(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 919 776**

(51) Int. CI.:

G08B 13/14	(2006.01)	***G06F 21/34***	(2013.01)
G08B 13/12	(2006.01)	***G06F 21/45***	(2013.01)
E05B 45/06	(2006.01)	***G06F 21/88***	(2013.01)
G06F 7/02	(2006.01)	***G08B 25/00***	(2006.01)
G06F 7/04	(2006.01)	***G07C 9/00***	(2010.01)
H04B 5/02	(2006.01)	***H04B 1/3816***	(2015.01)
B60R 25/10	(2013.01)	***H04B 1/3877***	(2015.01)
B60R 25/24	(2013.01)	***H04W 48/00***	(2009.01)
F17D 3/01	(2006.01)	***H04W 12/0471***	(2011.01)
G05B 19/04	(2006.01)	***H04W 12/082***	(2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **14.04.2017 PCT/US2017/027798**

(87) Fecha y número de publicación internacional: **19.10.2017 WO17181137**

(96) Fecha de presentación y número de la solicitud europea: **14.04.2017 E 17783328 (2)**

(97) Fecha y número de publicación de la concesión europea: **13.04.2022 EP 3443544**

(54) Título: **Control de autorización para un sistema de seguridad antirrobo**

(30) Prioridad:

15.04.2016 US 201662323466 P
15.04.2016 US 201662323511 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
28.07.2022

(73) Titular/es:

MOBILE TECH, INC. (100.0%)
5665 Meadows, Suite 150
Lake Oswego, OR 97035, US

(72) Inventor/es:

WYLIE, HUNTER A.;
SCHATZ, KRISTOPHER W. y
BLASER, ROBERT L.

(74) Agente/Representante:

DURAN-CORRETJER, S.L.P

DESCRIPCIÓN

Control de autorización para un sistema de seguridad antirrobo

Referencia cruzada y reivindicación de la prioridad de las solicitudes de Patente relacionadas:

Esta solicitud de Patente reivindica la prioridad de la Patente provisional US62/323,466, presentada el 15 de abril de 2016, y titulada “Security Alarm Key for Retail Security Display”.

Asimismo, esta solicitud de Patente reivindica la prioridad de la Patente provisional US62/323,511, presentada el 15 de abril de 2016, y titulada “Alarm Key System for Retail Security Display”.

Introducción:

En las tiendas se exponen muchos productos tales como dispositivos electrónicos (concretamente electrónica de mano, tal como teléfonos inteligentes, ordenadores de tableta, cámaras digitales, etc.), en posiciones de soporte individuales sobre mostradores o en expositores de estantería. Habitualmente, se emplea un conjunto de exposición de producto en cada posición de soporte, para facilitar la presentación de estos productos a los clientes. El conjunto de exposición de producto incluye, habitualmente, un conjunto de disco y un conjunto de base. Un producto tal como un dispositivo electrónico se monta sobre una superficie del conjunto de disco, y el conjunto de disco se acopla con el conjunto de base cuando el conjunto de disco está en reposo. Para tener la capacidad de que un cliente sostenga o mire más de cerca el dispositivo electrónico, el conjunto de disco puede ser levantado de su posición de reposo. Se puede emplear una correa para mantener el conjunto de disco conectado con el conjunto de base cuando el conjunto de disco está en la posición levantada, pero no es necesario que sea así.

Los conjuntos de exposición de producto incluyen, habitualmente, sistemas de seguridad que activarán alarmas cuando se producen acciones tales como una extracción indebida del producto del conjunto de disco o un movimiento inadecuado del conjunto de disco. Estos sistemas de seguridad a menudo están configurados para poder cambiar entre un estado activado y un estado desactivado. En un estado activado, el sistema de seguridad activará una alarma cuando se producen acciones no autorizadas. En un estado desactivado, el sistema de seguridad está deshabilitado.

Se han desarrollado llaves manuales que permiten al personal de una tienda activar o desactivar los sistemas de seguridad de los conjuntos de exposición de producto. Estas llaves se pueden denominar “llaveros” o “llaveros de seguridad” (“key fob” o “security fob”). Con un llavero de seguridad convencional, el llavero de seguridad y el conjunto de exposición de producto están programados para tener códigos coincidentes (un código de “activación/desactivación”). Este código programable convierte de manera efectiva el llavero de seguridad en una llave electrónica que encaja en una cerradura electrónica en el conjunto de exposición de producto, para que el llavero de seguridad pueda activar o desactivar el sistema de seguridad del conjunto de exposición de producto.

El documento de Patente US2015/0348381, 3 de diciembre de 2015 (03-12-2015), da a conocer un sistema de seguridad programable para proteger artículos de mercancías contra robos.

No obstante, este enfoque convencional de los llaveros de seguridad da como resultado un problema práctico que está relacionado con la rotación de personal en una tienda. Para reducir el riesgo de que un llavero de seguridad se use de manera no autorizada, los gerentes de las tiendas desean un mecanismo eficiente para controlar qué llaveros de seguridad están autorizados para controlar los estados de seguridad de uno o varios conjuntos de exposición de producto. Por ejemplo, cuando un empleado nuevo comienza a trabajar y necesita un nuevo llavero de seguridad, se desea un mecanismo eficiente para autorizar rápidamente el nuevo llavero de seguridad para su utilización con uno o varios conjuntos de exposición de producto. Como ejemplo adicional, cuando un empleado deja de trabajar, se desea un mecanismo eficiente para desautorizar rápidamente el llavero o llaveros de seguridad que habían sido utilizados previamente por ese empleado. Dada la relativa frecuencia de cambios en el personal de la tienda, la necesidad de técnicas eficientes de autorización y desautorización con respecto a los llaveros de seguridad es importante.

Para resolver estos problemas, en el presente documento se dan a conocer soluciones en las que el sistema puede agregar rápidamente un llavero de seguridad a una lista de autorizaciones para un conjunto de exposición de producto, realizando una secuencia definida de interacciones utilizando un primer llavero de seguridad y un segundo llavero de seguridad. El primer y el segundo llaveros de seguridad pueden ser un llavero de seguridad de gerente, para ser utilizado por un gerente de una tienda, y el nuevo llavero de seguridad que debe ser agregado a la lista de autorizaciones. Como ejemplo, la secuencia definida puede ser una conexión del llavero de seguridad del gerente con un conector del conjunto de exposición de producto, seguido de una desconexión del llavero de seguridad del gerente con el conector, seguido de una conexión del nuevo llavero de seguridad con el conector dentro de una ventana de tiempo definida. El inicio de la ventana de tiempo puede ser activado mediante la conexión del llavero de seguridad del gerente con el conector, o mediante la desconexión del llavero de seguridad del gerente, del conector. Esta secuencia puede activar el conjunto de exposición de producto para actualizar su lista de autorizaciones, con el

fin de agregar un identificador para el nuevo llavero de seguridad. Posteriormente, cuando el nuevo llavero de seguridad es conectado al conector del conjunto de exposición de producto, el conjunto de exposición de producto puede autenticar el nuevo llavero de seguridad basándose en su identificador comparándolo con la lista de autorizaciones. Una vez autenticado, el nuevo llavero de seguridad se puede utilizar para controlar un estado de seguridad para el conjunto de exposición de producto. Un ejemplo de un lapso de tiempo que se puede utilizar para la ventana de tiempo puede ser de 10 segundos.

Asimismo, en el presente documento se dan a conocer soluciones en las que el sistema puede desautorizar rápidamente uno o varios llaveros de seguridad que pueden estar incluidos en la lista de autorizaciones, mediante la realización de otra secuencia definida de interacciones. Por ejemplo, una secuencia definida para una desautorización puede ser una conexión del llavero de seguridad del gerente con un conector del conjunto de exposición de producto, seguido de una desconexión del llavero de seguridad del gerente con el conector, seguido de una reconexión del llavero de seguridad del gerente con el conector dentro de una ventana definida. Esta secuencia puede hacer que el conjunto de exposición de producto elimine su lista de autorizaciones, lo que anulará la autorización de cualquier llavero de seguridad previamente autorizado.

Estas y otras características y ventajas de la presente invención se describirán a continuación para los expertos en la materia.

Breve descripción de los dibujos:

La figura 1 da a conocer una realización de ejemplo de un sistema de autorización basado en una puerta de enlace para llaveros de seguridad.
La figura 2 muestra una realización de ejemplo de un llavero de seguridad.
Las figuras 3A a 3F muestran realizaciones de ejemplo de un conjunto de exposición de producto.
Las figuras 3G a 3H muestran realizaciones de ejemplo de un conjunto de disco.
La figura 3I muestra una realización de ejemplo de una circuitería de seguridad para un conjunto de exposición de producto.
La figura 4 muestra un flujo de proceso de ejemplo para su ejecución por una circuitería de seguridad, para facilitar la gestión de la autorización y la autenticación del llavero.
La figura 5 muestra una ejecución del flujo del proceso de ejemplo por parte de un llavero de seguridad cuando interactúa con la circuitería de seguridad.
La figura 6 representa un ejemplo de cómo se puede gestionar una lista de autorizaciones utilizando las técnicas descritas en el presente documento.
La figura 7 representa una realización de ejemplo de un llavero de seguridad.
La figura 8 representa otra realización de ejemplo de un llavero de seguridad.
Las figuras 9 a 14 dan a conocer realizaciones de seguridad de ejemplo, y de la circuitería relacionada.

Descripción detallada de realizaciones de ejemplo:

La figura 1 da a conocer una realización de ejemplo de un sistema para gestionar de manera segura cómo se autorizan y desautorizan los llaveros de seguridad con respecto al control sobre las funciones de seguridad de un conjunto de exposición de producto. El sistema puede incluir un conjunto 100 de exposición de producto para la colaboración con uno o varios llaveros de seguridad de gerente (o principal) 108 y uno o varios llaveros de seguridad de usuario 110.

El conjunto 100 de exposición de producto puede servir como un sistema de seguridad antirrobo, y puede ser utilizado para presentar un producto, tal como un dispositivo electrónico 106, a los consumidores, de manera segura. Tal como se mencionó, ejemplos de dispositivos electrónicos 106 adecuados pueden incluir dispositivos electrónicos portátiles de consumo, tales como teléfonos inteligentes, tabletas, cámaras digitales, etc. El conjunto 100 de exposición de producto puede incluir un sensor de seguridad 102 y una circuitería de seguridad 104, que colaboran entre sí para generar una señal de situación de seguridad en respuesta a la detección de un evento relacionado con la extracción del dispositivo electrónico 106 del conjunto 100 de exposición de producto. La circuitería de seguridad 104 puede ser controlada para que pueda conmutar entre un estado activado y un estado desactivado basándose en la interacción con un llavero de seguridad 110 autorizado.

Para habilitar la utilización autorizada de un llavero de seguridad 110 con el conjunto 100 de exposición de producto, un llavero de seguridad de gerente 108 y un llavero de seguridad de usuario 110 interactúan con el conjunto 100 de exposición de producto de acuerdo con una secuencia 118 definida, que activará una acción de gestión de la autorización del llavero por parte del conjunto 100 de exposición de producto. Por ejemplo, se puede definir una secuencia de interacciones que hace que el conjunto 100 de exposición de producto entre en un modo que agrega un nuevo llavero de seguridad 110 a una lista de uno o varios llaveros de seguridad que están autorizados para controlar el estado de seguridad del conjunto de exposición de producto. Una vez que se ha agregado un llavero de seguridad 110 a esta lista de autorizaciones utilizando las técnicas que se describen a continuación, ese llavero de seguridad puede interactuar con el conjunto 100 de exposición de producto (interacciones 120) para que el llavero

de seguridad 110 se pueda autenticar, con lo cual el llavero de seguridad 110 autenticado puede controlar una o varias funciones de seguridad.

De esta manera, los gerentes de una tienda pueden gestionar qué llaveros de seguridad están autorizados para controlar las funciones de seguridad de qué conjuntos de exposición de producto, de una manera simple y efectiva.

La figura 2 muestra una realización de ejemplo de un llavero de seguridad 108 o 110. El llavero de seguridad 108/110 puede adoptar la forma de un objeto de mano que es capaz de comunicarse con un conjunto 100 de exposición de producto. El llavero de seguridad 108/110 puede presentar cualquiera de un número de formas, tal como comprendería un profesional. Por ejemplo, el llavero de seguridad 108/110 puede tener una forma similar a las pequeñas memorias USB portátiles, y similares. Como ejemplo adicional, el llavero de seguridad 108/110 puede tener una forma similar a un disco, un cilindro o dispositivos de entrada sin llave para vehículos. En otras realizaciones de ejemplo, el llavero de seguridad 108/110 puede adoptar la forma de una placa o tarjeta o, incluso, de un dispositivo informático inalámbrico, tal como un teléfono inteligente o un ordenador de tableta (ejemplos de los cuales se explican a continuación).

El llavero de seguridad 108/110 puede incluir una interfaz 200, un procesador 202, una memoria 204 y una o varias luces 208, tal como uno o varios diodos emisores de luz (LED, Light Emitting Diodes), cada uno alojado o parcialmente alojado en el interior de un cuerpo envolvente de algún tipo, tal como una carcasa de plástico o de un material compuesto. Estos componentes pueden estar configurados para comunicarse entre sí a través de un bus o de una interconexión similar. Además, se debe comprender que el llavero de seguridad 108/110 no necesita incluir necesariamente todos los componentes que se muestran en la figura 2; por ejemplo, un profesional puede optar por emplear un llavero de seguridad que no incluye ninguna luz 208. Asimismo, también se debe comprender que el llavero de seguridad 110 puede incluir componentes adicionales que no se muestran en la figura 2 (por ejemplo, una E/S inalámbrica para comunicaciones inalámbricas a través de una red inalámbrica, con sistemas remotos, un dispositivo de almacenamiento de energía, tal como una batería y/o uno o varios condensadores, y/o dispositivos de entrada de usuario, tales como uno o varios botones, etc.).

A través de la interfaz 200, el llavero de seguridad 108/110 se puede comunicar con el conjunto 100 de exposición de producto. Como ejemplo, la interfaz 200 puede ser un conector físico, para conectar de manera desmontable el llavero de seguridad 108/110 con el conjunto 100 de exposición de producto. Como ejemplo adicional, la interfaz 200 puede ser un conector inalámbrico para conectar de manera inalámbrica el llavero de seguridad 108/110 con el conjunto de exposición de producto. La interfaz 200 puede ser cualquier tipo de interfaz adecuada para interconectar el llavero de seguridad 108/110 con una interfaz complementaria del conjunto 100 de exposición de producto para los fines descritos en el presente documento. Por ejemplo, en realizaciones en las que la interfaz 200 es un conector físico, este conector físico puede ser un conector físico que cumple con un estándar tal como el estándar de bus de serie universal (USB, Universal Serial Bus) (por ejemplo, un conector mini-USB).

El procesador 202 y la memoria 204 pueden ser cualquier dispositivo de hardware adecuado para realizar las operaciones descritas en el presente documento. Como ejemplo, el procesador 202 puede adoptar la forma de un microprocesador Atmel SAMD21. La memoria 204 puede ser parte integral del procesador 202 y/o externa al procesador 204.

La memoria 204 puede almacenar un identificador 212 para el llavero de seguridad 108/110. Este identificador 212 es, preferentemente, un identificador único (UID, Unique IDentifier) que distingue el llavero de seguridad 108/110 en cuestión de otros llaveros de seguridad 108/110 dentro del sistema. Esta singularidad puede ser una singularidad en un sistema, tal como dentro de una tienda determinada, o puede ser una singularidad en un sistema más amplio (por ejemplo, una cadena de tiendas). En su sentido más amplio, la singularidad puede ser universal, en cuyo caso el UID puede adoptar la forma de un UID universal (UUID, Universal UID). Un código UUID de ejemplo puede ser un código de múltiples bits (por ejemplo, un código de 128 bits), con un cierto número (o conjunto) de bits asignados para identificar al fabricante, otro conjunto de bits asignado a otra información (por ejemplo, la hora o fecha en que el código UUID fue grabado en el chip de memoria) y un tercer conjunto de bits asignado para expresar un número aleatorio generado de manera única. En consecuencia, el UUID 212 del llavero funciona como un número de serie único e identifica específicamente solo un llavero de seguridad 108/110. En una realización de ejemplo, este UUID 212 del llavero no es reprogramable.

La memoria 204 también puede almacenar uno o varios programas de software 250 para que los ejecute el procesador 202. El programa o programas de software 250 pueden adoptar la forma de una pluralidad de instrucciones ejecutables por el procesador que residen en un medio de almacenamiento no transitorio legible por ordenador, tal como la memoria 204 A continuación se describe una realización de ejemplo del programa o programas de software 250 haciendo referencia a la figura 5.

La luz o las luces 208 pueden adoptar la forma de cualquier fuente de luz adecuada para realizar las operaciones descritas en el presente documento. Como ejemplo, la luz o las luces 208 pueden ser un solo LED que se ilumina cada vez que el llavero de seguridad 110 controla con éxito el estado de seguridad de la circuitería de seguridad 104. Como ejemplo adicional, la luz o las luces 208 pueden ser múltiples LED (que pueden ser LED de diferentes

colores) que se utilizarán para indicar a un usuario si el llavero de seguridad ha sido agregado con éxito como un llavero de seguridad autorizado (una iluminación de un primer LED) y para indicar una acción de control con éxito con respecto a la circuitería de seguridad 104 (una iluminación de un segundo LED). Se debe comprender que otras combinaciones son posibles para indicar diferentes eventos si así lo desea un profesional.

Los llaveros de seguridad del gerente 108 y los llaveros de seguridad del usuario 110 pueden presentar la misma arquitectura básica, tal como se indica en la figura 2. Se puede emplear cualquiera de varias técnicas para hacer que los llaveros de gerente 108 se distingan de los llaveros de usuario 110 mediante un sistema lector empleado para gestionar la lista de autorizaciones. Por ejemplo, el identificador 212 de llavero de un llavero de gerente 108 puede ser conocido por un sistema lector. En una realización de ejemplo, el sistema lector puede formar parte de la circuitería de seguridad 104. En consecuencia, con dicha realización de ejemplo, la circuitería de seguridad 104 podría identificar los llaveros de gerente 108 leyendo sus identificadores 212 de llavero. No obstante, en otras realizaciones de ejemplo, se podrían utilizar indicadores de datos distintos al identificador de llavero para indicar el estado como un llavero de gerente 108 (por ejemplo, un indicador de un solo bit, que estaría a nivel alto si el llavero en cuestión es un llavero de gerente 108, y bajo si el llavero en cuestión es un llavero de usuario 110). Además, con otras realizaciones de ejemplo, un llavero puede utilizar alguna forma de codificación cableada para identificar su estado como un llavero de gerente 108. Por ejemplo, una o varias resistencias de configuración pueden ser utilizadas para identificar qué llaveros son llaveros de seguridad de gerente 108 y cuáles son llaveros de seguridad de usuario 110. Con las resistencias de configuración, la cantidad de resistencia puede ser detectada por un lector y utilizada para determinar el tipo de llavero. Por ejemplo, la resistencia correspondiente a X ohmios se puede asociar con un llavero de seguridad de gerente 108 y la resistencia correspondiente a Y ohmios se puede asociar con un llavero de seguridad de usuario 110.

Las figuras 3A a 3C muestran diversas realizaciones de ejemplo de diferentes tipos de conjuntos 100 de exposición de producto que se pueden utilizar con el sistema. Tal como se señaló anteriormente, el conjunto 100 de exposición de producto puede incluir un conjunto de disco 302 y un conjunto de base 304. El dispositivo electrónico 106 se puede montar en la superficie 306 del conjunto de disco 302 para que el dispositivo electrónico 106 pueda ser expuesto de manera segura, a los clientes, en una tienda. El conjunto de disco 302 puede ser movido entre una posición de reposo y una posición levantada. Cuando está en la posición de reposo, el conjunto de disco 302 hace contacto con el conjunto de la base 304, tal como se muestra en la figura 3A. Cuando está en la posición levantada, el conjunto de disco 302 está separado del conjunto de la base 304, tal como se muestra en las figuras 3B y 3C. La figura 3B muestra una realización de ejemplo en la que se utiliza un conjunto de correa 308 para conectar físicamente el conjunto de disco 302 con el conjunto de la base 304, incluso cuando el conjunto de disco 302 está en la posición levantada. Una señal de situación de seguridad (por ejemplo, para indicar una extracción no autorizada del dispositivo electrónico 106 del conjunto de disco 302) puede ser comunicada desde el conjunto de disco 302 a través del conjunto de correa 308 o mediante comunicación inalámbrica (con el conjunto de la base 304 o con algún otro sistema). La figura 3C muestra una realización de ejemplo de un conjunto 100 inalámbrico de exposición de producto. Con el ejemplo de la figura 3C, la comunicación inalámbrica 310 se puede utilizar para comunicar una señal de situación de seguridad del conjunto de disco 302 al conjunto de la base 304 (o a algún otro sistema).

Ejemplos de conjuntos 100 de exposición de producto que pueden ser adaptados para su utilización en la práctica de las realizaciones descritas en el presente documento, se dan a conocer en las Patentes US8,558,688, US8,698,617 y US8,698,618 y las publicaciones de Patente US2014/0159898 y US2017/0032636.

Por ejemplo, las figuras 3D y 3E reproducen las figuras 27 y 28 de la publicación de Patente US2017/0032636 y muestran un conjunto 100 de exposición de producto de ejemplo que se describe con más detalle en la publicación 2017/0032636. El conjunto 100 de exposición de producto mostrado en las figuras 3D y 3E incluye un conjunto de disco 302, un conjunto de base 304 y un conjunto de correa 308. Un cable de alimentación 312 proporciona una conexión eléctrica entre el conjunto de disco 302 y el dispositivo electrónico 106 a través del cual se puede cargar el dispositivo electrónico 106. El conjunto de disco 302 puede recibir energía de una fuente de alimentación a través del conjunto de la base 304 cuando el conjunto de disco está en reposo, tal como se muestra en la figura 3D. Los contactos incluidos en el conjunto de disco y el conjunto de la base (véase, por ejemplo, el contacto 314 que se muestra en la figura 3E) pueden hacer contacto entre sí cuando el conjunto de disco está en reposo, formando de este modo una conexión eléctrica a través de la cual se puede suministrar potencia desde una fuente de alimentación (no mostrada) al conjunto de disco, a través del conjunto de la base y de la conexión eléctrica formada por los contactos. Cuando se levanta el conjunto de disco 302, los contactos pierden contacto entre sí, interrumpiendo, por lo tanto, la conexión eléctrica. Opcionalmente, se puede incluir una batería u otro dispositivo de almacenamiento de potencia en el conjunto de disco 302 para almacenar potencia para su utilización por el conjunto de disco 302 cuando el conjunto de disco está en la posición levantada.

Como ejemplo adicional, la figura 3F reproduce la figura 8 de la patente US8,698,617 y muestra un ejemplo de conjunto 100 de exposición de producto que se describe con más detalle en la Patente '617. En esta vista, se muestra un conjunto 100 de exposición de producto de ejemplo con las piezas desmontadas, donde se pueden ver diversos componentes de un conjunto de disco 302, un conjunto de base 304 y un conjunto de correa 308.

La figura 3G representa un conjunto de disco 302 de ejemplo que incluye una interfaz 320, un sensor de seguridad 102 y una circuitería de seguridad 104. Cada uno de estos componentes puede estar alojado total o parcialmente en el interior de un cuerpo envolvente de algún tipo, tal como una carcasa de plástico o de un material compuesto. Estos componentes también pueden ser configurados para comunicarse entre sí a través de un bus o de una interconexión similar.

La interfaz 320 es para interconectar un llavero de seguridad 108/110 con el conjunto de disco 302. La interfaz 320 puede ser un tipo de interfaz que sea complementario con la interfaz 200 del llavero de seguridad 108/110. Por ejemplo, si la interfaz 200 es un conector mini-USB, entonces la interfaz 320 puede ser un conector mini-USB complementario. Como ejemplo adicional, si la interfaz 200 es un chip de RFID, la interfaz 320 puede ser un lector de RFID.

El sensor de seguridad 102 puede ser uno o varios sensores que estén adaptados para detectar eventos tales como la extracción del dispositivo electrónico 106 del conjunto de disco 302 u otros eventos que puedan indicar una posible situación de seguridad. Un sensor de seguridad de ejemplo 102 puede ser un botón de presión, incluido en la superficie del conjunto de disco 306, que se presiona cuando el dispositivo electrónico 106 es acoplado con el conjunto de disco 302, pero se suelta cuando el dispositivo electrónico 106 es extraído del conjunto de disco 302. La liberación del botón de presión puede activar la circuitería de seguridad 104 (cuando está activada) para generar una señal condicional de seguridad. No obstante, se debe comprender que se podrían emplear otros sensores de seguridad 102. Otro ejemplo de un sensor de seguridad 102 que puede ser utilizado con conjuntos 100 de exposición de producto que incluyen un conjunto de correa 308 puede ser un circuito que detecta cuando la correa está cortada o rota. Otro ejemplo adicional de un sensor de seguridad 102 puede ser un circuito de detección de posición, que detecta cuando el conjunto de disco 302 es desplazado una cierta distancia más allá del conjunto de la base o sale de una zona de cercado virtual designada. Por ejemplo, dicho circuito de detección de posición puede estar basado en señales inalámbricas y en estimaciones de intensidad de señal, para detectar distancias entre el conjunto de disco 302 y el conjunto de la base 304. Otros ejemplos adicionales de sensores de seguridad 102 pueden incluir sensores de consumo de potencia, cierres de contacto, sensores ópticos para detectar objetos (o la ausencia de objetos), sensores de vibración y/o sensores de aceleración.

La circuitería de seguridad 104 puede ser cualquier circuitería que esté configurada para ser (1) controlable entre una pluralidad de estados de seguridad, en respuesta al código de seguridad 116 y (2) generar una señal de situación de seguridad cuando sea apropiado (por ejemplo, cuando la circuitería de seguridad 104 está en un estado activado y el sensor de seguridad 102 detecta un evento de activación). Por ejemplo, la circuitería de seguridad 104 puede incluir lógica de conmutación y similares, que es controlada basándose en una señal de un procesador de control que controla la lógica de conmutación sobre la base de si se ha verificado el código de seguridad 116. La circuitería de seguridad 104 también puede incluir una circuitería tal como controladores de relé, controles de motor, unidades de alarma, controladores de solenoide y/o accionadores de bloqueo.

Tal como se muestra en la figura 3I, la circuitería de seguridad 104 puede incluir un procesador 350 y una memoria 352 que colaboran entre sí para ejecutar uno o varios programas de software 356 que proporcionan funciones de gestión y autenticación de llaveros. El programa de software 356 puede adoptar la forma de una pluralidad de instrucciones ejecutables por un procesador, que residen en un medio de almacenamiento no transitorio legible por ordenador, tal como la memoria 352. Un ejemplo de un programa de software 356 de este tipo se describe a continuación haciendo referencia a la figura 4. El procesador 350 y la memoria 352 pueden ser cualquier dispositivo de hardware adecuado para realizar las operaciones descritas en el presente documento. Como ejemplo, el procesador 352 puede adoptar la forma de un microprocesador Atmel SAMD21. La memoria 352 puede ser parte integral del procesador 350 y/o externa al procesador 350.

La memoria 352 puede almacenar el programa 356 de gestión/autenticación del llavero, así como la lista de autorizaciones 358 utilizada por el programa 356 cuando determina si un llavero de seguridad 110 es un llavero de seguridad autorizado. La lista de autorizaciones 358 puede adoptar la forma de una lista de uno o varios identificadores 212 de llavero para llaveros de seguridad 110 que están autorizados para controlar el estado de seguridad del conjunto 100 de exposición de producto.

La circuitería de seguridad 104 también puede incluir una circuitería 354 adicional relacionada con las funciones de seguridad proporcionadas por la circuitería de seguridad, cuyos ejemplos se muestran en las figuras 9 y 10 y 12 a 14.

Se debe comprender que el conjunto de disco 302 puede incluir componentes diferentes a los que se muestran en la figura 3G. Por ejemplo, la figura 3H muestra un conjunto de disco 302 de ejemplo que incluye componentes adicionales. El conjunto de disco 302 de la figura 3H incluye una interfaz adicional 322. Esta interfaz 322 puede interconectar el conjunto de disco 302 con un dispositivo electrónico 106 presentado a los clientes a través del conjunto 100 de exposición de producto. Por ejemplo, la interfaz 322 puede ser un conector físico, adaptado para la conexión desmontable con un cable de alimentación para proporcionar potencia al dispositivo electrónico 106. Se describen ejemplos de dichos cables de alimentación en las Patentes US8,558,688, 8,698,617 y 8,698,618 y las Publicaciones Patente US2014/0159898 y US2017/003263 mencionadas anteriormente.

El conjunto de disco 302 de la figura 3H incluye, asimismo, uno o varios contactos de carga 314. Estos contactos de carga 314 pueden crear una conexión eléctrica con una fuente de alimentación a través de contactos complementarios del conjunto de la base 304 cuando el conjunto de disco 302 está en la posición de reposo. Ejemplos de dichos contactos de carga 314 se describen en las Patentes US8,558,688, US8,698,617 y US8,698,618 y en las publicaciones de Patente US2014/0159898 y US2017/003263.

El conjunto de disco 302 de la figura 3H incluye, asimismo, un dispositivo de almacenamiento de potencia 330 que se carga por medio de la electricidad recibida a través de los contactos de carga 314 cuando el conjunto de disco 302 está en la posición de reposo, y que almacena potencia para ser utilizada por el conjunto de disco 302 cuando el conjunto de disco está en la posición levantada. El dispositivo de almacenamiento de potencia 330 puede adoptar la forma de una batería (preferentemente una batería recargable) o un condensador adecuado. Ejemplos de dicho dispositivo de almacenamiento de potencia 330 se describen en las Patentes US8,558,688, US8,698,617 y US8,698,618 y en las Publicaciones de Patente US2014/0159898 y US2017/003263 mencionadas anteriormente.

El conjunto de disco 302 de la figura 3H también puede incluir una circuitería adicional 332. Por ejemplo, la circuitería adicional 332 puede incluir circuitería para distribuir potencia desde los contactos de carga 314 hacia otros componentes del conjunto de disco 302 (por ejemplo, la circuitería de seguridad 104, las interfaces 320 y 322, el dispositivo de almacenamiento de energía 330, etc.) y/o circuitería para distribuir potencia desde el dispositivo de almacenamiento de potencia 330 hacia otros componentes del conjunto de disco 302 (por ejemplo, la circuitería de seguridad 104; las interfaces 320 y 322). Como ejemplo adicional, la circuitería adicional 332 puede incluir circuitería de comunicación inalámbrica, que proporciona al conjunto de disco la capacidad de transmitir de manera inalámbrica señales de condiciones de seguridad desde la circuitería de seguridad 104, o comunicarse de otro modo de manera inalámbrica con sistemas remotos. Ejemplos de circuitería 332 adicional se describen en las Patentes US8,558,688, US8,698,617 y US8,698,618 y en las Publicaciones de Patente US2014/0159898 y US2017/003263 mencionadas anteriormente.

La figura 4 representa un flujo de proceso de ejemplo para la circuitería de seguridad 104, que incluye la ejecución del programa de software 356 por parte del procesador 350 para facilitar la gestión de qué llaveros de seguridad 110 están autorizados y cómo se autentican los llaveros de seguridad autorizados. En la etapa 400, la circuitería de seguridad 104 detecta una conexión con un llavero de seguridad en la interfaz 320. Esta conexión puede ser una conexión física o una conexión inalámbrica, dependiendo de los deseos de un profesional. Esta detección se puede realizar de alguna de varias maneras. Por ejemplo, en una realización de ejemplo donde la conexión entre las interfaces 200 y 320 es una conexión física, la circuitería de seguridad 104 puede detectar una resistencia de configuración en el llavero de seguridad para identificar el dispositivo conectado como un llavero de seguridad. Los diferentes tipos de dispositivos que pueden ser conectados a través de la interfaz 320 pueden incluir diferentes valores para las resistencias de configuración, para permitir, de este modo, que la circuitería de seguridad 104 distinga entre diferentes tipos de dispositivos conectados. Por lo tanto, las resistencias de configuración no solo se pueden utilizar para distinguir los llaveros de seguridad de gerente 108 de los llaveros de seguridad de usuario 110, sino que también se pueden utilizar para distinguir entre diferentes tipos de dispositivos (por ejemplo, llaveros de seguridad frente a dispositivos electrónicos 106). La distinción entre diferentes tipos de llaveros (por ejemplo, llaveros de gerente frente a llaveros de usuario) también se puede comunicar digitalmente como parte de un mensaje de UID. Después de detectar el llavero de seguridad conectado, la circuitería de seguridad 104 puede proporcionar potencia de funcionamiento al llavero de seguridad a través de la conexión. En este punto, la circuitería de seguridad recibe información sobre el llavero de seguridad conectado a través de la conexión (etapa 404). Por ejemplo, esta información del llavero puede incluir el identificador 212 de llavero del llavero de seguridad conectado y/o cualquier otra información sobre el llavero de seguridad conectado que se necesite como parte del proceso de gestión/autenticación. Si el llavero de seguridad proporciona esta información en un formato cifrado para mejorar la seguridad, se debe comprender que la etapa 404 puede incluir una operación correspondiente de descifrado.

En la etapa 406, el procesador 350 determina si el llavero de seguridad conectado es un llavero de seguridad de gerente 108. Esta determinación se puede realizar basándose en la información del llavero recibida en la etapa 404. Tal como se mencionó anteriormente, esta determinación se puede realizar de varias maneras. Por ejemplo, la memoria 352 puede almacenar el identificador o los identificadores de llavero de todos los llaveros de seguridad de gerente 108. A continuación, en la etapa 408, el procesador puede comparar el identificador 212 del llavero recibido en la etapa 404 con el identificador o los identificadores de llavero conocidos para el llavero o los llaveros de seguridad de gerente 108. Si hay una coincidencia, entonces la etapa 406 puede resultar en una determinación de que el llavero de seguridad conectado es un llavero de seguridad de gerente 108. Como ejemplo adicional, el procesador 350 puede verificar si un bit de indicador de gerente o similar está establecido en el interior del llavero de seguridad conectado (este valor de bit puede ser comunicado al procesador 350 como parte de la información del llavero recibida en la etapa 404). Como un ejemplo adicional más, se puede detectar otra codificación cableada utilizada por el llavero de seguridad conectado, tal como resistencias de configuración, a través de la conexión entre 200 y 320 para identificar el llavero conectado como un llavero de seguridad de gerente 108. Si el llavero conectado es un llavero de seguridad de gerente 108, entonces el flujo del proceso puede continuar a la etapa 408, donde el programa 356 entra en un modo de gestión del llavero. Si el llavero conectado no es un llavero de seguridad de

gerente, entonces el flujo del proceso puede continuar a la etapa 430, donde el programa 356 entra en un modo de autenticación.

Cuando el flujo del proceso entra en el modo de gestión del llavero, el procesador 350 inicia un temporizador (etapa 408). Este temporizador define una primera ventana de tiempo durante la cual se debe eliminar el llavero de gerente 108 conectado, con el fin de permitir la agregación de un nuevo llavero de seguridad 110 a la lista de autorizaciones 358. En la etapa 410, el procesador detecta si el llavero de seguridad de gerente 108 conectado ha sido desconectado antes de que expire la primera ventana de tiempo. De lo contrario, el flujo del proceso puede terminar. Si es así, el flujo del proceso puede continuar a la etapa 412. La primera ventana de tiempo puede tener cualquier duración que un profesional considere adecuada para los fines del proceso de gestión de llaveros utilizado Por ejemplo, se podría utilizar una duración que se encuentre en un intervalo comprendido entre aproximadamente 5 segundos y aproximadamente 30 segundos (por ejemplo, una ventana de tiempo de 10 segundos). Como ejemplo, para conexiones físicas, se puede realizar una desconexión eliminando el llavero de gerente 108 de la interfaz 320. Como ejemplo adicional, para conexiones inalámbricas, se puede realizar una desconexión desplazando el llavero del gerente 108 fuera del alcance de la conexión inalámbrica de la interfaz 320.

En la etapa 412, el procesador 350 inicia de nuevo un temporizador. Este temporizador define una segunda ventana de tiempo durante la cual deben ocurrir uno o varios eventos definidos con uno o varios llaveros para conseguir una tarea de gestión deseada. La duración de esta segunda ventana de tiempo puede ser la misma duración que la primera ventana de tiempo si así lo desea un profesional (por ejemplo, 10 segundos), aunque este no tiene por qué ser el caso.

En este punto, el flujo del proceso espera una nueva conexión de un llavero de seguridad con la interfaz 320. En la etapa 414, el procesador determina si se ha realizado una conexión con un llavero de seguridad antes de que expire la segunda ventana de tiempo. La detección de un llavero conectado se puede realizar tal como se ha descrito anteriormente en relación con la etapa 400. Tras la detección de dicha conexión, el procesador 350 puede determinar si la segunda ventana de tiempo ha expirado. Si la conexión se produjo después de la expiración de la segunda ventana de tiempo, el flujo del proceso puede terminar. De lo contrario, el flujo del proceso puede continuar a la etapa 416, donde se proporciona potencia de funcionamiento al llavero de seguridad conectado (véase la etapa 402 anterior). A continuación, en la etapa 418, se recibe información del llavero desde el llavero de seguridad conectado, como en la etapa 404, y en la etapa 420 se determina si el llavero conectado es un llavero de seguridad de gerente 108 como en la etapa 406.

Si el llavero de seguridad conectado en la etapa 414 antes de la expiración de la segunda ventana de tiempo no es un llavero de seguridad de gerente, el procesador agrega este llavero de seguridad a la lista de autorizaciones en la etapa 422. Para hacerlo, el procesador puede escribir el identificador 212 del llavero recibido en la etapa 418 desde el llavero de seguridad 110 conectado a la lista de autorizaciones 358. A continuación, el procesador 350 puede enviar una notificación de acuse de recibo al llavero de seguridad 110 conectado a través de la interfaz 320 que sirve como mensaje para informar al llavero 110 conectado de que ha sido añadido con éxito a la lista de autorizaciones 358.

Si el llavero de seguridad conectado en la etapa 414 antes de la expiración de la segunda ventana de tiempo es un llavero de seguridad de gerente, el procesador elimina la lista de autorizaciones 358 en la etapa 426. Para hacerlo, el procesador puede eliminar todos los identificadores 212 de llavero que puedan estar presentes en la lista 358. A continuación, el procesador 350 puede enviar una notificación de acuse de recibo al llavero de gerente 108 conectado a través de la interfaz 320 que sirve como un mensaje para informar al llavero conectado 108 de que ha sido eliminado con éxito la lista de autorizaciones 358.

En consecuencia, se debe comprender que las etapas 400 a 428 definen dos secuencias para diferentes modos de gestión de llaveros después de una eliminación inicial de un llavero de seguridad de gerente 108. Para autorizar un nuevo llavero de seguridad 110, un gerente puede conectar el llavero de seguridad 110 que debe ser autorizado a la interfaz 320 durante ventana de tiempo definida después de la eliminación inicial del llavero de gerente 108. Esto corresponde aproximadamente a una secuencia de conexión y desconexión de un llavero de gerente 108, seguida de la conexión de un llavero de seguridad 110 que se debe agregar a la lista de autorizaciones 358 dentro de una ventana de tiempo definida después de la desconexión del llavero de gerente 108. Para desautorizar todos los llaveros de seguridad 110 actualmente autorizados, un gerente puede volver a conectar el llavero de gerente 108 durante un período de tiempo definido después de la retirada inicial del llavero de gerente 108. Esto corresponde aproximadamente a una secuencia de conexión y desconexión de un llavero de gerente 108 seguida de una reconexión del llavero de gerente 108 dentro de una ventana de tiempo definida después de la desconexión inicial del llavero de gerente 108 (y sin interconexión intermedia con un llavero de seguridad 110).

Aunque la figura 4 muestra un ejemplo de dos secuencias para dos tareas de gestión de llavero, se debe comprender que se podrían emplear diferentes secuencias y/o tareas de gestión de llavero adicionales. Por ejemplo, una tercera tarea de gestión de llaveros podría ser una desautorización de un llavero de seguridad 110 específico en lugar de la desautorización de todos los llaveros de seguridad 110. Dicha tarea de gestión de llaveros puede ser útil en un planteamiento en el que el gerente tiene posesión del llavero de seguridad 110 autorizado que va a ser

desautorizado. Para habilitar dicha tercera tarea de gestión, el flujo del proceso de gestión puede codificar una secuencia adicional, por ejemplo, haciendo que la tarea de gestión “eliminar todo” se active mediante una secuencia de conexión triple del llavero de seguridad de gerente 108, cuando una secuencia de conexión/desconexión del llavero del gerente 108 es seguida por otra secuencia de conexión/desconexión para el llavero del gerente 108 (dentro de una ventana de tiempo definida sin una conexión intermedia de un llavero de seguridad 110) y seguida a continuación por otra reconexión del llavero del gerente 108 durante una ventana de tiempo definida. Dicho patrón podría desencadenar la eliminación de la lista de autorizaciones 358. A continuación, la secuencia de doble conexión del llavero de seguridad del gerente 108 se puede utilizar para activar una opción para que un gerente solo desautorice un llavero de seguridad 110 específico conectando ese llavero de seguridad 110 específico dentro de una ventana definida después de la desconexión del llavero del gerente 108. Esta secuencia de desautorización específica sería, por lo tanto, una secuencia de conexión/desconexión del llavero del gerente 108, seguida de otra secuencia de conexión/desconexión del llavero del gerente 108 (dentro de una ventana de tiempo definida sin una conexión intermedia de un llavero de seguridad 110) y seguida, a continuación, de una conexión durante una ventana de tiempo definida del llavero de seguridad 110 específico a desautorizar.

Cuando el flujo del proceso entra en el modo de autenticación de llavero en la etapa 430, el procesador 352 compara el identificador 212 del llavero recibido en la etapa 404 con los identificadores de llavero de la lista de autorizaciones 358 (etapa 432). Si el identificador 212 del llavero recibido coincide con cualquiera de los identificadores de llavero en la lista de autorizaciones 358 tal como se determina en la etapa 434, el procesador 350 puede concluir que el llavero de seguridad 110 conectado está autorizado y continúa a la etapa 436. Si el identificador 212 del llavero recibido no coincide con ninguno de los identificadores de llavero en la lista de autorizaciones 358 tal como se determina en la etapa 434, el procesador 350 puede concluir que el llavero de seguridad 110 conectado no está autorizado, y continúa a la etapa 440.

En la etapa 436, el procesador 350 permite que el llavero de seguridad 110 conectado y autenticado ajuste el estado de seguridad de la circuitería de seguridad 104. Por ejemplo, si el llavero de seguridad 110 está diseñado para alternar la circuitería de seguridad 104 entre un estado activado y un estado desactivado después de la autenticación, el procesador 350 puede alternar, en consecuencia, el estado de seguridad de la circuitería de seguridad 104 en la etapa 436. Si el llavero de seguridad 110 está diseñado para proporcionar capas adicionales de control (por ejemplo, una función de seguridad definida por el usuario, tal como un comando de activación, un comando de desactivación y/o un comando de eliminar alarma que podría ser definido en respuesta a la entrada del usuario a través de un botón del llavero de seguridad 110), la etapa 436 puede implementar un comando definido recibido del llavero de seguridad 110 conectado a través de la interfaz 320.

A continuación, el procesador 350 puede enviar una notificación de acuse de recibo al llavero de seguridad 110 conectado a través de la interfaz 320 que sirve como un mensaje para informar al llavero 110 conectado de que el estado de seguridad de la circuitería de seguridad ha sido controlado con éxito (etapa 438).

En la etapa 440, el procesador 450 rechaza el llavero de seguridad conectado por fallo de autenticación. Esto puede ser seguido por la etapa 442, donde el procesador 350 envía una notificación de acuse de recibo al llavero de seguridad 110 conectado a través de la interfaz 320 que sirve como mensaje para informar al llavero 110 conectado de que no ha sido autenticado.

En consecuencia, se puede ver que el flujo del proceso de la figura 4 proporciona a los gerentes de tienda una técnica eficaz y fácil de utilizar para definir qué llaveros de seguridad 110 están autorizados y qué llaveros de seguridad no están autorizados para controlar las funciones de seguridad de un conjunto 100 de exposición de producto determinado.

Se debe comprender que la figura 4 es simplemente un ejemplo de un flujo de proceso para ejecución en conexión con el programa de software 356, y un profesional puede emplear flujos de proceso alternativos. Por ejemplo, un profesional puede optar por omitir una o varias de las etapas relacionadas con los mensajes de notificación de acuse de recibo si lo desea. Asimismo, en lugar de finalizar el flujo del proceso después de la realización de las etapas 422 y 424, el flujo del proceso también podría ser aumentado para permitir que un gerente agregue otro llavero de seguridad 110 a la lista de autorizaciones mientras el flujo del proceso está en el modo de “gestión de llavero”. Por ejemplo, después de realizar la etapa 422 y/o 424, el procesador podría reiniciar el temporizador para dar tiempo a que un gerente conecte otro llavero de seguridad 110 que se va a agregar a la lista de autorizaciones 158. Este reinicio del temporizador se puede repetir a medida que los llaveros de seguridad 110 adicionales son conectados y agregados a la lista de autorizaciones 358.

La figura 5 representa un flujo de proceso de ejemplo para el programa de software 250, para que lo ejecute el procesador 202 de un llavero de seguridad 108/110 para facilitar las tareas de gestión/autenticación tal como se describe en el presente documento. El flujo del proceso de la figura 5 comienza cuando el llavero de seguridad 108/110 interactúa con un conjunto de disco 302 a través de las interfaces 200 y 320. Si existe una conexión entre las interfaces 200 y 320, el llavero de seguridad 108/110 recibe potencia de funcionamiento del conjunto de disco 302 a través de la conexión (etapa 502). Por ejemplo, en una instancia de ejemplo de una conexión física, el llavero de seguridad 108/110 puede extraer corriente del conjunto de disco 302 a través de la conexión física. Utilizando

dicha potencia de funcionamiento, el procesador 202 puede activar y ejecutar el programa de software 250. El llavero de seguridad 108/110 también puede ser diseñado para tener suficiente capacitancia en el mismo para permitir que permanezca encendido durante un estado de suspensión durante un período de tiempo deseado (por ejemplo, aproximadamente 2 segundos).

Después de encenderse y comenzar la ejecución del programa 250, el procesador lee el identificador 212 del llavero de la memoria 204 (etapa 504). En la etapa 506, el procesador comunica este identificador 212 de llavero (y cualquier otra información deseada) al conjunto de disco 302 a través de la conexión entre el conjunto de disco 302 y el llavero de seguridad 108/110 (por ejemplo, a través de la conexión entre las interfaces 200 y 320). Para mejorar aún más la seguridad del sistema, la comunicación en la etapa 506 puede ser una comunicación cifrada, y esta comunicación cifrada emplea un cifrado variable en el tiempo. Por ejemplo, el procesador 202 puede emplear una técnica de cifrado tal como un protocolo en serie I^2C cifrado para la comunicación entre el llavero de seguridad 108/110 y el conjunto de disco 302 en la etapa 516. Además, para un profesional que puede operar múltiples tiendas, se puede utilizar un cifrado diferente para diferentes ubicaciones de tiendas (por ejemplo, diferentes claves de cifrado, diferentes modos de cifrado (por ejemplo, libro de códigos electrónicos (ECB, Electronic Code Book), encadenamiento de bloques cifrados (CBC, Cipher Block Chaining), etc.) y/o diferentes tipos de cifrado (por ejemplo, AES, Triple DES, etc.).

En la etapa 508, el procesador 202 espera recibir un mensaje de notificación de acuse de recibo del disco. Después de recibir e interpretar dicho mensaje, el procesador puede encender una o varias luces 208 basándose en el mensaje para notificar al gerente o a otro usuario si se realizó una tarea deseada (etapa 510). Por ejemplo, se pueden utilizar diversos esquemas de codificación de la luz para comunicar la finalización de diferentes tareas (tal como encendiéndose una primera luz de color si el llavero 110 en cuestión fue autenticado con éxito, encendiéndose una segunda luz de color si el llavero 110 en cuestión fue agregado con éxito a la lista de autorizaciones, etc.).

La figura 6 muestra cómo se puede gestionar la lista de autorizaciones 358 para controlar qué llaveros de seguridad 110 están autorizados (o desautorizados) con respecto al control del estado de seguridad de un conjunto 100 de exposición de producto. La figura 6 muestra un ejemplo de lista de autorizaciones 358 que identifica los UID de llavero para un número de llaveros de seguridad 110 autorizados. Mediante de la ejecución del programa 356 en combinación con las conexiones/desconexiones secuenciadas del llavero de seguridad del gerente 108 y del llavero de seguridad del usuario 110, el procesador 350 puede agregar el UID de llavero de un llavero de seguridad determinado a la lista de autorizaciones 358. A modo de ejemplo, la figura 6 muestra una etapa 600, en la que el flujo del proceso de la figura 4 se utiliza para agregar el llavero i a la lista de autorizaciones 358 (donde la lista de autorizaciones 358 actualizada se muestra por debajo de la etapa 600). Una vez que el UID 212 de llavero para el llavero i ha sido agregado a la lista de autorizaciones 358, ese llavero i se puede utilizar para controlar el estado de seguridad del conjunto 100 de exposición del producto en cuestión.

La figura 7 da a conocer otro ejemplo de realización de un llavero de seguridad 108/110, que se puede denominar una “Llave I” para introducir en un conjunto de disco 302. Tal como se indicó anteriormente, el conjunto de disco 302 puede alimentar la Llave I; por ejemplo, proporcionar tensión de +5VCC.

La Llave I de la figura 7 incluye un procesador en forma de microcontrolador (“U1”) que se activa y se comunica con el conjunto de disco 302 utilizando paquetes de datos/reloj I^2C. Estos paquetes pueden ser cifrados para que cada transacción de datos en serie nunca sea la misma en el bus I^2C.

La Llave I también contiene varios LED de estado (D1 a D4) que proporcionan indicadores rojo/verde controlados por el microcontrolador U1.

La figura 7 muestra, asimismo, la utilización de una resistencia de configuración que puede ser utilizada para configurar la Llave I como una “Llave principal” (por ejemplo, el llavero de gerente 108) o una “Llave de usuario” (por ejemplo, el llavero de seguridad de usuario 110) utilizando técnicas de relleno de resistencias. La resistencia de configuración puede ser una resistencia situada en el llavero 108/110 entre dos de los pines en la interfaz 200 (por ejemplo, un conector USB).

Tal como se indicó anteriormente, la comunicación entre la Llave I y el conjunto de disco 302 utiliza el protocolo I^2C, con el conjunto de disco como principal y la Llave I como secundaria.

Cada Llave I recibe un identificador numérico único por parte del proveedor (que puede servir como el UID 212 del llavero). Cuando la Llave I es introducida en el conjunto de disco 302, en ese momento, el conjunto de disco 302 inicia una transferencia de datos cifrados. La Llave I responde al disco con un paquete de datos cifrados que contiene su identificador numérico y un código que indica si es una Llave de usuario o una Llave de gerente.

Cuando se introduce una llave de gerente en el conjunto de disco 302, el conjunto de disco 302 inicia una sesión de programación y pone en marcha un temporizador de 10 segundos. Si se retira la Llave I antes de que expire el temporizador, el disco entrará en el modo “Agregar llave”. Cuando se retira la Llave I, el temporizador se restablece y cualquier llave de usuario introducida, antes de que expire el temporizador, se agregará a la memoria no volátil del

conjunto de disco como una llave de usuario válida. El temporizador se restablece cada vez que se introduce y retira una llave de usuario. Finalmente, el modo “Añadir llave” finaliza cuando el temporizador expira o se introduce de nuevo la llave del gerente. Si se vuelve a introducir la llave del gerente antes de que expire el temporizador, el conjunto de disco entrará en el modo “Eliminar llave” y todas las llaves de usuario almacenadas se eliminarán de la memoria del conjunto de disco.

Durante el funcionamiento, cuando la llave del usuario es introducida en el conjunto de disco, el conjunto de disco compara el identificador numérico transmitido por la llave del usuario con los identificadores en la memoria no volátil del conjunto de disco, para verificar que la llave del usuario es una llave válida. Si la identificación de la llave de usuario coincide con uno de los identificadores en la lista de llaves válidas del conjunto de disco, se permiten todas las funciones normales de las llaves (activar, desactivar, eliminar alarma). De lo contrario, si no hay coincidencia, la llave de usuario es ignorada.

En la figura 8 se muestra un esquema más detallado de la Llave I de la figura 7. Por ejemplo, la realización de ejemplo de la figura 8 muestra ejemplos de circuitería para el llavero 108/110 que se pueden utilizar para integrar el procesador/memoria 202/204 con la interfaz 200 y las luces 208.

Las figuras 9 y 10 y 12 a 14 muestran ejemplos de circuitería de seguridad 104. La figura 9 muestra una descripción general de la circuitería de seguridad 104. La figura 10 muestra una unidad de procesamiento local que puede ser incluida con la circuitería de seguridad 104, donde la unidad de procesamiento local se puede programar para recibir un identificador 112 de llavero (a través de la interfaz que se muestra en la figura 11) y autenticarlo utilizando la lista de autorizaciones. Tras la verificación del identificador del llavero, la unidad de procesamiento local puede controlar diversas funciones de seguridad, tales como un controlador de alarmas (véase la figura 12), un controlador/sensor de bloqueo (véase la figura 13) y/o una interfaz LED (véase la figura 14).

Se debe comprender que los profesionales pueden emplear otras variaciones con respecto a las realizaciones de ejemplo anteriores. Por ejemplo, mientras que las realizaciones de ejemplo explicadas anteriormente describen los procedimientos relacionados con el flujo del proceso de la figura 4 realizados por el conjunto de disco 302 en respuesta a la conexión de un llavero 108/110 a una interfaz 320 residente en el conjunto de disco 302, se debe comprender que se pueden emplear otras variaciones. Por ejemplo, se puede implementar un procesador o la circuitería correspondiente en el conjunto de la base 304 para realizar el flujo del proceso de la figura 4. Asimismo, la interfaz 320 puede residir en el conjunto de la base 304 en lugar de en el conjunto de disco 302 si así lo desea un profesional. En la medida en que sería necesario comunicar el estado de seguridad a los componentes en el conjunto de disco 302, dichas comunicaciones se podrían conseguir por medio de la conexión entre el conjunto de disco 302 y el conjunto de la base 304 cuando el conjunto de disco 302 está en reposo, o se podrían conseguir por medio de comunicación inalámbrica entre el conjunto de disco 302 y el conjunto de la base 304.

Como ejemplo adicional de una realización alternativa, el flujo del proceso de la figura 4 se podría implementar, al menos en parte, mediante un sistema informático remoto de los llaveros 108/110 y el conjunto 100 de exposición de producto. Por ejemplo, las etapas 400 a 428 pueden ser realizadas por el sistema informático remoto para gestionar la lista de autorizaciones 358. Las etapas 400 a 406 y 430 a 442 podrían ser realizadas por el conjunto 100 de exposición de producto después de que la lista de autorizaciones 358 haya sido transferida a la memoria dentro del conjunto 100 de exposición de producto. Además, la autenticación de un llavero también podría ser realizada por el sistema informático si lo desea un profesional. Por ejemplo, mientras que las técnicas de gestión de la lista de autorizaciones pueden ser realizadas por el sistema informático utilizando el flujo del proceso de las etapas 400 a 428 descritas anteriormente, el proceso de autenticación podría ser realizado por el sistema informático utilizando las técnicas descritas en la Patente Provisional US62/323,511, presentada el 15 de abril de 2016 y titulada “Alarm Key System for Retail Security Display” y en la Patente US, presentada este mismo día y titulada “Gateway-Based Anti-Theft Security System and Method” (identificada dicha solicitud de patente por el abogado de Thompson Coburn, número de expediente 60977-1 64207).

Como ejemplo adicional de una realización alternativa, los llaveros de seguridad 108/110 pueden adoptar la forma de placas o tarjetas que incluyen un chip de RFID u otras señales detectables. La interfaz 320 podría, por lo tanto, adoptar la forma de un lector de RFID que emite un campo en un intervalo corto. El chip de RFID se puede activar cuando está cerca del lector de RFID, y la activación del chip de RFID a través del campo del lector de RFID puede hacer que el chip emita su identificador. Con un sistema de este tipo, el llavero del gerente 108 puede ser acercado al lector de RFID para iniciar el temporizador, seguido de acercar el llavero de seguridad 110 a incluir en la lista blanca junto al lector de RFID antes de que expire el temporizador. En otras realizaciones alternativas adicionales, los llaveros de seguridad 108/110 pueden adoptar la forma de dispositivos informáticos inalámbricos, tales como teléfonos inteligentes o tabletas, y ser utilizados de manera similar. Además, una aplicación móvil ejecutada por el dispositivo informático inalámbrico puede proporcionar capas adicionales de control sobre la inclusión en la lista blanca de nuevos llaveros.

Además, con respecto a cualquiera de las realizaciones anteriores, se pueden utilizar sistemas de seguridad antirrobo alternativos en lugar del conjunto 100 de exposición de producto o junto con el mismo. Por ejemplo, los sistemas de seguridad antirrobo pueden incluir armarios, cajas, recipientes y/o contenedores que están protegidos

del acceso libre por medio de cerraduras y similares. Como ejemplo, la circuitería de seguridad 104 explicada en el presente documento podría estar incorporada en dichos armarios, cajas, recipientes y/o contenedores (por ejemplo, implementada en las cerraduras que regulan el acceso a los armarios, cajas, recipientes y/o contenedores).

Si bien la invención se ha descrito anteriormente en relación con sus realizaciones de ejemplo, se pueden realizar diversas modificaciones que aún se encuentran dentro del alcance de la invención. Dichas modificaciones a la invención serán reconocibles tras la revisión de las explicaciones del presente documento.

REIVINDICACIONES

1. Sistema, que comprende:

un conjunto (100) de exposición de producto, adaptado para recibir un producto (106) para exponerlo a un consumidor;
en el que el conjunto (100) de exposición de producto comprende una interfaz (320) y una circuitería de seguridad (104);
en el que la circuitería de seguridad (104) está configurada para controlar un estado de seguridad para el conjunto (100) de exposición de producto basándose en una autenticación de un llavero de seguridad, incluyendo la circuitería de seguridad (104) un procesador (350) y una memoria (352);
en el que la memoria (352) está configurada para almacenar una lista de autorizaciones (358), en la que la lista de autorizaciones (358) está configurada para identificar uno o varios identificadores para uno o varios llaveros de seguridad que están autorizados para controlar el estado de seguridad del conjunto (100) de exposición de producto;
en el que el procesador (350) está configurado para agregar un identificador (212) para un primer llavero de seguridad (110) a la lista de autorizaciones (358), en respuesta a una secuencia definida de interacciones (118) por parte del primer llavero de seguridad (110), y un segundo llavero de seguridad (108) con la interfaz (320).

2. Sistema, según la reivindicación 1, en el que la secuencia definida de interacciones (118) comprende una conexión del segundo llavero de seguridad (108) con la interfaz (320), seguida de una desconexión del segundo llavero de seguridad (108) con la interfaz (320), seguida de una conexión del primer llavero de seguridad (110) con la interfaz (320) dentro de una ventana de tiempo definida.

3. Sistema, según la reivindicación 2, en el que la conexión del primer llavero de seguridad (110) con la interfaz (320) dentro de la ventana de tiempo definida se produce sin la intervención de la reconexión del segundo llavero de seguridad (108).

4. Sistema, según cualquiera de las reivindicaciones 2 y 3, en el que el primer llavero de seguridad (110) corresponde a un llavero de seguridad de usuario que se va a autorizar para su utilización en el control del estado de seguridad del conjunto (100) de exposición de producto, y en el que el segundo llavero de seguridad (108) corresponde a un llavero de seguridad del gerente.

5. Sistema, según cualquiera de las reivindicaciones 2 a 4, en el que la circuitería de seguridad (104) está configurada, además, para (1) leer un identificador de llavero de un llavero de seguridad conectado a la interfaz (320), y (2) autenticar un llavero de seguridad conectado a la interfaz (320) basándose en el identificador de lectura en comparación con uno o varios identificadores en la lista de autorizaciones (358).

6. Sistema, según cualquiera de las reivindicaciones 2 a 5, en el que la memoria (352) está configurada, además, para almacenar un programa de software (356) para que lo ejecute el procesador (350) en respuesta a una conexión de un llavero de seguridad con la interfaz (320), en el que el programa de software (356) comprende una pluralidad de instrucciones ejecutables por el procesador que, al ser ejecutadas por el procesador (350), están configuradas para hacer que el procesador (350):

determine si el llavero de seguridad conectado corresponde al segundo llavero de seguridad (108); y
en respuesta a una determinación de que el llavero de seguridad conectado corresponde al segundo llavero de seguridad (108), (1) iniciar un temporizador que define la ventana de tiempo, (2) determinar si el primer llavero de seguridad (110) se ha conectado con la interfaz (320) antes de la expiración de la ventana de tiempo definida, y (3), en respuesta a una determinación de que el primer llavero de seguridad (110) se ha conectado con la interfaz (320) antes de la expiración de la ventana de tiempo definida, agregar un identificador (212) para el primer llavero de seguridad (110) a la lista de autorizaciones (358).

7. Sistema, según la reivindicación 6, en el que el programa de software (356) comprende, además, una pluralidad de instrucciones ejecutables por un procesador que, al ser ejecutadas por el procesador (350), están configuradas para hacer que el procesador (350):
reciba un identificador (212) para el primer llavero de seguridad (110) a través de la conexión, en respuesta a la conexión del primer llavero de seguridad (110) a la interfaz (320).

8. Sistema, según cualquiera de las reivindicaciones 6 y 7, en el que el programa de software (356) comprende, además, una pluralidad de instrucciones ejecutables por un procesador que, al ser ejecutadas por el procesador (350), están configuradas para hacer que el procesador (350):

reciba un identificador para el llavero de seguridad conectado a través de la interfaz (320); y
en respuesta a una determinación de que el llavero de seguridad conectado no corresponde al segundo llavero de seguridad (108), (1) comparar el identificador recibido con la lista de autorizaciones (358), y (2), en respuesta a la comparación que resulta en una determinación de que el identificador recibido coincide con un identificador (212) de

la lista de autorizaciones (358), permitir que el llavero de seguridad conectado controle el estado de seguridad para el conjunto (100) de exposición de producto.

9. Sistema, según cualquiera de las reivindicaciones 6 a 8, en el que el programa de software (356) comprende, además, una pluralidad de instrucciones ejecutables por el procesador que, al ser ejecutadas por el procesador (350), están configuradas para hacer que el procesador (350):
en respuesta a una determinación de que el llavero de seguridad conectado corresponde al segundo llavero de seguridad (108), (1) determine si el segundo llavero de seguridad (108) se ha vuelto a conectar con la interfaz (320) antes de que expire la ventana de tiempo definida, y (2), en respuesta a una determinación de que el segundo llavero de seguridad (108) ha sido reconectado con la interfaz (320) antes de la expiración de la ventana de tiempo definida, elimine uno o varios identificadores (212) de la lista de autorizaciones (358).

10. Sistema, según cualquiera de las reivindicaciones anteriores, en el que el procesador (350) está configurado, además, para desautorizar uno o varios llaveros de seguridad incluidos en la lista de autorizaciones (358), en respuesta a otra secuencia definida de interacciones.

11. Sistema, según cualquiera de las reivindicaciones anteriores, en el que el procesador (350) está configurado, además, para eliminar la lista de autorizaciones (358) en respuesta a una secuencia definida de interacciones del segundo llavero de seguridad (108) con la interfaz (320).

12. Sistema, según la reivindicación 11, en el que la secuencia definida de interacciones del segundo llavero de seguridad (108) con la interfaz (320) para eliminar la lista de autorizaciones (358) comprende una conexión del segundo llavero de seguridad (108) con la interfaz (320), seguida de una desconexión del segundo llavero de seguridad (108) con la interfaz (320), seguida de una reconexión del segundo llavero de seguridad (108) con la interfaz (320) dentro de una ventana definida después de la desconexión del primer llavero de seguridad (110) de la interfaz (320).

13. Sistema, según cualquiera de las reivindicaciones anteriores, que comprende, además:

el primer llavero de seguridad (110); y
el segundo llavero de seguridad (108);
en el que la interfaz (320) del conjunto de exposición de producto comprende un conector;
en el que cada uno del primer y segundo llaveros de seguridad (110, 108) comprende:
un conector (200), adaptado para conectarse de manera desmontable con el conector del conjunto de exposición de producto;
una memoria (204), configurada para almacenar un identificador (212) para ese llavero de seguridad; y
un procesador (202), configurado para, en respuesta a una conexión entre el conector (200) del llavero de seguridad y el conector del conjunto de exposición de producto, (1) leer el identificador (212) del llavero de la memoria (204) y (2) generar datos representativos del identificador (212) del llavero leído a través del conector (200) del llavero de seguridad; y

en el que cada uno del primer y segundo llaveros de seguridad (108), (110) es un llavero de seguridad pasivo que recibe potencia de funcionamiento del conjunto (100) de exposición de producto después de una conexión con el conjunto (100) de exposición de producto.

14. Sistema, según cualquiera de las reivindicaciones anteriores, en el que el conjunto (100) de exposición de producto comprende:

un conjunto de disco (302) adaptado para recibir un dispositivo electrónico (106); y
un conjunto de base (304);
en el que el conjunto de disco (302) está adaptado para ser movido entre (1) una posición de reposo, en la que el conjunto de disco (302) se acopla con el conjunto de la base (304) y (2) una posición levantada, en la que el conjunto de disco (302) se desconecta del conjunto de la base (304);
en el que el conjunto de disco (302) comprende (1) un contacto eléctrico del conjunto de disco, (2) circuitería del conjunto de disco conectada al contacto eléctrico del conjunto de disco, en el que la circuitería del conjunto de disco incluye la circuitería de seguridad (104), (3) un sensor de seguridad (102), y (4) otra interfaz, conectada a la circuitería del conjunto de disco, la otra interfaz adaptada para la conexión con un cable de alimentación (312) que se puede conectar a una entrada de alimentación del dispositivo electrónico (106);
en el que el contacto del conjunto de la base y el contacto del conjunto de disco están adaptados para hacer contacto entre sí cuando el conjunto de disco (302) está en la posición de reposo, para formar una conexión eléctrica entre la circuitería del conjunto de disco y la circuitería del conjunto de la base a través del cual se proporciona potencia al conjunto de disco (302);
en el que la circuitería del conjunto de disco está configurada para, cuando el conjunto de disco (302) está en la posición de reposo, extraer potencia de la fuente de alimentación a través de la conexión eléctrica y proporcionar la energía extraída a la otra interfaz para cargar el dispositivo electrónico (106) a través del cable de alimentación (312); y

en el que el contacto del conjunto de la base y el contacto del conjunto de disco están adaptados para perder contacto entre sí cuando el conjunto de disco (302) está en la posición levantada, para romper, de este modo, la conexión eléctrica.

15. Procedimiento, que comprende:

conectar un primer llavero de seguridad (108) con una interfaz (320), la interfaz (320) para colaborar con un procesador (350) que gestiona una lista de autorizaciones (358) para un conjunto (100) de exposición de producto adaptado para recibir un producto (106) para mostrar a un consumidor, la lista de autorizaciones (358) para listar uno o varios identificadores para uno o varios llaveros de seguridad que están autorizados para controlar un estado de seguridad para el conjunto (100) de exposición de producto;
desconectar el primer llavero de seguridad (108) de la interfaz (320);
en respuesta a la conexión o desconexión, iniciar un temporizador, definiendo el temporizador una ventana de tiempo;
conectar un segundo llavero de seguridad (110) con la interfaz (320);
lectura, por parte del procesador (350), de un identificador (212) para el segundo llavero de seguridad (110) conectado a través de la interfaz (320);
determinación, por parte del procesador (350), de que la conexión del segundo llavero de seguridad (110) se produjo antes de la expiración de la ventana de tiempo definida; y
en respuesta a la determinación de que la conexión del segundo llavero de seguridad (110) ocurrió antes de la expiración de la ventana de tiempo definida, el procesador (350) agrega el identificador (212) leído a la lista de autorizaciones (358) para autorizar, de este modo, la utilización del segundo llavero de seguridad (110) en el control del estado de seguridad del conjunto (100) de exposición de producto.

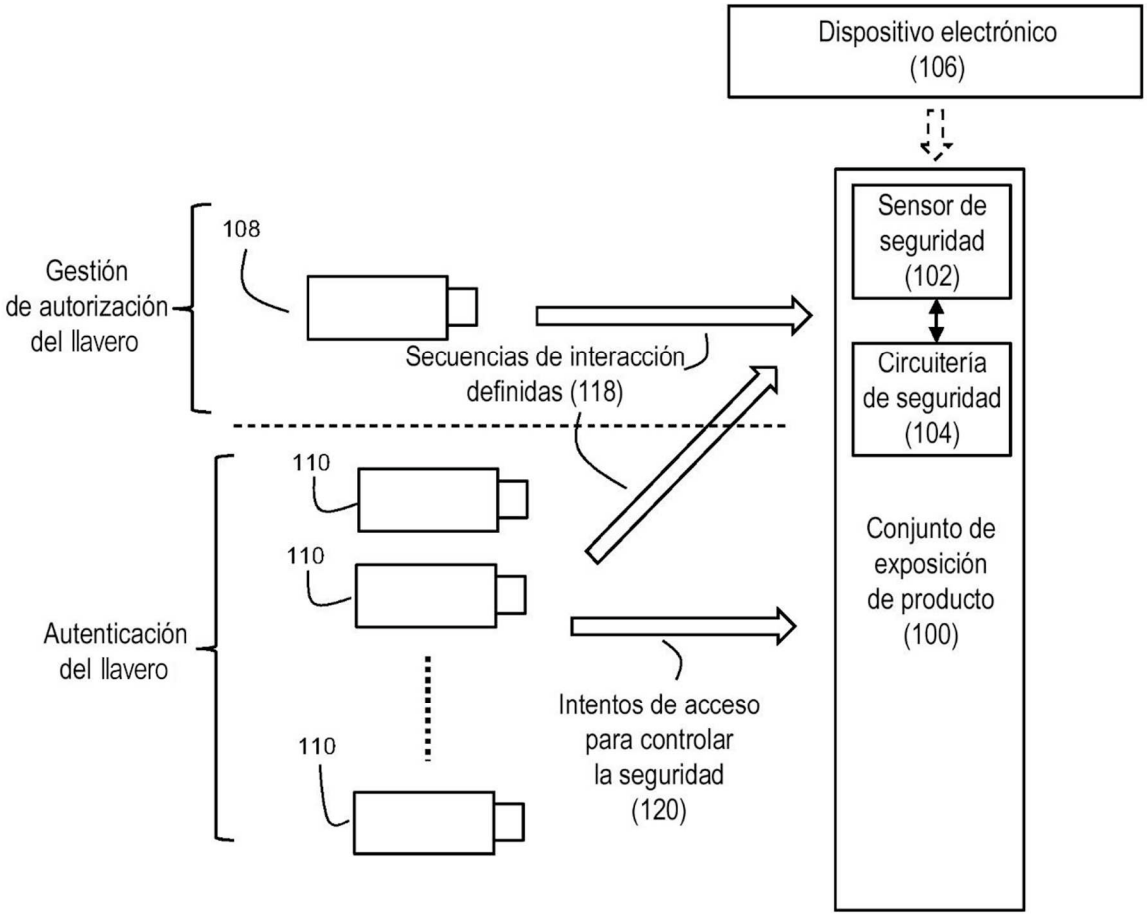
Dispositivo electrónico
(106)
Sensor de seguridad
(102)
Circuitería de seguridad
(104)
Conjunto de exposición de producto
(100)
Gestión de autorización del llavero
108
Secuencias de interacción definidas (118)
Autenticación del llavero
110
110
110
Intentos de acceso para controlar la seguridad
(120)

Figura 1

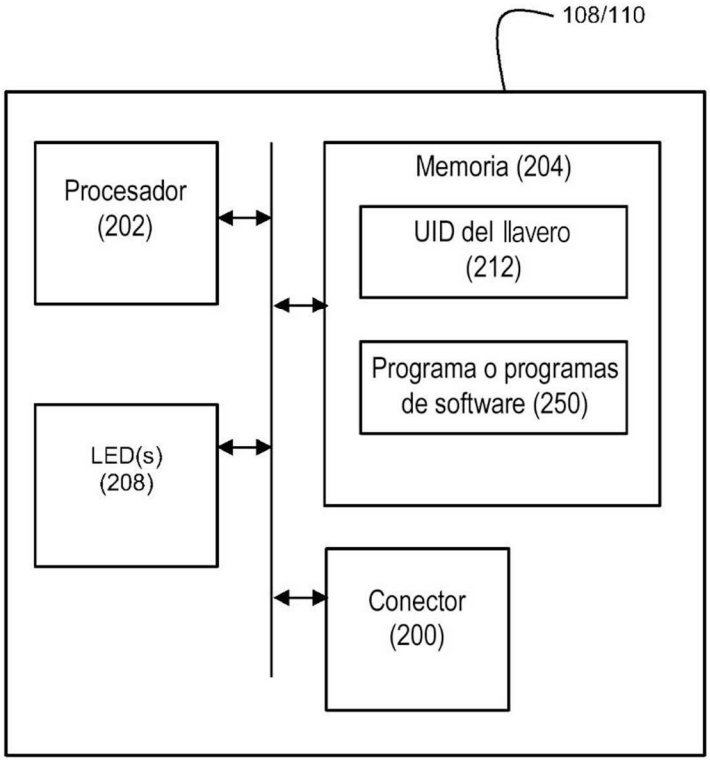

Figura 2

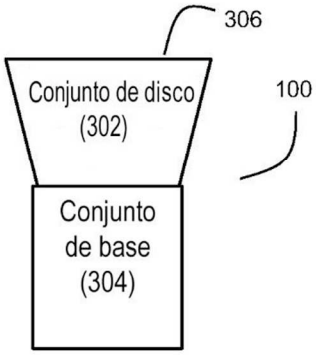

Figura 3A

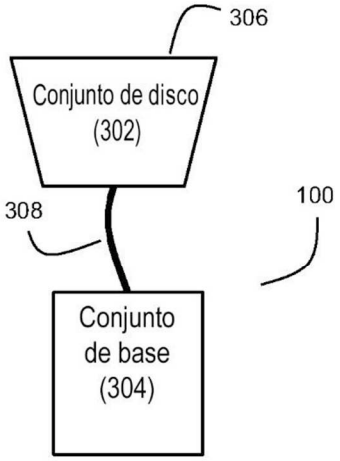

Figura 3B

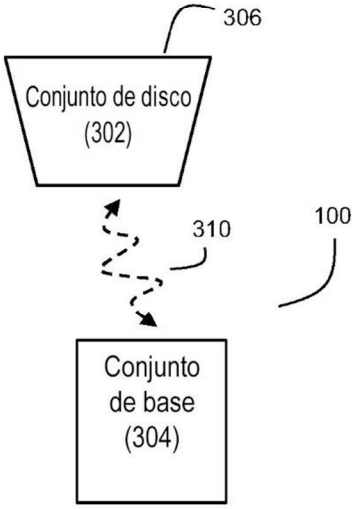

Figura 3C

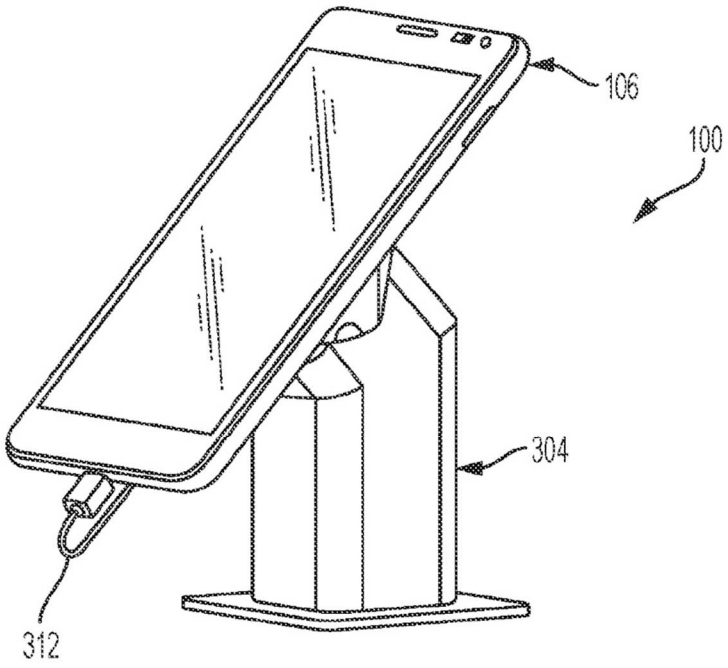

Figura 3D

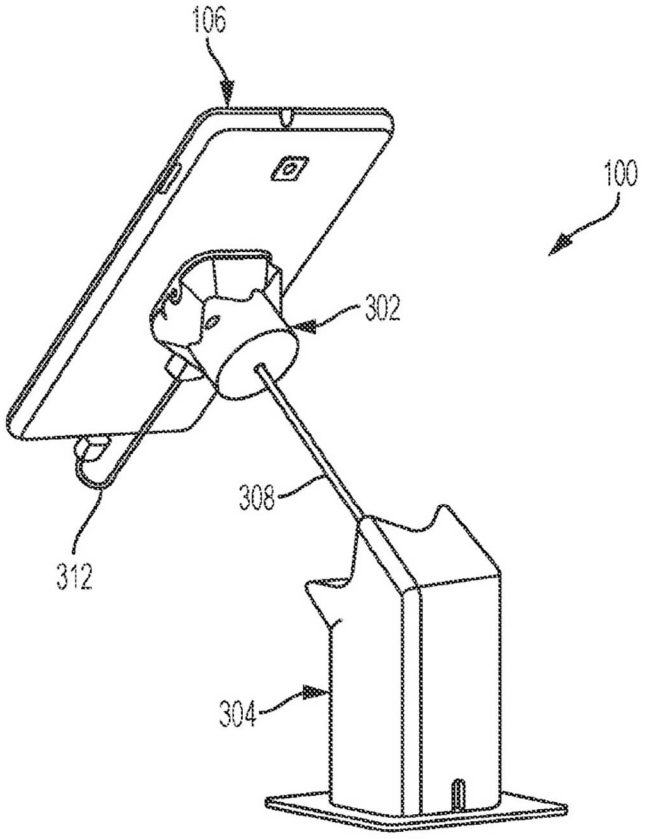

Figura 3E

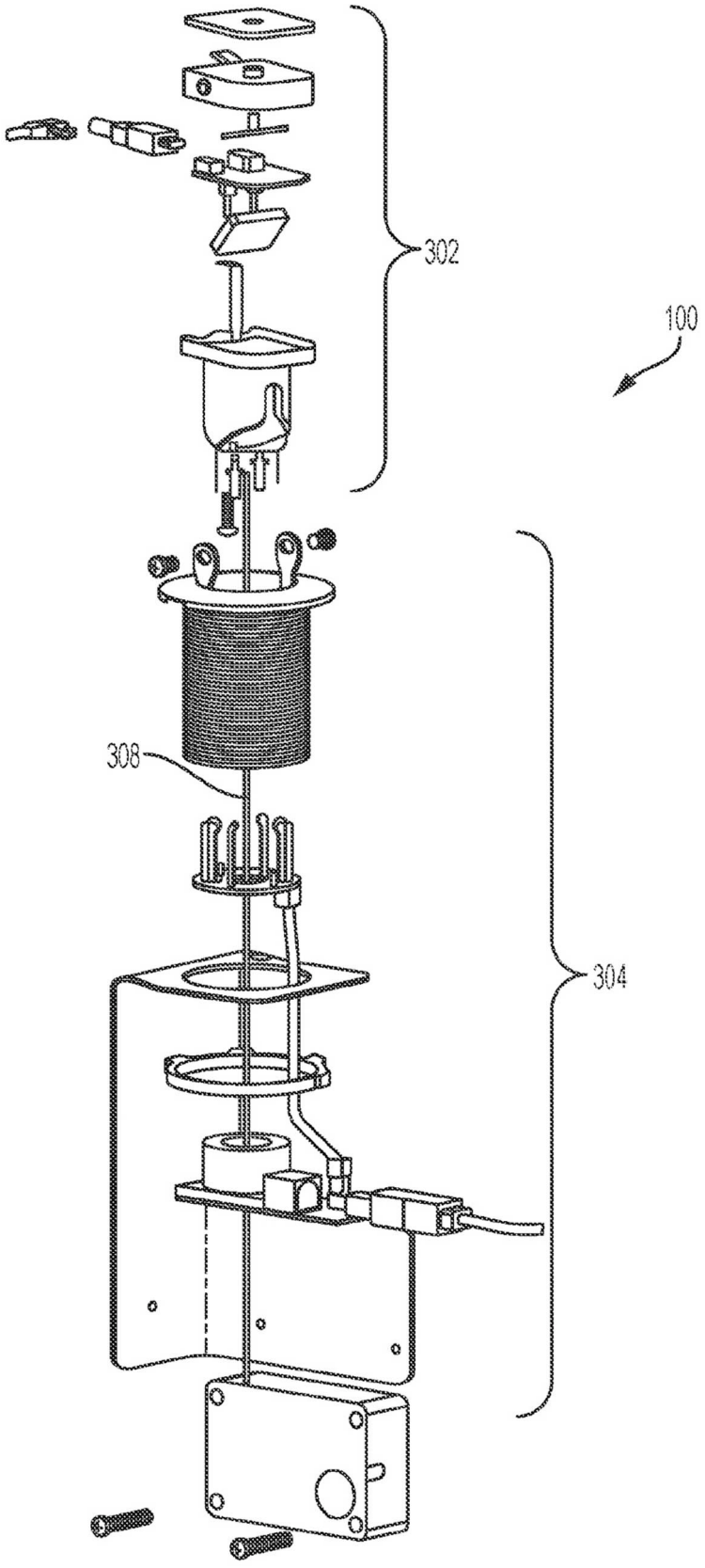

Figura 3F

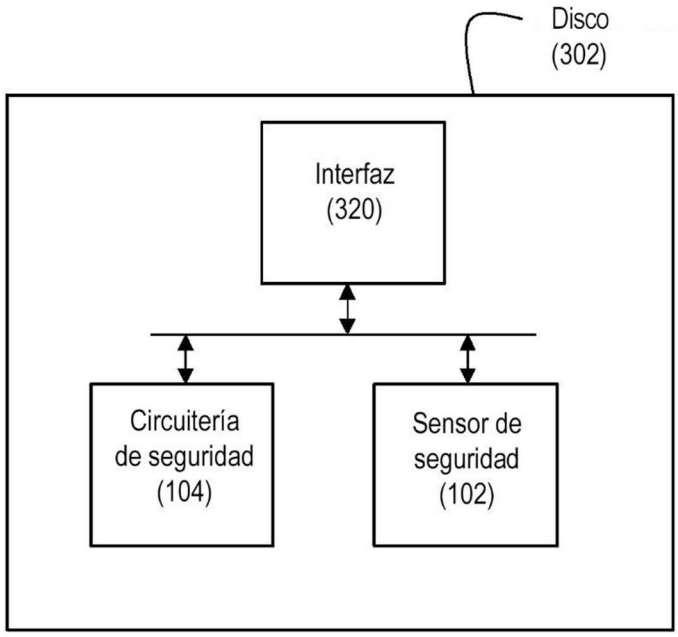

Figura 3G

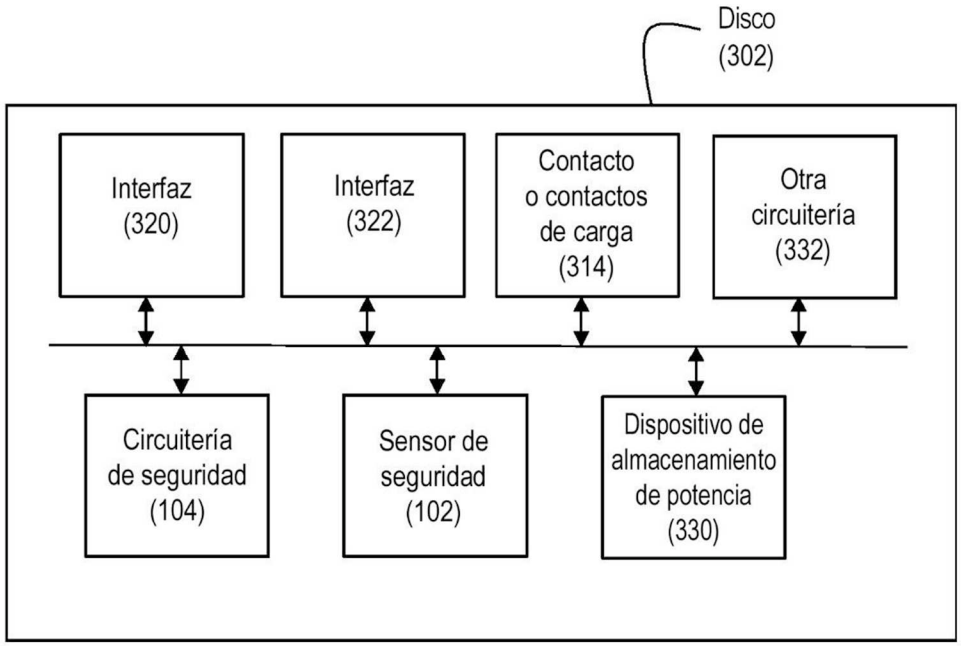

Figura 3H

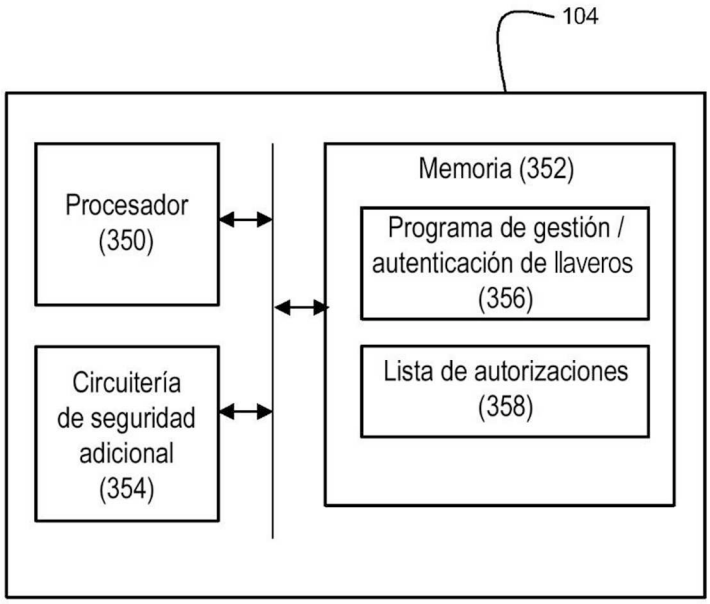
104
Procesador (350)
Circuitería de seguridad adicional (354)
Memoria (352)
Programa de gestión / autenticación de llaveros (356)
Lista de autorizaciones (358)

Figura 3I

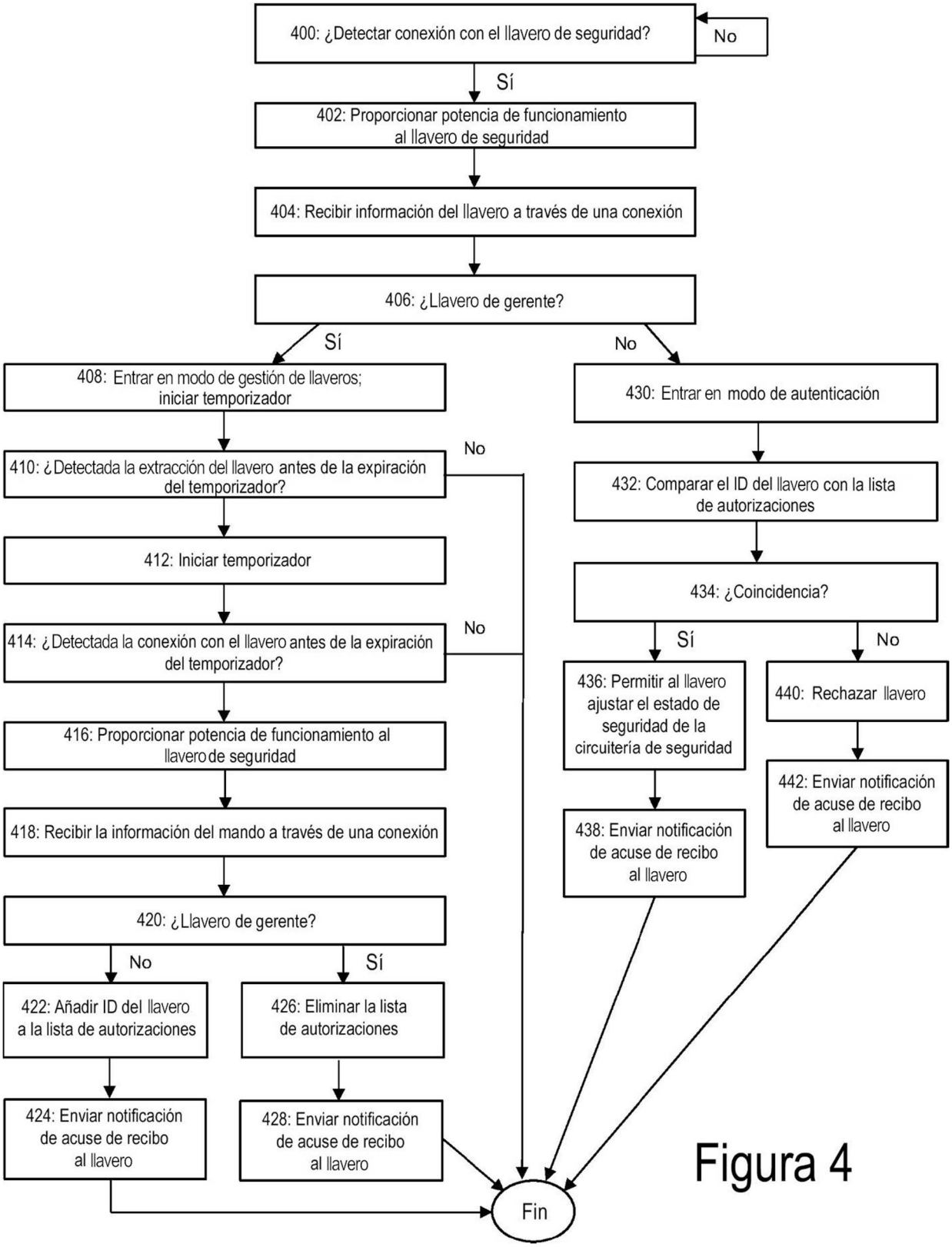
400: ¿Detectar conexión con el llavero de seguridad?
No
Sí
402: Proporcionar potencia de funcionamiento al llavero de seguridad
404: Recibir información del llavero a través de una conexión
406: ¿Llavero de gerente?
Sí
No
408: Entrar en modo de gestión de llaveros; iniciar temporizador
410: ¿Detectada la extracción del llavero antes de la expiración del temporizador?
No
412: Iniciar temporizador
414: ¿Detectada la conexión con el llavero antes de la expiración del temporizador?
No
416: Proporcionar potencia de funcionamiento al llavero de seguridad
418: Recibir la información del mando a través de una conexión
420: ¿Llavero de gerente?
No
Sí
422: Añadir ID del llavero a la lista de autorizaciones
426: Eliminar la lista de autorizaciones
424: Enviar notificación de acuse de recibo al llavero
428: Enviar notificación de acuse de recibo al llavero
430: Entrar en modo de autenticación
432: Comparar el ID del llavero con la lista de autorizaciones
434: ¿Coincidencia?
Sí
No
436: Permitir al llavero ajustar el estado de seguridad de la circuitería de seguridad
440: Rechazar llavero
438: Enviar notificación de acuse de recibo al llavero
442: Enviar notificación de acuse de recibo al llavero
Fin

Figura 4

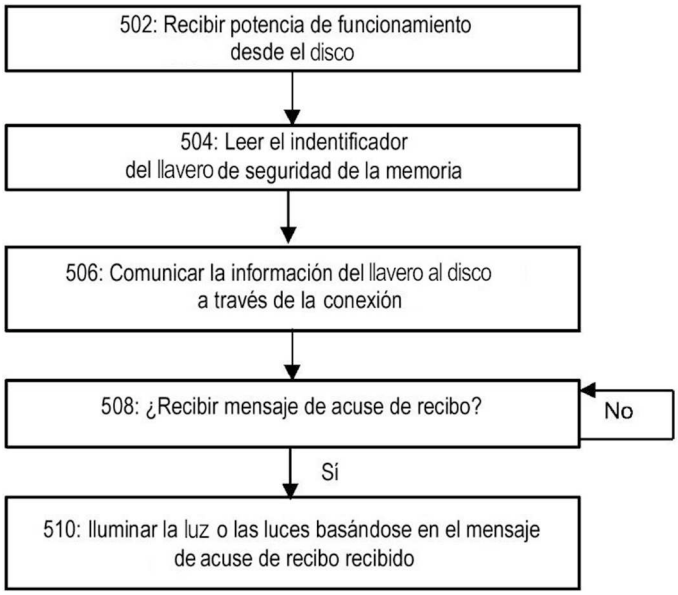
502: Recibir potencia de funcionamiento desde el disco
504: Leer el indentificador del llavero de seguridad de la memoria
506: Comunicar la información del llavero al disco a través de la conexión
508: ¿Recibir mensaje de acuse de recibo?
No
Sí
510: Iluminar la luz o las luces basándose en el mensaje de acuse de recibo recibido

Figura 5

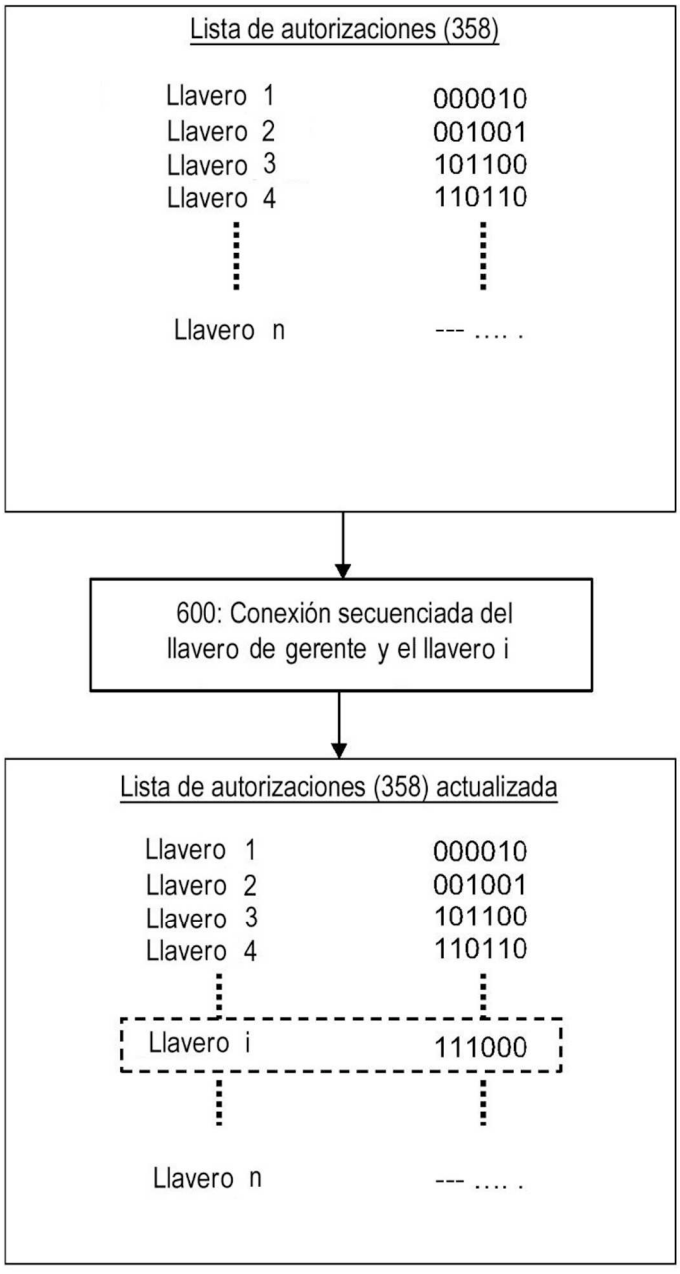
Lista de autorizaciones (358)
Llavero 1
Llavero 2
Llavero 3
Llavero 4
Llavero n
000010
001001
101100
110110
--- …. .
600: Conexión secuenciada del llavero de gerente y el llavero i
Lista de autorizaciones (358) actualizada
Llavero 1
Llavero 2
Llavero 3
Llavero 4
Llavero i
Llavero n
000010
001001
101100
110110
111000
--- …. .

Figura 6

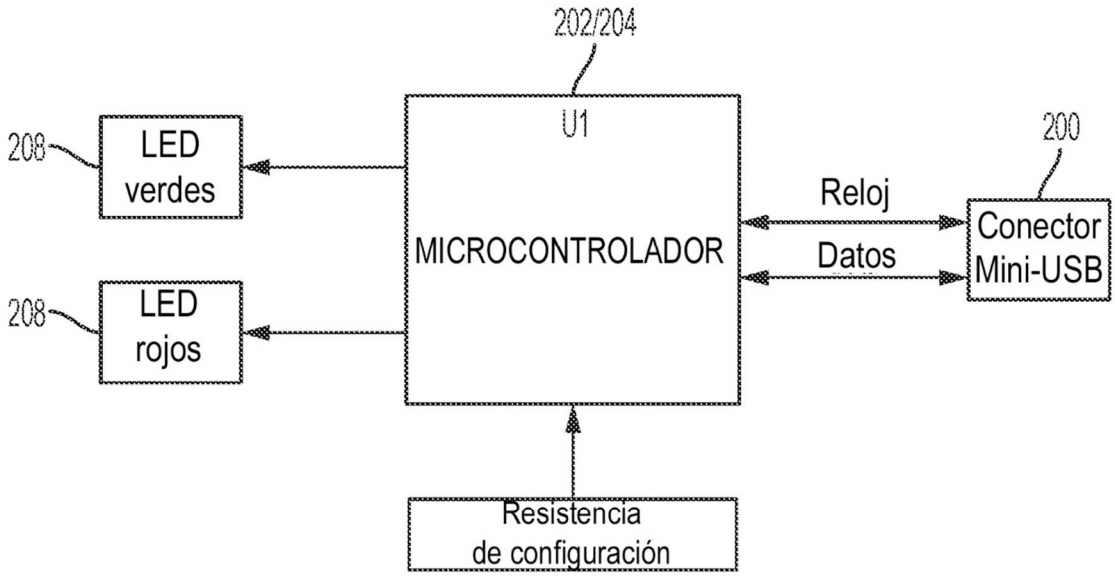
202/204
U1
208
LED
verdes
208
LED
rojos
MICROCONTROLADOR
Reloj
Datos
200
Conector
Mini-USB
Resistencia
de configuración

Figura 7

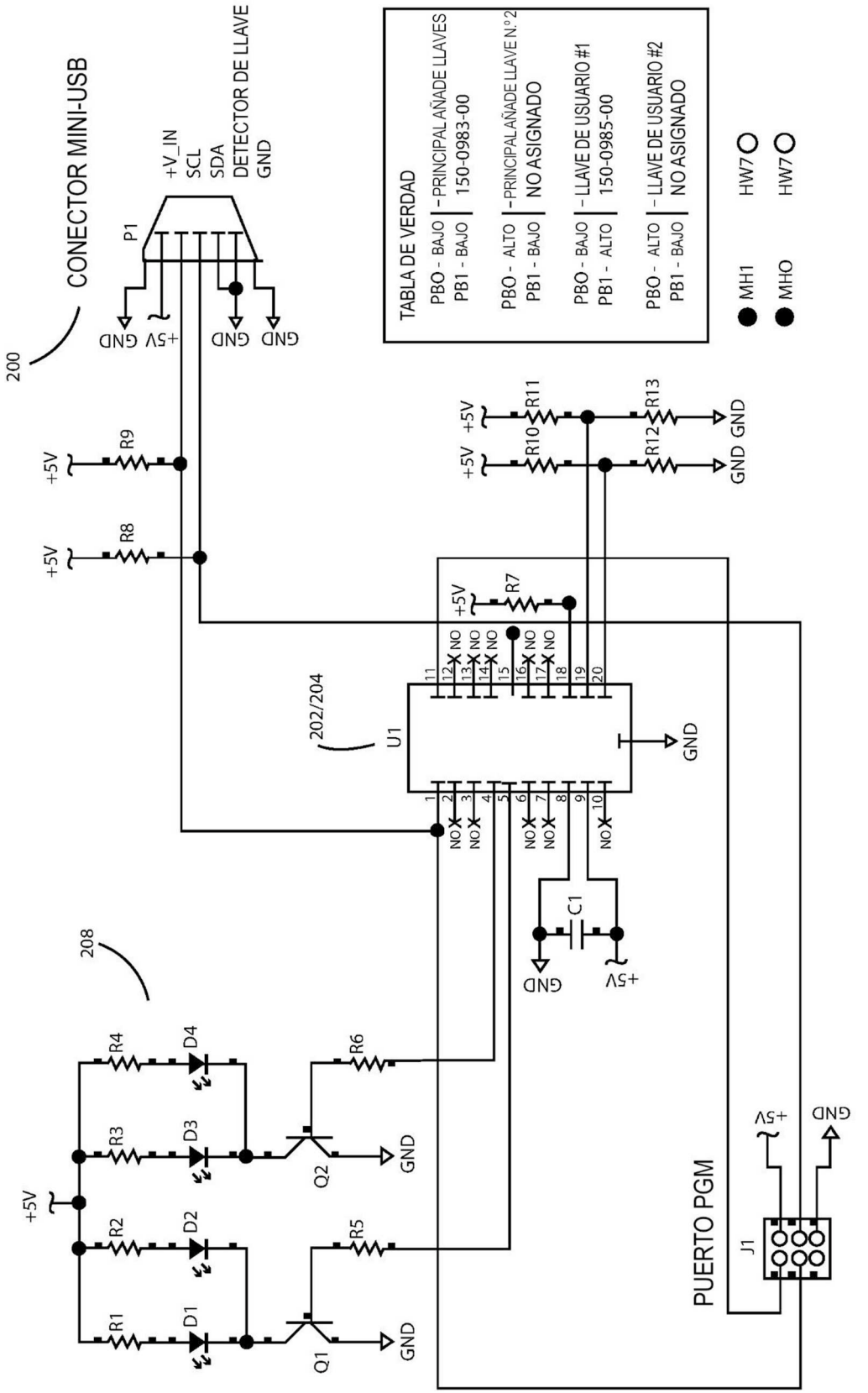
CONECTOR MINI-USB
200
P1
+V_IN
SCL
SDA
DETECTOR DE LLAVE
GND
TABLA DE VERDAD
PBO - BAJO | PRINCIPAL AÑADE LLAVES
PB1 - BAJO | 150-0983-00
PBO - ALTO | PRINCIPAL AÑADE LLAVE N.º2
PB1 - BAJO | NO ASIGNADO
PBO - BAJO | LLAVE DE USUARIO #1
PB1 - ALTO | 150-0985-00
PBO - ALTO | LLAVE DE USUARIO #2
PB1 - BAJO | NO ASIGNADO
MH1
HW7
MHO
HW7
202/204
U1
208
R1
R2
R3
R4
R5
R6
R7
R8
R9
R10
R11
R12
R13
D1
D2
D3
D4
Q1
Q2
C1
+5V
GND
NO
PUERTO PGM
J1

Figura 8

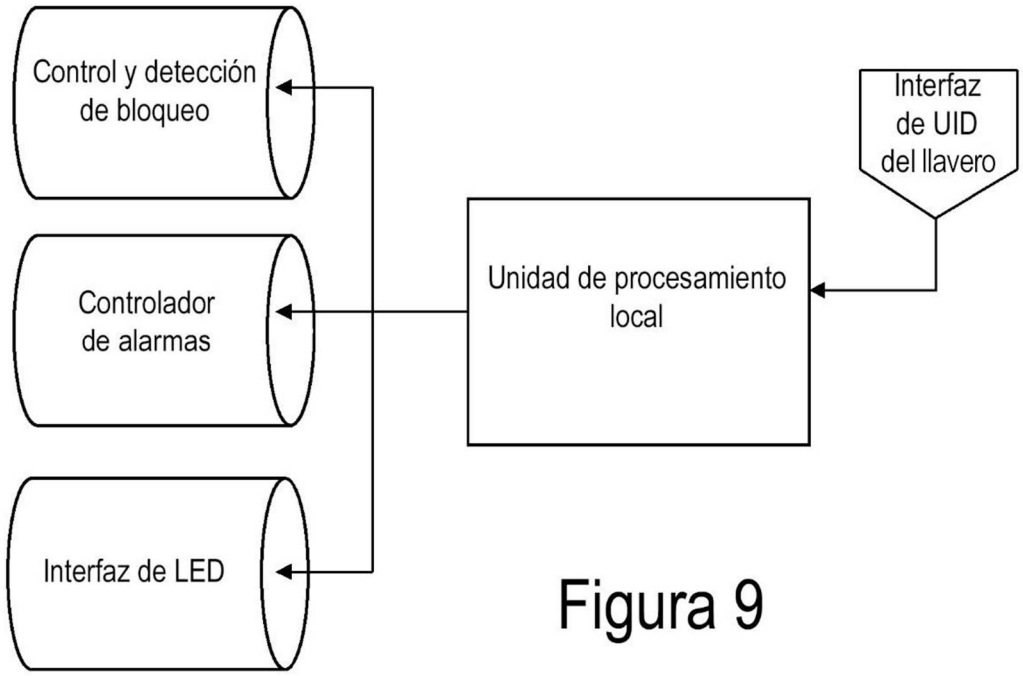
Control y detección de bloqueo
Controlador de alarmas
Interfaz de LED
Unidad de procesamiento local
Interfaz de UID del llavero

Figura 9

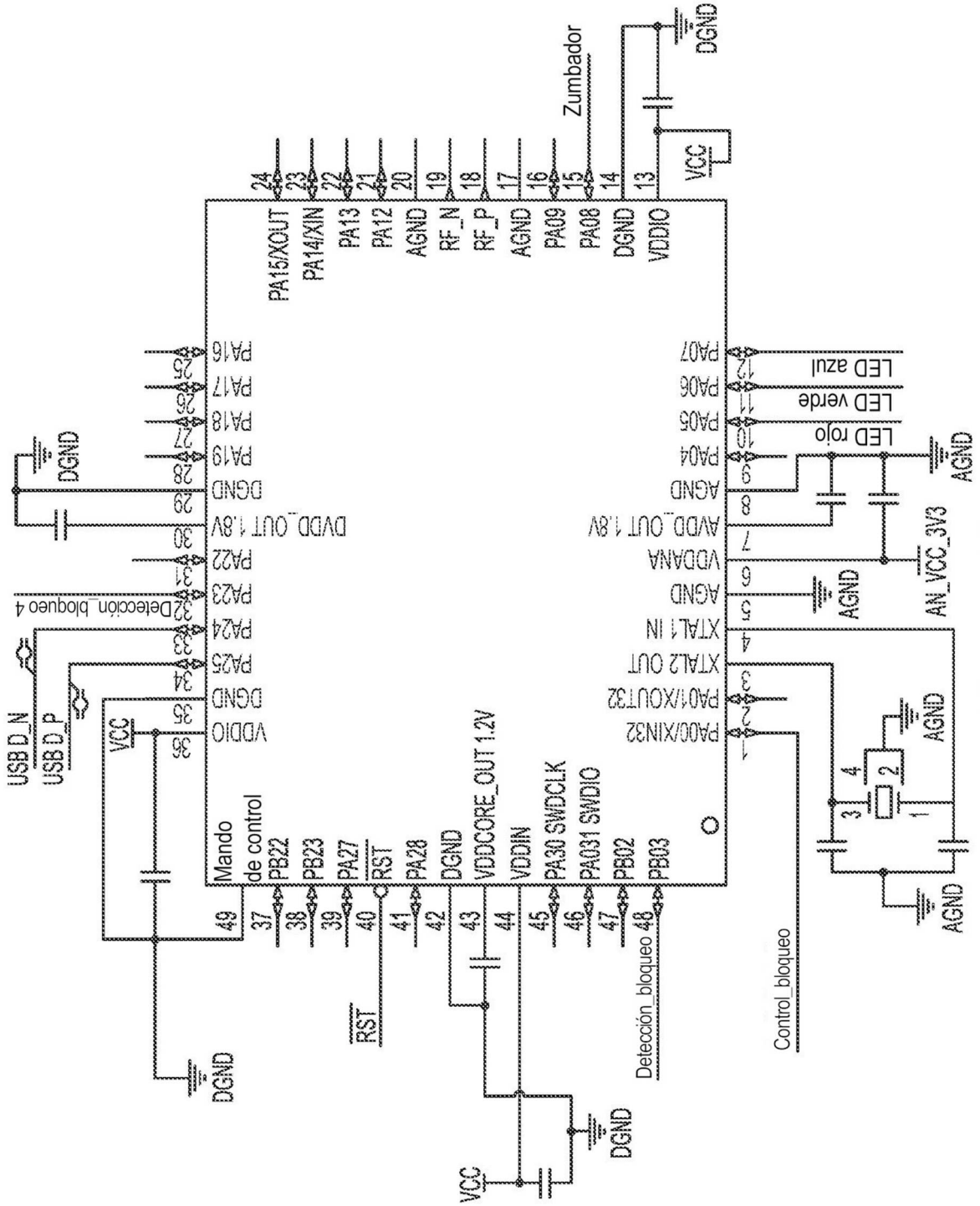
PA15/XOUT
PA14/XIN
PA13
PA12
AGND
RF_N
RF_P
AGND
PA09
PA08
DGND
VDDIO
Zumbador
VCC
DGND
PA16
PA17
PA18
PA19
DGND
DVDD_OUT 1,8V
PA22
PA23
PA24
PA25
DGND
VDDIO
Detección_bloqueo 4
USB D_N
USB D_P
VCC
DGND
Mando
de control
PB22
PB23
PA27
RST
PA28
DGND
VDDCORE_OUT 1.2V
VDDIN
PA30 SWDCLK
PA031 SWDIO
PB02
PB03
RST
Detección_bloqueo
VCC
DGND
PA07
PA06
PA05
PA04
AGND
AVDD_OUT 1,8V
VDDANA
AGND
XTAL1 IN
XTAL2 OUT
PA01/XOUT32
PA00/XIN32
LED azul
LED verde
LED rojo
AGND
AN_VCC_3V3
AGND
AGND
Control_bloqueo

Figura 10

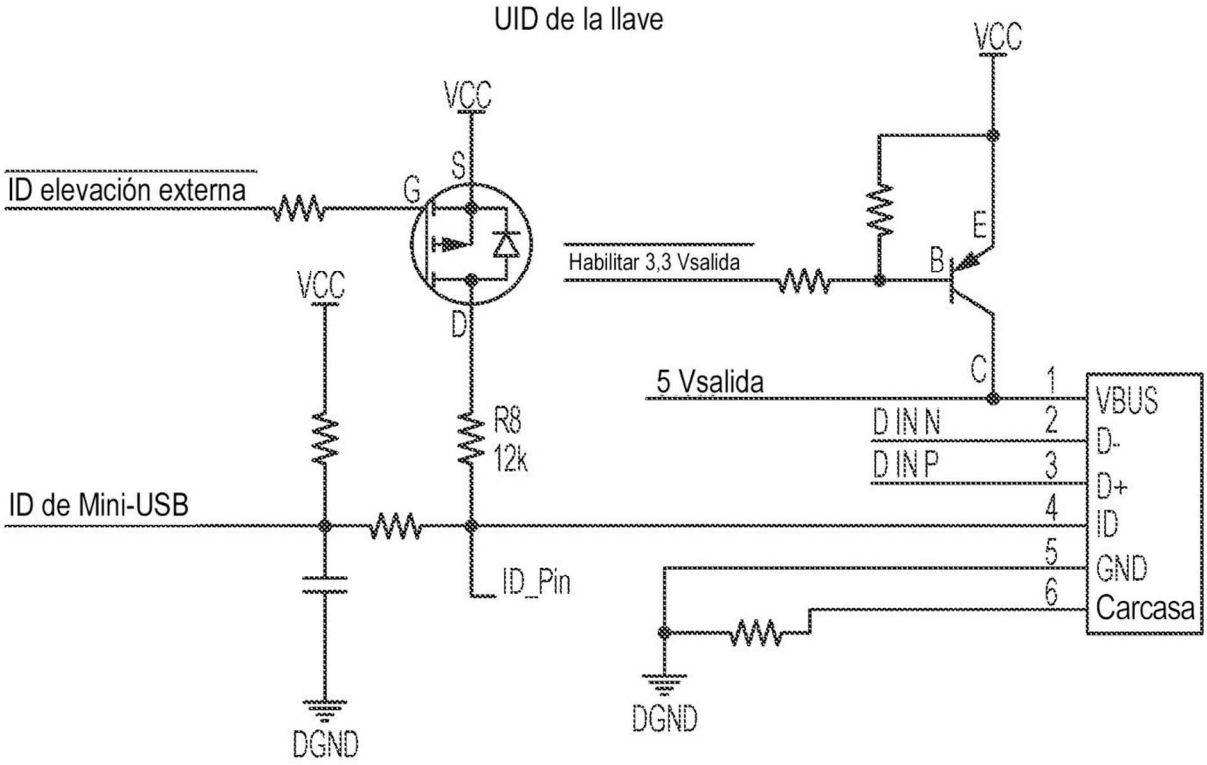
UID de la llave
VCC
VCC
S
G
D
ID elevación externa
Habilitar 3,3 Vsalida
E
B
C
VCC
5 Vsalida
R8
12k
DINN
DINP
ID de Mini-USB
ID_Pin
DGND
DGND
1
2
3
4
5
6
VBUS
D-
D+
ID
GND
Carcasa

Figura 11

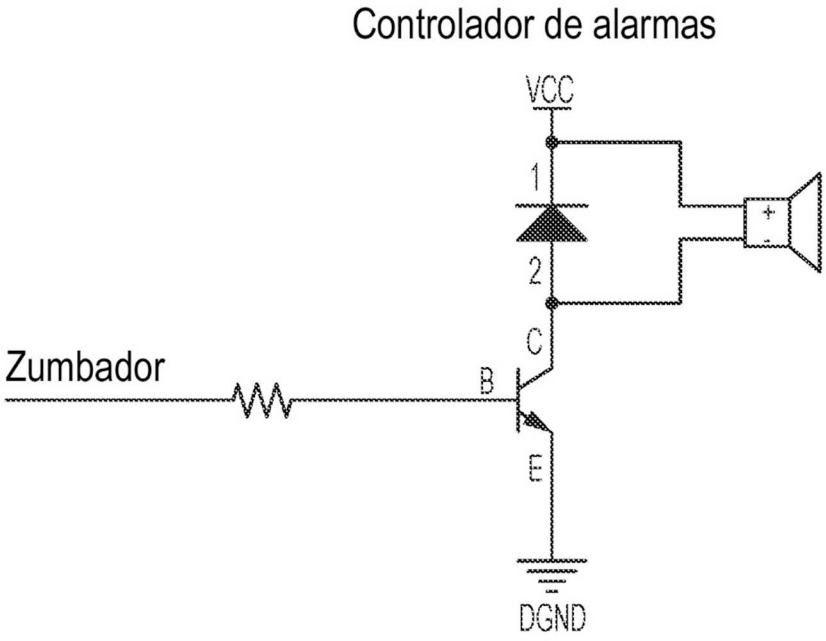

Figura 12

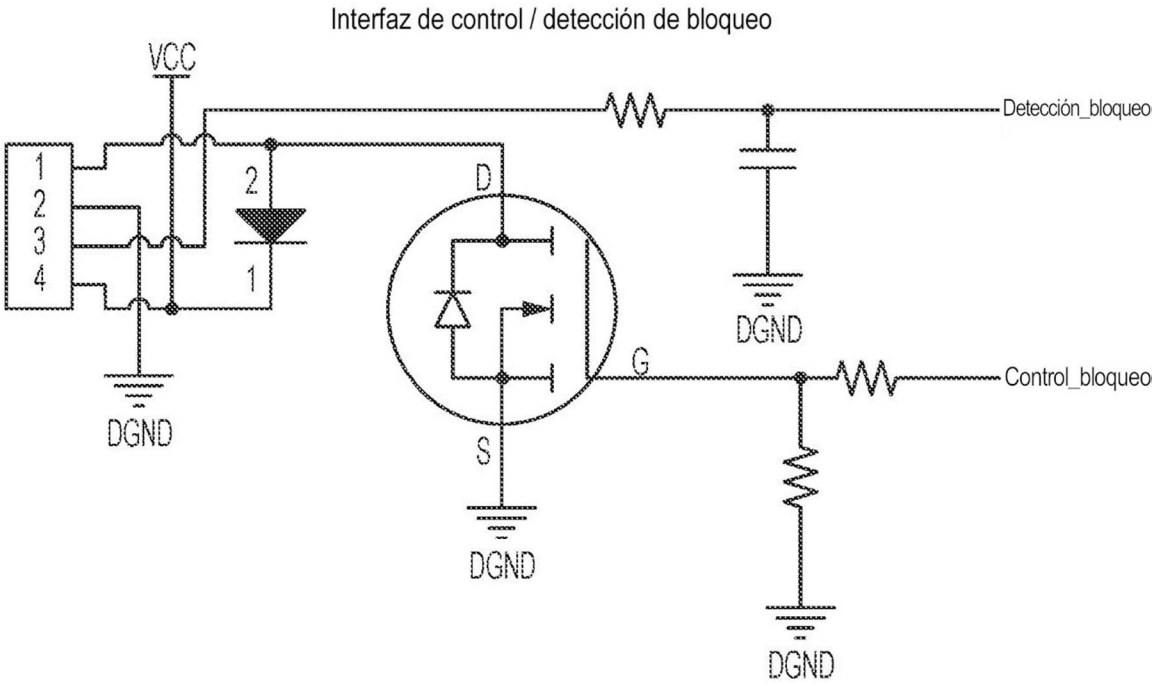
Interfaz de control / detección de bloqueo
VCC
1
2
3
4
2
1
DGND
D
S
G
DGND
DGND
Detección_bloqueo
Control_bloqueo

Figura 13

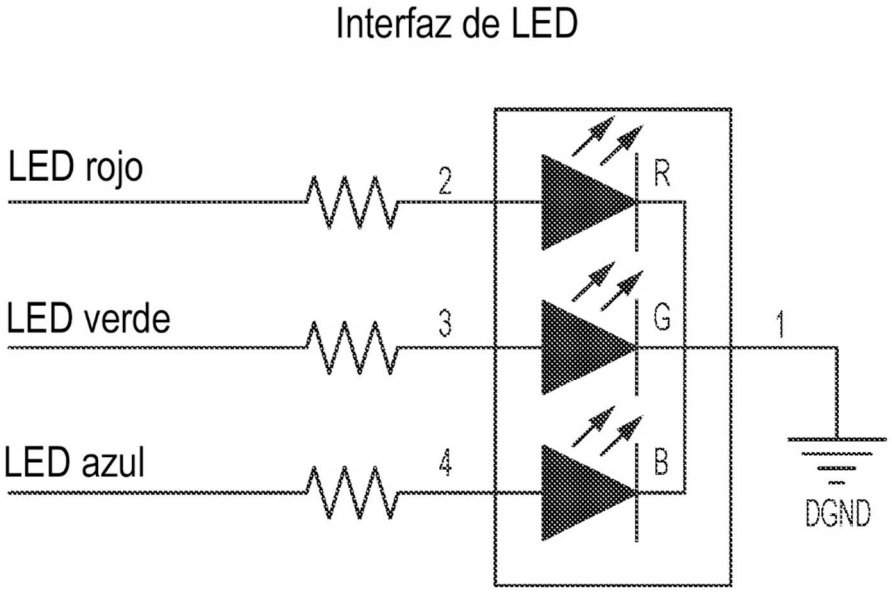

Figura 14

REFERENCIAS CITADAS EN LA DESCRIPCIÓN

Esta lista de referencias citada por el solicitante es únicamente para mayor comodidad del lector. No forman parte del documento de la Patente Europea. Incluso teniendo en cuenta que la compilación de las referencias se ha efectuado con gran cuidado, los errores u omisiones no pueden descartarse; la EPO se exime de toda responsabilidad al respecto.

Documentos de patentes citados en la descripción

- US 62323466
- US 62323511
- US 20150348381 A
- US 8558688 B
- US 8698617 B
- US 8698618 B
- US 20140159898
- US 20170032636
- US 20170032636 A
- US 2017003263