(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 684 593**

(21) Número de solicitud: 201700310

(51) Int. CI.:

***E05B 47/00*** (2006.01)
***E05B 49/00*** (2006.01)
***E05F 15/77*** (2015.01)
***G08C 17/02*** (2006.01)
***H04W 12/00*** (2009.01)

(12) SOLICITUD DE PATENTE A1

(22) Fecha de presentación:

**29.03.2017**

(43) Fecha de publicación de la solicitud:

**03.10.2018**

(71) Solicitantes:

**DASWARE TECHNOLOGIES, S.L. (100.0%)**
**Avda. de la Innovación, 1 - Edif. BIC, Ofic. 335,**
**Parque Tecnológico de la Salud**
**18100 ARMILLA (Granada) ES**

(72) Inventor/es:

**RIVERO IBAÑEZ, Manuel y**
**DE MARTIN JUAN, Ignacio**

(74) Agente/Representante:

**DOMÍNGUEZ COBETA, Josefa**

(54) Título: **Equipo de control de apertura de puertas de garaje o similar y procedimiento de control de apertura de dichas puertas mediante dicho equipo.**

(57) Resumen:

Equipo de control de apertura de puertas de garaje o similar y procedimiento de control de apertura de dichas puertas mediante dicho equipo comprendiendo, al menos, un receptor de seguridad (1), consistente en un dispositivo electrónico programable con conexión a Internet (I), como receptor conectado al mecanismo de apertura automática de la puerta (2) y, al menos un dispositivo electrónico emisor (3) "manos libres", consistente en un dongle BLE o módulo electrónico con microprocesador, memoria y antena Bluetooth, como emisor de la señal de radiofrecuencia, el cual, cuando está conectado a un puerto USB, por ejemplo de un vehículo (5), emite, constantemente y sin intervención del usuario, una señal de radiofrecuencia mediante protocolo bluetooth que detecta dicho receptor de seguridad (1) cuando se encuentra en un radio de alcance preestablecido.

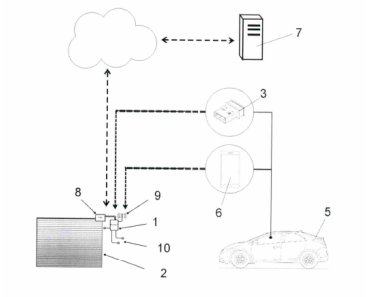


FIG. 1

ES 2 684 593 A1

## DESCRIPCIÓN

Equipo de control de apertura de puertas de garaje o similar y procedimiento de control de apertura de dichas puertas mediante dicho equipo.

### Objeto de la invención

La invención, tal como expresa el enunciado de la presente memoria descriptiva, se refiere a un equipo de control de apertura de puertas de garaje o similar y un procedimiento de control de apertura de dichas puertas mediante dicho equipo que supone una destacadle novedad en su campo de aplicación.

Más concretamente, el objeto de la invención se centra en un equipo que, comprendiendo, al menos, un receptor de seguridad, que está conectado a Internet y al mecanismo de apertura automática de una puerta de garaje o recinto similar, y, al menos, un dispositivo electrónico emisor, que llamaremos “manos libres” porque actúa sin que intervenga el usuario cuando lo conecta a un puerto USB del hardware informático de su vehículo, y que consiste en lo que se conoce como “*dongle*” (o llave de seguridad) de tipo BLE *(Bluetooth Low Energy*), es decir, un módulo electrónico con microprocesador, memoria y antena *Bluetooth,* que emite un código de señal de radiofrecuencia mediante protocolo bluetooth, haciendo que se accione automáticamente la apertura de dicha puerta cuando el vehículo se aproxima a ella a una distancia preestablecida, sin que el usuario deba interactuar en nada para ello, al mismo tiempo que el receptor de seguridad de la puerta comprueba la identificación del código que emite el dispositivo y, opcionalmente, efectúa una actualización de dicho código, siendo posible el uso del dispositivo para varios receptores pertenecientes al sistema del equipo que estén ubicados en diferentes puertas, para que un usuario acceda a cualquiera de ellas con su vehículo, así como el uso de múltiples dispositivos con el mismo receptor de cada puerta para que diferentes usuarios accedan a ellas. Es, por tanto, un segundo aspecto de la invención, el procedimiento de control de apertura de dichas puertas de garaje o recintos similares que se efectúa con dicho equipo.

### Campo de aplicación de la invención

El campo de aplicación de la presente invención se enmarca dentro del sector de la industria de la fabricación de aparatos y dispositivo electrónicos de control de acceso y apertura automática de puertas.

### Antecedentes de la invención

Como es sabido, cuando un vehículo, de cualquier tipo, accede a un recinto con restricción de acceso, como un parking público o privado, utiliza un mecanismo de identificación y autenticación para poder acceder. De esta forma existe un mecanismo para permitir que un vehículo acceda a utilizar el recinto bajo el servicio que se esté ofreciendo.

El aspecto en común entre todos los sistemas disponibles, en aparcamientos públicos o privados, en cancelas y vallas elevadoras, o en cualquier otro tipo de acceso restringido para vehículos, consiste en que en el momento de la identificación se requiere de interacción del usuario. Es decir, la persona, al llegar al control de accesos, se ve obligado a realizar una acción, bien sea recoger una tarjeta, mostrar un identificador, o accionar un dispositivo electrónico para identificarse y autenticarse, independientemente de que esta identificación sea más o menos segura.

Este es el primer elemento de los sistemas tradicionales, la interacción del usuario.

El segundo elemento es la seguridad, es decir, qué seguridad hay en el proceso de identificación y autenticación del usuario.

Otros sistemas que comparten este mismo concepto parten del uso de tecnología RF activa y pasiva, como RFID para identificar a la persona. El problema del uso de esta tecnología radica en que es una identificación única, no actualizable y, por lo tanto, estática.

Así pues, existen multitud de patentes e informes de estado de la técnica que hacen uso de sistemas de apertura automática de puertas de garaje y de otros tipos de recintos. Sin embargo, todos ellos llevan implícita la interacción del usuario en el momento de la identificación y autenticación.

Los sistemas más comunes utilizan un dispositivo o mando a distancia, emisor del código que el usuario posee de antemano y que está preparado para abrir la puerta. Sin embargo, este mando es único para una única puerta de garaje y siempre requiere la interacción del usuario en el momento de activar la apertura. Además, estos dispositivos están alimentados mediante baterías o pilas por lo que requieren de un mantenimiento periódico.

Esto ya implica dos factores de molestia para el usuario: la interacción y el mantenimiento.

Adicionalmente, los dispositivos tradicionales de acceso, tienen rangos de seguridad que van desde ninguna hasta muy elevada. Sin embargo, estas opciones de seguridad se circunscriben al uso de un dispositivo de apertura único con un receptor único, es decir, el mando A del usuario 1 sólo permite acceder al recinto R, pero no a otro recinto.

El objetivo de la presente invención es, pues, desarrollar un mejorado sistema de apertura automática de puertas de garaje que permita evitar dichos inconvenientes y, al mismo tiempo aumentar su seguridad, es decir, evitar la necesidad de que el usuario tenga que interactuar ni apretar ningún botón o aplicación electrónica del vehículo o de un mando a distancia, que no deba preocuparse por su mantenimiento, evitando el riesgo y la molestia que supone quedarse sin pilas en el mando o sin batería en el dispositivo electrónico y no poder acceder a la apertura de la puerta a no ser que lo haga manualmente, y, además, protegerse de manera segura frente a eventuales suplantaciones de código y acceso indebido a los recintos por parte de personas no autorizadas.

Es decir, el equipo propuesto viene a mejorar, con distintos elementos, los sistemas anteriormente descritos. La presente invención, en primer lugar, elimina la interacción que el usuario debe realizar cuando se encuentra en el control de acceso en puertas de garaje o aparcamientos u otros recintos y, además, implementa una seguridad adicional para evitar los ataques de suplantación mediante una evolución colaborativa de las huellas de generación de código.

Por otra parte, y como referencia al estado actual de la técnica, cabe señalar que, al menos por parte del solicitante se desconoce la existencia de ningún otro equipo de control de apertura de puertas de garaje ni invención de aplicación similar que presente unas características técnicas, estructurales y constitutivas iguales o semejantes a las que presenta el que aquí se preconiza y según se reivindica.

En dicho sentido, se conoce, por ejemplo, el documento US20150339869, referido a un sistema automático de apertura de puerta de garaje habilitado para Bluetooth®, abrepuertas u otro sistema y método automático de apertura de puerta que consiste en una aplicación para controlar, a través del protocolo Bluetooth, un abridor para una puerta enviando una señal Bluetooth a un receptor para activar la apertura o cierre de la puerta.

Dicho sistema, sin embargo, aunque tiene una aplicación similar al equipo de la invención, es esencialmente distinto, en especial por el hecho de que, como la mayoría de sistemas existentes, necesita de la intervención del usuario para interactuar en la aplicación y poder activar la apertura de la puerta, mientras que el equipo de la presente invención se basa, sobre todo como principal ventaja en que, gracias a que el emisor es un dispositivo tipo dongle, y que mientras está conectado está emitiendo la señal continuamente, el usuario no tiene que interactuar para activar la apertura de la puerta, y, como ventaja de seguridad adicional, también se diferencia con el sistema de dicha patente y con otros sistemas conocidos en que el receptor, conectado permanentemente a Internet, cambia el código de la señal cada vez que detecta la presencia del emisor.

**Explicación de la invención**

El equipo de control de apertura de puertas de garaje o similar y el procedimiento de control de apertura de dichas puertas mediante dicho equipo que la invención propone se configuran, pues, como una destacable novedad dentro de su campo de aplicación, ya que, a tenor de su implementación y de manera taxativa, se alcanzan satisfactoriamente los objetivos anteriormente señalados, estando los detalles caracterizadores que lo hacen posible y los distinguen de lo ya conocido convenientemente recogidos en las reivindicaciones finales que acompañan a la presente descripción.

De manera concreta, lo que la invención propone, como se ha apuntado anteriormente, es un equipo de control de apertura de puertas que comprende, por una parte, al menos un dispositivo emisor “manos libres” que emite una señal de radiofrecuencia que incluye un código seguro para identificarse y autenticarse y así accionar un sistema de apertura automática de puerta de garaje o recinto similar. Este dispositivo consiste en un “*dongle*” BLE *(Bluetooth Low Energy),* es decir, un módulo electrónico con microprocesador, memoria y antena Bluetooth, que llamaremos “manos libres” porque no precisa de la intervención del usuario para su funcionamiento.

Dicho dispositivo actúa únicamente como emisor de radiofrecuencia mediante protocolo bluetooth, con la peculiaridad de la generación segura del código de autenticación y de su sincronización con los receptores a los que esté asociado para aumentar considerablemente la seguridad.

El dispositivo emisor tiene unas dimensiones físicas mínimas y no tiene alimentación propia ni mantenimiento, ya que funciona alimentado desde el vehículo en el que se conecta, sea un coche o una motocicleta o un camión o cualquier otro vehículo al que, si no dispone de ello, se deberá instalar o conectar un puerto USB para efectuar dicha conexión. De esta forma, únicamente cuando el vehículo está encendido, el dispositivo puede funcionar, haciendo que el dispositivo no esté emitiendo en ningún momento adicional, evitando problemas de seguridad.

Adicionalmente, si mientras el vehículo se encuentra encendido, y por tanto, emitiendo el código, se intentase modificar el código de forma fraudulenta, el dispositivo emisor se bloqueará irremediablemente para garantizar la seguridad de toda la red, lo cual es posible debido a que estará programado para ello.

Paralelamente, el equipo comprende también, al menos un receptor de seguridad. El receptor es el módulo electrónico que acciona el mecanismo automático de apertura de la puerta en que esté instalado. Este receptor recibe los códigos emitidos por los dispositivos emisores “manos libres” como el antedicho de uno o más usuarios, convenientemente adscritos al sistema, así como los emitidos por otros sistemas como las aplicaciones móviles de Smartphones, si se programa para ello.

Si el dispositivo emisor de un usuario está habilitado para acceder al recinto, por estar adscrito al sistema, el receptor acciona la apertura de la puerta automáticamente cuando está a la distancia preestablecida.

La habilitación de usuarios se realiza a través de Internet por un servidor de gestión del sistema. El receptor de seguridad, que está conectado a Internet, recibe una lista de permisos de usuarios que tienen permiso de acceso y, en base a estos permisos y sus correspondientes códigos, el receptor activa la apertura de la puerta o no.

De manera más específica, el equipo de la invención comprende, esencialmente, las siguientes partes:

- Receptor de seguridad para accionar la apertura automática de la puerta y permitir la entrada al recinto correspondiente.

- Dispositivo emisor “manos libres” de acceso a recintos constituido por un *dongle* BLE.

Opcionalmente, el equipo contempla también la inclusión de otros dispositivos de acceso que no sean “manos libres” como Smartphones.

En cualquier caso, el receptor de seguridad y el dispositivo emisor cuentan con las siguientes características y prestaciones:

El receptor de seguridad es el dispositivo que tiene operativa la recepción de comunicaciones bluetooth en cualquier versión.

El receptor es el dispositivo que está conectado a Internet.

El receptor es el que recibe una petición de acceso a través de un dispositivo emisor *dongle* BLE o a través de un Smartphone.

El receptor es el que valida en primer lugar al usuario y, si éste está habilitado para el acceso, activa la apertura.

El dispositivo emisor “manos libres” es un dispositivo electrónico tipo “*dongle*” *bluetooth low energy* (Bluetooth de baja energía), cuya programación está preparada para comunicarse con cualquier receptor de seguridad asociado al sistema del equipo, emitiendo su identificador y su código de autenticación.

El dispositivo emisor “manos libres” no necesita nunca una interacción por parte del usuario. El usuario únicamente lo coloca en su vehículo, conectado a un puerto USB del mismo para que emita el código de acceso.

El dispositivo emisor “manos libres” está preparado para actualizar su código de autenticación tras cada proceso de apertura.

El dispositivo emisor “manos libres” es universal, es decir, se puede conectar a cualquier puerto USB de cualquier vehículo, y único para cada usuario y se comunica con cualquier receptor de seguridad del sistema para el que haya sido habilitado.

El dispositivo emisor “manos libres” se puede desconectar manualmente desconectándolo de la alimentación del vehículo.

El equipo no limita la posibilidad de que un Smartphone de un usuario, a través de una aplicación móvil específica que se incorpore al mismo, pueda realizar el mismo proceso de emisión del código que el dispositivo emisor “manos libres” con un receptor de seguridad del equipo para el que haya sido habilitado. Con ello, un usuario podrá acceder a un recinto con receptor de seguridad, utilizando indistintamente un dispositivo emisor “manos libres” dongle conectado al vehículo y/o su smartphone activando manualmente la aplicación para ello, pudiendo hacerlo tanto desde el propio vehículo o bien para acceder a pie. Asimismo, no se descarta que dicho usuario, para acceder a pie al recinto, pueda conectar momentáneamente el dispositivo emisor “manos libres” dongle, a través del correspondiente conector con puerto USB, a su smartphone, tableta electrónica, ordenador portátil, batería externa, u otro dispositivo apto para ello.

Con todo ello, las principales ventajas que proporciona el equipo de la invención, respecto a otros sistemas de control de apertura de puertas son las siguientes:

- Manos libres. El equipo de la invención supone una mejora de los sistemas existentes de apertura de la puerta del garaje mediante Bluetooth a través de una aplicación haciendo uso del móvil, ya que no requiere la activación de la persona para ejecutar la acción de apertura en la puerta, sino que sucede de manera automática dado que el dispositivo emisor constantemente lanza la señal de apertura mientras el vehículo en el que se encuentra conectado esté encendido, y cuando éste se aproxima lo suficiente como para que el aparato receptor reciba la señal con el código de apertura individualizado.

Este dispositivo emisor permite la identificación y autenticación y no requiere interacción, por lo que se elimina el factor de interacción ya explicado.

El dispositivo emisor “manos libres” está preparado para que, de forma dinámica y automática, sea actualizado para que su código sea en todo momento diferente.

El dispositivo emisor “manos libres” sólo puede interactuar con receptores específicos de este sistema.

Este dispositivo emisor no requiere de alimentación. Funciona conectado al vehículo y es éste el que lo alimenta para que el dispositivo emita su código de identificación y autenticación. Además, es removible manualmente si hiciese falta.

- Batería. El equipo de la invención supone una mejora respecto al uso de las comunicaciones Bluetooth de los dispositivos móviles para el control de apertura de la puerta de garajes, ya que no requiere el uso de batería para alimentarlo, dado que usa la alimentación del propio vehículo.

Con esto se consigue evitar los fallos por agotamiento de alimentación y la compra de reposiciones, pilas y/o baterías.

El dispositivo no está emitiendo constantemente el código, ya que cuando el vehículo se apaga éste también se apaga.

De esta forma, el dispositivo no requiere de mantenimiento, lo que supone un ahorro muy importante para el usuario, que ya no sólo no tiene que adquirir nuevas baterías o pilas, sino que también evita desplazamientos innecesarios a aquellos establecimientos concretos a los que el proveedor de la puerta obliga a acudir a sus clientes.

- Acceso universal. Otro factor que supone una ventaja en el equipo de la invención consiste en que el acceso mediante el dispositivo emisor “manos libres” es universal para todos aquellos recintos que cuenten con receptor de seguridad conectado al sistema de apertura de puerta y para los que haya sido habilitado, es decir, para los que tenga el permiso de entrada.

De esta forma, un mismo dispositivo emisor “manos libres” puede servir para acceder a dos o más recintos diferentes, con accesos no relacionados.

Además, el dispositivo emisor “manos libres” no solamente es un elemento para acceder a cualquier recinto con receptor de seguridad de este sistema, sino que también, aunque no pueda acceder porque no tenga permiso y el receptor no le active el acceso, también realiza un proceso de seguridad sobre el receptor.

- Receptor inteligente de gestión de accesos. El receptor de seguridad del equipo de la invención es un dispositivo a colocar en el control de accesos a un recinto conectado al mecanismo de accionamiento de la apertura de la puerta, cancela, valla, etc.

El receptor de seguridad dispone de un mecanismo de comunicaciones inalámbricas Bluetooth, de todas las versiones posibles, desde 1.0 hasta 5.X en este momento.

Asimismo, el receptor también dispone de un mecanismo de comunicaciones inalámbricas vía wifi, de todas las versiones posibles, desde wifi 802.11b hasta wifi 802.11ah y superiores; y/o de un mecanismo de comunicaciones móviles por tecnología 3G, 4G y hasta 5G; y/o de un mecanismo de comunicaciones inalámbricas según el estándar NB-IoT (NarrowBand IoT).

El receptor se conecta a un servidor de Internet para tener una lista de permisos de usuarios y códigos de identificación y autenticación de éstos.

El receptor está programado para comprobar, en cada intento de acceso por parte de un dispositivo emisor “manos libres” o por aplicación móvil, si los códigos de identificación y autenticación son correctos para permitir el paso.

El receptor actualiza el sistema de seguridad colaborativo con cada intento de acceso, sea positivo o negativo, actualizando la matriz de huella sincronizada entre todos los receptores.

- Actualización de códigos de seguridad. El equipo de la presente invención supone una mejora respecto al uso de sistemas de apertura mediante comunicaciones inalámbricas de código fijo, como las tarjetas pasivas RFID, ya que el formato USB dongle Bluetooth permite la actualización y reconfiguración del código de identificación y autenticación vía software, sin necesidad de retirar el dispositivo.

El código de identificación y autenticación es modificable y actualizable de forma inalámbrica y automática.

Cada vez que uno de los dispositivos emisores “manos libres” o Smartphone, trata de acceder a un receptor del equipo, utiliza su código de identificación y su código de autenticación e, independientemente de que el acceso sea positivo o negativo, su código de autenticación cambiará para el siguiente acceso.

La actualización del código de seguridad la realiza el receptor sobre el dispositivo, sea el dispositivo emisor “manos libres” o un Smartphone.

Adicionalmente, el receptor, tras el intento de acceso del dispositivo, sea “manos libres” o Smartphone, actualiza su código de receptor en el sistema mediante un proceso colaborativo.

- Sincronización de la seguridad colaborativa. El dispositivo emisor “manos libres” tiene diversas opciones de seguridad en la creación del código de autenticación. El receptor de seguridad es el encargado de modificar el código de autenticación del dispositivo emisor manos libres, por lo que se mantienen los sistemas de encriptación evolutivos de los mandos de seguridad.

Esto permite que el dispositivo emisor “manos libres”, sin ninguna interacción por parte del usuario en ningún momento, sea un sistema de encriptación de máxima seguridad.

Ello es posible gracias a que el receptor de seguridad es el que actualiza la huella del dispositivo emisor “manos libres” que es la que genera el código de autenticación para el siguiente uso. Sin embargo, todos los receptores del equipo están conectados a Internet, y la evolución de los códigos de seguridad y trazabilidad se realiza a través de la interacción entre todos los receptores, por ello, cuantos más receptores hay en la red de receptores, así como usuarios, mayor es la seguridad del sistema, puesto que la seguridad está distribuida y no centralizada.

- Sincronización de la seguridad colaborativa ampliada. La seguridad colaborativa es un incremento de las opciones de seguridad que tiene el equipo de la invención, puesto que son los usuarios los que, constantemente, y de forma transparente para ellos, sin interacción de ningún tipo, afectan a las actualizaciones del sistema de seguridad.

Por ello, a mayor número de usuarios con dispositivos emisores “manos libres” y Smartphones, con mayor número de receptores, la seguridad aumenta, dado que la interacción de los usuarios al acceder o salir de los recintos obedece al uso que los propios usuarios realizan, por lo que la generación de huellas y su evolución es impredecible dentro del sistema, y todos los dispositivos emisores “manos libres” y Smartphones son actualizados por la interacción de otros usuarios del sistema.

- Seguridad interrelacionada. El uso del dispositivo emisor “manos libres” proporciona una mejora adicional de seguridad.

Esta medida adicional de seguridad se basa en que el Smartphone de un usuario, que además disponga de dispositivo emisor “manos libres”, esté en las proximidades de dicho dispositivo “manos libres”, lo que permite deducir si el usuario se encuentra en el vehículo en el momento en el que se produce una apertura.

De esta forma, cuando se realiza una apertura a través de un dispositivo “manos libres”, el sistema en Internet puede consultar al Smartphone del usuario correspondiente si el propio Smartphone se encuentra en las proximidades del propio recinto y del dispositivo emisor “manos libres” concreto y así tener mayor información para detectar alertas de seguridad.

El sistema consulta al smartphone su localización geográfica gracias al uso de la tecnología GPS, pudiendo inferir situaciones anómalas, consultar al usuario y verificar el buen funcionamiento o alertar al usuario en caso de ruptura de la seguridad.

El equipo permite incluir en el sistema de seguridad interrelacionada cualquier otro uso de datos de sensores del smartphone como acelerómetro, giróscopo, magnetómetro, barómetro y antenas y cotejarlos con los sensores instalados en el receptor o con el patrón de conducta del usuario para establecer situaciones anómalas de peligro.

Este triángulo de seguridad formado entre el receptor de seguridad, el dispositivo emisor “manos libres” y el Smartphone se puede realizar exclusivamente gracias a estos elementos y gracias a su interrelación.

El descrito equipo de control de apertura de puertas de garaje o similar y el procedimiento de control de apertura de dichas puertas representa, pues, una innovación de características estructurales y constitutivas desconocidas hasta ahora, razones que unidas a su utilidad práctica, la dotan de fundamento suficiente para obtener el privilegio de exclusividad que se solicita.

**Descripción de los dibujos**

Para complementar la descripción que se está realizando y con objeto de ayudar a una mejor comprensión de las características de la invención, se acompaña a la presente memoria descriptiva, como parte integrante de la misma, de un juego de planos, en los que con carácter ilustrativo y no limitativo se ha representado lo siguiente:

Las figuras número 1.- Muestra una representación esquemática de un ejemplo del equipo de control de apertura de puertas de garaje o similar, objeto de la invención, apreciándose las principales partes y elementos que comprende, así como su configuración y disposición.

**Realización preferente de la invención**

A la vista de la descrita figura 1 y única, y de acuerdo con la numeración adoptada en ella, se puede observar cómo el equipo en cuestión comprende, al menos, un receptor de seguridad (1), consistente en un dispositivo electrónico programable con conexión a Internet (I), y conectado al mecanismo de apertura automática de una puerta (2) de acceso a un recinto de garaje o similar, y, al menos, un dispositivo electrónico emisor (3) “manos libres”, consistente en un *dongle* BLE o módulo electrónico con microprocesador, memoria y antena *Bluetooth* que, cuando está conectado a un puerto USB (4), por ejemplo de un vehículo (5) de un usuario, emite una señal de radiofrecuencia mediante protocolo bluetooth que es detectada por dicho receptor de seguridad (1) cuando se le aproxima a un radio preestablecido, momento en el cual, dicho receptor de seguridad (1), si el código y la autentificación que incluye dicha señal del dispositivo emisor (3) *dongle* están habilitados para dicho receptor de seguridad (1), acciona automáticamente la apertura de la puerta (2), sin que el usuario deba interactuar en nada para ello.

La existencia de un único receptor de seguridad (1) y un único dispositivo emisor (3) dongle, supone la opción básica del equipo, apta para que un solo usuario acceda a un único recinto y se le abra automáticamente la puerta (2) del mismo al aproximarse. Sin embargo, el equipo, preferentemente, está ideado para un uso más plural, es decir, de control de acceso a múltiples recintos y por múltiples usuarios.

Por ello, preferentemente, el equipo comprende dos o más receptores de seguridad (1) conectados en red, a través de Internet, e instalados cada uno en distintas puertas (2) de diferentes recintos, siendo aptos para detectar la señal, y comprobar el código y autentificación, de un mismo dispositivo emisor (3) *dongle*, para que un mismo usuario pueda acceder a cualquiera de ellos, así como, también de modo preferido, comprende múltiples dispositivos emisores (3) *dongle* de diferentes usuarios cuyas señales son detectadas, y comprobados sus códigos y autentificaciones, por uno o más de dichos receptores de seguridad (1).

Opcionalmente, el equipo comprende, además, la inclusión de dispositivos adicionales de acceso, tales como Smartphones (6), que emiten, vía Bluetooth, la señal con el código y la autentificación para el receptor de seguridad (1) al activar dicha emisión el usuario a través de una aplicación instalada al efecto, y que este detecta cuando se encuentra en su radio de alcance igualmente preestablecido.

La habilitación de los dispositivos emisores (3) dongle y, en su caso, de los dispositivos adicionales de acceso smartphones (6), se realiza a través de Internet por un servidor (7) de gestión del sistema. El receptor de seguridad (1) o receptores, que están conectados a Internet, reciben una lista de dispositivos de usuarios que tienen permiso de acceso y, en base a estos permisos y sus correspondientes códigos, tras su habilitación la primera vez que lo detecta cualquiera de dichos receptores, activan la apertura de la puerta o no en posteriores ocasiones en sean detectados.

Además, preferentemente, cada receptor de seguridad (1) está capacitado para efectuar una actualización de dicho código de cada dispositivo emisor (3) o smartphone (6) cada vez que lo detecta en su radio de alcance.

Cada receptor de seguridad (1) dispone de un mecanismo de comunicaciones inalámbricas Bluetooth en cualquiera de sus versiones, para detectar la señal de los dispositivos emisores (3) manos libres o smartphones (6) y, para la conexión a Internet, de mecanismo de comunicaciones inalámbricas vía wifi, también en cualquiera de sus versiones, desde wifi 802.11b hasta wifi 802.11 ah o superiores; y/o de un mecanismo de comunicaciones móviles 3G, 4G o 5G; y/o de un mecanismo de comunicaciones inalámbricas según el estándar NB- loT (NarrowBand loT).

Con todo ello, el procedimiento de control de apertura de puertas (2) de garaje o similar con el equipo descrito comprende esencialmente la habilitación de uno o más dispositivos emisores (3) dongle a través un servidor (7) de gestión del sistema, con el que conecta uno o más receptores de seguridad (1) a través de Internet, y del que reciben una lista de dispositivos de usuarios que tienen permiso de acceso y, en base a lo cual, genera y asigna códigos para cada uno de dichos dispositivos emisores (3) que, tras su habilitación la primera vez que alguno de los receptores de seguridad (1) detecta la señal de radiofrecuencia que emiten vía bluetooth cuando están conectados a un puerto USB (4) dichos dispositivos emisores (3), activan la apertura de la puerta o no en posteriores ocasiones en que sean detectados al encontrarse en su radio de alcance.

Del mismo modo, dispositivos adicionales de acceso como smartphones (6), son igualmente habilitados por receptores de seguridad (1) la primera vez que los detectan, al activar la aplicación implementada en ellos para emitir la señal de radiofrecuencia, y activan la apertura de la puerta o no en posteriores ocasiones en que sean detectados, en este caso, al ser activados por el usuario, además de encontrarse en su radio de alcance.

Y, preferentemente, cada receptor de seguridad (1) efectúa una actualización del código asignado a cada dispositivo emisor (3) o, en su caso, a cada smartphone (6), cada vez que lo detecta en su radio de alcance, independientemente de si activa o no el mecanismo de la puerta (2).

En la figura 1 se ha realizado una representación esquemática del dispositivo (1) instalado en una puerta, mostrando todos los elementos que intervienen para su funcionamiento, pudiendo apreciarse que, se conecta en la puerta (2) al cuadro de maniobra (8) que controla el accionamiento del motor que mueve el mecanismo de apertura de la misma, así como que dispone de antena (9) para la comunicación inalámbrica con Internet y de sensores (10)

bluetooth para detectar la señal que envía el dongle (3) o el smartphone (6) que lleva el usuario en el vehículo (5).

Descrita suficientemente la naturaleza de la presente invención, así como la manera de ponerla en práctica, no se considera necesario hacer más extensa su explicación para que cualquier experto en la materia comprenda su alcance y las ventajas que de ella se derivan, haciéndose constar que, dentro de su esencialidad, podrá ser llevada a la práctica en otras formas de realización que difieran en detalle de la indicada a título de ejemplo, y a las cuales alcanzará igualmente la protección que se recaba siempre que no se altere, cambie o modifique su principio fundamental.

## REIVINDICACIONES

1. EQUIPO DE CONTROL DE APERTURA DE PUERTAS DE GARAJE O SIMILAR que, siendo de los que comprende, al menos, un receptor conectado al mecanismo de apertura automática de una puerta (2) de acceso a un recinto de garaje o similar, y, al menos, un emisor susceptible de emitir una señal de radiofrecuencia detectable por dicho receptor para que active el mecanismo de la puerta (2), está **caracterizado** por comprender, como receptor conectado al mecanismo de apertura automática de una puerta (2), al menos, un receptor de seguridad (1) consistente en un dispositivo electrónico programable con conexión a Internet (I), y como emisor de la señal de radiofrecuencia, al menos, un dispositivo electrónico emisor (3) "manos libres", consistente en un *dongle* BLE o módulo electrónico con microprocesador, memoria y antena *Bluetooth,* el cual, cuando está conectado a un puerto USB, por ejemplo de un vehículo (5), emite, constantemente y sin intervención del usuario, una señal de radiofrecuencia mediante protocolo bluetooth que detecta dicho receptor de seguridad (1) cuando se encuentra en un radio de alcance preestablecido.

2. EQUIPO DE CONTROL DE APERTURA DE PUERTAS DE GARAJE O SIMILAR, según la reivindicación 1, **caracterizado** porque comprende dos o más receptores de seguridad (1) conectados en red, a través de Internet, e instalados cada uno en distintas puertas (2) de diferentes recintos, siendo todos ellos aptos para detectar la señal, de un mismo dispositivo emisor (3) *dongle.*

3. EQUIPO DE CONTROL DE APERTURA DE PUERTAS DE GARAJE O SIMILAR, según la reivindicación 2, **caracterizado** porque comprende múltiples dispositivos emisores (3) *dongle* de diferentes usuarios cuyas señales son detectables por uno o más receptores de seguridad (1).

4. EQUIPO DE CONTROL DE APERTURA DE PUERTAS DE GARAJE O SIMILAR, según cualquiera de las reivindicaciones 1 a 3, **caracterizado** porque además comprende uno o más dispositivos adicionales de acceso, tales como Smartphones (6), que emiten, vía Bluetooth, una señal detectable por un receptor de seguridad (1) cuando se activa a través de una aplicación instalada al efecto.

5. EQUIPO DE CONTROL DE APERTURA DE PUERTAS DE GARAJE O SIMILAR, según cualquiera de las reivindicaciones 1 a 4, **caracterizado** porque cada receptor de seguridad (1) dispone de un mecanismo de comunicaciones inalámbricas Bluetooth en cualquiera de sus versiones, para detectar la señal de los dispositivos emisores (3) dongle y, en su caso, de dispositivos smartphones (6).

6. EQUIPO DE CONTROL DE APERTURA DE PUERTAS DE GARAJE O SIMILAR, según cualquiera de las reivindicaciones 1 a 5, **caracterizado** porque cada receptor de seguridad (1) dispone, para la conexión a Internet, de mecanismo de comunicaciones inalámbricas vía wifi.

7. EQUIPO DE CONTROL DE APERTURA DE PUERTAS DE GARAJE O SIMILAR, según cualquiera de las reivindicaciones 1 a 6, **caracterizado** porque cada receptor de seguridad (1) dispone, para la conexión a Internet, de un mecanismo de comunicaciones móviles 3G, 4G o 5G.

8. EQUIPO DE CONTROL DE APERTURA DE PUERTAS DE GARAJE O SIMILAR, según cualquiera de las reivindicaciones 1 a 7, **caracterizado** porque cada receptor de seguridad (1) dispone, para la conexión a Internet, de mecanismo de comunicaciones inalámbricas según el estándar NB-loT (NarrowBand loT).

9. PROCEDIMIENTO DE CONTROL DE APERTURA DE PUERTAS, mediante un equipo como el descrito en las reivindicaciones 1 a 8, **caracterizado** por comprender la habilitación de uno o más dispositivos emisores (3) dongle a través un servidor (7) de gestión del sistema, con el que conecta uno o más receptores de seguridad (1) a través de Internet, y del que reciben una lista de dispositivos de usuarios que tienen permiso de acceso y, en base a lo cual, genera y asigna los códigos que, tras su habilitación la primera vez que alguno de los receptores de seguridad (1) detecta la señal de radiofrecuencia que emiten vía bluetooth cuando están conectados a un puerto USB (4) cada uno de dichos dispositivos emisores (3), activan la apertura de la puerta o no en posteriores ocasiones en que sean detectados al encontrarse en su radio de alcance.

10. PROCEDIMIENTO DE CONTROL DE APERTURA DE PUERTAS, según la reivindicación 9, **caracterizado** porque dispositivos adicionales de acceso como smartphones (6), son igualmente habilitados por receptores de seguridad (1) la primera vez que los detectan, al activar la aplicación implementada en ellos para emitir la señal de radiofrecuencia, y activan la apertura de la puerta o no en posteriores ocasiones en que sean detectados al ser activados por el usuario y encontrarse en su radio de alcance.

11. PROCEDIMIENTO DE CONTROL DE APERTURA DE PUERTAS, según la reivindicación 9 ó 10, **caracterizado** porque cada receptor de seguridad (1) efectúa una actualización del código asignado a cada dispositivo emisor (3) o, en su caso, smartphone (6), cada vez que lo detecta en su radio de alcance, independientemente de si activa o no el mecanismo de la puerta (2).

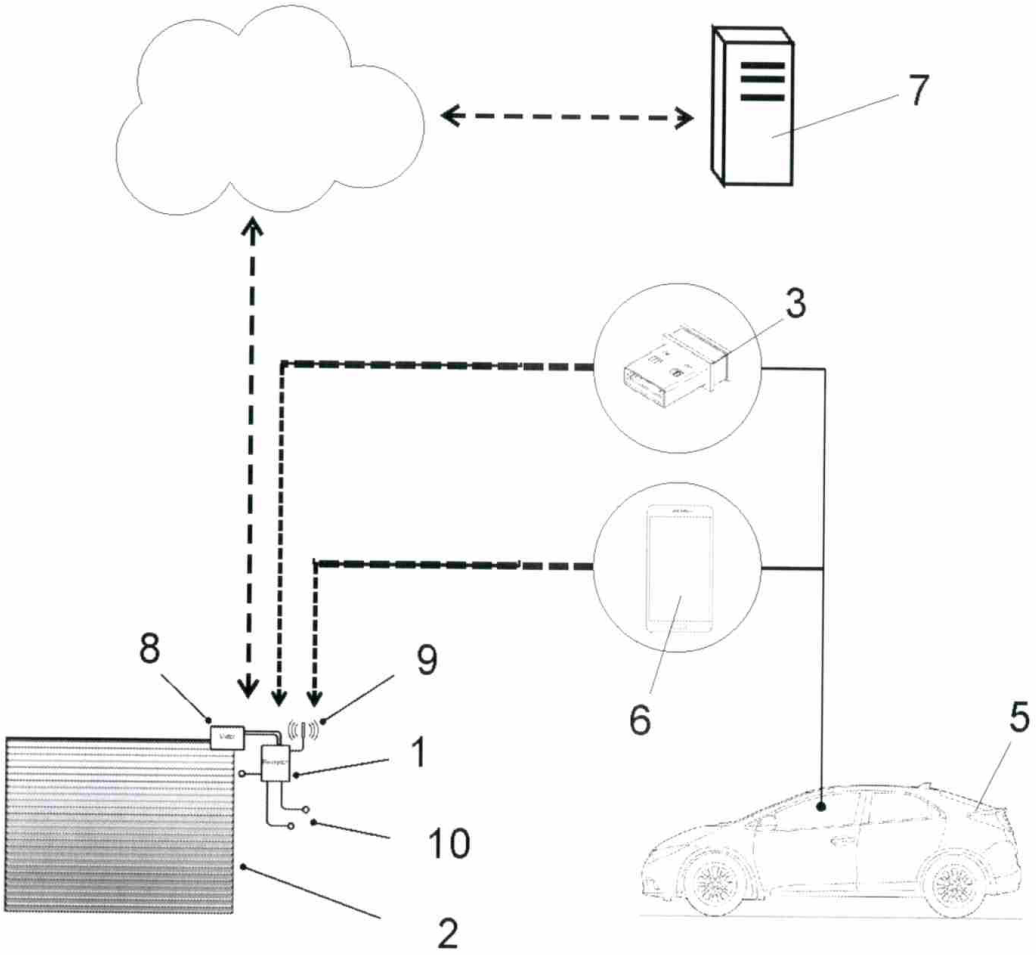


FIG. 1

OFICINA ESPAÑOLA
DE PATENTES Y MARCAS

ESPAÑA

(21) N.º solicitud: 201700310

(22) Fecha de presentación de la solicitud: 29.03.2017

(32) Fecha de prioridad:

# INFORME SOBRE EL ESTADO DE LA TECNICA

(51) **Int. Cl. :** Ver Hoja Adicional

DOCUMENTOS RELEVANTES

| **Categoría** | (56) **Documentos citados** | **Reivindicaciones afectadas** |
|---|---|---|
| X | US 2015302738 A1 (GEERLINGS STEVEN L et al.) 22/10/2015, párrafos [0002 - 0169]; figuras 1 - 10. | 1-11 |
| X | US 2015302732 A1 (WRIGHT THOMAS S et al.) 22/10/2015, párrafos [0002 - 0214]; figuras 1 - 6. | 1-11 |
| A | US 2009212939 A1 (RICHMOND ROBERT C) 27/08/2009, Descripción; figuras. | 1-11 |
| A | US 2016019790 A1 (TOBOLSKI TRICIA et al.) 21/01/2016, Descripción; figuras. | 1-11 |
| A | US 2016308971 A1 (SWEENEY JEFFREY MICHAEL et al.) 20/10/2016, Descripción; figuras. | 1-11 |
| A | US 2017078398 A1 (HAIDAR MAHMOUD et al.) 16/03/2017, Descripción; figuras. | 1-11 |
| A | WO 2014134148 A2 (POLARIS INC) 04/09/2014, Descripción; figuras. | 1-11 |
| A | US 2016125412 A1 (CANNON ROYCE E) 05/05/2016, Descripción; figuras. | 1-11 |
| A | CN 204002500U U (CHENGDU BESTVISION TECHNOLOGY CO LTD) 10/12/2014, Descripción; figuras. | 1-11 |

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** | **Examinador** | **Página** |
|---|---|---|
| 08.03.2018 | I. Rodríguez Goñi | 1/7 |

OFICINA ESPAÑOLA
DE PATENTES Y MARCAS

ESPAÑA

(21) N.º solicitud: 201700310

(22) Fecha de presentación de la solicitud: 29.03.2017

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TECNICA

(51) **Int. Cl. :** Ver Hoja Adicional

DOCUMENTOS RELEVANTES

| **Categoría** | (56) **Documentos citados** | **Reivindicaciones afectadas** |
|---|---|---|
| A | ES 2205868T T3 (HORMANN KG ANTRIEBSTECHNIK) 01/05/2004, Descripción; figuras. | 1-11 |

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** | **Examinador** | **Página** |
|---|---|---|
| 08.03.2018 | I. Rodríguez Goñi | 2/7 |

CLASIFICACIÓN OBJETO DE LA SOLICITUD

***E05B47/00*** (2006.01)
***E05B49/00*** (2006.01)
***E05F15/77*** (2015.01)
***G08C17/02*** (2006.01)
***H04W12/00*** (2009.01)

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

H04W, G08C, E05F, E05B

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

INVENES, EPODOC, WPI

Fecha de Realización de la Opinión Escrita: 08.03.2018

**Declaración**

| | | | |
|---|---|---|---|
| **Novedad (Art. 6.1 LP 11/1986)** | Reivindicaciones | 1-11 | **SI** |
| | Reivindicaciones | | **NO** |
| **Actividad inventiva (Art. 8.1 LP11/1986)** | Reivindicaciones | | **SI** |
| | Reivindicaciones | 1-11 | **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 | US 2015302738 A1 (GEERLINGS STEVEN L et al.) | 22.10.2015 |

**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**

Se considera D01 el documento del estado de la técnica más cercano para el objeto de la reivindicación 1.
El documento D01 describe (se incluyen entre paréntesis referencias a D01):

**equipos de control de apertura de puertas de garaje** (Párrafo (0002); "A trainable transceiver generally sends and/or receives wireless signals using a transmitter, receiver, and/or transceiver. For example, a trainable transceiver may send a wireless control signal to operate a garage door opener.").

**que comprenden, al menos, un receptor conectado al mecanismo de apertura automática de una puerta de acceso a un recinto de garaje o similar** (Párrafo (0027); "Generally, a trainable transceiver controls one or more home electronic devices and/or remote devices. Home electronic devices may include devices such as a garage door opener, gate opener, lights, security system, and/or other device which is configured to receive activation signals and/or control signals."
Párrafo (0121); "Referring now to FIG. 9, the trainable transceiver 10 may be configured to operate with a second trainable transceiver 204 in physical contact with the original transmitter 14 in some embodiments. The first trainable transceiver 10 may send an activation signal and/or other information to the second trainable transceiver 204 which is in physical contact with the original transmitter 14 of the home electronics device 12, remote device 18, and/or other device. In response to the signal received from the first trainable transceiver 10, the second trainable transceiver 204 may physically activate the original transmitter 14. The original transmitter 14 may send an activation signal to the corresponding home electronics device 12, remote device 18, and/or other device in response to being physically activated.")

**y, al menos, un emisor susceptible de emitir una señal de radiofrecuencia detectable por dicho receptor para que active el mecanismo de la puerta** (Párrafo (0031); "In some embodiments, the trainable transceiver transmits and/or receives information (e.g., activation signals, control signals, control data, status information, or other information) using a radio frequency signal."),

**y que además comprende como receptor conectado al mecanismo de apertura automática de una puerta, al menos, un receptor de seguridad consistente en un dispositivo electrónico programable con conexión a Internet** (Párrafo (0117); "In some embodiments, the home electronics device 12, remote device 18, and/or other device is configured to connect to the internet 200. For example, the device may include a radio frequency transceiver allowing for communication with an internet connected WiFi router."
Párrafo (0120); "In some embodiments, the home electronics device 12, remote device 18, and/or other device may be configured to connect to the internet 200. The device may include a WiFi transceiver for connecting to a router, network card, wired connection to a router or modem, cellular transceiver, and/or other hardware for accessing the internet 200. For example, a garage door opener may include a WiFi transceiver for connecting to a router and/or home network with access to the internet 200."
Párrafo (0028); "Activation signals may be wired or, preferably, wireless signals transmitted to a home electronic device and/or remote device. Activation signals may include control signals, control data, encryption information (e.g., a rolling code, rolling code seed, look-a-head codes, secret key, fixed code, or other information related to an encryption technique), or other information transmitted to a home electronic device and/or remote device.").
Párrafo (0045); "For example, the transceiver circuit 26 may be configured to send activation signals to the home electronic device 12 (e.g., a garage door opener) using an encrypted radio wave transmission.").

**y como emisor de la señal de radiofrecuencia, al menos, un dispositivo electrónico emisor (3) "manos libres", consistente en un dongle BLE o módulo electrónico con microprocesador, memoria y antena Bluetooth, el cual, cuando está conectado a un puerto USB, por ejemplo de un vehículo, emite, constantemente y sin intervención del usuario, una señal de radiofrecuencia mediante protocolo bluetooth que detecta dicho receptor de seguridad cuando se encuentra en un radio de alcance preestablecido.**
(Párrafo (0083); "Referring now to FIGS. 3A and 3B, the trainable transceiver 10 may include two modules, a remote user interface module 140 and a base station 142.""
Párrafo (0086); "In some embodiments, the base station 142 is coupled to, connected to, and/or otherwise in communication with a system of the vehicle. For example, the base station 142 may be plugged into a power source of the vehicle such as a USB port, 12 volt power port, cigarette lighter, and/or other power source of the vehicle.").

Párrafo (0051); “The mobile communications device 16, which may communicate with the trainable transceiver 10 in some embodiments of the trainable transceiver 10, may be a device purchased by a consumer separately from the trainable transceiver 10. For example, the mobile communications device 16 may be a cell phone purchased from a third party retailer. In some embodiments, the mobile communications device 16 (e.g., smartphone, tablet, cellular telephone, laptop, key fob, dongle, etc.) includes a control circuit 40.”
Párrafo (0049); “In some embodiments, the trainable transceiver 10 includes a Bluetooth Low Energy (BLE) transceiver 32.”
Párrafo (0043); “The transceiver circuit 26 allows the trainable transceiver 10 to transmit and/or receive wireless communication signals. The wireless communication signals may be transmitted to or received from a variety of wireless devices (e.g., the original transmitter 14, home electronic device 12, mobile communications device 16, and/or remote device). In some embodiments, the transceiver circuit 26 may include additional hardware such as processors, memory, integrated circuits, antennas, etc.”
Párrafo (0114); “In some embodiments, the trainable transceiver 10 may determine if a device is the within transmission range 192 using two-way (e.g., bidirectional) communication with the device as described with reference to FIG. 5. For example, the trainable transceiver 10 may send out a request transmission to the device, continuously, periodically, and/or based on the location of the trainable transceiver 10 relative to the device.”).

La diferencia entre la reivindicación 1 y lo descrito en el documento D01 es que en dicho documento no se encuentra una única forma de realización que recoja todas las características reivindicadas, sino que las características reivindicadas se encuentran repartidas en diferentes formas de realización. Sin embargo, para el experto en la materia, que conoce el documento D01 resultaría obvio a partir de las enseñanzas del mismo, llegar a la reivindicación 1, yuxtaponiendo las características de las diversas formas de realización. Por ello cabe concluir que si bien la reivindicación 1 sería nueva (Art. 6.1 LP 11/1986), carecería de actividad inventiva (Art. 8.1 LP 11/1986).

La reivindicación 2 es dependiente e incorpora que **comprende dos o más receptores de seguridad conectados en red, a través de Internet, e instalados cada uno en distintas puertas de diferentes recintos, siendo todos ellos aptos para detectar la señal, de un mismo dispositivo emisor dongle**. En el documento D01 se describe que un dispositivo emisor (véase el conjunto de “Trainable Transceiver” (10) y “Mobile Comunications Device” (16), que en el párrafo (0051) se indica que puede ser un dongle) puede controlar uno o más receptores (Párrafo (0027); “Generally, a trainable transceiver controls one or more home electronic devices and/or remote devices”) de seguridad conectados en red, a través de Internet, e instalados cada uno en distintas puertas (véase párrafos (0118), (0120) y (0134-0135)). Por ello se considera que la reivindicación 2 carecería de actividad inventiva (Art. 8.1 LP 11/1986).

La reivindicación 3 es dependiente e incorpora que **comprende múltiples dispositivos emisores dongle de diferentes usuarios cuyas señales son detectables por uno o más receptores de seguridad**. Para el experto en la materia se trata de una opción de diseño obvia (véase al respecto en el documento D01 los párrafos (0111) y (0130)); que en un sistema de control entre un emisor y un receptor se pase a un conjunto de emisores y receptores, sin proporcionar ninguna característica técnica concreta de la que pueda deducirse algún efecto técnico inesperado, más que la mera escalación del sistema, no se considera que exija esfuerzo inventivo. Por ello se considera que la reivindicación 3 carecería de actividad inventiva (Art. 8.1 LP 11/1986).

La reivindicación 4 es dependiente e incorpora que además **comprende uno o más dispositivos adicionales de acceso, tales como Smartphones que emiten, vía Bluetooth, una señal detectable por un receptor de seguridad cuando se activa a través de una aplicación instalada al efecto**. Para el experto en la materia que conoce los párrafos (0037) y (0087) del documento D01 se trataría de una opción evidente, por lo que se considera que la reivindicación 4 carecería de actividad inventiva (Art. 8.1 LP 11/1986).

Las reivindicaciones 5 a 8 se consideran así mismo opciones de diseño evidentes, bien por lo que se conoce del propio documento D01, bien porque se trata de elecciones obvias, por lo que se considera que dichas reivindicaciones carecerían de actividad inventiva (Art. 8.1 LP 11/1986).

Se considera D01 el documento del estado de la técnica más cercano para el objeto de la reivindicación 9. El documento D01 describe (se incluyen entre paréntesis referencias a D01):

**equipos de control de apertura de puertas de garaje y métodos de funcionamiento de dichos equipos, que comprenden la habilitación de uno o más dispositivos emisores** (Párrafo (0102); “The trainable transceiver 10 may be configured such that no activation signals are sent unless the trainable transceiver 10 receives information from the mobile communications device 16. The information received from the mobile communications device 16 may be a unique key which, when received by the trainable transceiver 10, allows the trainable transceiver 10 to function. Other cryptographic techniques may be used such that the trainable transceiver 10 does not function unless in communication with the or a particular mobile communications device.“)

**dongle** (en el párrafo (0051) se dice que el "mobile communications device" 16 puede ser un dongle. El "mobile communications device" junto con el "trainable transceiver" constituyen un dispositivo emisor, pero incluso el "mobile communications device" por sí mismo, según puede leerse en el párrafo (0144), puede controlar los "home electronics device 12" como p.e. "a garage door opener" mediante las técnicas descritas en D01)

**a través de un servidor de gestión del sistema** (párrafo (0088) The mobile communications device 16 may serve as intermediary device which is used by the trainable transceiver 10 to communicate with other devices (e.g., servers, networking equipment, other mobile communications device, home electronics devices, remote devices, and/or other devices),

**con el que conecta uno o más dispositivos emisores a través de Internet** (párrafo (0088); "In some embodiments, the trainable transceiver 10 may access the internet using a communications connection with the mobile communications device 16.")

**y del que reciben una lista de dispositivos de usuarios que tienen permiso de acceso** (Párrafo (0106) "In some embodiments, the trainable transceiver 10 includes a database of keys which when transmitted to the trainable transceiver 10 allow the trainable transceiver 10 to function.")

**y, en base a lo cual, genera y asigna los códigos que, tras su habilitación la primera vez que alguno de los receptores de seguridad detecta la señal de radiofrecuencia que emiten vía bluetooth cuando están conectados a un puerto USB cada uno de dichos dispositivos emisores activan la apertura de la puerta o no en posteriores ocasiones en que sean detectados al encontrarse en su radio de alcance** (ver párrafos (0149)-(0154) "temporary code", "rolling code" y lo comentado en la reivindicación 1).

La diferencia principal entre la reivindicación 9 y lo descrito en el documento D01 es que en la reivindicación 9 se dice que son los receptores de seguridad los que conectan con el servidor, mientras que en el documento D01 se habla de que son los dispositivos emisores los que se conectan con el servidor. Sin embargo, de una manera implícita se puede considerar que los receptores de seguridad ("home electronics device 12", "second trainable transceiver 204") estarían conectados al servidor de manera indirecta, pues dichos receptores de seguridad se comunican, entre otras maneras, vía internet, con los dispositivos emisores y acceder así al servidor.

Por otra parte, hay que señalar que no existe en el documento D01 una única forma de realización que recoja todas las características que se han mencionado antes, sino que obedecen a distintas formas de realización. Sin embargo, para el experto en la materia, que conoce el documento D01 resultaría obvio a partir de las enseñanzas del mismo, llegar a la reivindicación 9, yuxtaponiendo las características de las diversas formas de realización.

Por ello cabe concluir que si bien la reivindicación 9 sería nueva (Art. 6.1 LP 11/1986), carecería de actividad inventiva (Art. 8.1 LP 11/1986).

La reivindicación 10 es dependiente e incorpora que **dispositivos adicionales de acceso como smartphones, son igualmente habilitados por receptores de seguridad la primera vez que los detectan, al activar la aplicación implementada en ellos para emitir la señal de radiofrecuencia, y activan la apertura de la puerta o no en posteriores ocasiones en que sean detectados al ser activados por el usuario y encontrarse en su radio de alcance**. Por lo ya explicado para las reivindicaciones 4 y 9 se considera que se trataría de una opción de diseño obvia, por lo que dicha reivindicación carecería de actividad inventiva (Art. 8.1 LP 11/1986).

La reivindicación 11 es dependiente e incorpora que **cada receptor de seguridad efectúa una actualización del código asignado a cada dispositivo emisor o, en su caso, smartphone, cada vez que lo detecta en su radio de alcance, independientemente de si activa o no el mecanismo de la puerta**. En el documento D01 se dice (Fig. 5, Párrafo (0114); "In some embodiments, the trainable transceiver 10 may determine if a device is the within transmission range 192 using two-way (e.g., bidirectional) communication with the device as described with reference to FIG. 5. For example, the trainable transceiver 10 may send out a request transmission to the device, continuously, periodically, and/or based on the location of the trainable transceiver 10 relative to the device.") que el emisor puede, entre otras posibilidades, cada vez que detecte a un receptor, emitir una petición de transmisión. También se dice (Párrafo (0149); "In some embodiments, the trainable transceiver 10 is configured to provide a temporary code which allows for communication (e.g., sending activation signals) to the home electronics device 12, remote device 18, and/or other device.") que el emisor está configurado para proporcionar un código temporal que permite la comunicación con los receptores. Esto tiene como consecuencia que cada vez que un emisor y un receptor se detectan se solicite la comunicación y se utilice un código temporal. Como también se dice (Párrafo (0154); "In other embodiments, the temporary code may be a one-time use code") que dicho código puede ser de un solo uso, cabe concluir que, una actualización del código cada vez que un emisor detecte a un receptor resultaría obvio a partir de lo descrito en D01. Si bien, en la reivindicación 11 se dice que es el receptor el que efectúa la actualización, en D01 la actualización la efectúa el emisor, pero el hecho de que la actualización la realice uno u otro de los dos tipos de equipos, no supone que se tenga que utilizar esfuerzo inventivo para ello. Por todo lo expuesto se considera que la reivindicación 11, no sería sino una opción de diseño evidente a partir de lo que se describe en el documento D01 y que por ello carecería de actividad inventiva (Art. 8.1 LP 11/1986).