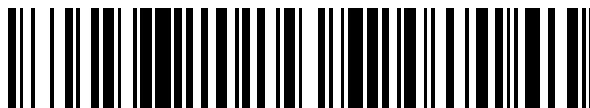


19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 550 733**

21 Número de solicitud: 201430670

51 Int. Cl.:

G06K 7/00

(2006.01)

12

SOLICITUD DE PATENTE

A1

22 Fecha de presentación:

07.05.2014

43 Fecha de publicación de la solicitud:

11.11.2015

71 Solicitantes:

MATRIX ELECTRÓNICA, S.L. (100.0%)
C/ Belmonte de Tajo, N° 76-3° B
28016 Madrid ES

72 Inventor/es:

VILALLONGA PRESAS, José María

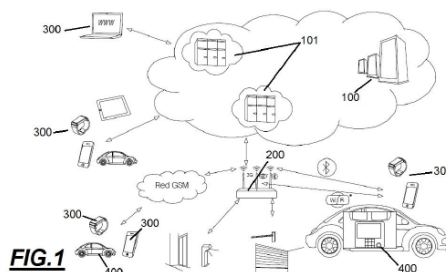
74 Agente/Representante:

MALDONADO JORDAN, Julia

54 Título: **Sistema de acceso en puertas automatizadas**

57 Resumen:

Sistema de control de accesos para puertas automatizadas configurado para permitir el acceso físico a cualquier tipo de puerta automatizada a través de una aplicación software instalada en un dispositivo electrónico de usuario (300, 400) capaz de comunicarse de forma inalámbrica con un dispositivo de control de la puerta (200) y gestionado por un servidor remoto (100, 101).



SISTEMA DE ACCESO EN PUERTAS AUTOMATIZADAS

DESCRIPCIÓN

5 El objeto de la presente invención es un sistema universal para permitir el acceso físico a cualquier tipo de puerta automatizada a través de una aplicación software instalada en un dispositivo electrónico capaz de comunicarse de forma inalámbrica con un dispositivo de control de la puerta. Dicho dispositivo electrónico es uno de tipo móvil, como un teléfono inteligente, un reloj inteligente o una tableta electrónica.

10

También es de aplicación en vehículos que dispongan de un dispositivo electrónico empotrado similar a los indicados. Estos dispositivos electrónicos están configurados para permitir la descarga remota de la aplicación de software necesaria para interactuar con el sistema.

15

Es un objeto de la invención que la aplicación de software que lo integra tenga múltiples opciones de comunicación redundantes para asegurar el proceso de apertura y que se garantice un nivel de seguridad adecuado frente a cualquier intento de acceso fraudulento o no autorizado, garantizando un nivel de seguridad muy superior al de los sistemas actuales.

20

Estado de la técnica

En la actualidad, la cuota de penetración media de los teléfonos inteligentes o *Smartphones* en Europa está en torno al 65% de la población, aunque la tendencia natural es que estos
25 teléfonos alcancen una cuota del 100% en un futuro.

Gran cantidad de acciones y actividades de la vida diaria se realizan mediante un teléfono inteligente. El ámbito de aplicación aumenta día a día mediante nuevos programas de software (aplicaciones o apps) y servicios ofertados desde las distintas compañías de
30 distribución de sistemas operativos móviles (como la AppStore® de Apple®, GooglePlay® para el sistema operativo Android® o la Windows Store® de Microsoft®).

A finales de 2012 y principios de 2013 aparecieron los primeros relojes inteligentes (o *Smartwatches*) como accesorio o extensión de los citados teléfonos y comunicados con ellos mediante tecnología inalámbrica de corto alcance, normalmente bajo el estándar Bluetooth®. No obstante, estos relojes han ido aumentando sus capacidades hasta equiparar o superar las de los teléfonos (ver, por ejemplo, el documento US20130044215).

Finalmente, las tabletas electrónicas (como los conocidos iPad de Apple® y GalaxyTab® de Samsung®) son dispositivos electrónicos portátiles que, generalmente, tienen una potencia de cómputo mayor que la de los teléfonos y similar a la de algunos ordenadores personales, pero con capacidades de portabilidad y usabilidad equivalentes a las de un teléfono.

Por otro lado, en el mercado automovilístico existe la tendencia de integrar dispositivos electrónicos de control y comunicaciones con capacidades similares a los teléfonos y a las tabletas, que ofrecen también la posibilidad de instalar aplicaciones de software para para ampliar sus posibilidades de empleo (ver, por ejemplo, el siguiente enlace: http://es.wikipedia.org/wiki/Veh%C3%ADculo_conectado).

En la presente invención, se entiende que cualquier referencia a un dispositivo electrónico portátil está referida indistintamente a relojes, teléfonos o tabletas, así como dispositivos similares que están empotrados en vehículos.

En las grandes comunidades de vecinos, cada vez más habituales en la periferia de las grandes ciudades, existen numerosas puertas de acceso comunitario. Para evitar el empleo de multitud de llaves se suele usar el proceso de amaestrado, de tal forma que una única llave sirva para varias puertas distintas. No obstante, esta solución presenta los siguientes problemas:

- a) Las llaves y cerraduras tienen un coste muy elevado.
- b) El proceso de amaestrado implica usar un solo diente/muelle para cada puerta distinta y, por tanto, la seguridad se reduce.
- c) Debido al uso tan frecuente de las llaves y cerraduras, la cerradura sufre un desgaste rápido, perdiendo sus características de seguridad y acaba bloqueándose,

haciendo necesaria su reparación.

Además, en caso de pérdida o robo de un control remoto o de una llave comunitaria amaestrada, por seguridad, es necesario reprogramar todos los controles remotos de la comunidad uno a uno, o bien cambiar todas las cerraduras y llaves amaestradas, con elevados costes y un tiempo de varias semanas empleado para coordinar a todos los usuarios, con el consiguiente peligro de intrusión en ese periodo.

En consonancia con lo anterior, es posible sustituir la clásica llave mecánica y los mandos remotos o controles remotos para la apertura de puertas de acceso a garajes o comunidades de vecinos mediante una aplicación instalada en un dispositivo electrónico portátil o en un vehículo con un dispositivo electrónico de comunicaciones empotrado. En la presente invención, las puertas, de forma genérica, son puertas automatizadas o con portero automático. Para emplear el sistema de la invención en puertas no automatizadas sería necesario realizar un cambio en el mecanismo de abertura.

Los documentos EP2085934 o ES2429393, a modo de ejemplo, describen una cerradura electrónica que, además de incorporar un lector de tarjetas magnéticas como las empleadas comúnmente en las habitaciones de los hoteles, incluye un módulo de comunicaciones con el usuario de tal forma que éste pueda establecer una comunicación con la cerradura electrónica a través de un dispositivo móvil con una aplicación previamente validada. Por otro lado, la cerradura también puede ser controlada desde un centro de control vía internet.

Descripción de la invención

La presente invención sustituye a llaves, llaves amaestradas, controles R, Tarjetas magnéticas, tarjetas proximidad, los mandos de control remoto o a las llaves amaestradas de cada puerta por una única aplicación de software instalada en un dispositivo electrónico portátil, solucionando de esta forma los problemas indicados en el estado de la técnica.

Más concretamente, en un primer aspecto de la invención, el método de acceso a

puertas automatizadas que comprende las etapas de:

- i) instalar al menos un dispositivo de control de acceso en, al menos, una puerta automatizada;
 - 5 ii) descargar en un dispositivo electrónico de usuario, desde un servidor remoto, un programa configurado para la comunicación entre el servidor remoto, el dispositivo electrónico de usuario y, al menos, un dispositivo de control de acceso;
 - 10 iii) dar de alta el dispositivo móvil de usuario en al menos una base de datos instalada en al menos un servidor remoto;
 - iv) identificar el dispositivo electrónico de usuario a través de un código único de identificación enviado por el dispositivo electrónico de usuario a un servidor remoto a través del dispositivo de control de acceso conectado con dicha puerta; y
 - 15 v) permitir el acceso de un usuario en una puerta automatizada cuando el código de único de identificación del dispositivo electrónico de usuario coincide con un código único de identificación habilitado para dicho acceso en una base de datos de un servidor remoto.
- 20 En un segundo aspecto de la invención, el sistema de control de accesos en puertas automatizadas que comprende al menos, un dispositivo de control de accesos; y al menos un dispositivo electrónico de usuario; que comprende al menos un servidor remoto accesible vía web a través de una red de comunicaciones que comprende uno o más programas en el que dichos programas están almacenados en una memoria y configurados para ejecutarse
- 25 mediante al menos un procesador, caracterizado porque los programas incluyen instrucciones para:
- a) facilitar la descarga en un dispositivo electrónico de usuario un programa configurado para la comunicación cifrada entre un servidor remoto, un dispositivo
 - 30 electrónico de usuario y, al menos, un dispositivo de control de acceso;
 - b) dar de alta el dispositivo móvil de usuario en al menos una base de datos instalada en al menos un servidor remoto;

c) identificar el dispositivo electrónico de usuario a través de un código único de identificación enviado por el dispositivo electrónico de usuario a través del dispositivo de control de acceso; y

5 d) permitir el acceso de un usuario en una puerta automatizada cuando el código de
único de identificación del dispositivo electrónico de usuario coincide con un
código único de identificación habilitado para dicho acceso en una base de datos
del servidor remoto.

10 El sistema objeto de la invención aporta una mayor seguridad frente a los controles remotos
y las llaves amaestradas, que son muy fáciles de copiar. Con el sistema propuesto, el
dispositivo electrónico del usuario está identificado mediante tres identificadores únicos: el
IMEI, la MAC WIFI y la MAC Bluetooth® del dispositivo electrónico del usuario, registrados
en la base de datos del servidor remoto y que son imposibles de copiar en otro dispositivo.

15 Además, cualquier intercambio de datos está encriptado con RSA de clave pública/privada
de 8192 bits. Esta información tiene un segundo cifrado diferente en función de si la
comunicación es WIFI, Bluetooth o de datos 3G.

20 Sólo los dispositivos electrónicos registrados y autorizados en el sistema para cada puerta
tienen acceso libre. Además, en el caso de pérdida del teléfono, éste se puede desactivar a
través de la aplicación Web, no afectando al resto de usuarios.

25 Finalmente, cabe indicar que frente a otros sistemas de abertura de puertas mediante
teléfono móvil, el sistema objeto de la invención aumenta la seguridad ya que, además de
las medidas de seguridad indicadas anteriormente, permite obtener un histórico del uso del
acceso para comprobarlos y, complementariamente, emite una alarma en el caso de que se
detecte un número exagerado de intentos fallidos porque alguien está intentando sabotear el
acceso a base de prueba y error en un intento de búsqueda de posibles puntos débiles del
sistema.

30 Todo el sistema descrito está especialmente diseñado para garantizar la máxima seguridad
en caso de hurto del dispositivo electrónico del usuario, ya que basta notificar una baja a

través de la Web del sistema.

Por tanto, el sistema objeto de la invención consistirá en un gran ecosistema con todas las puertas y dispositivos electrónicos de los usuarios conectados entre sí por los servidores remotos. Algunos ejemplos de uso, no limitativos, son los siguientes: puertas de garajes comunitarios, puertas de casas de comunidades de vecinos, garajes de oficinas, hoteles y apartamentos turísticos que tengan necesidad de otorgar acceso temporal, accesos a edificios de oficinas, tanto para empleados, como para visitas que reciben previamente un código de autorización por correo electrónico, SMS o cualquier otro medio de mensajería electrónica, para una franja horaria determinada, urbanizaciones con varias puertas para peatones y vehículos, así como aparcamientos públicos o privados.

No obstante, el sistema puede ser utilizado en multitud de entornos ya que el sistema simplemente sustituye el empleo de una cerradura, candado, o accionamiento controlado, de una forma permanente o temporal como podrían ser: alquiler público de bicicletas, alquiler de vehículos en recintos cerrados, alquiler de todo tipo de maquinaria y en general cualquier control de acceso a través de cerraduras.

La presente invención soluciona el problema de las cerraduras susceptibles de vandalismo. Al no necesitar una llave o candado, se evitan todos los problemas relacionados con estos, como la inutilización de la cerradura mediante silicona.

A lo largo de la descripción y las reivindicaciones la palabra "comprende" y sus variantes no pretenden excluir otras características técnicas, aditivos, componentes o pasos. Para los expertos en la materia, otros objetos, ventajas y características de la invención se desprenderán en parte de la descripción y en parte de la práctica de la invención. Los siguientes ejemplos y dibujos se proporcionan a modo de ilustración, y no se pretende que restrinjan la presente invención. Además, la presente invención cubre todas las posibles combinaciones de realizaciones particulares y preferidas aquí indicadas.

Breve descripción de las figuras

A continuación se pasa a describir de manera muy breve una serie de dibujos que ayudan a comprender mejor la invención y que se relacionan expresamente con una realización de dicha invención que se presenta como un ejemplo no limitativo de ésta.

- 5 FIG 1 - Muestra un esquema del sistema objeto de la invención.
- FIG 2 - Muestra un esquema del sistema objeto de la invención durante un proceso de
abertura de una puerta a través de una red de comunicaciones tipo Internet.
- FIG 3 - Muestra un esquema del sistema objeto de la invención durante un proceso de
abertura de una puerta mediante comunicación directa entre la puerta y el
10 dispositivo electrónico del usuario.

Exposición de un modo detallado de realización de la invención

Tal y como se puede observar en las figuras adjuntas, el sistema de acceso en puertas
15 automatizadas, objeto de la presente invención comprende un servidor remoto (100)
configurado para el control y gestión de la operativa del sistema por parte de instaladores,
distribuidores y administradores de fincas. El servidor remoto (100) está configurado para
operar telemáticamente a través de un acceso seguro las altas, bajas, modificaciones,
configuraciones, niveles de acceso y permisos de acceso, estadísticas o cobros.

20 Para ello, en una realización práctica, el servidor remoto (100) comprende un procesador,
una memoria incluyendo una base de datos y una serie de programas, donde dichos
programas están almacenados en la memoria y configurados para ejecutarse por el
procesador. Dichos programas incluyen instrucciones configuradas para:

- 25 a) enviar y recibir datos de al menos un usuario a través de una red de comunicaciones;
y
- b) enviar y recibir datos de al menos un dispositivo de control de acceso (200) instalado
y conectado en el cuadro de automatismos de una puerta.

30 Así pues, el servidor remoto (100) comprende una aplicación Web para el acceso de un
usuario a sus datos contenidos en la base de datos desde un ordenador personal o desde

cualquier otro dispositivo capaz de comunicarse vía Web, como los dispositivos electrónicos portátiles (300) del usuario (un teléfono, un reloj inteligente o una tableta) o vehículo (400).

5 En una realización particular se contempla el hecho de utilizar hasta tres servidores remotos (100) redundantes, para mejorar las prestaciones del sistema, con disponibilidad 24h los 365 días del año.

10 En otra realización, el servidor remoto será virtual (101) en la nube, de tal forma que no sea necesario un hardware dedicado ni una ubicación física determinada, estando cada servidor virtual (101) al menos un programa con instrucciones configuradas para enviar y recibir datos de al menos un usuario a través de una red de comunicaciones; y enviar y recibir datos de al menos un dispositivo de control de acceso (200) instalado y conectado en el cuadro de automatismos de una puerta, del mismo modo que se ha descrito anteriormente. La virtualización de los servidores remotos permite que, a medida que el número de
15 usuarios crezca, se puedan administrar los recursos bajo demanda. Es decir, que en función de la demanda de usuarios que acceden vía Web a un servidor virtual (101) y del número de usuarios que realizan aberturas de puertas desde una aplicación en sus dispositivos electrónicos de usuario (300,400), se añadirán el número de servidores remotos virtuales (101) necesarios en la nube para satisfacer la demanda.

20 El software de la página Web está configurado para la gestión general del sistema, con miles de puertas y usuarios finales. Así, por ejemplo, un distribuidor en una ciudad puede gestionar todas las puertas que ha instalado, el administrador de cada finca puede dar altas y bajas de usuarios finales en su finca, transferir licencias de teléfono a uno nuevo y
25 gestionar los datos de los dispositivos de control de accesos (200). El servidor remoto (100,101), además, debe mantener una pluralidad de bases de datos con licencias de usuarios, distribuidores, medios de cobro y en general con todos los datos requeridos para un correcto funcionamiento del sistema.

30 Los dispositivos de control de accesos (200) están instalados en el cuadro eléctrico o cuadro de automatismos de al menos una puerta y están equipados con un módulo de comunicaciones que incluye los medios electrónicos necesarios para establecer una

comunicación vía GSM/GPRS/3G, WIFI y Bluetooth. Además, el dispositivo de control de accesos incluye un módulo de localización y posicionamiento GPS y, opcionalmente, un lector y una antena RFID. Todos estos módulos están conectados y controlados por un procesador tipo ARM que incluye un sistema operativo basado en Linux.

5

Más concretamente, un dispositivo de control de accesos (200) comprende un procesador ARM, una memoria, un módulo de comunicaciones GSM/GPRS/3G, un módulo de comunicaciones inalámbricas WIFI, un módulo de comunicaciones Bluetooth, un módulo GPS y una pluralidad de programas almacenados en la memoria y configurados para ejecutarse por el procesador, de tal forma que los programas incluyen instrucciones para enviar y recibir datos con un dispositivo electrónico de usuario (300,400) y enviar y recibir datos con un servidor remoto (100,101).

10

Todos los datos enviados y recibidos por el dispositivo de control de accesos (200) están cifrados y encriptados mediante un algoritmo RSA con clave pública/privada de 8192 bits. Adicionalmente, la comunicación vía GSM/GPRS/3G es privada, la comunicación WIFI está cifrada bajo el protocolo WPA2 y la comunicación vía Bluetooth tiene un cifrado adicional de 128 bits.

15

Como se ha indicado, el dispositivo de control de accesos (200) comprende opcionalmente un lector RFID de tal forma que el usuario puede además disponer de una etiqueta RFID (*tag*) pegada, por ejemplo, en la parte posterior de su propio dispositivo electrónico de usuario (300) o bien en el parabrisas frontal de su vehículo (400), de tal forma que, al aproximarse a una distancia de 4 o 5 metros (variable en función de la potencia de la antena) de la puerta se inicia automáticamente el proceso de abertura. Como se ha indicado, el lector RFID será de alcance variable y ajustable, desde 1 metro hasta los 9 metros, según las necesidades específicas de cada acceso.

20

25

El dispositivo electrónico del usuario (300,400) comprende una pantalla táctil, para permitir la interacción con el usuario, un procesador, una memoria y una pluralidad de programas que están almacenados en la memoria y configurados para ejecutarse mediante el procesador. Los programas, esto es, la aplicación de software y el sistema operativo,

30

incluyen instrucciones para visualizar todas las puertas a las que tiene acceso autorizado por el servidor remoto (100,101) y para iniciar el proceso de abertura de la puerta estableciendo un primer contacto por Bluetooth con el dispositivo de control de acceso (200), de tal forma que si éste primer intento de comunicación falla, establece la
5 comunicación vía WIFI, y si aún este falla, se conecta vía datos 3G/GPRS, conectándose como último recurso mediante una llamada perdida GSM de forma automática en el caso que los otros medios fallen.

En una realización particular, la abertura automática puede requerir también la posición
10 GPS. En todo caso, el dispositivo de control de accesos (200) identifica al usuario del dispositivo móvil (300,400) a través de tres códigos únicos de identificación: el IMEI del dispositivo, MAC WIFI y MAC Bluetooth.

Es decir, que para dar la orden de acceso, el sistema cuenta con dos maneras de apertura
15 en línea (ver figura 2): mediante WIFI y/o red de datos 3G/GPRS. Además tiene tres formas alternativas de apertura fuera de línea: Bluetooth, WIFI y opcionalmente RFID como se puede observar en la figura 3.

En la presente descripción se ha definido la red de datos móvil como 3G/GPRS.
20 Obviamente, redes de datos móviles de última generación 4G/HSDPA/LTE son igualmente válidas para los propósitos de la presente invención y se incluyen directamente en la generalización de red de datos móviles.

REIVINDICACIONES

1 – Método de acceso a puertas automatizadas que comprende las etapas de:

- 5 i) instalar al menos un dispositivo de control de acceso (200) en, al menos, una puerta automatizada;
- ii) descargar en un dispositivo electrónico de usuario (300,400), desde un servidor remoto (100,101), un programa configurado para la comunicación entre el servidor remoto (100,101), el dispositivo electrónico de usuario (300,400) y, al menos, un dispositivo de control de acceso (200);
- 10 iii) dar de alta el dispositivo móvil de usuario (300,400) en al menos una base de datos instalada en al menos un servidor remoto (100,101);
- iv) identificar el dispositivo electrónico de usuario (300,400) a través de un código único de identificación enviado por el dispositivo electrónico de usuario (300,400) a un servidor remoto (100,101) a través del dispositivo de control de acceso (200) conectado con dicha puerta; y
- 15 v) permitir el acceso de un usuario en una puerta automatizada cuando el código de único de identificación del dispositivo electrónico de usuario (300,400) coincide con un código único de identificación habilitado para dicho acceso en una base de datos de un servidor remoto (100,101).
- 20

2 – El método de la reivindicación 1 donde la comunicación entre el dispositivo electrónico de usuario (300,400) y el dispositivo de control de accesos (200) se realiza mediante al menos uno seleccionado entre: red de datos móviles 3G/GPRS; red inalámbrica
25 WIFI; conexión directa inalámbrica Bluetooth® o conexión RFID.

3 – El método de acuerdo con cualquiera de las reivindicaciones 1-2 donde el código único de identificación es uno seleccionado entre: el código IMEI del dispositivo electrónico de usuario (300,400); el código MAC de la WIFI; el código MAC del Bluetooth; o una
30 combinación de los anteriores.

4 - El método de acuerdo con cualquiera de las reivindicaciones 1-3 donde las

comunicaciones están encriptadas con un algoritmo RSA con clave privada/pública de 8192 bits.

5 5 – El método de acuerdo con cualquiera de las reivindicaciones 1-4 donde la red de comunicaciones GPRS/3G es privada.

6 – El método de acuerdo con cualquiera de las reivindicaciones 1-5 donde las comunicaciones WIFI están cifradas con el protocolo WPA2.

10 7 - El método de acuerdo con cualquiera de las reivindicaciones 1-6 donde las comunicaciones Bluetooth están cifradas con 128 bits.

15 8 - El método de acuerdo con cualquiera de las reivindicaciones 1-7 donde el dispositivo electrónico de usuario (300,400) establece la comunicación con el dispositivo de control de acceso (200) primero mediante Bluetooth; en caso de fallo del Bluetooth establece comunicación mediante WIFI; en caso de fallo establece la comunicación mediante la red móvil de datos 3G/GPRS y finalmente, si fallan los anteriores realiza una llamada perdida al servidor remoto (100,101).

20 9 - Un dispositivo electrónico de usuario (300,400) que comprende:

una pantalla táctil;

un procesador;

un módulo de comunicación Bluetooth;

un módulo de comunicación inalámbrica WIFI;

25 un módulo de comunicaciones 3G/GPRS;

una memoria; y

una pluralidad de programas que están almacenados en la memoria y configurados para ejecutarse mediante el procesador; caracterizado porque los programas incluyen instrucciones para:

30 a) visualizar todas las puertas a las que tiene acceso autorizado en un servidor remoto (100,101);

b) identificarse en dicho servidor remoto (100,101) mediante un código único de

identificación;

c) enviar y recibir datos cifrados con un dispositivo de control de acceso (200); e

d) iniciar el proceso de abertura de la puerta estableciendo un primer contacto por Bluetooth con un dispositivo de control de acceso (200), de tal forma que si éste primer intento de comunicación falla, establece la comunicación vía WIFI, y si aún este falla, se conecta vía datos 3G/GPRS, conectándose mediante una llamada perdida de forma automática en el caso que los otros medios fallen.

10 – El dispositivo electrónico de usuario (300) de acuerdo con la reivindicación 9 que es uno seleccionado entre: un teléfono móvil, un reloj inteligente o una tableta.

11 – El dispositivo electrónico de usuario (400) de acuerdo con la reivindicación 9 que está empotrado en un vehículo.

12 – El dispositivo electrónico de usuario (300,400) de acuerdo con cualquiera de las reivindicaciones 9-11 donde el código único de identificación es uno seleccionado entre: el código IMEI del dispositivo electrónico de usuario (300,400); el código MAC de la WIFI; el código MAC del Bluetooth; o una combinación de los anteriores.

13 – El dispositivo electrónico de usuario (300,400) de acuerdo con cualquiera de las reivindicaciones 9-12 que comprende una etiqueta RFID.

14 – Un dispositivo de control de accesos (200) instalado en el cuadro de automatismos de una puerta automatizada que comprende:

un procesador;

un módulo de comunicación Bluetooth;

un módulo de comunicación inalámbrica WIFI;

un módulo de comunicaciones 3G/GPRS;

una memoria; y

una pluralidad de programas que están almacenados en la memoria y configurados para ejecutarse mediante el procesador; caracterizado porque los programas incluyen instrucciones para:

- a) enviar y recibir datos cifrados con un dispositivo electrónico de usuario (300,400);
- b) enviar y recibir datos cifrados con un servidor remoto (100,101); y
- c) permitir el acceso de un usuario en una puerta automatizada cuando el código de
único de identificación del dispositivo electrónico de usuario (300,400) coincide
5 con un código único de identificación habilitado para dicho acceso en una base
de datos de un servidor remoto (100,101).

15 – El dispositivo de control de accesos (200) de acuerdo con la reivindicación 14
donde el código único de identificación es uno seleccionado entre: el código IMEI del
10 dispositivo electrónico de usuario (300,400); el código MAC de la WIFI; el código MAC del
Bluetooth; o una combinación de los anteriores.

16 – Un sistema de control de accesos en puertas automatizadas que comprende al
menos:

15 un dispositivo de control de accesos (200) de acuerdo con cualquiera de las
reivindicaciones 14-15; y

al menos un dispositivo electrónico de usuario de acuerdo con cualquiera de las
reivindicaciones 9-13;

y que comprende al menos un servidor remoto (100,101) accesible vía web a través
20 de una red de comunicaciones que comprende:

uno o más programas en el que dichos programas están almacenados en una
memoria y configurados para ejecutarse mediante al menos un procesador, caracterizado
porque los programas incluyen instrucciones para:

- a) facilitar la descarga en un dispositivo electrónico de usuario (300,400) un
25 programa configurado para la comunicación cifrada entre un servidor remoto
(100,101), un dispositivo electrónico de usuario (300,400) y, al menos, un
dispositivo de control de acceso (200);
- b) dar de alta el dispositivo móvil de usuario (300,400) en al menos una base de
datos instalada en al menos un servidor remoto (100,101);
- 30 c) identificar el dispositivo electrónico de usuario (300,400) a través de un código
único de identificación enviado por el dispositivo electrónico de usuario (300,400)
a través del dispositivo de control de acceso (200); y

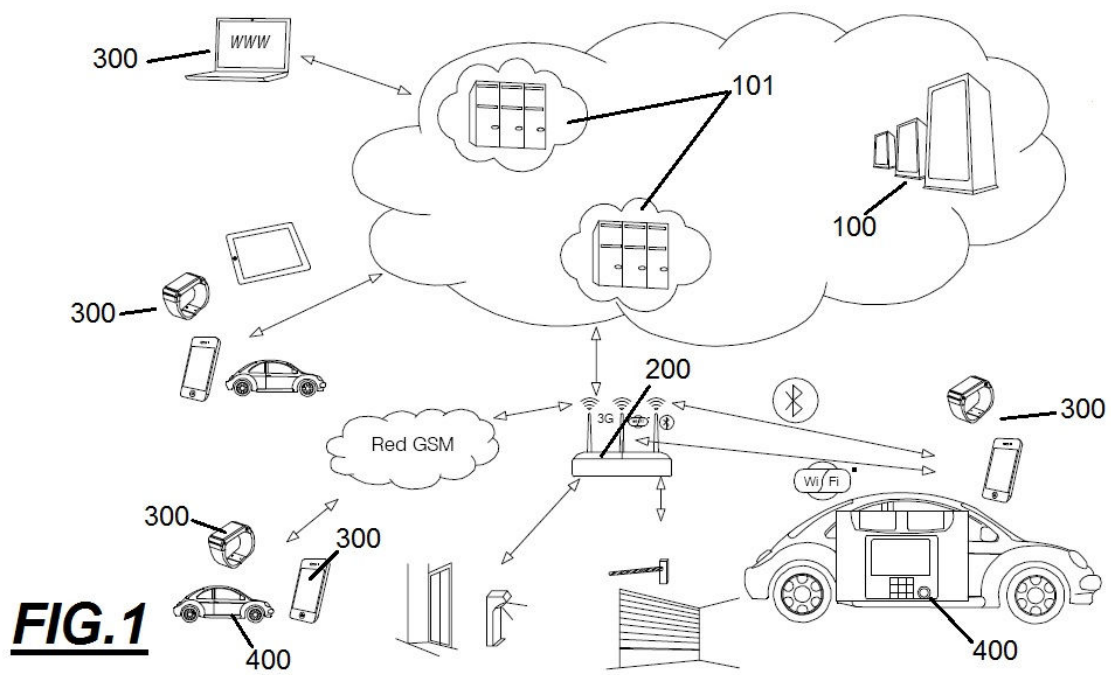
- d) permitir el acceso de un usuario en una puerta automatizada cuando el código de único de identificación del dispositivo electrónico de usuario (300,400) coincide con un código único de identificación habilitado para dicho acceso en una base de datos del servidor remoto (100,101).

5

17 – El sistema de la reivindicación 16 donde el servidor remoto es virtual (101).

18 – Un producto de programa informático con instrucciones configuradas para su ejecución por uno o más procesadores que, cuando son ejecutadas por un sistema de acuerdo con cualquiera de las reivindicaciones 16-17 hacen que el sistema lleve a cabo el método según cualquiera de las reivindicaciones 1 a 8.

10



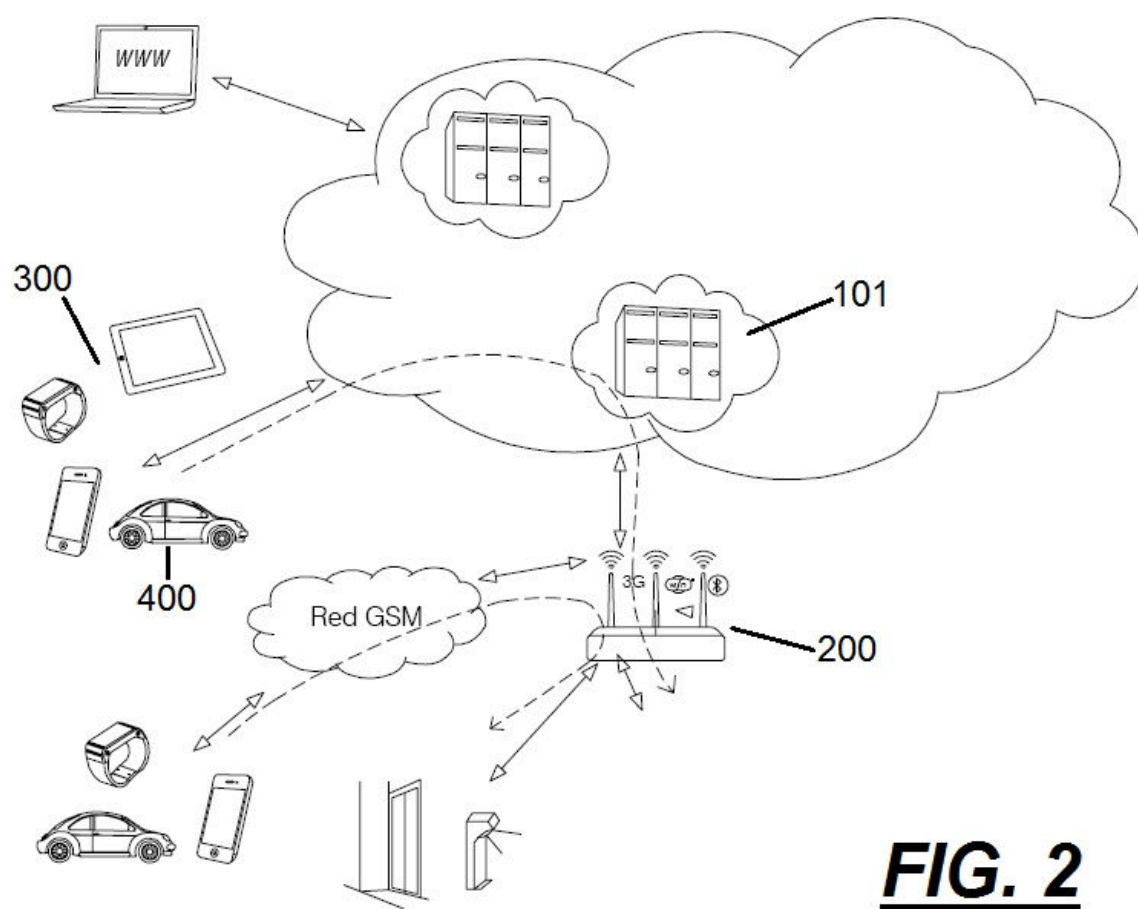


FIG. 2

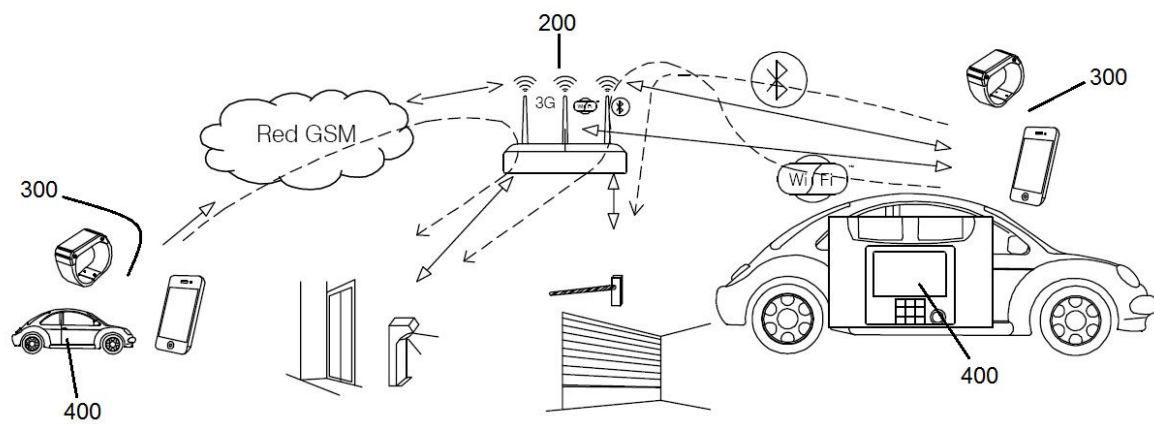


FIG. 3



- ②① N.º solicitud: 201430670
②② Fecha de presentación de la solicitud: 07.05.2014
③② Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TÉCNICA

⑤① Int. Cl.: **G06K7/00** (2006.01)

DOCUMENTOS RELEVANTES

Categoría	⑤⑥ Documentos citados	Reivindicaciones afectadas
X	ES 2429393 A1 (BIELET, INC.) 14.11.2013, todo el documento.	1
Y		2-18
Y	ES 2426749 T3 (BORRACCI, FABRIZIO et al.) 25.10.2013, párrafos (0012,0021-0034); figuras.	2-18
A	EP 2085934 A1 (FORBRUGER KONTAKT DISTRIBUTION et al.) 05.08.2009, resumen; figura 2.	1-18
A	ES 2431016 T3 (UNITED VIDEO PROPERTIES, INC.) 22.11.2013, todo el documento.	1-18

Categoría de los documentos citados

X: de particular relevancia

Y: de particular relevancia combinado con otro/s de la misma categoría

A: refleja el estado de la técnica

O: referido a divulgación no escrita

P: publicado entre la fecha de prioridad y la de presentación de la solicitud

E: documento anterior, pero publicado después de la fecha de presentación de la solicitud

El presente informe ha sido realizado

☒ para todas las reivindicaciones

☐ para las reivindicaciones nº:

Fecha de realización del informe
23.04.2015

Examinador
G. Foncillas Garrido

Página
1/4

Documentación mínima buscada (sistema de clasificación seguido de los símbolos de clasificación)

G07C, G06K

Bases de datos electrónicas consultadas durante la búsqueda (nombre de la base de datos y, si es posible, términos de búsqueda utilizados)

INVENES, EPODOC

Fecha de Realización de la Opinión Escrita: 23.04.2015

Declaración

Novedad (Art. 6.1 LP 11/1986)	Reivindicaciones	SI
	Reivindicaciones 1	NO
Actividad inventiva (Art. 8.1 LP11/1986)	Reivindicaciones	SI
	Reivindicaciones 2-18	NO

Se considera que la solicitud cumple con el requisito de aplicación industrial. Este requisito fue evaluado durante la fase de examen formal y técnico de la solicitud (Artículo 31.2 Ley 11/1986).

Base de la Opinión.-

La presente opinión se ha realizado sobre la base de la solicitud de patente tal y como se publica.

1. Documentos considerados.-

A continuación se relacionan los documentos pertenecientes al estado de la técnica tomados en consideración para la realización de esta opinión.

Documento	Número Publicación o Identificación	Fecha Publicación
D01	ES 2429393 A1 (BIELET, INC.)	14.11.2013
D02	ES 2426749 T3 (BORRACCI, FABRIZIO et al.)	25.10.2013
D03	EP 2085934 A1 (FORBRUGER KONTAKT DISTRIBUTION et al.)	05.08.2009
D04	ES 2431016 T3 (UNITED VIDEO PROPERTIES, INC.)	22.11.2013

2. Declaración motivada según los artículos 29.6 y 29.7 del Reglamento de ejecución de la Ley 11/1986, de 20 de marzo, de Patentes sobre la novedad y la actividad inventiva; citas y explicaciones en apoyo de esta declaración**Reivindicación 1**

El documento más próximo al objeto de la invención es D01, dicho documento presenta un sistema de acceso a puertas automatizadas que comprende un dispositivo de control de acceso (3) en la puerta, un servidor remoto (8) y un programa configurado para la comunicación entre el servidor remoto y el dispositivo electrónico de usuario (7).

El sistema presenta un módulo de comunicaciones vía Internet (9), de forma que a través del propio teléfono podría comunicarse directamente con el control de acceso o de forma remota a través de un centro de control. De esta manera, a través de una aplicación informática cada usuario, podrán obtener los códigos de acceso, y mediante la comunicación por radiofrecuencias entre el teléfono móvil del usuario y la cerradura electrónica, ésta se abrirá de forma totalmente automática al detectar a través de su módulo de comunicaciones al usuario que pretende acceder a la instalación o zona de la misma de que se trate, siempre y cuando, el código enviado por el dispositivo emisor sea el adecuado a los niveles de seguridad programados para la cerradura.

Por tanto, la reivindicación 1 no es nueva (Artículo 6 LP)

Reivindicaciones 2 -8

La comunicación (figura 1) entre el dispositivo electrónico de usuario (7) y el dispositivo de control de acceso (3) se realiza mediante radiofrecuencia o internet.

En la presente solicitud se considera la comunicación bajo Bluetooth y RFID.

Dichos sistemas de comunicaciones se describen en el documento D02, que presenta una tarjeta inteligente.

En combinación de ambos documentos, un experto en la materia podría llegar a la solución de los problemas planteados de forma evidente.

Por otro lado, cabe destacar que no presenta dificultad técnica alguna considerar que el dispositivo electrónico de usuario sea una tableta, un reloj inteligente o un teléfono móvil al no presentarse problema técnico a resolver, respecto a la utilización de códigos IMEI o MAC, red de comunicaciones encriptado con un algoritmo RSA, un sistema de comunicación GPRS/3G, o la utilización de una pantalla táctil se considera que son aspectos no tenidos en cuenta en D01 pero que, no obstante se consideran que forman parte del conocimiento común del estado de la técnica, son elementos conocidos y por tanto no establecen un avance, es decir la solución técnica a un problema planteado que no pueda ser resuelto por un experto en la materia del sector que nos ocupa.

En base a lo indicado y a la dependencia con la primera reivindicación, dichas reivindicaciones son nuevas (Artículo 6 LP) pero carecen de actividad inventiva (Artículo 8 LP).

Reivindicación 9

El manejo y presentación de información como tal bajo un programa software se considera que no presenta carácter técnico, por tanto se establece como una opción de diseño que no tiene aportación técnica alguna.

Por tanto, la reivindicación 9 es nueva (Artículo 6 LP) pero carece de actividad inventiva (Artículo 8 LP).

Reivindicaciones 10-13

En base a lo indicado y a la dependencia con la reivindicación 9, dichas reivindicaciones son nuevas (Artículo 6 LP) pero carecen de actividad inventiva (Artículo 8 LP).

Reivindicaciones 14

Teniendo en consideración lo dicho en las reivindicaciones anteriores, la reivindicación 14 es nueva (Artículo 6 LP) pero carece de actividad inventiva (Artículo 8 LP).

Reivindicaciones 15

En base a lo indicado y a la dependencia con la reivindicación anterior, la reivindicación 15 es nueva (Artículo 6 LP) pero carece de actividad inventiva (Artículo 8 LP).

Reivindicaciones 16

Teniendo en consideración lo dicho en las reivindicaciones anteriores, la reivindicación 16 es nueva (Artículo 6 LP) pero carece de actividad inventiva (Artículo 8 LP).

Reivindicaciones 17

En base a lo indicado y a la dependencia con la reivindicación anterior, la reivindicación 16 es nueva (Artículo 6 LP) pero carece de actividad inventiva (Artículo 8 LP).

Reivindicación 18

Teniendo en consideración lo dicho en las reivindicaciones anteriores, la reivindicación 18 es nueva (Artículo 6 LP) pero carece de actividad inventiva (Artículo 8 LP).