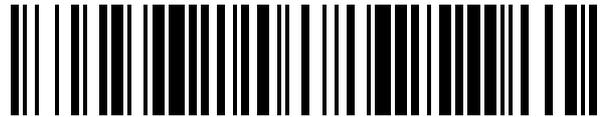


19



OFICINA ESPAÑOLA DE  
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **1 233 034**

21 Número de solicitud: 201930838

51 Int. Cl.:

**G07C 9/00** (2006.01)

12

SOLICITUD DE MODELO DE UTILIDAD

U

22 Fecha de presentación:

**20.05.2019**

43 Fecha de publicación de la solicitud:

**30.07.2019**

71 Solicitantes:

**NAOME INVERSIONES S.L (100.0%)  
AVD. TENIENTE MONTESINOS Nº 8 TORRE A 4º  
PLANTA  
30100 ESPINARDO (Murcia) ES**

72 Inventor/es:

**ANGEL O , Franco Fenollar**

74 Agente/Representante:

**ABELLÁN PÉREZ, Almudena**

54 Título: **Dispositivo autónomo para control de accesos**

**ES 1 233 034 U**

## DESCRIPCIÓN

Dispositivo autónomo para control de accesos

### 5 **Campo técnico de la invención**

La presente invención corresponde al campo técnico de los sistemas de control de accesos que presentan cerradura electrónica, en concreto a un dispositivo autónomo para control de accesos mediante al menos un dispositivo móvil que presenta una aplicación apta para  
10 establecer conexión a una base de datos contenida en un servidor para la obtención de un código de acceso.

### **Antecedentes de la Invención**

15 En la actualidad cada vez está más extendido el uso de controles de accesos, que inicialmente iban dirigidos al control en instalaciones de empresas, pero a día de hoy se están orientando igualmente a instalaciones privadas como urbanizaciones, viviendas...

Estos controles de accesos permiten que exista una vigilancia de quién puede acceder o no  
20 al interior de determinados espacios, de manera que la función principal es la de establecer un filtro en los accesos principales de instalaciones como edificios de oficinas, obras, industrias, urbanizaciones, parques empresariales, etc.

Entre las ventajas que presenta la utilización de un control de accesos puede destacarse la  
25 comodidad a la hora de poder acceder al lugar determinado, por ejemplo un centro de trabajo, sin tener que disponer de llaves del mismo y sin necesidad de que nadie deba interrumpir su trabajo para abrir la puerta. Del mismo modo, permite entrar en el centro en horarios en los que no existe personal encargado para abrir las puertas, por ejemplo para trabajos en horario nocturno.

30 Por otro lado, aumenta la seguridad del espacio cuyo acceso está controlado, pudiendo evitar de forma efectiva la entrada de intrusos.

En determinadas situaciones pueden ser muy necesarios, como el caso de empresas con  
35 elevada rotación de personal, pues este hecho no permite que el personal de seguridad sea capaz de reconocer a todos los trabajadores de las mismas. Con el uso de un sistema de

control de accesos, cada usuario posee su identificación, que puede ser de múltiples formas, para poder acceder al recinto.

5 Por otra parte, para que un control de accesos a unas instalaciones sea eficaz, al mismo tiempo que se impiden los accesos no autorizados, debe garantizarse un acceso ágil a las mismas.

10 Dentro de los sistemas de control de accesos, pueden distinguirse dos tipos de control fundamentales. El primer tipo son los sistemas autónomos que no requieren de ningún tipo de infraestructura ni conectividad a la red y en los que el propio terminal permite controlar una o más puertas, sin estar conectados a un PC o un sistema central, por lo tanto, no guardan registro de eventos. Para ello, el usuario presenta una clave contenida en un dispositivo, por ejemplo en una tarjeta magnética, y debe ser identificada por el lector del sistema para permitir el acceso.

15

Presentan la ventaja de no depender de la existencia de una conexión a la red para poder funcionar, siendo altamente fiables y de gran utilidad en multitud de lugares. Por contra presentan una capacidad más limitada en cuanto a usuarios y, son más limitados en la funcionalidad de los mismos. Además, es necesario que el usuario acceda directamente al lector mostrando su identificación y, los dispositivos utilizados como identificación, tales como tarjetas magnéticas o similares, suelen tener un elevado riesgo de fallo.

20

El segundo tipo son los sistemas de control de acceso en red, que se integran a través de un PC local o remoto, donde se hace uso de un software de control que permite llevar un registro de todas las operaciones realizadas sobre el sistema. Estos sistemas requieren de una conectividad con el software, mediante una red (Ethernet, RS232, wifi...).

25

En estos sistemas centralizados el lector de la identificación se conecta mediante un bus a una o varias unidades centrales que son las que almacenan toda la información de la instalación, tanto de configuración como de registro de incidencias.

30

Pueden gestionar miles de usuarios y accesos y la gestión se realiza desde uno o varios ordenadores conectados a un servidor que es el responsable de permitir o no el acceso del usuario. Así pues, la identificación detectada por el lector se envía al servidor que revisa el cumplimiento de ciertos valores para permitir el acceso o no y comunica el resultado.

35

En la actualidad cada vez están más extendidos los sistemas de control de acceso en red, que precisan la conexión del usuario con un servidor central, normalmente a través de un dispositivo móvil. Son sistemas más cómodos, pues el usuario no precisa tener que acercarse mucho al dispositivo, al activar el control de acceso vía internet.

5

El inconveniente es que al estar condicionados a la existencia de una red de comunicación vía internet y a que exista cobertura de la misma en el lugar a instalarlo, estos sistemas pueden tener errores de funcionamiento ante caídas de la red o por falta de cobertura de los dispositivos móviles utilizados.

10

Existen múltiples usos de control de accesos que no requieren de un registro de tiempos de entradas y salidas, como por ejemplo aquellos en los que únicamente se busca la seguridad de que sea una persona autorizada la que pueda acceder a una instalación y nunca una persona sin autorización, pero no importa la hora de llegada de dicha persona. En estos casos podría ser muy conveniente aprovechar las ventajas de un sistema de control autónomo, que se encargue de estas funciones sin necesidad de conectarse a un servidor que lo controle a él y al mismo tiempo, conseguir un aumento de las funcionalidades del dispositivo, para que sea capaz de administrar una gran cantidad de usuarios e incluso controlar más de una cerradura.

20

Por tanto, sería deseable encontrar un dispositivo de control de accesos que resulte autónomo pero que tuviera una mayor funcionalidad que los sistemas de control autónomos actuales. Que sea capaz de controlar distintos accesos, evitando el uso de los dispositivos de identificación físicos que presentan alto porcentaje de error y al mismo tiempo, que sea un dispositivo de control que resulte igual de cómodo y eficaz que un sistema vía red pero manteniendo una completa autonomía que le permita determinar si debe aceptarse o denegarse un acceso por sí solo, sin necesidad de conectarse a la red en ningún momento, para evitar los inconvenientes de una necesaria conectividad a la red.

30 **Descripción de la invención**

El dispositivo autónomo para control de accesos, para accesos con cerradura electrónica, mediante al menos un dispositivo móvil que presenta una aplicación apta para establecer conexión a una base de datos contenida en un servidor para la obtención de un código de acceso que aquí se presenta, comprende una carcasa de contención dispuesta próxima a la cerradura electrónica.

35

Dicha carcasa comprende en su interior una placa de circuito impreso que presenta un microcontrolador de código abierto y un software, donde dicha placa presenta unos primeros medios de conexión directa a la cerradura electrónica y unos segundos medios de conexión directa a la corriente eléctrica.

Comprende además unos medios de comunicación con el al menos un dispositivo móvil que permiten la recepción del correspondiente código de acceso. Estos medios de comunicación están formados por al menos dos antenas bluetooth conectadas a dicha placa, compatibles cada una de ellas con un sistema operativo de dispositivos móviles.

De este modo, el dispositivo móvil, en función del sistema operativo con el que opere, se conecta con la placa de circuito impreso mediante la antena de bluetooth correspondiente a dicho sistema y mediante dicha conexión comunica el código de acceso que previamente le ha sido otorgado a través de la aplicación.

El dispositivo comprende a su vez un módulo relé de al menos dos canales conectado a la placa.

Con el dispositivo autónomo para control de accesos que aquí se propone se obtiene una mejora significativa del estado de la técnica.

Esto es así pues se consigue un dispositivo completamente autónomo, en el que el microcontrolador de código abierto y el software de la placa permiten una programación de los mismos para realizar unas funciones concretas de control de acceso, de manera que el dispositivo va a trabajar en la dirección que le marque la programación previamente definida.

Una vez configurado el funcionamiento del dispositivo, únicamente va a poder ser modificado mediante un acceso físico al mismo, pues esta placa no presenta medios de conexión al servidor ni a la base de datos del mismo, ni medios de sincronización con ningún servidor externo que le permitan obtener datos como los tiempos de acceso o listados de usuarios..., por lo que va a funcionar según las reglas y condicionantes establecidos en el momento de su programación.

La única conexión posible con el dispositivo es mediante el dispositivo móvil del usuario y a través de una de sus antenas bluetooth. El dispositivo se controla en su totalidad mediante el microcontrolador de la placa y el software del mismo.

5 Dado que la conexión del dispositivo móvil con el dispositivo de control se realiza mediante una comunicación vía bluetooth, y no se considera la conexión del mismo a ningún tipo de servidor en red, el funcionamiento del dispositivo de control no queda condicionado en ningún momento a la existencia de red, de wifi o de la cobertura de la zona en la que se utilice.

10

Esto permite asegurar un correcto funcionamiento del dispositivo en cualquier momento, simplemente por aproximación del usuario con el dispositivo móvil a donde se encuentra el dispositivo de control. De esta manera, si el usuario presenta el bluetooth de su dispositivo móvil conectado, puede activarse el dispositivo de control con dos posibles modalidades, un primer modo únicamente por aproximación, en cuyo caso la antena del dispositivo de control detecta el dispositivo móvil del usuario y se enlazan vía bluetooth realizándose el envío del código de acceso o bien, un segundo modo en el que el usuario debe activar la función de enlace con el dispositivo de control y posteriormente se realiza el envío de dicho código.

15

20 Las funcionalidades de este dispositivo son muy amplias, pues además de poder utilizarse para el control de acceso a zonas protegidas mediante una cerradura electrónica, también puede usarse para el paso por accesos que previamente requieren de una operación de pago, por ejemplo. Así pues, al salir de estacionamientos que requieren un paso previo por caja, tras haberse realizado el pago vía online o incluso pudiendo contratar los pagos en períodos, por ejemplo mensuales, la aplicación ha dotado previamente al usuario de un código de acceso con dichos condicionantes que le permite la apertura de la barrera al aproximarse a la misma.

25

Es un dispositivo muy eficaz y sencillo de utilizar para el usuario, que mejora las condiciones de relación del usuario con este tipo de controles, pues únicamente por aproximación al mismo el dispositivo nos permite el acceso, sin tener que realizar ninguna acción ni depender de elementos externos tales como llaves o tarjetas magnéticas.

30

Resulta igualmente muy cómodo y rápido, pues no es preciso que el usuario descienda de su posible medio de transporte o que utilice ningún elemento de apertura a través de ningún tipo de clavija, ni tenga que recordar ningún código de acceso de memoria...

35

Así mismo, resulta muy eficaz igualmente en la seguridad de los usuarios, pues cualquier persona que no sea autorizada al acceso no va a poder acceder a la zona al no disponer de un código de acceso. Además, los datos del dispositivo son inalterables por terceros, dado  
5 que el dispositivo de control no es accesible desde la red.

Por otra parte, este dispositivo de control de accesos no presenta un número límite de usuarios. Así pues, al existir un servidor con una base de datos para el registro de los usuarios y la generación del código de acceso, se permite la posibilidad de que un  
10 dispositivo de control pueda dar acceso a todos los usuarios que presenten en su dispositivo móvil dicho código, sin límite de cantidad, únicamente con el condicionante de que previamente se hayan registrado en el servidor para una cerradura en concreto a través de la aplicación y se les haya admitido, generando el código correspondiente.

15 Resulta por tanto un dispositivo de control de acceso que permite la interacción del mismo con un gran número de usuarios, todos ellos con su código, generado por un servidor y entregado previamente a través de una aplicación cuando se registran en el sistema, y que al mismo tiempo, una vez que los usuarios poseen el código, el dispositivo funciona de forma completamente autónoma determinando la aceptación o el rechazo del acceso al  
20 usuario, según el código que éste aporte vía bluetooth y la compatibilidad del mismo con la programación de la placa del dispositivo.

### **Breve descripción de los dibujos**

25 Con objeto de ayudar a una mejor comprensión de las características del invento, de acuerdo con un ejemplo preferente de realización práctica del mismo, se aporta como parte integrante de dicha descripción, una serie de dibujos donde, con carácter ilustrativo y no limitativo, se ha representado lo siguiente:

30 Las Figuras 1.1 y 1.2.- Muestran unas vistas en planta y alzado de la placa de circuito impreso del dispositivo autónomo para control de accesos, para un modo de realización preferente de la invención.

La Figura 2.- Muestra una vista en perfil de la carcasa del dispositivo autónomo para control  
35 de accesos, para un modo de realización preferente de la invención.

La Figura 3.- Muestra una vista en perspectiva del interior del dispositivo autónomo para control de accesos, para un modo de realización preferente de la invención.

### **Descripción detallada de un modo de realización preferente de la invención**

5

A la vista de las figuras aportadas, puede observarse cómo en un modo de realización preferente de la invención, el dispositivo (1) autónomo para control de accesos, para accesos con cerradura electrónica mediante al menos un dispositivo móvil que presenta una aplicación apta para establecer conexión a una base de datos contenida en un servidor para la obtención de un código de acceso que aquí se propone, comprende una carcasa (10) de contención dispuesta próxima a la cerradura electrónica.

10

Como se muestra en las Figuras 1.1 y 1.2, esta carcasa (10) comprende en su interior una placa (2) de circuito impreso que presenta un microcontrolador (3) de código abierto y un software con una entrada (4) al mismo. Esta placa (2) presenta unos primeros medios de conexión (5) directa a la cerradura electrónica y unos segundos medios de conexión (6) directa a la corriente eléctrica.

15

Así pues, la el microcontrolador (3) de código abierto y el software se programan para una funcionalidad determinada y para una pluralidad de códigos de acceso.

20

En este modo de realización se considera que el acceso se trata de una puerta de parking de una urbanización, aunque también puede considerarse la puerta de acceso directa a la urbanización a pie o cualquier otra.

25

El microcontrolador (3) y el software se programan para realizar esta función y la placa (2) se conecta directamente a la cerradura de la puerta del parking de dicha urbanización y a los medios de suministro de la energía eléctrica. Es por ello que el dispositivo se sitúa próximo a la cerradura electrónica.

30

En el interior de la carcasa (10) el dispositivo (1) comprende también unos medios de comunicación con el al menos un dispositivo móvil que permiten la recepción del correspondiente código de acceso. En este caso la comunicación se realiza con una pluralidad de dispositivos móviles, los pertenecientes a los usuarios de la urbanización a la que pertenece el parking.

35

- Estos medios de comunicación están formados por al menos dos antenas bluetooth (7) conectadas a dicha placa (2), compatibles cada una de ellas con un sistema operativo de dispositivos móviles. En este modo de realización se consideran dos antenas bluetooth (7), una apta para el sistema operativo android y otra apta para un sistema operativo iOS. De este modo se asegura la compatibilidad de los medios de comunicación con cualquier dispositivo que presente uno de esos dos sistemas operativos, pero en otros modos de realización puede llevar más antenas en caso de que aparezcan nuevos sistemas operativos en el mercado.
- 5 Este dispositivo (1) está programado para que las conexiones bluetooth al mismo sean multiacceso, permitiendo la conexión de una gran cantidad de usuarios a la misma antena de bluetooth. Esto es posible porque el software de la placa (2) del dispositivo está programado para establecer un límite de tiempo de conexión de cada usuario.
- 10 En este modo de realización este tiempo de conexión está establecido en 4 segundos, aunque en otros modos de realización puede ser un tiempo diferente. Así pues, cuando un usuario se aproxima al control de acceso y su dispositivo móvil presenta el bluetooth activado, éste se enlaza con la antena bluetooth (7) correspondiente del dispositivo de control. A partir de ese momento, envía el código de acceso y el dispositivo de control
- 15 permite o no el acceso, cuando lo permite, se desconecta el enlace existente con dicho dispositivo móvil, y siempre con un tiempo máximo de 4 segundos tras los que, si no se ha permitido el acceso, igualmente se realiza la desconexión del enlace existente, de manera que la antena queda libre para un nuevo usuario.
- 20 Por otra parte, este dispositivo (1) además, comprende en el interior de la carcasa (10) un módulo (8) relé de al menos dos canales conectado a la placa (2).
- En este modo de realización preferente de la invención, se considera un módulo (8) de dos canales, de manera que uno de dichos canales es un canal de reserva. De ese modo, el
- 25 canal de reserva queda sin utilización salvo que exista la necesidad de una reparación o de la sustitución del otro canal, en cuyo caso se pone en funcionamiento el canal de reserva para que el dispositivo pueda seguir funcionando.
- En otros modos de realización, el dispositivo (1) puede presentar un número mayor de
- 30 canales en el módulo, pudiendo estar conectado cada relé a un acceso diferente, de manera

que el dispositivo de control de accesos sea capaz de controlar más de una cerradura electrónica.

5 Por otra parte, como puede observarse en la Figura 3, en este modo de realización preferente de la invención, el dispositivo (1) comprende un transformador (9) conectado en los primeros medios de conexión (5) entre la placa (2) y la cerradura electrónica, para transformar la baja potencia de la electrónica del dispositivo (1) en una potencia más elevada compatible con el mecanismo electrónico del acceso.

10 En este modo de realización preferente de la invención, los segundos medios de conexión (6) directa a la corriente eléctrica están formados por un conector macho y un cable de conexión entre el mismo y la corriente eléctrica.

15 Por otra parte, como se muestra en la Figura 2, la carcasa (10) de contención está formada por dos mitades y comprende medios de sujeción entre ambas. De este modo, si hubiera necesidad de reparación es fácilmente revisable.

20 El funcionamiento del dispositivo (1) consiste pues en los siguientes pasos: cuando un usuario va a utilizar este dispositivo para el control de accesos lo primero que debe realizar es descargarse la aplicación en su dispositivo móvil y a través de la misma, realizar el registro en la base de datos del servidor y solicitar un código de acceso para una cerradura electrónica determinada así como los datos de conexión de la antena correspondiente al dispositivo de control.

25 Una vez que el usuario presenta el código en el móvil ya puede acceder libremente a la apertura de la cerradura, de manera que cuando se aproxime a la misma, la aplicación realiza la petición de conexión a la correspondiente antena. Esta conexión es posible gracias a que la aplicación cuenta con los datos de conexión de la antena del dispositivo (1).

30 A continuación, la antena del dispositivo se comunica con la aplicación del dispositivo móvil del usuario. Esta comunicación de la antena la realiza de forma aislada respecto al dispositivo, sólo se comunica la antena, el resto del dispositivo se mantiene aislado.

35 La antena solicita el código de acceso a la aplicación del dispositivo móvil y dicha aplicación debe responder con dicho código que el servidor le aportó en el momento del registro.

En caso de que el código de acceso sea correcto la trama del mismo coincida con lo esperado, se establece la vinculación con el dispositivo, y éste inicia la activación de la apertura del acceso y seguidamente fuerza la desconexión con el dispositivo móvil.

5 En el modo de realización presentado en esta memoria, se ha propuesto la función de apertura de una puerta de garaje, pero este dispositivo plantea la posibilidad de múltiples funcionalidades, como por ejemplo, la posibilidad de realizar un control de accesos a cerraduras en locales alquilados, en los que se generan códigos de acceso que permitan acceder al local durante un horario concreto o por un tiempo determinado, en función del  
10 horario o del plazo durante el que esté vigente el contrato y una vez pasado el mismo el código queda sin efecto.

En este sentido, los códigos de acceso generados por el servidor pueden ser de distintos tipos. Así, un código de un usuario normal, que podría ser como en el modo de realización  
15 propuesto, un propietario de una plaza en el parking, tendría un código de acceso en propiedad.

Este código de acceso en propiedad así mismo puede cederse, en caso de alquilar la plaza de parking por ejemplo, en cuyo caso el propietario pierde el derecho de uso del mismo.  
20 Este propietario puede recuperar el código en cualquier momento, anulando la cesión del mismo, cuando rescinda el contrato de alquiler, en este caso. Un código de acceso cedido puede ser controlado mediante temporización horaria si se desea, pudiendo establecer intervalos horarios en los que se puede acceder y otros en los que no, como lo comentado anteriormente al respecto del alquiler de un local.

25 Otro tipo de código de acceso que puede generarse es un código temporal, que va a estar ligado a un código de acceso en propiedad. Este código temporal está habilitado entre fechas y horas concretas y en principio es válido para un único uso, aunque esto puede modificarse si interesara establecer un número de usos limitado. Una vez que el código se  
30 ha utilizado o en el caso de tener más de un uso, ha llegado al límite establecido, el código queda inservible.

Este tipo de códigos plantean otras múltiples opciones de funcionalidad de este dispositivo, pues es posible entregar un código temporal por ejemplo a un repartidor que tiene horario de  
35 entrega que no permite recibirle en persona. De este modo se le puede dar acceso temporalmente a una zona de entrada de unas instalaciones, a un rellano de una

urbanización, a una cabina de entrega/recogida de paquetes... cualquier espacio con una cerradura electrónica, de manera que el repartidor va a tener acceso a la misma una única vez y tras la entrega el código queda anulado. Para esta función el repartidor únicamente precisa tener un dispositivo móvil y la aplicación instalada en el mismo, y no debe preocuparse de nada más, pues la aplicación y la antena del dispositivo van a comunicarse y enlazarse ellas mismas sin que él deba hacer nada.

También pueden generarse códigos de acceso duplicados, en cuyo caso no presentan límite de uso y son asimilables a una copia de una llave tradicional. El usuario inicial determina la vigencia del código duplicado y aquel usuario que va a hacer uso del mismo debe registrarse igualmente en el servidor.

De este modo, las posibles tipologías de código de acceso posibilitan múltiples funcionalidades del dispositivo, de las que en esta memoria se han dado algunos ejemplos pero que podrían ser muchas más, distintas y variadas, en función de las necesidades de los usuarios.

La forma de realización descrita constituye únicamente un ejemplo de la presente invención, por tanto, los detalles, términos y frases específicos utilizados en la presente memoria no se han de considerar como limitativos, sino que han de entenderse únicamente como una base para las reivindicaciones y como una base representativa que proporcione una descripción comprensible así como la información suficiente al experto en la materia para aplicar la presente invención.

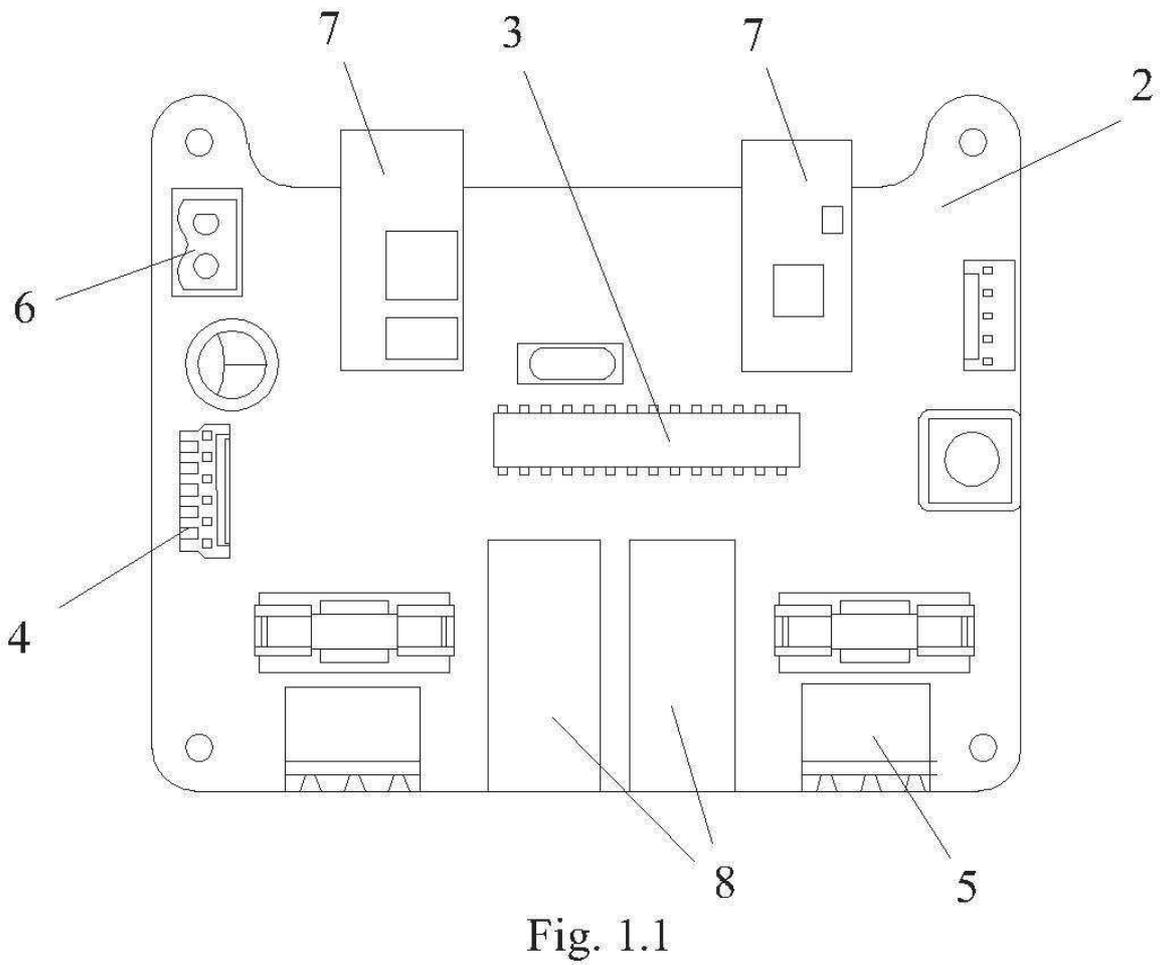
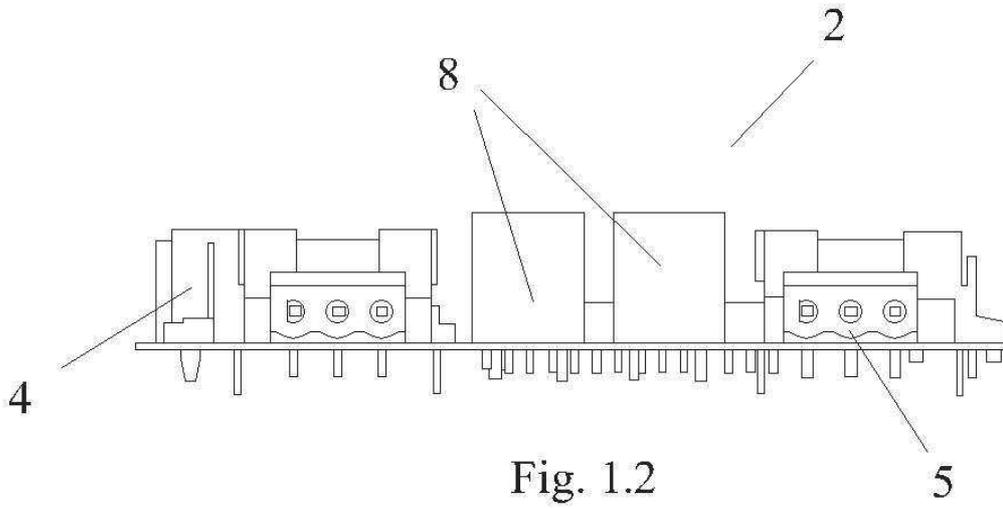
25

30

35

## REIVINDICACIONES

- 1- Dispositivo (1) autónomo para control de accesos, para accesos con cerradura electrónica mediante al menos un dispositivo móvil que presenta una aplicación apta para establecer conexión a una base de datos contenida en un servidor para la obtención de un código de acceso, **caracterizado por que** comprende una carcasa (10) de contención dispuesta próxima a la cerradura electrónica, en cuyo interior comprende
- una placa (2) de circuito impreso que presenta un microcontrolador (3) de código abierto y un software, donde dicha placa (2) presenta unos primeros medios de conexión (5) directa a la cerradura electrónica y unos segundos medios de conexión (6) directa a la corriente eléctrica;
  - unos medios de comunicación con el al menos un dispositivo móvil que permiten la recepción del correspondiente código de acceso;
  - donde dichos medios de comunicación están formados por al menos dos antenas bluetooth (7) conectadas a dicha placa (2), compatibles cada una de ellas con un sistema operativo de dispositivos móviles, y;
  - un módulo relé (8) de al menos dos canales conectado a la placa (2).
- 2- Dispositivo (1) autónomo para control de accesos con cerradura electrónica, según la reivindicación 1, **caracterizado por que** comprende un transformador (9) conectado en los primeros medios de conexión (5) entre la placa (2) y la cerradura electrónica.
- 3- Dispositivo (1) autónomo para control de accesos con cerradura electrónica, según cualquiera de las reivindicaciones anteriores, **caracterizado por que** los segundos medios de conexión (6) directa a la corriente eléctrica están formados por un conector macho y un cable de conexión entre el mismo y la corriente eléctrica.
- 4- Dispositivo (1) autónomo para control de accesos con cerradura electrónica, según cualquiera de las reivindicaciones anteriores, **caracterizado por que** uno de los canales del módulo relé (8) es un canal de reserva.
- 5- Dispositivo (1) autónomo para control de accesos con cerradura electrónica, según cualquiera de las reivindicaciones anteriores, **caracterizado por que** la carcasa (10) de contención está formada por dos mitades y comprende medios de sujeción entre ambas.



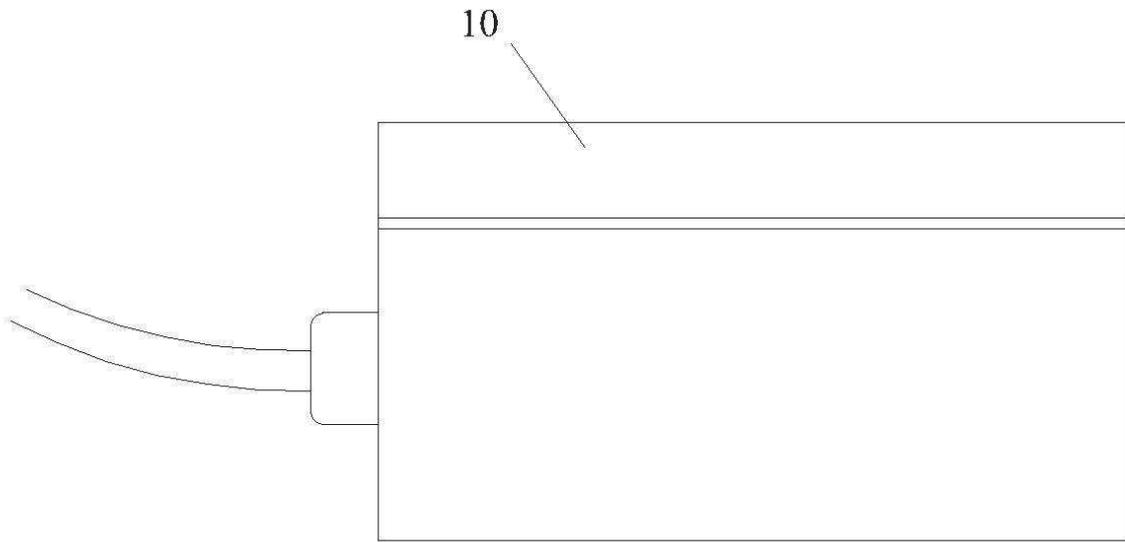


Fig. 2

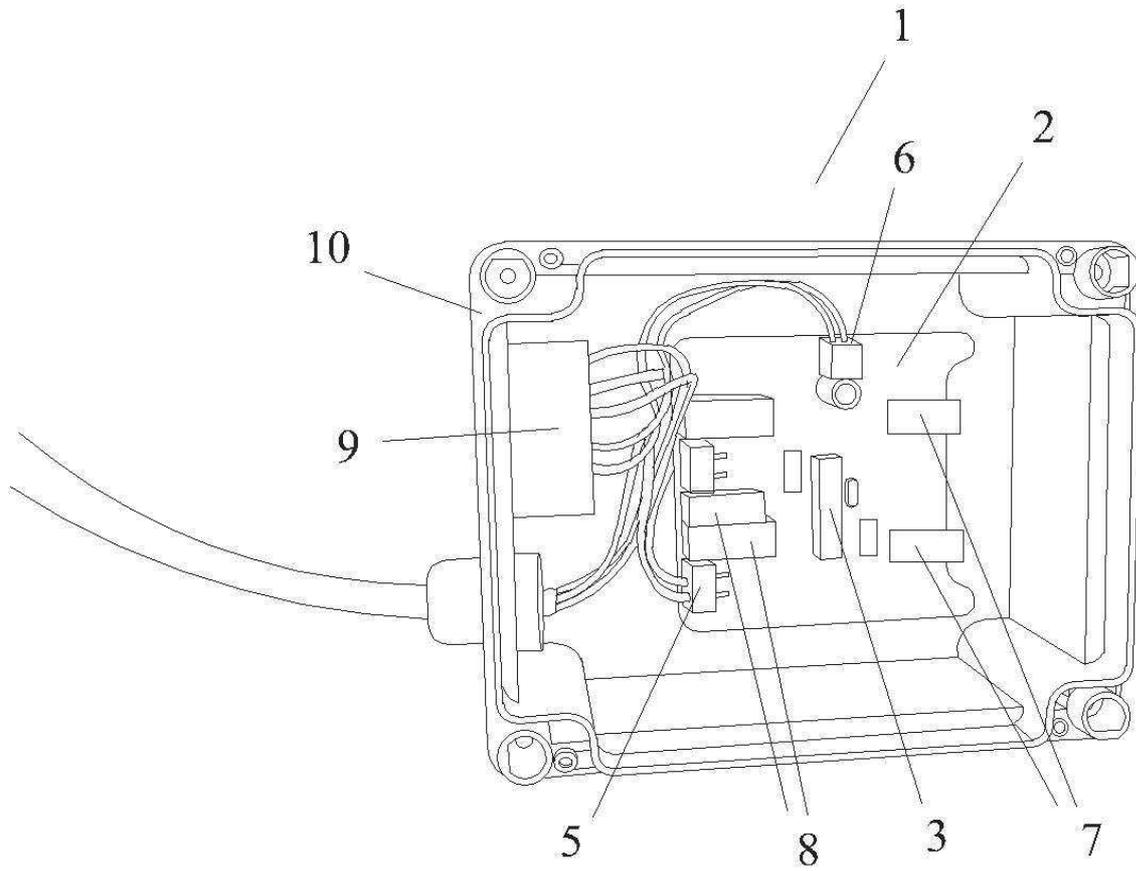


Fig. 3