(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 577 882**

(51) Int. CI.:

G07C 9/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **05.07.2013 E 13175282 (6)**

(97) Fecha y número de publicación de la concesión europea: **27.04.2016 EP 2821970**

(54) Título: **Dispositivo de comunicación de control de acceso, método, programa informático y producto de programa informático**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
19.07.2016

(73) Titular/es:

ASSA ABLOY AB (100.0%)
P.O. Box 70340
107 23 Stockholm, SE

(72) Inventor/es:

BORG, ANDERS;
CEDERBLAD, MATS;
GARMÉN, DANIEL;
JONSSON, TOMAS y
SIKLOSI, PETER

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Dispositivo de comunicación de control de acceso, método, programa informático y producto de programa informático

Campo técnico

La invención se refiere a un dispositivo de comunicación de control de acceso, un método asociado, un programa informático y un producto de programa informático para facilitar la comunicación entre un dispositivo de llave y un dispositivo de control de acceso.

Antecedentes

En la actualidad, los sistemas de control de acceso basados en acceso electrónico se proporcionan usando una diversidad de topologías diferentes. Una de estas soluciones es cuando los dispositivos de bloqueo electrónicos se instalan sin una fuente de alimentación. Los dispositivos de bloqueo pueden entonces alimentarse cuando se inserta un dispositivo de llave de coincidencia, usando una conexión eléctrica con el dispositivo de llave.

Existe un problema en cómo se proveen los dispositivos de bloqueo de derechos de acceso actualizados. Por ejemplo, si una persona pierde un dispositivo de llave, debería ser fácil y fiable que un operador del sistema de control de acceso prohibiera al dispositivo de llave perdido obtener el acceso a cualquiera de los dispositivos de bloqueo del sistema de control de acceso.

En la técnica anterior, los dispositivos de llave se actualizan usando dispositivos de actualización de llave dedicados conectados a ordenadores portátiles. Aunque esto puede proporcionar derechos de acceso actualizados a los dispositivos de llave para la provisión a los dispositivos de bloqueo, los dispositivos de actualización de llave son grandes y pesados, por lo que las llaves no se actualizan con mucha frecuencia. Esto hace que la seguridad se vea comprometida, ya que puede pasar una cantidad significativa de tiempo desde que un operador actualiza los derechos de acceso hasta que los derechos de acceso actualizados se propagan a todos los dispositivos de bloqueo.

El documento US 2011/140838 A1 presenta un centro de control a través del que, en unos medios codificados de identificación de llave y de usuario, se registran un código de identificación de los propios medios, un código de identificación del usuario, un primer conjunto de información referente a las operaciones de apertura permitidas en los medios de lectura para permitir el acceso, un tercer conjunto de información referente a los medios invalidados y un segundo conjunto de información, proporcionada por los medios de lectura, correspondiente a las diferentes aperturas realizadas. Se evita la conexión entre el centro de control y los medios de lectura con los medios que constituyen los medios de comunicación entre los mismos.

El documento WO 2012/097917 A1 presenta una identificación de usuario/vehículo por la que unos derechos de acceso, unos privilegios y/o una configuración de usuario pueden asociarse a un usuario específico asignado a un vehículo específico (por ejemplo, el conductor). En particular, la aplicación se refiere al uso de un ID de usuario/vehículo almacenado en un control remoto de llave de coche para asociar los derechos de acceso, los privilegios y/o la configuración de usuario que tienen una relación con el vehículo, identificado por el ID del vehículo, con el usuario del control remoto de llave de coche. Se describe un sistema para la autenticación de un usuario de un vehículo. El sistema comprende un dispositivo de identificación adaptado para almacenar una cadena de ID de usuario/vehículo, en el que la cadena de ID de usuario/vehículo identifica el usuario del vehículo y el vehículo asociado; y un dispositivo de autenticación adaptado para recibir la cadena de ID de usuario/vehículo del dispositivo de ID, y para asociar los derechos de acceso, los privilegios y/o la configuración de usuario con el usuario del dispositivo de ID, cuando se ha verificado el ID de usuario/vehículo.

El documento EP 1 321 901 A2 presenta un método para controlar el acceso a un objeto en el que se usa un objeto móvil o llave para deshacer o liberar un bloqueo cuando se autoriza la llave.

Sumario

Un objeto es proporcionar una manera más conveniente de facilitar una comunicación entre un dispositivo de control de acceso y un dispositivo de bloqueo.

De acuerdo con un primer aspecto, se presenta un dispositivo de comunicación de control de acceso que comprende: un módulo de comunicación por radio de corta distancia; un módulo de comunicación por radio móvil; y un controlador dispuesto para comunicar los derechos de acceso asociados con un dispositivo de llave, usando el módulo de comunicación por radio móvil, con un dispositivo de control de acceso a través de una red de comunicación móvil una vez que el dispositivo de control de acceso está en comunicación con un dispositivo de llave, usando el módulo de comunicación por radio de corta distancia. Tal dispositivo de comunicación de control de acceso simplifica enormemente la comunicación entre el dispositivo de llave y el dispositivo de control de acceso en

comparación con la técnica anterior. Además, tal dispositivo de comunicación de control de acceso puede fabricarse pequeño y podría, por ejemplo, llevarse en el bolsillo de un usuario. La comunicación puede producirse desde el dispositivo de llave al dispositivo de control de acceso y/o viceversa.

El controlador puede estar dispuesto para realizar una cualquiera o más de las siguientes comunicaciones con el dispositivo de control de acceso, después de que el dispositivo de control de acceso entra en contacto con un dispositivo de llave, usando el módulo de comunicación por radio de corta distancia: recibir los derechos de acceso actualizados para uno o más dispositivos de bloqueo, recibir los derechos de acceso actualizados específicamente para el dispositivo de llave, recibir un tiempo de validez actualizado para el dispositivo de llave, recibir un tiempo actualizado para un reloj del dispositivo de llave, enviar un registro de auditoría para uno o más dispositivos de bloqueo, y enviar un registro de auditoría para el dispositivo de llave. Esto proporciona una mayor seguridad suministrando datos de acceso entre el dispositivo de llave y el dispositivo de control de acceso.

El controlador puede estar dispuesto solo para realizar la comunicación con el dispositivo de control de acceso cuando se ha determinado que una condición de disparo es verdadera.

La condición de disparo puede ser verdadera cuando expira un temporizador del dispositivo de comunicación de control de acceso.

El dispositivo de comunicación de control de acceso puede comprender además un dispositivo de entrada de usuario, en cuyo caso, la condición de disparo es verdadera cuando se detecta un comando de actualización usando el dispositivo de entrada de usuario.

El dispositivo de comunicación de control de acceso puede formar parte de un terminal de comunicación móvil.

El dispositivo de comunicación de control de acceso puede comprender además un dispositivo de entrada de código, en cuyo caso, el controlador está dispuesto para ampliar un tiempo de validez de un dispositivo de llave en comunicación con el dispositivo de comunicación de control de acceso, cuando se ha introducido un código correcto usando el dispositivo de entrada de código.

De acuerdo con un segundo aspecto, se presenta un método, realizado en un dispositivo de comunicación de control de acceso. El dispositivo de comunicación de control de acceso comprende un módulo de comunicación por radio de corta distancia; un módulo de comunicación por radio móvil; y un controlador. El método comprende las etapas de: determinar que un dispositivo de llave está en comunicación con el dispositivo de control de acceso usando el módulo de comunicación por radio de corta distancia; y comunicar los derechos de acceso asociados con el dispositivo de llave, usando el módulo de comunicación por radio móvil, con un dispositivo de control de acceso a través de una red de comunicación móvil.

La etapa de comunicar puede comprender la realización de una cualquiera o más de las siguientes tareas de comunicación con el dispositivo de control de acceso: recibir los derechos de acceso actualizados para uno o más dispositivos de bloqueo, recibir los derechos de acceso actualizados específicamente para el dispositivo de llave, recibir un tiempo de validez actualizado para el dispositivo de llave, recibir un tiempo actualizado para un reloj del dispositivo de llave, enviar un registro de auditoría para uno o más dispositivos de bloqueo, y enviar un registro de auditoría para el dispositivo de llave.

El método puede comprender además las etapas de: determinar si una condición de disparo es verdadera; en cuyo caso, la etapa de comunicar con el dispositivo de control de acceso solo se produce cuando se ha determinado que la condición de disparo es verdadera.

En la etapa de determinar si una condición de disparo es verdadera, la condición de disparo puede ser verdadera cuando expira un temporizador del dispositivo de comunicación de control de acceso.

El dispositivo de comunicación de control de acceso puede comprender además un dispositivo de entrada de usuario, en cuyo caso, en la etapa de determinar si una condición de disparo es verdadera, la condición de disparo es verdadera cuando se detecta un comando de actualización del usuario usando el dispositivo de entrada de usuario.

El método puede comprender además las etapas de: recibir, usando un dispositivo de entrada de código, un código introducido por un usuario; y ampliar un tiempo de validez de un dispositivo de llave en comunicación con el dispositivo de comunicación de control de acceso.

La etapa de comunicar con el dispositivo de control de acceso puede comprender actuar como una pasarela entre el dispositivo de llave y el dispositivo de control de acceso.

De acuerdo con un tercer aspecto, se proporciona un programa informático que comprende un código de programa informático que, cuando se ejecuta en un dispositivo de comunicación de control de acceso, obliga al dispositivo de

comunicación de control de acceso a: determinar que un dispositivo de llave está en comunicación con el dispositivo de control de acceso usando el módulo de comunicación por radio de corta distancia; y comunicar los derechos de acceso asociados con el dispositivo de llave, usando el módulo de comunicación por radio móvil, con un dispositivo de control de acceso a través de una red de comunicación móvil.

De acuerdo con un cuarto aspecto, se proporciona un producto de programa informático que comprende un programa informático de acuerdo con el tercer aspecto y un medio legible por ordenador en el que se almacena el programa informático.

Cabe señalar que, cuando proceda, puede aplicarse cualquier característica de los aspectos primero, segundo, tercero y cuarto a cualquier otro de estos aspectos.

En general, todos los términos usados en las reivindicaciones deben interpretarse de acuerdo con su significado habitual en el campo técnico, a menos que se defina explícitamente lo contrario en el presente documento. Todas las referencias a “un/el elemento, aparato, componente, medio, etapa, etc.” deben interpretarse en sentido amplio en referencia a al menos un ejemplo del elemento, aparato, componente, medio, etapa, etc., a menos que se indique explícitamente lo contrario. Las etapas de cualquier método desvelado en el presente documento no tienen que realizarse en el orden exacto desvelado, a menos que se indique explícitamente.

Breve descripción de los dibujos

A continuación, se describe la invención, a modo de ejemplo, con referencia a los dibujos adjuntos, en los que:

la figura 1 es un diagrama esquemático que ilustra un sistema de control de acceso en el que pueden aplicarse las realizaciones presentadas en el presente documento;

la figura 2 es un diagrama esquemático que ilustra de manera más detallada un dispositivo de llave y un dispositivo de bloqueo de la figura 1;

la figura 3 es un diagrama esquemático que ilustra algunos componentes del dispositivo de llave de las figuras 1 y 2;

la figura 4 es un diagrama esquemático que ilustra el dispositivo de comunicación de control de acceso de la figura 1; y

la figura 5 es un diagrama esquemático que ilustra un método realizado en el dispositivo de comunicación de control de acceso de las figuras 1 y 4.

Descripción detallada

A continuación, se describirá la invención de manera más detallada en lo sucesivo en el presente documento con referencia a los dibujos adjuntos, en los que se muestran ciertas realizaciones de la invención. Esta invención puede, sin embargo, realizarse de muchas formas diferentes y no debe interpretarse como limitada a las realizaciones expuestas en el presente documento; por el contrario, estas realizaciones se proporcionan a modo de ejemplo, de manera que esta divulgación sea minuciosa y completa, y transmita totalmente el alcance de la invención a los expertos en materia. Los mismos números se refieren a los mismos elementos en toda la descripción.

La figura 1 es un diagrama esquemático que ilustra un sistema de control de acceso 3 en el que pueden aplicarse las realizaciones presentadas en el presente documento. Hay una serie de dispositivos de bloqueo 20. Los dispositivos de bloqueo 20 realizan el control de acceso de los dispositivos de llave 1 presentados a los mismos, por ejemplo, mediante la inserción de uno de los dispositivos de llave 1 en cuestión en el dispositivo de bloqueo 20, por lo que el dispositivo de bloqueo 20 se alimenta por el dispositivo de llave 1. Además, hay una comunicación entre el dispositivo de llave 1 y el dispositivo de bloqueo 20, por lo que el dispositivo de bloqueo realiza el control de acceso electrónico del dispositivo de llave 1. Cuando se concede el acceso, el dispositivo de bloqueo 20 se establece como un estado que puede abrirse, por lo que un usuario puede, por ejemplo, abrir una puerta cuyo acceso está controlado por el dispositivo de bloqueo 20.

El dispositivo de llave 1 está equipado con un módulo de comunicación por radio, por lo que puede comunicarse con un dispositivo de control de acceso 30 del sistema de control de acceso 3. El módulo de comunicación por radio está adaptado para una red de radio de corto alcance (tal como Bluetooth, WiFi, etc.), por lo que el dispositivo de llave 1 se comunica a través de un enlace de radio de corto alcance 36 con un dispositivo de comunicación de control de acceso 70. El dispositivo de comunicación de control de acceso 70 se comunica, a su vez, a través de un enlace de red móvil 35 con la red móvil 32. De esta manera, el dispositivo de comunicación de control de acceso 70 actúa como una pasarela, proporcionando el acceso al dispositivo de control de acceso 30 para el dispositivo de llave 1 y viceversa.
El dispositivo de control de acceso 30 actúa como un controlador en el sistema de control de acceso 3 y puede, por

ejemplo, implementarse usando uno o más ordenadores, por ejemplo, un servidor y un terminal de operador. De este modo, un operador puede controlar los derechos de control de acceso y monitorizar otros aspectos de seguridad del sistema de control de acceso usando el dispositivo de control de acceso 30.

La conexión entre el dispositivo de llave 1 y el dispositivo de control de acceso 30 puede usarse para varios fines. Por ejemplo, los dispositivos de llave 1 pueden usarse para proporcionar datos desde el dispositivo de control de acceso 30 a los dispositivos de bloqueo 20. Para que esto suceda, los dispositivos de llave 1 se conectan en ocasiones al dispositivo de control de acceso 30 para descargar dichos datos. Cuando cada uno de estos dispositivos de llave 1 se introduce posteriormente en un dispositivo de bloqueo 20, los datos vinculados al dispositivo de bloqueo 20 se transfieren al dispositivo de bloqueo 20.

A continuación, se presentará un ejemplo relacionado con los derechos de acceso. El dispositivo de llave 1, en ocasiones, descarga los derechos de acceso que se proporcionan posteriormente a los dispositivos de bloqueo 20 cuando se inserta el dispositivo de llave 1. Los derechos de acceso se almacenan en una memoria del dispositivo de llave 1, proporcionando de este modo una comunicación asíncrona hacia (o desde) los dispositivos de bloqueo 20. Estos derechos de acceso pueden incluir una lista de revocaciones, que indica los dispositivos de llave a los que debe prohibirse obtener el acceso. La lista de revocaciones es global en el sistema de control de acceso y, por lo tanto, se aplica a todos los dispositivos de llave 1 y a todos los dispositivos de bloqueo 20. De esta manera, cualquier cambio en la lista de revocaciones se propaga eficiente e indiscriminadamente por todo el sistema de control de acceso 3 a los dispositivos de bloqueo, aunque estos no tengan una fuente de alimentación por sí mismos y no puedan comunicarse directamente con el dispositivo de control de acceso 30. Sin embargo, ciertos elementos en los derechos de acceso pueden asociarse con un dispositivo de bloqueo específico o un grupo de dispositivos de bloqueo.

Si un usuario en el sistema de control de acceso 3 pierde un dispositivo de llave, el operador del dispositivo de control de acceso 30 puede actualizar los derechos de acceso en el dispositivo de control de acceso, de tal manera que la lista de revocaciones incluya la identidad del dispositivo de llave perdido. Cuando uno o más dispositivos de llave 1 descargan la nueva lista de revocaciones, la lista de revocaciones se proporciona a cualquier dispositivo de bloqueo 20 en el que se inserta el dispositivo de llave 1. Incluso, en muchos casos, el dispositivo de llave perdido descargará la nueva lista de revocaciones, por lo que se denegará el intento de un ladrón de obtener acceso usando el dispositivo de llave perdido.

Alternativa o adicionalmente, los derechos de acceso puede incluir una lista de accesos, que comprende una lista de identificadores de dispositivos de llave que son para obtener acceso. Los derechos de acceso pueden ser globales dentro del sistema, para todos los dispositivos de bloqueo, para dispositivos de bloqueo individuales o para un grupo de dispositivos de bloqueo.

Alternativa o adicionalmente, cada dispositivo de llave 1 puede, en ocasiones, recibir un tiempo de validez actualizado para el dispositivo de llave 1 en cuestión. Cada dispositivo de llave 1 puede tener derechos de acceso que solo son válidos hasta un momento específico, después del cual, el dispositivo de llave 1 pierde sus derechos de acceso. Cuando el dispositivo de llave 1 está en contacto con el dispositivo de control de acceso, su tiempo de validez puede ampliarse. De esta manera, el dispositivo de llave 1 pierde sus derechos de acceso después de una cierta cantidad de tiempo a menos que entre en contacto con el dispositivo de control de acceso 30. En una realización, los derechos de acceso actualizados se descargan en la misma ocasión en que se amplía el tiempo de validez del dispositivo de llave.

La importancia de esta combinación de derechos de acceso y tiempos de validez se ilustrará a continuación en un ejemplo. Digamos que se roba un dispositivo de llave 1. El propietario original informa de esto, y el dispositivo de control de acceso 30 se actualiza con nuevos derechos de acceso, prohibiendo el acceso del dispositivo de llave robado a los dispositivos de bloqueo en el sistema de control de acceso 3. El ladrón no quiere que estos nuevos derechos de acceso se proporcionen a los dispositivos de bloqueo y puede evitar que se produzca la comunicación entre el dispositivo de llave y el dispositivo de control de acceso 30. Sin embargo, el tiempo de validez expirará finalmente y, de esta manera, se evita que el dispositivo de llave robado 1 obtenga acceso. Si, a continuación, el ladrón sabe de alguna manera que el tiempo de validez ha expirado y permite que el dispositivo de llave 1 se comunique con el dispositivo de control de acceso 30, el tiempo de validez puede ampliarse, pero el dispositivo de llave 1 también descargará los derechos de acceso actualizados, por lo que, de esta manera, el dispositivo de llave robado 1 prohibirá el acceso. Opcionalmente, el dispositivo de control de acceso 30 ni siquiera concederá un tiempo de validez ampliado, ya que el dispositivo de llave robado podría marcarse como prohibido (o robado).

Alternativa o adicionalmente, cada dispositivo de llave 1 puede, en ocasiones, recibir un tiempo de validez actualizado para el reloj del dispositivo de llave. Esto garantiza que el reloj del dispositivo de llave sea preciso, lo que garantiza que los tiempos de validez se apliquen con precisión.

La comunicación entre los dispositivos de llave 1 y el dispositivo de control de acceso 30 también puede usarse en la otra dirección, hacia el dispositivo de control de acceso. Cuando la comunicación se produce a través del dispositivo de comunicación de control de acceso 70, el mecanismo es el mismo. Pero en este caso, los datos se transmiten

desde el dispositivo de bloqueo 20 al dispositivo de llave 1. Cuando el dispositivo de llave 1 entra en contacto con el dispositivo de control de acceso 30, los datos se cargan en el dispositivo de control de acceso 30.

De esta manera, el dispositivo de llave 1 usa su memoria como almacenamiento temporal para los datos de los dispositivos de bloqueo 20 en el dispositivo de control de acceso 30. De manera análoga, el dispositivo de comunicación de control de acceso 70 también puede usar su memoria como almacenamiento temporal para los datos de los dispositivos de bloqueo 20 en el dispositivo de control de acceso 30. Por ejemplo, un registro de auditoría de los dispositivos de bloqueo 20 puede cargarse de esta manera en el dispositivo de control de acceso 30. El registro de auditoría en el dispositivo de control de acceso incluye datos sobre el éxito y/o los intentos fallidos de obtener acceso al dispositivo de bloqueo en cuestión.

Además, un registro de auditoría del dispositivo de llave 1 puede cargarse en el dispositivo de control de acceso 30, indicando el éxito y/o los intentos fallidos del dispositivo de llave en cuestión de obtener acceso a los dispositivos de bloqueo.

Opcionalmente, el dispositivo de llave 1 se comunica con el dispositivo de control de acceso 30 para obtener autorización para que se conceda acceso al dispositivo de llave 1 por un dispositivo de bloqueo 20 en tiempo real, cuando se inserta el dispositivo de llave 1 en el dispositivo de bloqueo 20. De esta manera, el dispositivo de control de acceso 30 tiene el control total sobre a qué dispositivo de llave 1 se le permite obtener acceso usando el dispositivo de bloqueo 20.

Como se explica en más detalle a continuación, pueden usarse diversas condiciones de disparo para iniciar la comunicación entre los dispositivos de llave 1 y el dispositivo de control de acceso 30.

La figura 2 es un diagrama esquemático que ilustra con más detalle un dispositivo de llave y un dispositivo de bloqueo de la figura 1.

El dispositivo de llave 1 comprende un conector 12 y una hoja 13, que están aislados eléctricamente uno de otro. El dispositivo de bloqueo 20 comprende un casquillo con un primer conector 22 y un segundo conector 23. El primer conector 22 se coloca de tal manera que, cuando el dispositivo de llave 1 se inserta en el casquillo, el primer conector 22 entra en contacto galvánico con el conector 12 del dispositivo de llave. Análogamente, el segundo conector 23 se coloca de tal manera que, cuando el dispositivo de llave 1 se inserta en el casquillo, el segundo conector 23 entra en contacto galvánico con la hoja 13 del dispositivo de llave 1. Esta disposición proporciona una conexión terminal dual entre el dispositivo de llave 1 y el dispositivo de bloqueo 20 cuando el dispositivo de llave 1 se inserta en el casquillo del dispositivo de bloqueo 20. La conexión terminal dual se usa tanto para la comunicación entre el dispositivo de llave 1 y el dispositivo de bloqueo como para la alimentación del dispositivo de bloqueo mediante la transferencia de energía eléctrica desde una fuente de alimentación del dispositivo de llave 1 al dispositivo de bloqueo 20. Como alternativa, pueden proporcionarse unos conectores separados (no mostrados) para alimentar el dispositivo de bloqueo 20 y la comunicación entre el dispositivo de llave 1 y el dispositivo de bloqueo 20.

La figura 3 es un diagrama esquemático que ilustra algunos componentes del dispositivo de llave de las figuras 1 y 2. Se proporciona un procesador 2 usando cualquier combinación de uno o más de entre una unidad de procesamiento central (CPU), un multiprocesador, un microcontrolador, un procesador digital de señales (DSP), un circuito integrado de aplicación específica, etc., adecuados, capaces de ejecutar instrucciones de software almacenadas en una memoria 17, que, por lo tanto, puede ser un producto de programa informático.

La memoria 17 puede ser cualquier combinación de memoria de lectura y escritura (RAM) y memoria de solo lectura (ROM). La memoria 17 también comprende un almacenamiento permanente, que, por ejemplo, puede ser una sola o una combinación de una memoria de estado sólido, una memoria magnética, o una memoria óptica.

El dispositivo de llave 1 también comprende un módulo de comunicación por radio 6. El módulo de comunicación por radio 6 comprende uno o más transceptores, que comprenden componentes analógicos y digitales, y un número adecuado de antenas. El módulo de comunicación por radio puede proporcionarse para la comunicación a través de radio de corto alcance (tal como, Bluetooth, WiFi, etc.) con el dispositivo de comunicación de control de acceso 70. Opcionalmente, el módulo de comunicación por radio 6 también puede estar adaptado para conectarse de manera independiente a una red móvil para la comunicación con el dispositivo de control de acceso. Usando el módulo de comunicación por radio 6, el dispositivo de llave 1 puede comunicarse con un dispositivo de control de acceso, como se ha explicado anteriormente.

Se proporciona un reloj 4 como parte del dispositivo de llave 1 y se usa para hacer cumplir los tiempos de validez descritos anteriormente.

Se proporciona una batería 18 para alimentar todos los componentes eléctricos del dispositivo de llave y también para alimentar los dispositivos de bloqueo de energía, como se ha explicado anteriormente. La batería 18 puede ser una batería recargable o una batería desechable intercambiable.

Opcionalmente, el dispositivo de llave 1 está provisto de un elemento de entrada de usuario, tal como un botón pulsador 7 o similar, que, por ejemplo, puede usarse por un usuario para iniciar la comunicación con el dispositivo de control de acceso.

Se omiten otros componentes del dispositivo de llave 1 con el fin de no complicar los conceptos presentados en el presente documento.

El dispositivo de llave 1 comprende una hoja 13 para maniobrar mecánicamente un dispositivo de bloqueo 20 tras un control de acceso exitoso. El conector 12 está provisto de un aislamiento eléctrico 14 de la hoja, para facilitar dos terminales de contacto galvánico independientes con un dispositivo de bloqueo.

La figura 4 es un diagrama esquemático que ilustra algunos componentes del dispositivo de comunicación de control de acceso 70 de la figura 1. Se proporciona un procesador 72 usando cualquier combinación de una o más de entre una unidad de procesamiento central (CPU), un multiprocesador, un microcontrolador, un procesador digital de señales (DSP), un circuito integrado de aplicación específica, etc., adecuados, capaces de ejecutar instrucciones de software almacenadas en una memoria 78, que, por lo tanto, puede ser un producto de programa informático. El procesador 72 puede configurarse para ejecutar el método descrito a continuación con referencia a la figura 5.

La memoria 78 puede ser cualquier combinación de memoria de lectura y escritura (RAM) y memoria de solo lectura (ROM). La memoria 78 también comprende un almacenamiento permanente, que, por ejemplo, puede ser una sola o una combinación de una memoria de estado sólido, una memoria magnética, o una memoria óptica. Opcionalmente, una parte o la totalidad de la memoria 78 se incluye en un módulo de identidad de abonado (SIM), implementando de este modo un entorno de almacenamiento y de ejecución de aplicaciones seguro, y puede proporcionar credenciales que pueden usarse por un módulo de comunicación móvil 76.

El módulo de comunicación móvil 76 comprende uno o más transceptores, que comprenden componentes analógicos y digitales, y un número adecuado de antenas. El módulo de comunicación móvil 76 se proporciona para la comunicación con una red móvil, tal como la red móvil 32 de la figura 1, para conectarse con el dispositivo de control de acceso 30.

Se proporciona un módulo de comunicación por radio de corta distancia 75 para la comunicación a través de radio de corto alcance (tal como Bluetooth, WiFi, etc.), por ejemplo, con el dispositivo de llave 1, como se ha explicado anteriormente.

Se proporciona un reloj 74 y se proporciona una batería 79 para alimentar todos los componentes eléctricos del dispositivo de comunicación de control de acceso 70. La batería 79 puede ser una batería recargable o una batería desechable intercambiable.

Se proporciona una interfaz de usuario 71 para permitir a un usuario introducir datos y para recibir la salida de datos. Por ejemplo, la interfaz de usuario 71 puede comprender uno o más de entre una pantalla, que es opcionalmente una pantalla táctil, un teclado, un micrófono, un altavoz, etc.

Opcionalmente, se proporciona un dispositivo de entrada de código 77 como parte de la interfaz de usuario 71. El dispositivo de entrada de código 77 puede, por ejemplo, usarse para permitir al usuario ampliar el tiempo de validez de un dispositivo de llave 1 en contacto con el dispositivo de comunicación de control de acceso 70, cuando el acceso al dispositivo de control de acceso no está disponible a través de la red móvil, por ejemplo, debido a las condiciones de radio/el aislamiento de radio actuales. El dispositivo de entrada de código puede ser, por ejemplo, un teclado o una parte de una pantalla táctil adecuadamente controlada.

Se omiten otros componentes del dispositivo de comunicación de control de acceso 70 con el fin de no complicar los conceptos presentados en el presente documento.

En una realización, el dispositivo de comunicación de control de acceso 70 forma parte de un terminal de comunicación móvil.

La figura 5 es un diagrama esquemático que ilustra un método realizado en el dispositivo de comunicación de control de acceso 70 de las figuras 1 y 4.

En una etapa de *disparar* opcional 91, se determina si una condición de disparo es verdadera. Si este es el caso, el método continúa a una etapa de *determinar comunicación con dispositivo de llave* 90. De lo contrario, el método repite la etapa de *disparar* condicional 91, opcionalmente después de un período de inactividad.

La condición de activación puede ser, por ejemplo, que expire un temporizador del dispositivo de comunicación de control de acceso. Alternativa o adicionalmente, la condición de disparo puede ser que accione un elemento de entrada del usuario (71 de la figura 4) del dispositivo de comunicación de control de acceso, indicando un comando de actualización. Cuando se omite esta etapa, el método comienza con una etapa de *determinar comunicación con*

dispositivo de llave 90.

En la etapa de *determinar comunicación con dispositivo de llave* 90, el dispositivo de comunicación de control de acceso determina que un dispositivo de llave está en comunicación con el dispositivo de control de acceso usando su módulo de comunicación por radio de corta distancia (véase 75 de la figura 4).

En la etapa de *comunicar con dispositivo de control de acceso* 92, el dispositivo de comunicación de control de acceso se comunica con el dispositivo de control de acceso, cuando es posible, actuando como una pasarela para la comunicación descrita anteriormente con referencia a la figura 1, por ejemplo, para actualizar derechos de acceso y/o para proporcionar registros de auditoría. El dispositivo de comunicación de control de acceso puede, por lo tanto, actuar como una pasarela entre el dispositivo de llave y el dispositivo de control de acceso. Si el dispositivo de comunicación de control de acceso es incapaz de comunicarse con el dispositivo de control de acceso, se considera que el dispositivo de comunicación de control de acceso está fuera de línea.

En la etapa de *introducir código* condicional 93, se determina si debe introducirse un código. Esto puede deberse, por ejemplo, a que el dispositivo de comunicación de control de acceso (y, por lo tanto, cualquier dispositivo de llave conectado) esté fuera de línea y se necesite introducir un código para ampliar el tiempo de validez del dispositivo de llave en contacto con el dispositivo de comunicación de control de acceso. En una realización, se requiere introducir un código de vez en cuando para ampliar el tiempo de validez de un dispositivo de llave. Esto podría ser cada vez que se amplía el tiempo de validez, o con menor frecuencia (o mayor frecuencia) que eso. Esto evita que alguien que no conoce el código obtenga el acceso usando un dispositivo de llave perdido, incluso si la lista de revocaciones no se ha actualizado todavía. En una realización, se requiere introducir un código cada vez que se necesita el acceso a un dispositivo de bloqueo, independientemente de si el dispositivo de llave está fuera de línea o en línea. Si es necesario introducir un código, el método continúa a una etapa de *recibir entrada de código* 94. De lo contrario, el método finaliza.

En la etapa de *recibir entrada de código* 94, se recibe un código del usuario del dispositivo de comunicación de control de acceso usando el dispositivo de entrada de código de dispositivo de comunicación de control de acceso.

En una etapa de *corregir código* condicional 95, se evalúa si el código que se ha introducido por el usuario es correcto o no. Si este es el caso, el método continúa a una etapa de *ampliar tiempo de validez* 96. De lo contrario, el método o bien vuelve a la etapa de *recibir entrada de código* 94 o el método finaliza, si se han detectado demasiados intentos fallidos de introducción de código.

En la etapa de *ampliar tiempo de validez* 96, se amplía el tiempo de validez del dispositivo de llave en contacto con el dispositivo de comunicación de control de acceso, como se ha explicado anteriormente.

Opcionalmente, el método se repite para estar listo para más comunicaciones entre el dispositivo de control de acceso y el dispositivo de llave.

Principalmente, la invención se ha descrito anteriormente con referencia a unas pocas realizaciones. Sin embargo, como se apreciará fácilmente por los expertos en la materia, otras realizaciones distintas de las desveladas anteriormente son igualmente posibles dentro del alcance de la invención, como se define por las reivindicaciones de patente adjuntas.

REIVINDICACIONES

1. Un dispositivo de comunicación de control de acceso (70) que comprende:

un módulo de comunicación por radio de corta distancia (75);
un módulo de comunicación por radio móvil (76); y
un controlador (72) dispuesto para comunicar los derechos de acceso asociados con un dispositivo de llave, usando el módulo de comunicación por radio móvil (76), con un dispositivo de control de acceso (30) a través de una red de comunicación móvil (32) después de que el dispositivo de comunicación de control de acceso (70) entra en comunicación con el dispositivo de llave (1), usando el módulo de comunicación por radio de corta distancia (75), en el que los derechos de acceso comprenden los derechos de acceso actualizados para uno o más dispositivos de bloqueo (20).

2. El dispositivo de comunicación de control de acceso (70) de acuerdo con la reivindicación 1, en el que el controlador está dispuesto para realizar una cualquiera o más de las siguientes comunicaciones con el dispositivo de control de acceso (30) después de que el dispositivo de comunicación de control de acceso (70) entra en contacto con un dispositivo de llave (1), usando el módulo de comunicación por radio de corta distancia (75): recibir los derechos de acceso actualizados para uno o más dispositivos de bloqueo (20), recibir los derechos de acceso actualizados específicamente para el dispositivo de llave (1), recibir un tiempo de validez actualizado para el dispositivo de llave (1), recibir un tiempo actualizado para un reloj del dispositivo de llave (1), enviar un registro de auditoría para uno o más dispositivos de bloqueo (20), y enviar un registro de auditoría para el dispositivo de llave (1).

3. El dispositivo de comunicación de control de acceso (70) de acuerdo con la reivindicación 1 o 2, en el que el controlador (72) está dispuesto solo para realizar la comunicación con el dispositivo de control de acceso (30) cuando se ha determinado que una condición de disparo es verdadera.

4. El dispositivo de comunicación de control de acceso (70) de acuerdo la reivindicación 3, en el que la condición de disparo es verdadera cuando expira un temporizador del dispositivo de comunicación de control de acceso (70).

5. El dispositivo de comunicación de control de acceso (70) de acuerdo con las reivindicaciones 3 o 4, en el que el dispositivo de comunicación de control de acceso (70) comprende además una interfaz de usuario (71), y la condición de disparo es verdadera cuando se detecta un comando de actualización usando la interfaz de usuario (71).

6. El dispositivo de comunicación de control de acceso (70) de acuerdo con una cualquiera de las reivindicaciones 1 a 5, en el que el dispositivo de comunicación de control de acceso (70) forma parte de un terminal de comunicación móvil (79).

7. El dispositivo de comunicación de control de acceso (70) de acuerdo una cualquiera de las reivindicaciones 1 a 6 que comprende además un dispositivo de entrada de código (77), en el que el controlador (2) está dispuesto para ampliar un tiempo de validez de un dispositivo de llave (1) en comunicación con el dispositivo de comunicación de control de acceso (70), cuando se ha introducido un código correcto usando el dispositivo de entrada de código (77).

8. Un método, realizado en un dispositivo de comunicación de control de acceso (70), comprendiendo el dispositivo de comunicación de control de acceso un módulo de comunicación por radio de corta distancia (75); un módulo de comunicación por radio móvil (76); y un controlador (72), comprendiendo el método las etapas de:

determinar (90) que un dispositivo de llave (1) está en comunicación con el dispositivo de comunicación de control de acceso (70) usando el módulo de comunicación por radio de corta distancia (75); y
comunicar (92) los derechos de acceso asociados con el dispositivo de llave usando el módulo de comunicación por radio móvil (76), con un dispositivo de control de acceso (30) a través de una red de comunicación móvil (32), en el que los derechos de acceso comprenden los derechos de acceso actualizados para uno o más dispositivos de bloqueo (20).

9. El método de acuerdo con la reivindicación 8, en el que la etapa de comunicar (92) comprende realizar una cualquiera o más de las siguientes tareas de comunicación con el dispositivo de control de acceso (30): recibir los derechos de acceso actualizados para uno o más dispositivos de bloqueo (20), recibir los derechos de acceso actualizados específicamente para el dispositivo de llave (1), recibir un tiempo de validez actualizado para el dispositivo de llave (1), recibir un tiempo actualizado para un reloj del dispositivo de llave (1), enviar un registro de auditoría para uno o más dispositivos de bloqueo (20), y enviar un registro de auditoría para el dispositivo de llave (1).

10. El método de acuerdo con la reivindicación 8 o 9, que comprende además la etapa de:

determinar (91) si una condición de disparo es verdadera;
y en el que la etapa de comunicar (92) con el dispositivo de control de acceso solo se produce cuando se ha determinado que la condición de disparo es verdadera.

11. El método de acuerdo con la reivindicación 10, en el que en la etapa de determinar (91) si una condición de disparo es verdadera, la condición de disparo es verdadera cuando expira un temporizador del dispositivo de comunicación de control de acceso (70).

12. El método de acuerdo con las reivindicaciones 10 u 11, en el que el dispositivo de comunicación de control de acceso (70) comprende además una interfaz de usuario (71), y en la etapa de determinar (91) si una condición de disparo es verdadera, la condición de disparo es verdadera cuando se detecta un comando de actualización del usuario usando la interfaz de usuario (71).

13. El método de acuerdo con una cualquiera de las reivindicaciones 9 a 12, que comprende además las etapas de:

recibir (94), usando un dispositivo de entrada de código (77), un código introducido por un usuario; y
ampliar (96) un tiempo de validez de un dispositivo de llave (1) en comunicación con el dispositivo de comunicación de control de acceso (70).

14. El método de acuerdo con una cualquiera de las reivindicaciones 9 a 13, en el que la etapa de comunicarse con el dispositivo de control de acceso (92) comprende actuar como una pasarela entre el dispositivo de llave (1) y el dispositivo de control de acceso (30).

15. Un programa informático (66) que comprende un código de programa informático que, cuando se ejecuta en un dispositivo de comunicación de control de acceso (70), obliga al dispositivo de comunicación de control de acceso (70) a:

determinar que un dispositivo de llave (1) está en comunicación con el dispositivo de comunicación de control de acceso (70) usando el módulo de comunicación por radio de corta distancia (75); y
comunicar los derechos de acceso asociados con el dispositivo de llave, usando el módulo de comunicación por radio móvil (76), con un dispositivo de control de acceso (30) a través de una red de comunicación móvil (32), en el que los derechos de acceso comprenden los derechos de acceso actualizados para uno o más dispositivos de bloqueo (20).

16. Un producto de programa informático (78) que comprende un programa informático de acuerdo con la reivindicación 15 y un medio legible por ordenador en el que se almacena el programa informático.

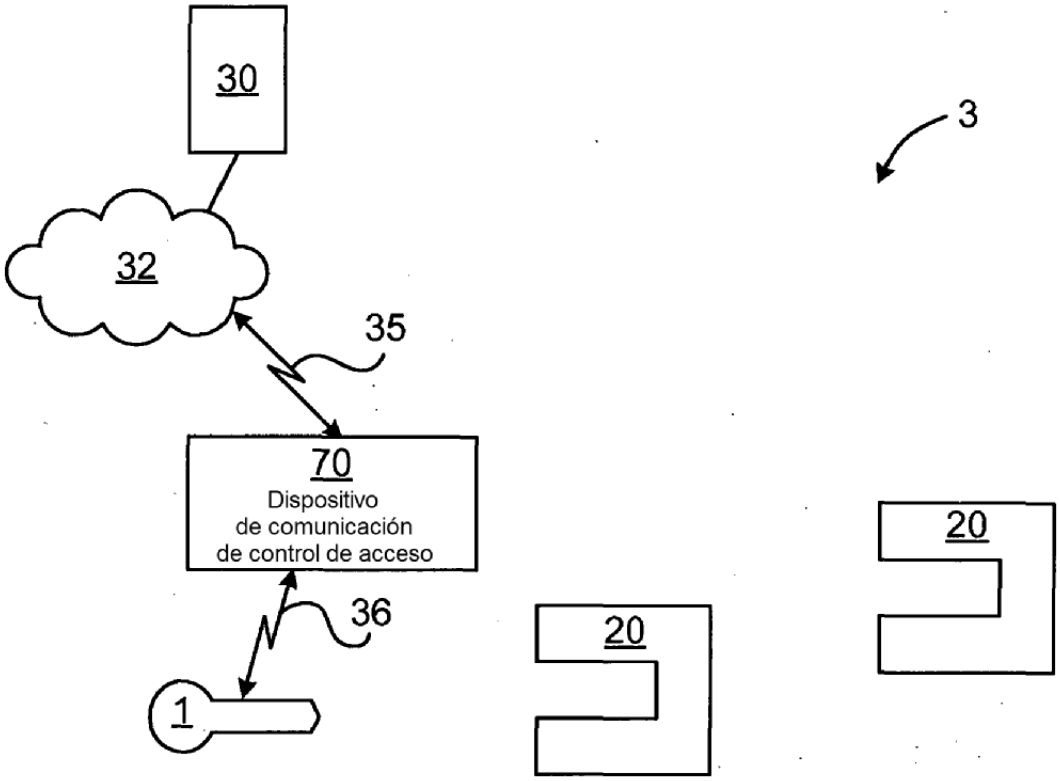
30
3
32
35
70
Dispositivo
de comunicación
de control de acceso
20
20
36
1

Fig. 1

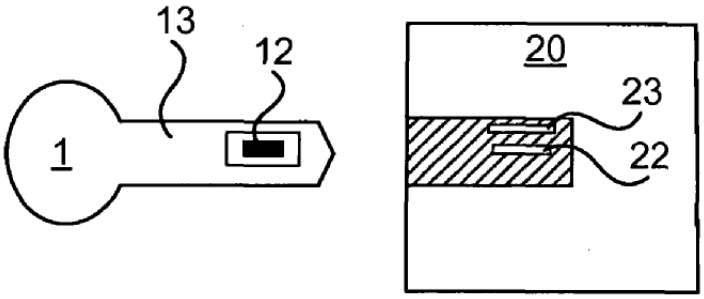
13
12
20
23
1
22

Fig. 2

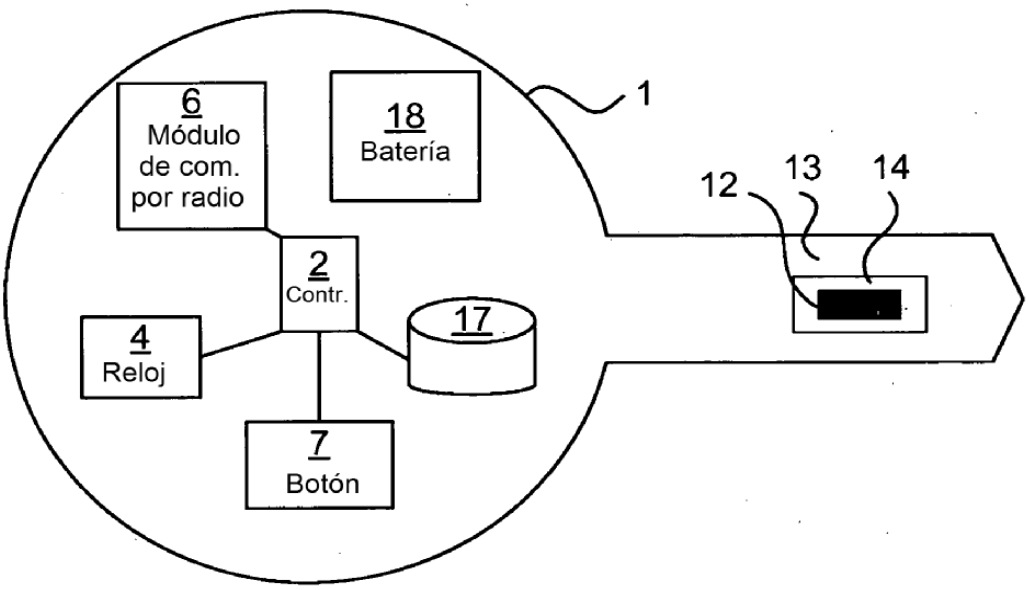
6
Módulo de com. por radio
18
Batería
1
12
13
14
2
Contr.
17
4
Reloj
7
Botón

Fig. 3

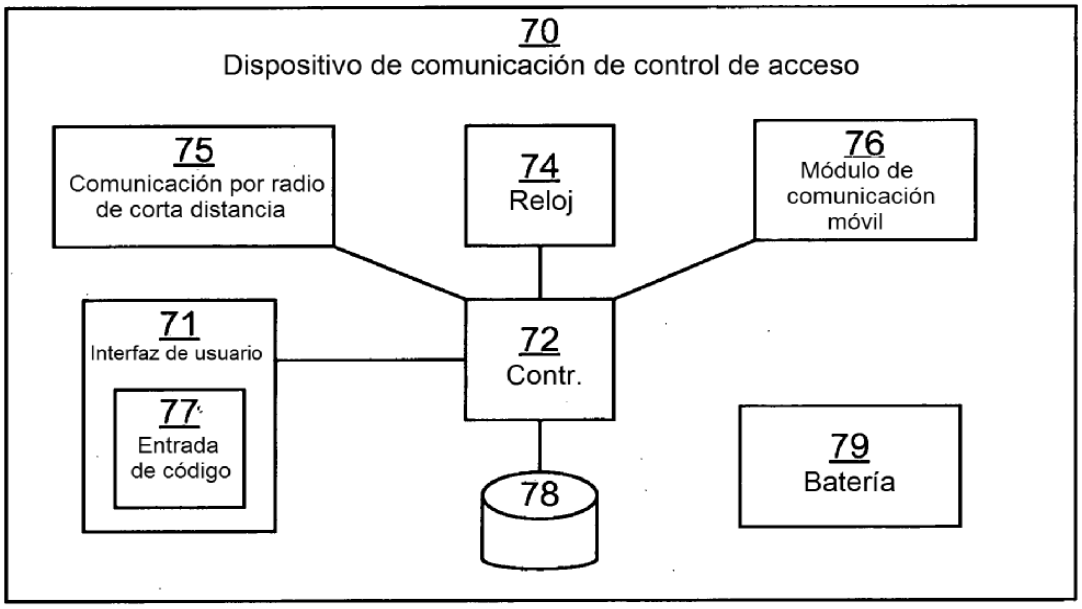
70
Dispositivo de comunicación de control de acceso
75
Comunicación por radio de corta distancia
74
Reloj
76
Módulo de comunicación móvil
71
Interfaz de usuario
77
Entrada de código
72
Contr.
78
79
Batería

Fig. 4

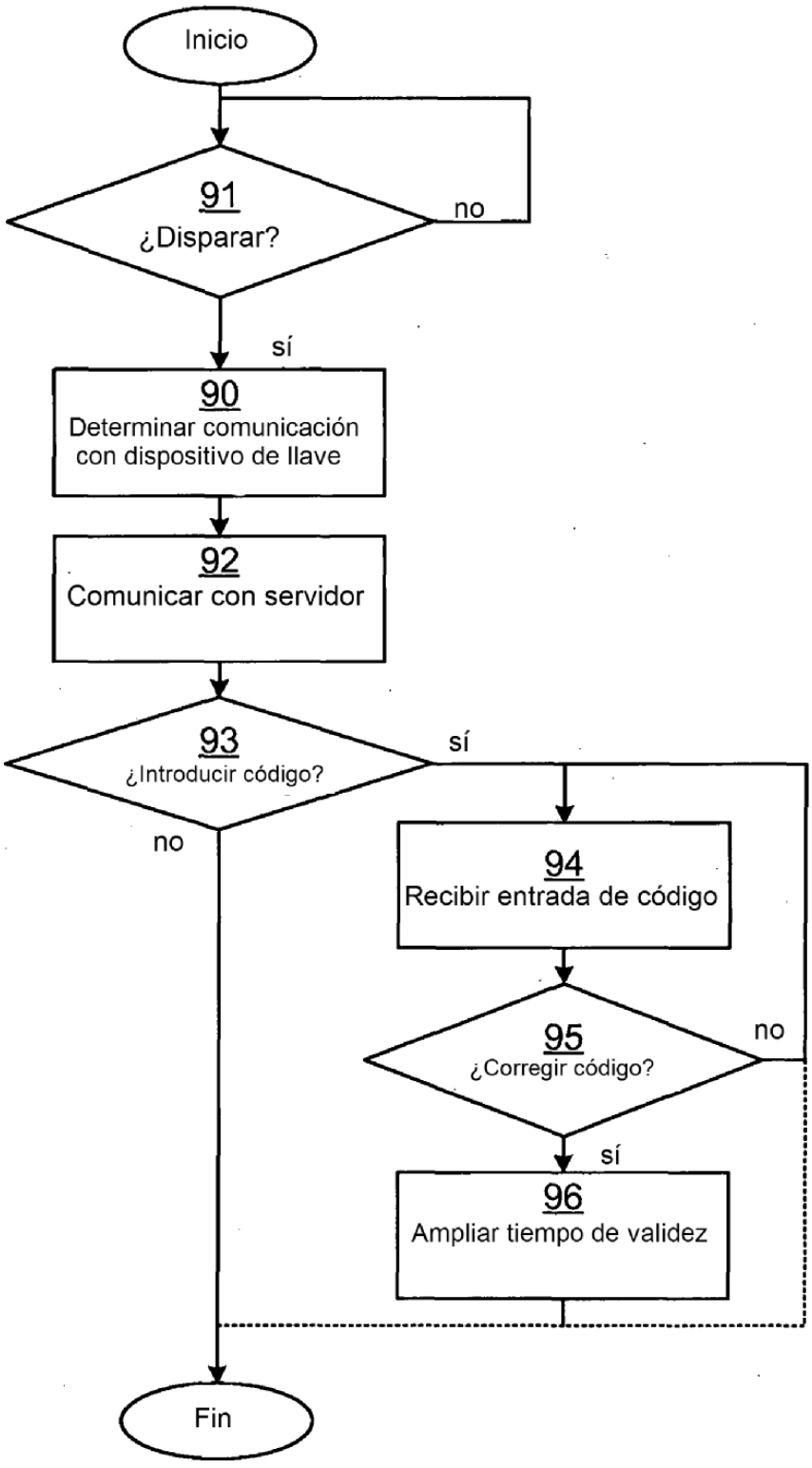
Inicio
91
¿Disparar?
no
sí
90
Determinar comunicación con dispositivo de llave
92
Comunicar con servidor
93
¿Introducir código?
sí
no
94
Recibir entrada de código
95
¿Corregir código?
no
sí
96
Ampliar tiempo de validez
Fin

Fig. 5