecha de publicación de la solicitud: **29.09.2004**

54 Título: **Procedimiento de acceso a servicios de televisión a través de un descodificador esclavo.**

30 Prioridad: **19.03.2003 FR 03 50053**

45 Fecha de publicación de la mención BOPI:
06.05.2009

45 Fecha de la publicación del folleto de la patente:
06.05.2009

73 Titular/es: **Sagem Communications**
27, rue Leblanc
75512 Paris, FR

72 Inventor/es: **Grosset, Gilles y**
Chevreur, Jean-Jacques

74 Agente: **Elzaburu Márquez, Alberto**

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

Procedimiento de acceso a servicios de televisión a través de un descodificador esclavo.

5 Campo técnico de la invención

La presente invención tiene como objeto un procedimiento de acceso a servicios de televisión a través de un descodificador esclavo. Permite definir y controlar unas condiciones particulares de utilización de un descodificador esclavo, es decir de un descodificador cuyo funcionamiento depende; al menos para algunas de sus funcionalidades, de otro descodificador, llamado descodificador maestro.

El campo de la invención es, de una manera general, el de la televisión digital. En este campo, se asocia frecuentemente al televisor un descodificador de televisión digital. Éste último ofrece la posibilidad a un abonado de recibir una multitud de programas, o servicios, de televisión. El abonado ha comprado previamente o alquilado el descodificador a un operador de televisión o a un intermediario y ha suscrito un abono que le permite recibir y visualizar un conjunto de servicios de televisión codificados. Este conjunto de servicios depende de la naturaleza del abono que haya escogido el usuario, y no incluye necesariamente todos los servicios de televisión disponibles del operador escogido.

Un descodificador básico de la técnica anterior está representado de manera esquemática en la Figura 1. Esta Figura muestra un descodificador 100 que comporta un módulo de recepción 101 de un flujo de señales de televisión emitido por uno o varios operadores de televisión. El módulo de recepción 101 incorpora especialmente medios de demultiplexación de las diferentes señales recibidas en el flujo. En algunos casos, también puede comportar elementos compatibles con un sistema de control de los elementos periféricos. Está conectado, a través de un cable de radio frecuencia 102, llamado cable RF, con medios de recepción 103, simbolizados por una antena. En la práctica, los medios de recepción 103 asociados al descodificador 100 pueden ser un dispositivo de recepción terrestre, un dispositivo de recepción por cable, o incluso un dispositivo de recepción por satélite. Además del cable RF, el descodificador 100 dispone de diferentes posibilidades de conexión, no representadas, con su entorno: se encuentra especialmente un cable de alimentación de red, un cable peritel (SCART o euroconector), un conector que hace posible una conexión con una red telefónica, esencialmente para tener acceso a servicios interactivos...

Un microprocesador 104 está conectado a través de un primer bus de comunicación bidireccional 105 con una memoria de programas 106, con una memoria de datos 107, con un módulo de descodificación 111 y con un módulo de recepción 101. El microprocesador 104 indica al módulo de recepción 101 especialmente qué servicio de televisión debe extraer del flujo de informaciones que recibe por los medios de recepción 103. Un sensor 108, en este ejemplo infrarrojo, recibe las señales emitidas por un mando a distancia 109. Una célula infrarroja del sensor 108 emite una señal que se transmite al microprocesador 104. Las señales digitales procedentes del módulo de recepción 101 son enviadas, a través de una primera conexión unidireccional 110 hacia el módulo de descodificación 111. Las señales, eventualmente descodificadas se transmiten a continuación hacia un descompresor audio/vídeo 112 a través de una segunda conexión unidireccional 113.

La memoria de datos 107 está especialmente destinada a memorizar diferentes informaciones, valores o parámetros necesarios en el funcionamiento del descodificador. La memoria de programas 106 está especialmente destinada a la gestión de diferentes operaciones ejecutables para llevar a cabo diferentes funcionalidades del descodificador. Comporta varias aplicaciones, y podrá especialmente contener algunas que se dedicarán a la ejecución del procedimiento según la invención. Estas aplicaciones se detallarán a continuación. En otros ejemplos de realización del descodificador 100, estas aplicaciones podrían estar reemplazadas por circuitos electrónicos específicos.

El bus de comunicación bidireccional 105 transporta señales de comando, de dirección o de datos. Se trata de una representación funcional; todas las otras conexiones representadas son, en la práctica, bus de datos que aseguran intercambios de datos entre dos elementos del descodificador descrito. Algunas de estas conexiones podrían estar integradas en el bus de comunicación bidireccional 105.

En el descodificador 100, se ha previsto una abertura para introducir una tarjeta 114, por ejemplo una tarjeta tipo tarjeta con chip. El descodificador está equipado con un interfaz para poder intercambiar informaciones con la tarjeta 114 a través de un segundo bus de comunicación bidireccional 115. La tarjeta 114 es un elemento básico en el funcionamiento de la gestión de los derechos de acceso a los servicios de televisión. Para ello, una tarjeta de este tipo lleva especialmente diferentes memorias que contienen diferentes claves de descodificación y un conjunto de informaciones relativas a derechos de acceso. El módulo de descodificación 111 recibe mensajes de descodificación desde la tarjeta 114 y a través de los diferentes bus de comunicación del descodificador 100 que permiten, cuando el abono de un usuario incluye un servicio seleccionado, descodificar las señales de audio y vídeo de este servicio.

Segundo plano tecnológico de la invención

Actualmente, cuando un abonado desea suscribirse a un segundo abono, y, así, utilizar un segundo descodificador de televisión digital, no se beneficia generalmente de tarifas ventajosas por parte del operador en el que ha suscrito su primer abono. Ahora bien, actualmente existe una proporción nada desdeñable de clientes de los operadores de televisión, que han suscrito un primer abono, llamado abono principal, que estarían dispuestos a suscribir un segundo

abono, llamado abono anexo, si este último ofreciese una tarifa ventajosa respecto al primero. Un doble abono les permitiría efectivamente disponer de derechos de acceso - eventualmente diferentes - para varios descodificadores de televisión que, al estar situados en diferentes habitaciones de una vivienda, permitirían a diferentes personas de la vivienda visualizar simultáneamente servicios de televisión de pago diferentes.

Una de las dificultades con las que se ven enfrentados los diferentes operadores de televisión, a la hora de proponer abonos anexos a un abono principal con una tarifa preferente, es que deben tener la garantía de que el descodificador esclavo que ponen a disposición de un abonado será utilizado efectivamente como descodificador esclavo, es decir en una vivienda en la que un descodificador maestro se utiliza de un modo lícito. En efecto, no sería viable económicamente poner a disposición del público unos descodificadores que se benefician de un abono de tarifa preferente si tales descodificadores pudiesen ser utilizados por alguna persona que no haya suscrito ya un abono.

En la técnica anterior, se conoce la solicitud de patente Europea EP 0 726 676 presentada por Philips Electronics, que aporta un principio de solución al problema que acaba de plantearse. En este documento, está previsto que, para obtener derechos de acceso, debe colocarse regularmente una tarjeta de gestión de los derechos de acceso del descodificador esclavo para que los derechos de acceso del descodificador esclavo queden registrados. Un funcionamiento de este tipo es, en función de la frecuencia impuesta para el registro de los derechos en la tarjeta de gestión de los derechos de acceso, engorroso para el abonado, el hecho de recargar frecuentemente la tarjeta de control se convertiría pronto en algo pesado, o bien no lo suficientemente seguro, ya que un usuario amigo del abonado principal podría recargar su tarjeta en casa del abonado principal sin problemas tantas veces como fuese necesario, siempre que la periodicidad de la recarga máxima no sea demasiado débil.

Se conoce también, en la técnica anterior, la patente americana US-A-4633309, que propone un sistema en el que un operador de televisión emite periódicamente un mensaje de inhibición de derechos hacia el conjunto de los descodificadores esclavos de su red, habiendo transmitido previamente al conjunto de los descodificadores maestros un mensaje llamado mensaje antídoto; el mensaje antídoto habrá sido inmediatamente, o al menos antes de la emisión por parte del operador de un mensaje de inhibición, redistribuido por cada descodificador maestro hacia cada descodificador esclavo al que esté asociado. Los descodificadores esclavos que hayan recibido el mensaje antídoto no se verán afectados por el mensaje de inhibición emitido por el operador, y pueden continuar beneficiándose de los diferentes derechos de acceso que se les atribuyó cuando se suscribieron al abono cuyas condiciones quedan reservadas a la utilización de un descodificador esclavo que coopera con un descodificador maestro. Sin embargo, esta solución no es satisfactoria ya que necesita una intervención regular del operador de televisión, que debe integrar periódicamente en su flujo de señales mensajes de inhibición y mensajes antídotos.

Se conoce también, en la técnica anterior, el documento US 2003/002886 A1 que describe un dispositivo de acceso, para un único abonado, con una multitud de descodificadores.

Se conoce también, en la técnica anterior, el documento JP2000-324465 que es una solicitud de patente presentada por SONY. En este documento, un descodificador maestro transmite a un descodificador esclavo al que se le ha asociado una clave de descodificación. Esta transmisión se efectúa en la puesta en marcha. Es necesario equipar el descodificador esclavo y el descodificador maestro con medios bidireccionales de comunicación para que puedan intercambiar entre ellos un conjunto de informaciones. Un equipo de este tipo es engorroso y costoso de instalar. Además, la clave de descodificación que se transmite es similar a los derechos de acceso que se facilitan al descodificador esclavo; después de la conexión a la red eléctrica del descodificador esclavo y una vez los derechos están memorizados, nada puede impedir a un abonado que vaya a otra vivienda con su descodificador maestro para transmitir los mismos derechos a otro descodificador esclavo.

Descripción general de la invención

La presente invención propone una solución a todos los problemas e inconvenientes que acaban de mencionarse. En la invención, se propone una solución particular que hace posible el uso de un descodificador esclavo que no sería utilizado cerca de un descodificador maestro. Una ventaja significativa del procedimiento según la invención es que la ejecución no necesita modificaciones importantes ni en los descodificadores que intervienen en el susodicho procedimiento, ya sean maestros o esclavos, ni en el contenido de los flujos de señales difundidas por los diferentes operadores de televisión.

Con este fin, está previsto en la invención, un funcionamiento particular de cada descodificador esclavo, funcionamiento según el cual cada descodificador esclavo no realiza más operaciones de descodificación cuando no ha recibido, desde hace algún tiempo, mensajes específicos, llamados mensajes de autorización, de parte del descodificador maestro. En la invención, el descodificador esclavo es capaz de bloquearse por sí mismo suspendiendo sus operaciones de descodificación, sin recibir instrucciones de bloqueo desde el exterior, por ejemplo del operador; dispone de un sistema de reloj que le permite realizar una cuenta atrás.

Cuando la cuenta atrás del descodificador esclavo finaliza sin haber sido reinicializado, es decir sin haber sido puesto a cero desde el principio de la cuenta atrás, como consecuencia de la ausencia de recepción de un mensaje de autorización procedente de un descodificador maestro, el esclavo cesa todas las operaciones de descodificación denegando así el acceso a los programas codificados. Además, los mensajes de autorización se emiten regularmente a través del descodificador maestro, sin que éste último haya recibido previamente, del exterior, instrucciones específicas

solicitando una emisión de ese tipo. La gestión de los derechos de acceso para un descodificador esclavo propuesta en el procedimiento según la invención es automática y no hace intervenir a elementos exteriores, tales como operadores de televisión o los usuarios de descodificadores, en los descodificadores implicados.

5 En un modo de ejecución ventajoso del procedimiento según la invención, los descodificadores esclavos se asocian a un descodificador maestro único, es decir que sólo pueden aceptar mensajes de autorización por parte del descodificador maestro que se les ha sido asignado. Con este fin, los descodificadores esclavos y el descodificador maestro habrán sido objeto de una operación llamada *pairing* o asociación. De un modo más ventajoso, los mensajes de autorización se transmiten del descodificador maestro hacia cada descodificador esclavo destinatario del mensaje a través del cable RF.

La invención implica un procedimiento de acceso a los servicios de televisión a través de al menos un descodificador esclavo, el susodicho procedimiento implica las diferentes etapas que consisten en:

- 15 - equipar una vivienda a través de un descodificador maestro y al menos un descodificador esclavo;
- recibir, a través de los medios de recepción de la vivienda, un flujo de señales de televisión emitidos por un operador de televisión, el flujo que comporta especialmente un conjunto de servicios de televisión;
- 20 - determinar para el descodificador maestro, un conjunto de derechos de acceso a un primer conjunto autorizado de servicios de televisión;

caracterizado porque el procedimiento comporta las diferentes etapas complementarias que consisten en:

- 25 - transmitir automática y regularmente, desde un descodificador maestro hacia cada descodificador esclavo, un mensaje de autorización de acceso a un segundo conjunto autorizado de servicios de televisión, el susodicho mensaje de autorización que ha sido elaborado a través de una aplicación del descodificador maestro sin transmisión previa, por el operador de televisión, de un mensaje específico que inicie la transmisión de un mensaje de autorización de este tipo;
- 30 - bloquear una operación de descodificación del segundo conjunto de servicios de televisión para cada descodificador esclavo activo que no haya recibido algún mensaje apropiado de autorización durante una duración de autonomía, previamente determinada, de los descodificadores esclavos.
- 35 - la etapa de bloqueo de la operación de descodificación que se ejecuta sin transmisión previa por el operador de televisión de un mensaje específico que inicia el bloqueo de la operación de descodificación, por cada descodificador esclavo que no haya recibido, durante su duración de autonomía, el mensaje de autorización;

caracterizado porque el procedimiento comporta las diferentes etapas suplementarias que consisten en:

- 40 - memorizar (312; 313), antes de cada puesta en modo de espera (314) de uno de los descodificadores esclavos (100'), un estado de autorización de acceso del descodificador esclavo (100');
- 45 - en cada nuevo posicionamiento en un estado activo (301) del descodificador esclavo, colocar (307) el susodicho descodificador esclavo (100') en un estado de autorización de acceso correspondiente al estado de autorización del acceso memorizado.

El procedimiento según la invención puede presentar de un modo ventajoso una o varias características suplementarias de las que se citan a continuación:

- 50 - la etapa de bloqueo de la operación de descodificación se ejecuta sin transmisión previa por el operador de la televisión de un mensaje específico que inicie el bloqueo de la operación de descodificación, por cada descodificador esclavo que no haya recibido durante su duración de autonomía, el mensaje de autorización;
- 55 - la transmisión del mensaje de autorización de acceso es periódica;
- la transmisión del mensaje de autorización de acceso se efectúa a través de un cable RF que une cada descodificador a los medios de recepción de la vivienda;
- 60 - la transmisión de un mensaje de autorización de acceso se efectúa en una banda de frecuencia no utilizada por la recepción del flujo de señales de televisión;
- la transmisión del mensaje de autorización de acceso se efectúa según un protocolo definido por los sistemas de control de los equipos periféricos en el marco de las recepciones satélites, por ejemplo el sistema DiSEqC;
- 65 - la duración de autonomía de los descodificadores esclavos es superior a dos veces el periodo de transmisión del mensaje de autorización;

- el procedimiento comporta la etapa complementaria que consiste en asociar el descodificador maestro a cada descodificador esclavo de la vivienda. Esta asociación entre el descodificador maestro y cada descodificador esclavo de la vivienda es irreversible a no ser que se cuente con la intervención del operador o del fabricante de descodificadores.

En un primer modo de ejecución, la etapa de asociación de un maestro con un esclavo comporta las siguientes operaciones que consisten en:

- calcular, en el descodificador maestro, una clave de codificación a partir de opciones aleatorias disponibles en el mismo descodificador maestro;
- transmitir una clave de descodificación asociada a la clave de codificación hacia cada descodificador esclavo;
- memorizar una clave de codificación, respectivamente la clave de descodificación en una memoria del descodificador maestro, respectivamente en una memoria de cada descodificador esclavo; la operación de memorización de la clave de descodificación en cada descodificador esclavo es en un ejemplo ventajoso, único e irreversible.

En un segundo modo de ejecución, la etapa de asociación de un maestro con un esclavo comporta las siguientes operaciones que consisten en:

- recibir, en el descodificador maestro y en cada descodificador esclavo de la vivienda, uno o varios mensajes específicos, de tipo EMM, que comporten las claves de codificación y de descodificación;
- memorizar la clave de codificación en una memoria del descodificador maestro y la clave de descodificación en una memoria del descodificador esclavo.
- el procedimiento comporta la etapa suplementaria que consiste en codificar, respectivamente descodificar, a través de la clave de codificación, respectivamente de descodificación, memorizada, los mensajes de autorización transmitidos, respectivamente recibidos, por el descodificador maestro, respectivamente por cada descodificador esclavo.
- el mensaje de autorización de acceso (MESS.AUTO) codificado comporta una información relativa al momento de su envío.
- la etapa de bloqueo de una operación de descodificación se efectúa a través de una tarjeta de gestión de los derechos insertada en cada descodificador esclavo.

La invención y sus diferentes aplicaciones se verán más claras en la lectura de la descripción que sigue al examen de las Figuras que la acompañan.

Breve descripción de las figuras

Estas Figuras sólo se presentan a título indicativo y de ningún modo restrictivo de la invención. Las Figuras muestran:

- en la Figura 1, ya descrita, una representación esquemática de un descodificador clásico de la técnica anterior;
- en la Figura 2, una representación esquemática de dos descodificadores susceptibles de ejecutar el procedimiento según la invención para la gestión de los derechos de acceso de un descodificador esclavo;
- en la Figura 3, un organigrama que ilustra diferentes etapas de un modo de ejecución particular del procedimiento según la invención.

Descripción de las formas de realización preferidas de la invención

A continuación se hace referencia a las Figuras 2 y 3 que ilustran una ejecución particular de la invención, varias de las etapas descritas no deben considerarse en nada como limitativas del alcance general del procedimiento según la invención.

En la Figura 2, se ha representado un primer descodificador 100, que será considerado como el descodificador maestro, y un segundo descodificador 100', que será considerado como el descodificador esclavo. Estos dos descodificadores son similares, en su estructura general, al descrito en la Figura 1; los diferentes elementos representados han guardado las mismas referencias que las dadas en la Figura 1, la extensión "prima" ha sido añadida a las referencias del descodificador 100' para evitar confusiones. Para la ejecución del procedimiento según la invención, se ha adap-

tado esencialmente, respecto a los descodificadores conocidos de la técnica anterior, el contenido de las memorias de programas 106, 106' y las memorias de datos 107 y 107'. Los dos descodificadores están unidos a medios de recepción comunes 103 a través de su cable de radio frecuencia respectivo 102 y 102'.

- 5 En la invención, se propone de manera ventajosa que los cables de radio- frecuencia 102 y 102' sean utilizados para que el descodificador maestro 100 transmita mensajes, especialmente los mensajes de autorización, al descodificador esclavo 100'. En modos de ejecución diferentes de la invención, se pueden utilizar otros medios de transmisión de los mensajes de autorización entre los dos descodificadores, estos medios son, sin embargo, menos apropiados:
- 10 - se puede prever una conexión física suplementaria entre los descodificadores; sin embargo el abonado tendrá la molestia de tener un cable suplementario que deberá pasar de una habitación a otra;
 - se puede utilizar una tecnología de PLC (power lines communication); pero su ejecución es costosa, y no existe una garantía total de que la comunicación no pueda efectuarse entre descodificadores situados en las
 - 15 casas vecinas;
 - se pueden utilizar las ondas de radio; en este caso no se tiene una garantía total de que la comunicación no pueda efectuarse entre los descodificadores situados en las casas vecinas;
 - 20 - se pueden utilizar las líneas telefónicas; pero esto obliga al usuario a colocar sus descodificadores cerca de tomas telefónicas, algo que pocas veces resulta posible teniendo en cuenta la concepción de las viviendas.

La utilización del cable RF aporta una garantía de que los mensajes transmitidos del descodificador maestro hacia el descodificador esclavo no saldrán de los límites de la vivienda, y presenta además la ventaja de un escaso coste de adaptación de los descodificadores para la ejecución del procedimiento según la invención. Además, la utilización del cable RF permite utilizar, para transmitir mensajes desde el descodificador maestro hacia los descodificadores esclavos, los protocolos que se definen para los sistemas de control de los equipos periféricos en el marco de las recepciones satélites y que están presentes en algunos descodificadores. Un sistema de este tipo es por ejemplo el

25 DiSEqC (marca registrada) (por Digital Satellite Equipment Control en inglés) que permite dirigir un cierto número de equipos (entrada de recepción de la parabólica, motor, acopladores, conmutadores...) directamente por el cable RF. La Figura 2 ilustra la transmisión regular, por los cables RF 102 y 102', de un mensaje de autorización MESS.AUTO desde el descodificador maestro 100 hacia el descodificador esclavo 100'.

35 La transmisión de los mensajes de autorización, basada en los protocolos existentes o no, se efectúa en las bandas de frecuencia no utilizadas para la recepción de los flujos de señales de televisión.

Ahora nos referimos básicamente a la Figura 3. El organigrama representado comporta una primera etapa 300 que consiste en la instalación de un descodificador esclavo. Para la instalación, se designa aquí el conjunto de operaciones de empalme al sector, a los medios de recepción 103, y cualquier otra ramificación del descodificador esclavo. Una vez esté correctamente conectado, el descodificador esclavo puede, en una etapa 301, estar puesto en un estado activo, en oposición a un estado en espera en el que el descodificador no intenta realizar operaciones de descodificación.

Interviene una etapa de decisión 302, etapa en la que el usuario indica si se trata de una primera utilización del descodificador esclavo. Si este es el caso, el usuario tiene la posibilidad de acceder a un menú que se despliega en la pantalla de su televisor; simultáneamente, el usuario despliega un menú similar en una segunda pantalla asociada al descodificador maestro. La aparición de estos menús, que, en un modo de ejecución particular puede que esté limitada únicamente a la primera utilización del descodificador esclavo, permite parametrizar en una etapa 303, un conjunto de funcionalidades del descodificador esclavo, e igualmente proceder, en una etapa 304, a una operación de asociación, o *pairing*, entre el descodificador maestro y el descodificador esclavo. Esta operación de *pairing* se detallará posteriormente en las diferentes variantes que pueden considerarse en la invención. En todos los casos considerados, la operación de *pairing* o *asociación* conduce a la memorización, en una zona particular 203 de la memoria de datos 107, respectivamente 200' de la memoria de datos 107', de una clave de codificación K, respectivamente de una clave de descodificación K'.

55 La clave de descodificación K' permite descodificar el conjunto de los mensajes codificados a través de la clave de codificación K. Estas claves pueden especialmente utilizarse para que el mensaje de autorización MESS.AUTO sea transmitido de manera codificada del descodificador maestro hacia cada descodificador esclavo destinatario. Estas claves, en función de los algoritmos de codificación utilizados, son diferentes o idénticas y únicamente los descodificadores esclavos que contienen la buena clave de descodificación K' pueden descodificar el mensaje de autorización codificado a través de la clave de codificación K, e interpretarlo como tal.

A partir del momento en el que el descodificador maestro 100' se asocia con uno o varios descodificadores esclavos, trabaja solo y trasmite regularmente los mensajes de autorización de acceso MESS.AUTO a través de una aplicación 210 de la memoria de programas 106, llamada aplicación de cálculo del mensaje de autorización. Para alcanzar un nivel de seguridad óptimo además de una codificación a través de la clave de codificación K, el mensaje de autorización elaborado comporta una información relativa al momento en el que se transmite, por ejemplo la fecha y la hora de su transmisión. La regularidad de la transmisión del mensaje de autorización se define por una variable 204 de la memoria

ES 2 319 287 T3

de datos 107; cuando esta variable adopta un valor constante, la emisión del mensaje de autorización es periódica, por ejemplo de un periodo equivalente a cinco minutos.

Después de la operación de *pairing o asociación*, se efectúa una operación 305 de primera memorización, en una zona particular 201' de la memoria de datos 107' del descodificador esclavo, de un estado de autorización de acceso a servicios de televisión. Por defecto, después de la operación de *pairing o asociación* 304, el acceso está autorizado.

Después de la etapa 305, o después de la etapa 302 cuando el descodificador no está colocado en un estado activo por primera vez, se procede, en una etapa 306, a una operación de lectura del estado de autorización de acceso a los servicios de televisión. Las operaciones de lectura/escritura del estado de autorización de acceso se efectúan a través de una aplicación 212' de la memoria de programas 106'. Esta etapa de lectura va seguida de una etapa de decisión 307 después de la cual el descodificador esclavo se coloca, en una etapa 308, en un modo de bloqueo cuando el acceso a los servicios de televisión está memorizado como denegado; el funcionamiento de la etapa de bloqueo 308, como el de las otras etapas de bloqueo que pueden intervenir, se detallará a continuación.

Después de la etapa 308, o de la etapa de decisión 307 cuando el acceso a los servicios de televisión está memorizado como autorizado, se procede, en una etapa 309, al inicio de una cuenta hacia atrás, o temporizador, a través de una aplicación 213' de la memoria de programas 106'. Se trata aquí de una etapa esencial del procedimiento según la invención. Efectivamente, a partir del momento en el que el temporizador se pone en marcha, el descodificador esclavo está a la espera de un mensaje de autorización que debe ser transmitido por el descodificador maestro. Una etapa de decisión 310 ilustra esta espera.

Si termina la cuenta atrás, es decir si una duración llamada duración de autonomía, memorizada en la zona particular 202' de la memoria de datos 107' del descodificador esclavo, ha transcurrido desde el inicio de la cuenta atrás, y si no ha aparecido ningún mensaje de autorización adecuado en el descodificador esclavo, éste último entra en un estado de bloqueo en una etapa 311; el estado de autorización de acceso a los servicios de televisión por los cuales el descodificador esclavo ha adquirido los derechos se memoriza entonces como denegado, en una etapa 312, en la zona de memoria reservada para este efecto. Por el contrario, si la duración de autonomía del descodificador esclavo no ha llegado a su término en el momento de la recepción de un mensaje de autorización apropiado por parte del descodificador maestro, el estado de acceso a los servicios de televisión para los que el descodificador esclavo ha adquirido los derechos se ha memorizado, en una etapa 313, como autorizado en la zona de memoria 201' reservada a este efecto. En un modo de ejecución particular de la invención, la duración de la cuenta atrás es superior a dos veces un intervalo de tiempo mínimo definido entre dos transmisiones sucesivas del mensaje de autorización. En los dos casos, es decir después de la etapa 312 o después de la etapa 313, el procedimiento se reanuda en la etapa 309 en el momento en que la cuenta atrás se inicia. Igualmente, se podrá contar el número de puestas en modo de espera realizadas desde la última recepción del mensaje de autorización y hacer pasar el estado de autorización de acceso memorizado en el estado denegado, cuando este número sobrepasa un cierto valor (por ejemplo 5).

La memorización de un estado de autorización de acceso constituye un perfeccionamiento de la invención que permite evitar un fraude que consiste en poner en modo de espera y a volver a ponerlo en un estado activo, inmediatamente después, un descodificador esclavo que no habría recibido, en el espacio de tiempo disponible, el mensaje de autorización y cuyas funcionalidades de descodificación habrían sido bloqueadas. Efectivamente, si no se hubiese memorizado una información de este tipo, cada nueva puesta en marcha de un descodificador esclavo permitiría obtener un flujo de señales descodificadas durante la totalidad de la duración de autonomía del descodificador esclavo. El hecho de retomar el procedimiento en la etapa 309 después de las etapas 311 y 312 permite limitar las consecuencias de una perturbación en la transmisión del mensaje de autorización. Así, en el caso en que la no recepción del mensaje de autorización muestra una disfunción, el descodificador esclavo utilizado correctamente sólo quedará bloqueado cuando se reciba el siguiente mensaje de autorización.

En cualquier momento, la etapa de decisión 310 puede quedar interrumpida por el usuario que decida, en una etapa 314, colocar el descodificador esclavo en modo de espera. El procedimiento según la invención es reanudado en la etapa 301 cuando el usuario vuelve a colocar el descodificador esclavo en un estado activo.

Para la etapa de asociación 304, se han considerado dos alternativas principales en el procedimiento según la invención:

La primera es la llamada *pairing o asociación* local. En esta alternativa, el descodificador maestro calcula, a través de una aplicación llamada cálculo de codificación 211 de la memoria de programas 106, la clave de codificación K, por ejemplo de tipo AES, a partir de las opciones aleatorias a su disposición, como son la hora, el nivel de ocupación de sus memorias intermedias... Después de haberlo memorizado, se transmite a cada descodificador esclavo la clave de descodificación correspondiente K', donde se memoriza de manera única e irreversible, haciendo definitivamente imposible el uso de estos descodificadores esclavos con otro descodificador maestro.

La segunda alternativa es el llamado *pairing o asociación* centralizada. En esta alternativa, el operador de televisión emite mensajes de gestión de derechos de tipo EMM (Entitlement Management Message en inglés) específicos, destinados a una pareja maestro/esclavo de un mismo abonado, que contienen las claves de codificación K y de descodificación K'. El o los mensajes EMM codificados que contienen las claves pueden, por razones de seguridad, llevar el número de serie de los descodificadores maestro y esclavo.

ES 2 319 287 T3

Para las etapas de bloqueo 308 y/o 311, se consideran igualmente dos alternativas principales en el procedimiento según la invención:

5 La primera alternativa se aplica cuando las tarjetas de gestión de los derechos 114 y 114' son idénticas en términos de funcionamiento (no necesariamente en términos de servicios a los que dan acceso). En este caso, una aplicación de bloqueo 214' de la memoria de programas 106' se pone en marcha en las diferentes etapas del bloqueo. Ésta tiene como objeto impedir la transmisión de las palabras de descodificación desde la tarjeta de gestión de derechos de acceso 114' hacia el módulo de descodificación 111'.

10 En la segunda alternativa, las tarjetas de gestión de los derechos 114 y 114' no son idénticas. En este caso está previsto elaborar los mensajes de autorización del maestro, ya no en su memoria de programa 106, sino en su tarjeta de gestión de los derechos 114. Las tarjetas de gestión de los derechos 114' de los descodificadores esclavos son las que pueden bloquear directamente las operaciones de descodificación. En esta segunda alternativa, se utilizará de un modo ventajoso el *pairing o asociación* centralizada, los EMM específicos que transmiten a las tarjetas de gestión derechos
15 de los descodificadores maestros y esclavos, la clave común en caso de codificación simétrica, o las dos claves, en el caso de una codificación RSA.

El descodificador maestro que debe enviar periódicamente los mensajes de autorización de acceso para permitir la utilización de los descodificadores esclavos que le son asociados podrá para ello estar en modo activo permanente-
20 mente, o, preferentemente, activarse con cierta periodicidad.

25

30

35

40

45

50

55

60

65

REIVINDICACIONES

1. Procedimiento de acceso a servicios de televisión a través de al menos un descodificador esclavo (100'), el
susodicho procedimiento comprende las diferentes etapas que consisten en:

- equipar una vivienda a través de un descodificador maestro (100) y de al menos un descodificador esclavo (100');
- recibir, a través de medios de recepción (103) de la vivienda, un flujo de señales de televisión emitidas por un operador de televisión, flujo que comporta especialmente un conjunto de servicios de televisión;
- determinar para el descodificador maestro (100), un conjunto de derechos de acceso a un primer conjunto autorizado de servicios de televisión;
- transmitir automática y regularmente, desde el descodificador maestro (100) hacia cada descodificador esclavo (100') un mensaje de autorización de acceso (MESS.AUTO) a un segundo conjunto autorizado de servicios de televisión, el llamado mensaje de autorización que ha sido elaborado a través de una aplicación del descodificador maestro (100) sin transmisión previa, por el operador de televisión, de un mensaje específico que pone en marcha la transmisión de un mensaje de autorización de este tipo;
- bloquear (311) una operación de descodificación del segundo conjunto de servicios de televisión para cada descodificador esclavo (100) activo que no haya recibido un mensaje apropiado de autorización (MESS.AUTO) durante una duración de autonomía, previamente determinada, de los descodificadores esclavos (100'), la etapa de bloqueo de la operación de descodificación que ha sido ejecutada sin transmisión previa por el operador de televisión de un mensaje específico que ponga en marcha el bloqueo de la operación de descodificación para cada descodificador esclavo (100') que no haya recibido durante su duración de autonomía el mensaje de autorización (MESS.AUTO);

caracterizado porque el procedimiento comprende las diferentes etapas suplementarias que consisten en:

- memorizar (312; 313), antes de cada puesta en modo de espera (314) de uno de los descodificadores esclavos (100'), un estado de autorización de acceso del descodificador esclavo (100');
- en cada nuevo posicionamiento en un estado activo (301) del descodificador esclavo, colocar (307) el susodicho descodificador esclavo (100') en un estado de autorización de acceso correspondiente al estado de autorización del acceso memorizado.

2. Procedimiento según la reivindicación precedente **caracterizado** porque la transmisión del mensaje de autorización de acceso (MESS.AUTO) es periódica.

3. Procedimiento según al menos una de las reivindicaciones precedentes **caracterizado** porque la transmisión del mensaje de autorización de acceso (MESS.AUTO) se efectúa a través de un cable de radio-frecuencia (102; 102') que une cada descodificador (100; 100') con los medios de recepción (103) de la vivienda.

4. Procedimiento según la reivindicación precedente **caracterizado** porque la transmisión del mensaje de autorización de acceso (MESS.AUTO) se efectúa en una banda de frecuencia no utilizada para la recepción de un flujo de señales de televisión.

5. Procedimiento según al menos una de las reivindicaciones 3 o 4 **caracterizado** porque la transmisión del mensaje de autorización de acceso (MESS.AUTO) se efectúa según un protocolo definido para los sistemas de control de los equipos periféricos en el marco de las recepciones satélites.

6. Procedimiento según al menos una de las reivindicaciones 2 a 5 **caracterizado** porque la duración de la autonomía de los descodificadores esclavos (100') es superior a dos veces el periodo de transmisión del mensaje de autorización (MESS.AUTO).

7. Procedimiento según al menos una de las reivindicaciones precedentes **caracterizado** porque comporta la etapa suplementaria que consiste en realizar la asociación (304) del descodificador maestro (100) a cada descodificador esclavo (100') de la vivienda.

8. Procedimiento según la reivindicación precedente **caracterizado** porque la asociación entre el descodificador maestro (100) y cada descodificador esclavo (100') de la vivienda es irreversible al menos sin la intervención del operador o del fabricante de los descodificadores.

9. Procedimiento según al menos una de las reivindicaciones 7 u 8 **caracterizado** porque la etapa suplementaria (304) de asociación del descodificador maestro con cada descodificador esclavo comprende las diferentes operaciones que consisten en:

ES 2 319 287 T3

- calcular, en el descodificador maestro (100), una clave de codificación (K) a partir de opciones aleatorias disponibles en el mismo descodificador maestro (100);
- transmitir una clave de descodificación (K') asociada a la clave de codificación (K) hacia cada descodificador esclavo (100');
- memorizar la clave de codificación (K), respectivamente la clave de descodificación (K') en una memoria del descodificador maestro (100), respectivamente en una memoria de cada descodificador esclavo (100').

5

10 10. Procedimiento según la reivindicación precedente **caracterizado** porque la operación de memorización de la clave de descodificación en cada descodificador esclavo (100') es única e irreversible.

15 11. Procedimiento según al menos una de las reivindicaciones 7 u 8 **caracterizado** porque la etapa suplementaria (304) de asociación del descodificador maestro con cada descodificador esclavo comporta las diferentes operaciones que consisten en:

- recibir, en el descodificador maestro (100) y en cada descodificador esclavo (100') de la vivienda, uno o varios mensajes específicos, de tipo EMM, que llevan una clave de codificación (K) y una clave de descodificación (K')
- memorizar la clave de codificación (K) en una memoria del descodificador maestro (100) y la clave de descodificación (K') en una memoria de cada descodificador esclavo (100').

20

25 12. Procedimiento según al menos una de las reivindicaciones 9 a 11 **caracterizado** porque comprende la etapa suplementaria que consiste en codificar, respectivamente descodificar, a través de la clave de codificación (K), respectivamente de descodificación (K'), memorizada, los mensajes de autorización de acceso (MESS. AUTO) transmitidos, respectivamente recibidos por el descodificador maestro (100'), respectivamente por cada descodificador esclavo (100').

30 13. Procedimiento según la reivindicación precedente **caracterizado** porque el mensaje de autorización de acceso (MESS. AUTO) codificado comporta una información relativa al momento de su envío.

35 14. Procedimiento según al menos una de las reivindicaciones precedentes **caracterizado** porque la etapa de bloqueo (311) de una operación de descodificación se efectúa a través de una tarjeta de gestión (114') de los derechos insertada en cada descodificador esclavo (100').

40

45

50

55

60

65

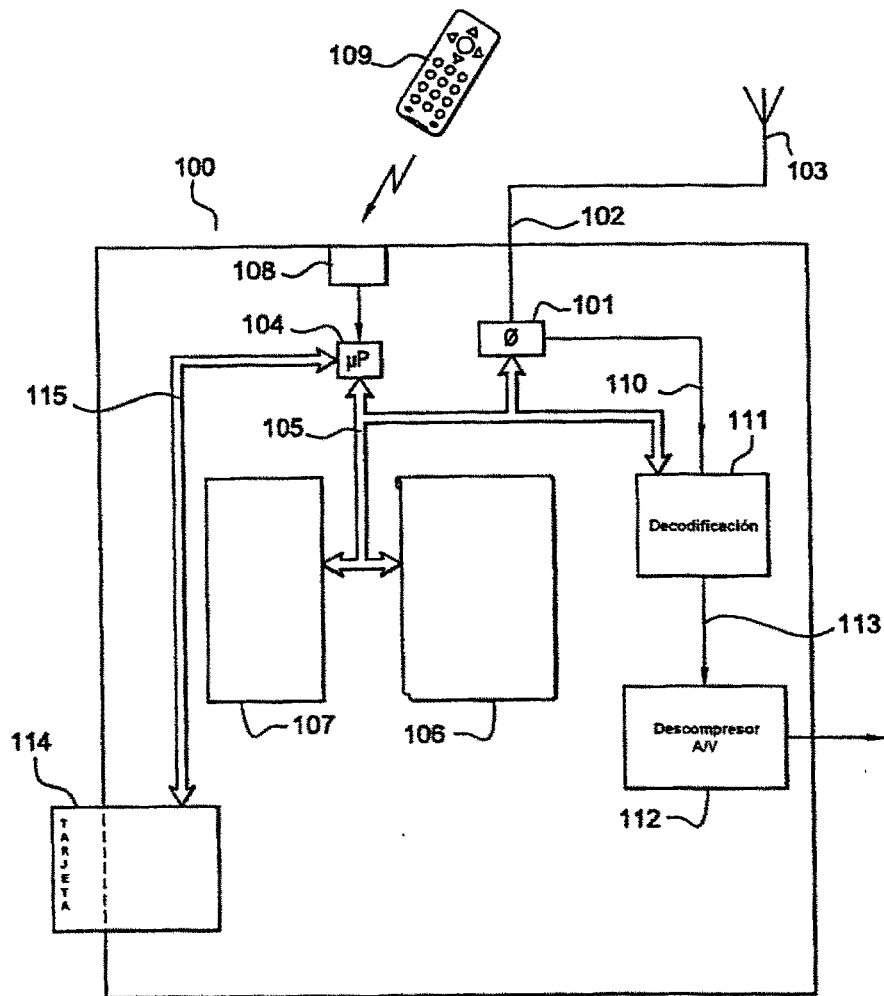


Fig. 1

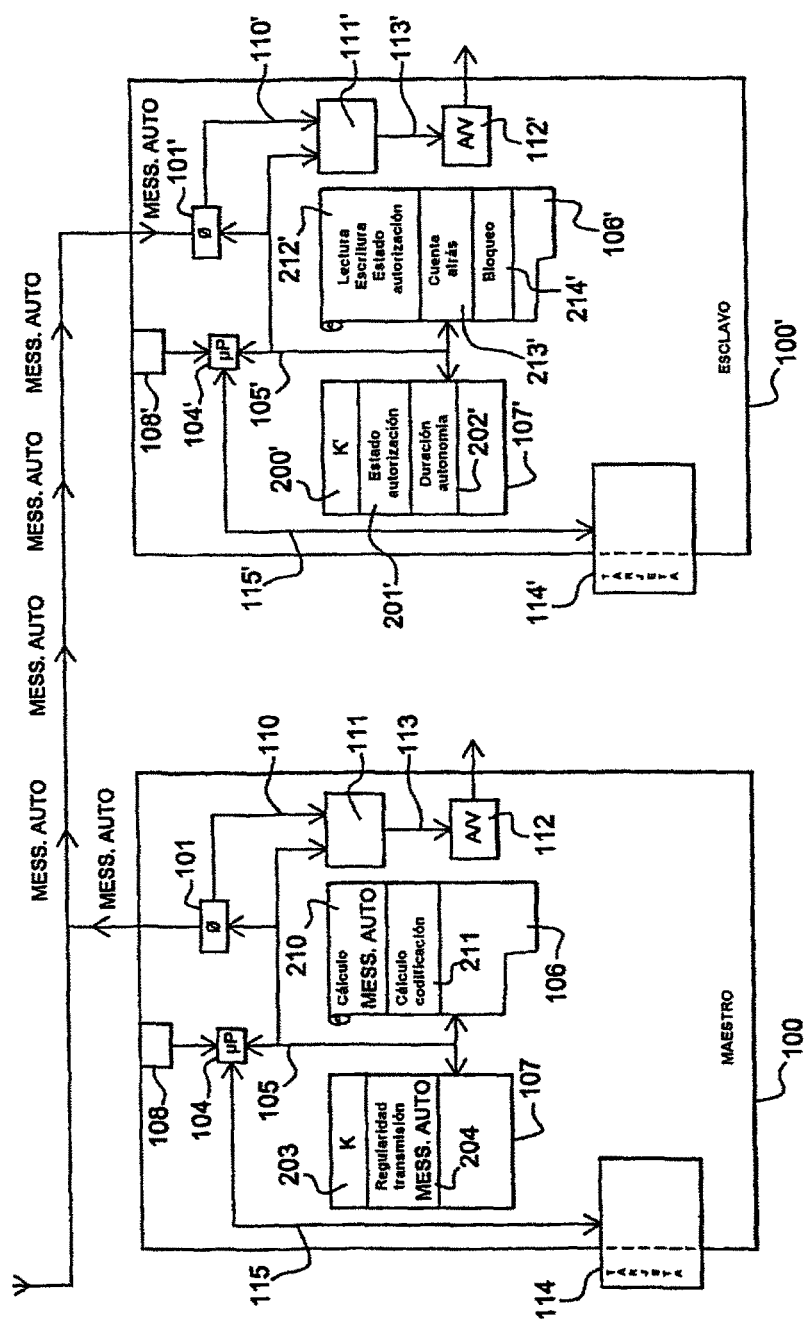


Fig. 2

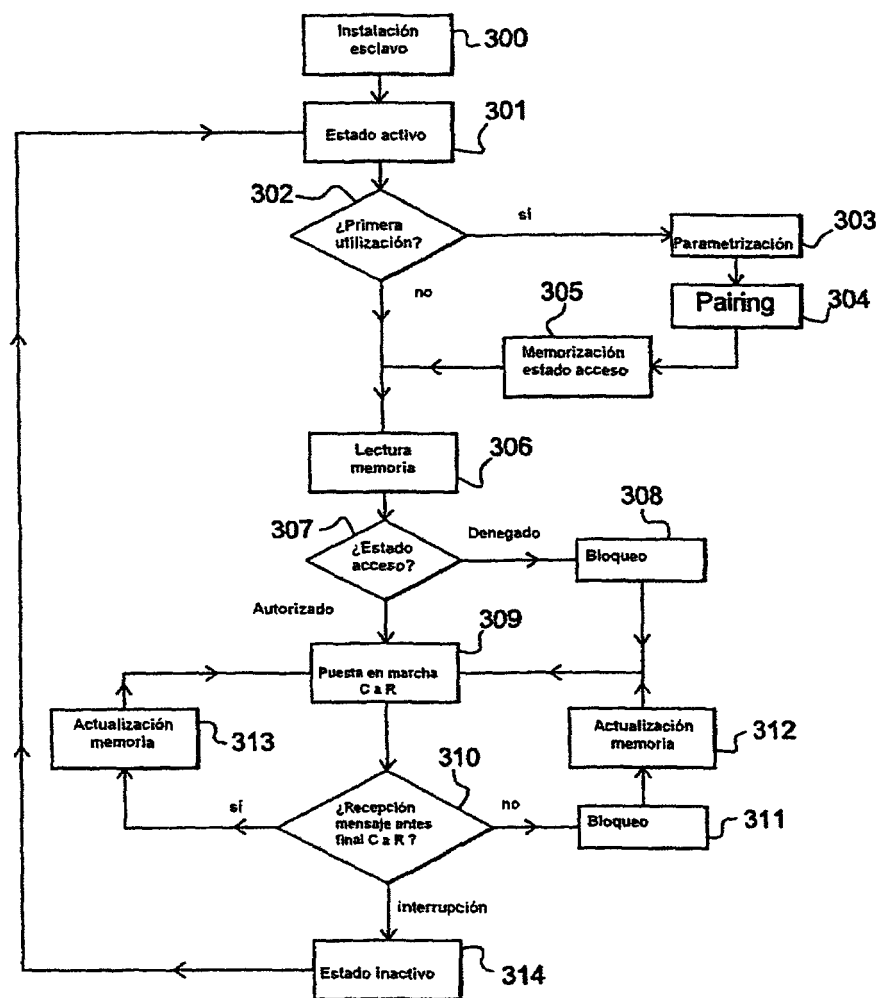


Fig. 3