(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 802 250**

(51) Int. CI.:

G07C 9/00 (2010.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **06.06.2013 E 13170955 (2)**

(97) Fecha y número de publicación de la concesión europea: **25.03.2020 EP 2677506**

(54) Título: **Estructura de cerradura inteligente y método de operación correspondiente**

(30) Prioridad:

22.06.2012 US 201213531478

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
18.01.2021

(73) Titular/es:

CHEN, GUN (50.0%)
15F.-4, No.82, Sec. 2, Anhe Rd. Da'an Dist.
106 Taipei City, TW y
LIN, SHU-SHIAN (50.0%)

(72) Inventor/es:

CHEN, GUN y
LIN, SHU-SHIAN

(74) Agente/Representante:

SANZ-BERMELL MARTÍNEZ, Alejandro

DESCRIPCIÓN

Estructura de cerradura inteligente y método de operación correspondiente

ANTECEDENTES DE LA INVENCIÓN

1. Sector de la Invención

La presente invención se refiere a una estructura de cerradura inteligente, y más particularmente a una estructura de cerradura inteligente que tiene una alta seguridad para configurar y procesar la funcion de desbloqueo correspondiente a través de tecnología de radiofrecuencia de acuerdo con un control de seguridad y una autentificación efectivos.

2. Estado de la técnica relacionado

La tecnología RFID es ampliamente adoptada para acceder a ciertas propiedades aseguradas hoy en día. No obstante, es preferible no utilizar dicha tecnología en lugares de alta seguridad debido a su vulnerabilidad a una brecha de seguridad intencionada. Además, para la mayoría de los bienes o áreas aseguradas, el coste y la carga de trabajo que acompaña a hacer o mantener estas llaves de seguridad en especial son siempre enormes

En la solicitud de patente US 2011/0001603 A1, se describe un método de recepción de información de seguridad desde un dispositivo de comunicación móvil para controlar un dispositivo de autorización en un sistema de seguridad. La solución puede superar o aliviar algunos de los problemas mencionados arriba. No obstante, no hay un agujero para la llave convencional definido en la patente, lo que puede resultar problemático en una situación de corte de energía.

En la solicitud de patente US 2006/0072755, se define un sistema de cerradura y llave inalámbrica que utiliza un par de llaves de cifrado. El sistema también carece de un agujero de llave convencional y no funcionará cuando no haya energía suministrada al sistema

RESUMEN DE LA PATENTE DE INNOVACIÓN

La presente invención proporciona una estructura de cerradura inteligente de acuerdo con las características de la reivindicación independiente 1.

En una realización preferente de la presente invención, esta comprende además un dispositivo de prueba de caída equipado junto al dispositivo de interrogación para impedir la caída del dispositivo móvil cuando éste se utiliza para comunicarse con el dispositivo de interrogación.

En una realización preferente de la presente invención, se proporciona un valor de semilla al procesador desde el dispositivo móvil, en la base de datos para el uso del procesador está preestablecida una función de permutación para que el procesador permute las secuencias de datos de la información de autenticación basada en el valor de semilla y para que el procesador además encripte y desencripte la información de autenticación.

En una realización preferente de la presente invención, el dispositivo de interrogación comprende además un modulo para recibir la información de autenticación antes de que sea guarda durante la configuración de la estructura de cerradura inteligente.

En una realización preferente de la presente invención, el dispositivo de interrogación comprende además un interruptor de configuración para permitir la configuración de la estructura de cerradura inteligente.

En una realización preferente de la presente invención, el dispositivo de interrogación comprende además un interruptor de llave móvil para controlar una ruta del dispositivo de interrogación que envía un comando de desbloqueo al mecanismo de la cerradura.

En una realización preferente de la presente invención, el dispositivo de interrogación comprende además un chipset para encriptar o desencriptar los datos transmitidos o recibidos a través del lector de radiofrecuencia.

En una realización preferente de la presente invención, donde la estructura de cerradura inteligente incluye tres modos básicos: un modo de configuración, un modo de operación y un modo de llave, y el modo de operación es el modo por defecto de la estructura de cerradura inteligente.

En una realización preferente de la presente invención, el valor de la semilla comprende al menos una de información de identificación del dispositivo móvil, información de identificación de la estructura de cerradura inteligente, y un tiempo sincronizado preestablecido entre el dispositivo móvil y el dispositivo de interrogación.

En una realización preferente de la presente invención, cuando el dispositivo móvil envía de vuelta la información de la llave encriptada, el dispositivo móvil permuta la secuencia de datos de la información de la llave.

En una realización preferente de la presente invención, este comprende además la configuración de la TITULO antes de que la TITULO reciba la solicitud de desbloqueo desde el dispositivo móvil, comprendiendo:

al menos un dispositivo de configuración seleccionado de entre el dispositivo móvil y otros ordenadores de configuración que soliciten la configuración de la estructura de cerradura inteligente para modificar una lista de permisos en la primera base de datos preestablecida de la estructura de cerradura inteligente

la estructura de cerradura inteligente que verifica el acceso de al menos un dispositivo de configuración a la primera base de datos preestablecida;

al menos un dispositivo de configuración que modifique la lista de permisos de la estructura de cerradura inteligente; y

la estructura de cerradura inteligente que guarda la modificación de la lista de permisos en la primera base de datos preestablecida para la autenticación para desbloquear la estructura de cerradura inteligente

En una realización preferente de la presente invención, la modificación de la lista de permisos comprende la creación de al menos una de una cuenta y claves en los nombres de usuario, números de teléfono móvil, contraseñas, números de serie del dispositivo móvil, números MAC del dispositivo móvil, ICCID del dispositivo móvil, IMEI de las tarjetas SIM, y periodos válidos de autorización para cualquier acceso.

En una realización preferente de la presente invención, cuando se crea una cuenta, la estructura de cerradura inteligente genera automáticamente una criptografía correspondiente de acuerdo con una de las criptografías de clave simétrica y asimétrica que se guardan en el dispositivo móvil y en la estructura de cerradura inteligente para la codificación, y la decodificación del uso del dispositivo móvil y la estructura de cerradura inteligente.

En una realización preferente de la presente invención, esta comprende además una etapa en la que el dispositivo de interrogación cuenta los tiempos de fallo de la información clave verificada que es incomparable en la primera base

de datos preestablecida, y comprueba si los tiempos de fallo contados son más que un valor límite durante un período de tiempo preestablecido.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La presente invención será evidente para aquellos expertos en el estado de la técnica mediante la lectura de la siguiente descripción de la misma, con referencia a los dibujos adjuntos, en los que:

Las FIGS. 1A, 1B y 1C son visas de planta esquemáticas de una estructura de cerradura inteligente de acuerdo con las realizaciones de la presente invención;

Las FIGS. 2A y 2B son vistas en perspectiva esquemáticas de estructura de cerradura inteligente de acuerdo con otras realizaciones de la presente invención;

La FIG. 3 es una vista esquemática de la estructura de cerradura inteligente de acuerdo con otras realizaciones de la presente invención que muestra varias formas de un dispositivo de prueba de caída de al menos una vista frontal y una vista del perfil derecho;

La FIG. 4 es un diagrama esquemático que muestra los métodos de configuración de la estructura de cerradura inteligente de acuerdo realizaciones de la presente invención;

FIG. 5 es un diagrama esquemático que muestra la estructura de cerradura inteligente en funcionamiento después de su configuración de acuerdo con realizaciones de la presente invención.

Las FIGS. 6A-6D son diagramas de bloques esquemáticos que muestran respectivamente realizaciones de la estructura de cerradura inteligente de acuerdo con la presente invención;

La FIG. 7 es un diagrama esquemático que muestra una tabla de operación de la estructura de cerradura inteligente de acuerdo con realizaciones de la presente invención, listando la relación entre los cambios de la estructura de cerradura inteligente y los modos de operación y funciones de la misma;

La FIG. 8 es un diagrama de flujo esquemático que muestra un método de operación de la estructura de cerradura inteligente de la presente invención en su modo de configuración de acuerdo con realizaciones de la presente invención;

La FIG. 9 es un diagrama de flujo esquemático que muestra un método de operación de la estructura de cerradura inteligente de la presente invención en su modo de operación normal de acuerdo con realizaciones de la presente invención;

DESCRIPCIÓN DETALLADA DE LAS REALIZACIONES

Para explicar con más detalle las soluciones técnicas adoptadas en la presente invención y las ventajas de las mismas, se da una descripción detallada de las realizaciones preferentes de la presente invención para una mejor comprensión refiriéndose a los dibujos adjuntos.

La presente invención es aplicable a cualquier sistema de cerradura convencional que incorpore un dispositivo de interrogación por radiofrecuencia (RF). Un usuario autorizado puede cerrar o abrir una puerta, una taquilla, o acceder

a un bien o área particularmente segura interactuando con el dispositivo de interrogación por radiofrecuencia (RF) y los sistemas de cerradura. Sin sistemas informáticos complicados o bases de datos que soporten simultáneamente, la presente invención funciona por sí sola para ser tan simple como cualquier cerradura convencional para usos domésticos o aplicaciones comerciales.

Las FIGS. 1A-1C representan respectivamente una estructura de cerradura inteligente de la presente invención. En el lado exterior de una puerta, una taquilla o cualquier acceso a un bien o área asegurada, refiriéndose a la FIG. 1A, la estructura de cerradura inteligente 1 de la presente invención comprende un agujero de llave física 101 y un dispositivo de interrogación 105 que utiliza una de las tecnologías de radiofrecuencia (RF) como la Comunicación de Campo Cercano, Bluetooth, Comunicación Infrarroja, y/o otros protocolos de comunicación inalámbrica, estando integrados por antenas de transmisión y recepción. Una manija o un pomo 102 se dispone opcionalmente en el lugar descrito en la FIG. 1A. En el lado interior de la puerta, armario o acceso a un bien o área asegurada, la estructura de cerradura inteligente de la presente invención está opcionalmente equipada con una manija, un pomo, un puerto Ethernet, un puerto serie, una entrada de energía, un puerto USB, y/o dos interruptores para la configuración y para activar el control móvil (No se muestra).

En realizaciones de la estructura de cerradura inteligente de la presente invención con una manija o un pomo como se muestra en las FIGS. 1A, 1B y 1C, la estructura de cerradura inteligente 1' o 1" se muestra para disponer el dispositivo interrogatorio 105 en la parte superior de la misma (refiriéndose a la FIG. 1A), a la izquierda de la misma (refiriéndose a la FIG. 1C), o en la parte inferior de la misma (refiriéndose a la FIG. 1B) correspondiente a las ubicaciones de la manija 102 y el orificio de la llave 101 en el lado exterior asumiendo que la puerta/cerradura/acceso está abierta en el lado izquierdo. Todo lo mencionado anteriormente está comprensiblemente invertido horizontalmente mientras que la puerta/cierre/acceso está abierta a la derecha de la misma.

Un indicador de luz LED (Diodo Emisor de Luz) 104 se coloca en la parte superior del dispositivo de interrogación, en el lado exterior. Los LED comprendidos en el indicador de luz se utilizan para indicar respectivamente un estado de funcionamiento del interrogador, un estado de la energía o de la batería de la estructura de cerradura inteligente, y/o un estado que describa si un acceso se concede.

Las FIGS. 2A y 2B muestran realizaciones de la estructura de cerradura inteligente de la presente invención sin una manija o pomo. En las realizaciones de la estructura de cerradura inteligente sin manija o pomo, como se muestra en las FIGS. 2A y 2B, la estructura de cerradura inteligente 2 o 2' se muestra para disponer el dispositivo de interrogación 105 en la parte inferior de la misma o debajo del agujero de la llave física 101 (refiriéndose a 2A), o en la parte superior o por encima del agujero de la llave física 101 (refiriéndose a 2B), como se muestra en un lado exterior. La estructura de cerradura inteligente 2, 2' está conectada de forma controlada y se comunica con cerraduras de la puerta/cierre/acceso a través del agujero de la llave física 101.

La FIG. 3 muestra un dispositivo a prueba de caída 103 de la estructura de cerradura inteligente 1 de la presente invención, estando el dispositivo a prueba de caídas 103 dispuesto en la parte inferior del dispositivo de interrogación 105. El dispositivo a prueba de caídas 103 es preferentemente un borde que sobresale de la estructura de cerradura inteligente 1 para prevenir una caída accidental del teléfono móvil M mientras se acerca el teléfono móvil M al dispositivo de interrogación 105 para abrir la puerta. El dispositivo a prueba de caídas 103 está hecho para ser más ancho y grueso que el teléfono móvil M. El dispositivo a prueba de caídas 103 es alternativamente un borde plano, en forma de relleno con paredes inclinadas o curvadas, como se muestra respectivamente en el lado derecho de la FIG. 3.

La FIG. 4 muestra respectivamente dos diagramas de la arquitectura de la configuración de la estructura de cerradura inteligente 1 de la presente invención, según realizaciones de la presente invención. La FIG. 5 muestra un diagrama que muestra la estructura de cerradura inteligente 1 de la presente invención en funcionamiento después de su configuración, de acuerdo con realizaciones de la presente invención.

Refiriéndose a la FIG. 4, en la configuración de la estructura de cerradura inteligente 1, un usuario crea una lista de permisos en un base de datos de estructura de cerradura inteligente 1 de la presente invención mediante un dispositivo de configuración 20 como un ordenador de escritorio, un ordenador portátil, un ordenador de panel, un teléfono móvil, o cualquier tipo de dispositivo móvil. La estructura de cerradura inteligente 1 incorpora sólo un dispositivo de configuración en una vez.

Los procesos de configuración que se muestran en la FIG. 4 pueden realizarse con conexión a la red de Internet (como se muestra en la mitad inferior de la FIG. 4) o sin conexión a la red de Internet (como se muestra en la mitad superior de la FIG. 4). En la configuración sin conexión a la red de Internet (como se muestra en la mitad superior de la FIG. 4), el dispositivo de configuración 20 se comunica directamente con la estructura de cerradura inteligente 1 a través de la conexión de comunicación 201, como un puerto USB (Bues Universal en Serie), un puerto serie (RS-232/422/485), Bluetooth o comunicación de campo cercano (NFC). En la realización con la red de Internet (como se muestra en la mitad inferior de la FIG. 4), el interruptor alámbrico o inalámbrico 21 desarrolla una Red de Área Local (LAN), vinculando el dispositivo de configuración 20 a través de una conexión de comunicación 202 como un puerto Ethernet alámbrico o Wi-Fi inalámbrico o Zig-Bee, y vinculando la estructura de cerradura inteligente 1 a través de una conexión de comunicación 203 como un puerto Ethernet, un puerto de alimentación a través de Ethernet o Wi-Fi inalámbrico o Zig-Bee.

Durante el modo de configuración de la estructura de cerradura inteligente 1, como se muestra en la FIG. 4, un usuario autorizado crea o modifica la lista de permisos permitiendo que cualquier identidad específica acceda a los recursos permitidos y guarde la lista de permisos en la base de datos de estructura de cerradura inteligente 1. La lista de permisos también abarca al menos una de las informaciones de autenticación, como los nombres de usuario y las contraseñas, información de la etiqueta NFC, números de teléfono móvil, números de serie del teléfono móvil/dispositivo móvil M, MAC (Media Control de Acceso) del teléfono móvil/dispositivo móvil M, ICCID (Tarjeta de identificación de circuito integrado) del teléfono móvil/dispositivo móvil M, IMEI (Identidad de Equipamiento Móvil Internacional) de SIM (Módulo de Identidad del Suscriptor), tarjetas utilizadas en el teléfono móvil/dispositivo móvil M, autenticación biométrica como el reconocimiento de voz y reconocimiento de cara, y/o períodos válidos de acceso permitido.

Después de que se haya realizado la configuración de la estructura de cerradura inteligente 1, el acceso a la base de datos en la estructura de cerradura inteligente 1 está completamente desconectado del dispositivo de configuración 20. Refiriéndome además a la FIG. 5, en la operación de la estructura de cerradura inteligente 1 después de la configuración de la misma, la estructura de cerradura inteligente 1 funciona de forma independiente y en espera. Con un dispositivo móvil equipado con la función de comunicación por radiofrecuencia, un usuario cuya información de autenticación está previamente configurada en la lista de permisos en la base de datos de la estructura de cerradura inteligente 1, puede adquirir acceso interactuando sin contacto con la estructura de cerradura inteligente 1 con el dispositivo móvil M situado dentro de un rango efectivo de comunicación por radiofrecuencia 204 del dispositivo de interrogación 105 dispuesto en la estructura de cerradura inteligente 1.

La comunicación por radiofrecuencia 204 entre la estructura de cerradura inteligente 1 y el dispositivo móvil M se realiza mediante la comunicación de campo cercano, Bluetooth, comunicación infrarroja, y/u otros protocolos de comunicación inalámbrica.

Según la información transmitida desde el dispositivo móvil M, la estructura de cerradura inteligente 1 verificará la información de autenticación de acuerdo con la de la base de datos previamente guardada. Si los datos de autenticación se identifican y verifican como coincidentes, la estructura de cerradura inteligente 1 envía una señal electrónica a un sistema de cerradura de la puerta para desbloquearla. De lo contrario, el acceso de los usuarios será denegado y la estructura de cerradura inteligente 1 enviará una información de denegación, reclamará otro conjunto de solicitudes de desbloqueo, retrasará la aceptación de otra solicitud de desbloqueo, apagará temporalmente la función de desbloqueo a través del dispositivo de interrogación por radiofrecuencia 105, o apagará permanentemente la función de desbloqueo a través del dispositivo de interrogación por radiofrecuencia 105 hasta que se utilice otra llave física para desbloquear la puerta en su lugar y reconfigurará la estructura de cerradura inteligente 1 utilizando los métodos descritos en la FIG. 4.

La FIG. 6A muestra un diagrama de bloques de una primera realización de la estructura de cerradura inteligente 1 de la presente invención. La estructura de cerradura inteligente 1 comprende un dispositivo interrogación por radiofrecuencia (RF) 105 como se mencionó anteriormente y un mecanismo de cierre 50 que puede ser una cerradura ordinaria teniendo el agujero de llave 101 como se mencionó anteriormente. El dispositivo de interrogación por radiofrecuencia 105 comprende un procesador 511, una base de datos 512 creada por/en una memoria, un lector de radiofrecuencia 513, un módulo 514 para recibir información de autenticación, dos interruptores incluyendo un interruptor de configuración 515, y un interruptor de lave móvil 516 para controlar una ruta de envío de señales electrónicas como un comando de desbloqueo al mecanismo de cierre 50, una fuente de energía 517, y/o opcionalmente un chipset 518 como se muestra en las FIGS 6C y 6D para cifrar o descifrar los datos transmitidos a través de la lector de radiofrecuencia 513.

En un modo de configuración de la estructura de cerradura inteligente 1, el procesador 511 descifra los datos del módulo 514 para recibir información de autenticación y guarda los datos encriptados para evitar la lectura/escritura no autorizada de los datos guardados en la base de datos 512. Durante un modo de operación normal de la estructura de cerradura inteligente 1, el procesador 511 encripta los datos al lector de radiofrecuencia 513 o los descifra, y luego identifica información de autenticación entre la guardada en la base de datos/memoria 512 y la recuperada de los datos recibidos del lector de radiofrecuencia 513. Después, el procesador 511 envía un comando de desbloqueo a el mecanismo de cierre 50 basado en el resultado de la identificación de información de autenticación. Los procesos de cifrado y el descifrado se llevan a cabo mediante cualquiera de los programas informáticos del procesador 511 o el hardware del chipset 518 específicamente utilizado para el cifrado y descifrado como se muestra en FIGS. 6C y 6D.

La base de datos/memoria 512 carga toda la base de datos de autenticación como nombres de usuario, contraseñas, información de la etiqueta NFC, números de teléfono móvil, números de serie de los dispositivos móviles, números MAC de los dispositivos móviles, ICCID de los dispositivos móviles, IMEI de las tarjetas SIM, autenticación biométrica como el reconocimiento de voz y rostro, y/o períodos válidos de acceso. La base de datos 512 en la memoria comprende múltiples cuentas en una lista de permisos. El historial de acceso también se registra en la memoria. La base de datos/memoria 512 es una RAM no volátil (memoria de acceso aleatorio) u otros almacenamientos magnéticos, que mantienen los datos asegurados con o sin suministro de energía.

Trabajando bajo la comunicación de campo cercano, Bluetooth, comunicación infrarroja, y/u otros protocolos de comunicación inalámbrica conocidos en el estado de técnica, el lector de radiofrecuencia 513 está diseñado para

comunicarse con un dispositivo móvil exterior M (teléfonos móviles, PDA, ordenadores de panel, tabletas), que solicita desbloquear la puerta controlada por la estructura de cerradura inteligente 1. El módulo 514 para recibir información de autenticación recibe los datos de autenticación a través de un puerto Ethernet, un puerto de alimentación a través de Ethernet, un módulo Wi-Fi inalámbrico o ZigBee a 2,4GHz bajo IPv4 o IPv6, un lector de comunicación de campo cercano a 13,56 MHz, Bluetooth, un puerto USB, y/o un puerto serie de RS-232, 422, 485. La función principal del módulo 514 es recoger información de autenticación de la lista de permisos.

En una realización alternativa, el lector de radiofrecuencia 513 también desempeña un papel como módulo receptor de autenticación, y por consiguiente el correspondiente diagrama de bloques se simplifica como se muestra en las FIGS. 6B y 6D.

El interruptor de llave móvil 516 es un interruptor para activar/desactivar el dispositivo de interrogación por radiofrecuencia 105 sobre el mecanismo de bloqueo 50. Cuando el interruptor 516 pasa al modo "Llave y móvil", se permite el desbloqueo a través del dispositivo de interrogación por radiofrecuencia 105. En caso de que el interruptor 516 pase al modo "Sólo Llave", la comunicación entre el dispositivo de interrogación por radiofrecuencia 105 y el mecanismo de cierre 50 se desactiva, degradando la estructura de cerradura inteligente 1 a cerradura de puerta ordinaria. Sin embargo, el usuario siempre puede desbloquear el mecanismo de cierre de la estructura de cerradura inteligente 1 con su correspondiente llave física en ambos modos.

El interruptor de configuración 515 es un implemento para evitar la modificación no autorizada de la lista de permisos a través de cualquier conexión de Internet o inalámbrica. Si y sólo si el usuario está físicamente presente en la estructura de cerradura inteligente 1 y cambia personalmente la estructura de cerradura inteligente 1 a su modo de configuración, se permite la modificación a través de la base de datos 512 mediante el procesador 511.

El interruptor de llave-móvil 516 también interactúa con el interruptor de configuración 515. Si el interruptor de configuración 515 se enciende, el interruptor de llave-móvil 516 cambia automáticamente a su modo "Sólo Llave". Por lo tanto, el envío de una señal electrónica como el comando de desbloqueo al mecanismo de cierre 50 bajo el modo de configuración de la estructura de cerradura inteligente 1 está por consiguiente bloqueado. Durante el modo de configuración, desbloquear el mecanismo de cierre 50 sólo puede hacerse con una llave física.

Después de introducir toda la información de la lista de permisos, el interruptor de configuración 515 tiene que ser cambiado a su modo de funcionamiento "Normal", bajo el cual la base de datos de la lista de permisos ya no puede ser modificada. Mientras tanto, si el interruptor de llave-móvil 516 se enciende en su modo "Llave y Móvil", el procesador 511 de la estructura de cerradura inteligente 1 puede enviar comandos de desbloqueo al mecanismo de cierre 50.

La FIG. 7 muestra una tabla de operaciones que ilustra la relación entre tres modos de operación, los interruptores de la estructura de cerradura inteligente 1 y el mecanismo de cierre de la misma. El interruptor de configuración 515 y el interruptor de llave-móvil 516 puede ser actuados automática o manualmente por hardware o software. La conexión/desconexión del dispositivo de configuración 20 al módulo 514 para recibir información de autenticación de la estructura de cerradura inteligente 1 habilita/deshabilita automáticamente el modo de configuración de la estructura de cerradura inteligente 1. Además, un usuario puede configurar un programa disponible de llave móvil, basado en el cual la estructura de cerradura inteligente 1 puede ser cambiada automáticamente entre el modo "Sólo llave" y el modo "Llave y móvil".

El mecanismo de cierre 50 puede estar compuesto alternativamente por pestillos de resorte que se retraen mediante una palanca y por cerrojos de seguridad (es decir, la manija 102 como se ha descrito anteriormente) que se extienden y retraen mediante llaves o pomos giratorios (no se muestra). Además de ser controlados manualmente, ambos o cualquiera de los pestillos y/o cerrojos de seguridad son controlados por el dispositivo de interrogación por radiofrecuencia 105 en su modo de funcionamiento normal con el interruptor 516 en su modo "Llave y Móvil". Por otra parte, el mecanismo de cierre 50 podría ser bloqueado por el dispositivo móvil M, es decir, después de desbloquear manualmente la estructura de cerradura inteligente 1 desde el interior de una puerta, el usuario puede bloquear al menos uno de los cerrojos de la estructura de cerradura inteligente 1 interactuando el dispositivo de interrogación por radiofrecuencia 105 con el dispositivo móvil M desde el exterior de la puerta en un período de tiempo determinado.

La estructura de cerradura inteligente puede alimentarse con una energía 517 que utiliza corrientes eléctricas directas de la batería recargable, corrientes eléctricas alternativas, alimentación a través de IEEE 802.3 o 802.3 en el estándar PoE, o energía de las manijas recargables, es decir, balanceando la manija 102 de la estructura de cerradura inteligente 1 para generar la energía necesaria (sólo para las realizaciones de la estructura de cerradura inteligente 1 que equipan manijas). Diseñado para la emergencia, la energía 517 generada por las manijas recargables es diminuta y desbloquea el uso para una sola vez.

La FIG. 8 muestra un diagrama de flujo de la presente invención que ilustra un método de operación utilizado entre el dispositivo de configuración 20 y la estructura de cerradura inteligente 1 en su modo de configuración.

El dispositivo de configuración 20 se selecciona de entre uno de un ordenador portátil, ordenador de escritorio, ordenador de panel, tableta o teléfono móvil equipado con funciones de Ethernet/Wi-Fi/Zig-Bee, USB, Bluetooth, Puerto Serie (RS232,422,485), y/o comunicación de campo cercano. Durante el modo de configuración de la estructura de cerradura inteligente 1, en una etapa de iniciación de configuración 801, tanto el dispositivo de configuración 20 y la estructura de cerradura inteligente 1 deben estar encendidos en sus modos de configuración. En la etapa de iniciación del software 802, se requiere un software de la llave inteligente para que funcione en el dispositivo de configuración 20.

En una etapa de solicitud 803, a través de una red de área local, puerto USB, puerto serie (RS-232/422/485), Bluetooth, o comunicación de campo cercano, un dispositivo móvil o un ordenador de configuración usado como dispositivo de configuración 20 envía una petición de configuración a la estructura de cerradura inteligente 1 con contraseñas para crear, modificar o eliminar cuentas de la lista de permisos en la base de datos 512 de la estructura de cerradura inteligente 1.

En una etapa de determinación 804, después de recibir la solicitud de configuración del dispositivo de configuración 20, la estructura de cerradura inteligente comprueba y determina si al usuario se le permite acceder a la base de datos 512. Si la solicitud es de usuarios no autorizados, en una etapa de denegación 805, la estructura de cerradura inteligente 1 envía comandos para negar la solicitud, para enviar una advertencia a los usuarios autorizados o autoridades seguras afiliadas, y/o para registrar la solicitud de modificación infructuosa. Si la solicitud es de usuarios autorizados con contraseñas correctas, en una etapa de permisión 806, la estructura de cerradura inteligente 1 permite la solicitud de modificación. En una etapa de modificación 807, el usuario permitido crea una cuenta y claves en nombres de usuario, números de teléfono móvil, contraseñas, números de serie del dispositivo móvil M, número MAC del dispositivo móvil M, ICCID del dispositivo móvil M, IMEI de las tarjetas SIM, y/o periodos válidos de autorización para cualquier acceso, y en una etapa de guardado 808, la modificación mencionada anteriormente se guarda en la lista de permisos de la base de datos 512 de la estructura de cerradura inteligente 1 como información de autenticación

para cualquier solicitud de acceso en el futuro. Además, la estructura de cerradura inteligente 1 genera automáticamente una clave de cifrado que se guarda en el dispositivo móvil M y en sí misma.

Después de la configuración, si el dispositivo móvil de configuración 20 es exactamente el mismo dispositivo móvil M que desbloquea la estructura de cerradura inteligente 1, toda la información de identificación relacionada y las identificaciones para usar la estructura de cerradura inteligente 1 se guardan en otra base de datos del software de la llave inteligente en el dispositivo móvil 20 para convertirse en una de las llaves para abrir. En un procedimiento de apertura para el dispositivo móvil 20, este accederá a su base de datos para la clave de desbloqueo.

En caso de que el dispositivo móvil 20 autorice a otro dispositivo móvil M para la entrada de la puerta, el dispositivo móvil de configuración 20 envía una autenticación segura y las identificaciones para usar la estructura de cerradura inteligente 1 al dispositivo móvil específico M, que se utiliza para desbloquear la estructura de cerradura inteligente 1 mediante el software de la llave inteligente, es decir, después de una configuración exitosa, el software de la llave inteligente en el dispositivo de configuración 20 codifica y sube la información de identificación a un servidor específico en una red de área amplia (WAN) por Internet o comunicación móvil inalámbrica. El servidor genera entonces un enlace de Internet hacia la información de identificación en el servidor y reenvía el enlace a un posible usuario por correo electrónico y/o servicio de mensajes cortos. Al recibir el enlace, el posible usuario simplemente hace clic en el enlace para sincronizar la identidad objetivo y la información de autenticación para utilizar la estructura de cerradura inteligente 1 en una base de datos de un software de la llave inteligente en el dispositivo móvil M del usuario. Para verificar la autenticación, el software de la llave inteligente en el dispositivo móvil M comprueba dos veces los números de teléfono móvil, las contraseñas, los números de serie del dispositivo móvil M, los números MAC del dispositivo móvil M, el ICCID del dispositivo móvil M, o IMEI de las tarjetas SIM con las del dispositivo móvil M. Una vez que los datos coincidan, la autorización del dispositivo móvil M para usar la estructura de cerradura inteligente 1 está completamente concedida.

Se pueden crear múltiples cuentas para la lista de permisos mediante una etapa de repetición 809que repite la etapa de permisión 806. La base de datos puede ser modificada ilimitadamente bajo el modo de configuración de la estructura de cerradura inteligente 1 si el usuario autorizado lo solicita. En una etapa de terminación 810, el modo de configuración de la estructura de cerradura inteligente 1 puede ser terminada mediante el apagado del interruptor de configuración 515.

La FIG. 9 es un diagrama de flujo de un método de operación de la presente invención que explica la interacción entre la estructura de cerradura inteligente 1 de la presente invención y el dispositivo móvil M con el software de la llave inteligente instalado como teclas inalámbricas en un modo de operación, o modo normal de la estructura de cerradura inteligente 1 mientras un usuario intenta desbloquear la estructura de cerradura inteligente 1.

Durante el funcionamiento normal, en una etapa inicial 901, la estructura de cerradura inteligente 1 se enciende mientras su modo de configuración está apagado, y el dispositivo de interrogación por radiofrecuencia 105 en espera. Mientras que un usuario tiene la intención de desbloquear la estructura de cerradura inteligente 1, en una etapa de solicitud 902, el usuario enciende el software de lave inteligente instalado en el dispositivo móvil M, teclea las contraseñas requeridas como solicitud de desbloqueo, y presenta el dispositivo móvil M dentro de un rango de transmisión efectivo del dispositivo de interrogación por radiofrecuencia 105 incorporado en la estructura de cerradura inteligente 1.

En una etapa de comunicación 903, con el fin de controlar la estructura de cerradura inteligente 1, el software de la llave inteligente en el dispositivo móvil M comunica con la estructura de cerradura inteligente 1 a través del dispositivo

de interrogación por radiofrecuencia 105 a través de comunicación de campo cercano, Bluetooth, Infra Comunicación Roja, y/o cualquier otro protocolo de comunicación inalámbrica. En respuesta a la petición del teléfono móvil M, en una etapa de respuesta 904, la estructura de cerradura inteligente 1 responde con un valor semilla que abarca respectivamente la identificación y la información de tiempo de la estructura de cerradura inteligente 1 y el dispositivo móvil M para el propósito de decodificación. En una etapa de devolución 905, el software de la llave inteligente elige la información de la llave de cifrado, que coincide con la identificación de la estructura de cerradura inteligente 1 en el valor de semilla de la base de datos del dispositivo móvil M. A través del lector por radiofrecuencia 513, el dispositivo móvil M enviará información de la clave cifrada como se ha configurado previamente, mediante cifrado utilizando la clave de cifrado elegida, incluyendo nombres de usuario, contraseñas, números de teléfono móvil, números de serie del dispositivo móvil M, números MAC del dispositivo móvil M, ICCID del dispositivo móvil M, y/o IMEI de las tarjetas SIM.

Si la información de identificación de la estructura de cerradura inteligente 1 no está en la base de datos del dispositivo móvil M, en una etapa de omisión 906, el dispositivo móvil M muestra la denegación de acceso en el dispositivo móvil M, y la estructura de cerradura inteligente 1 ignora directamente la petición, y vuelve al modo de espera 901.

En una etapa de verificación 907, la estructura de cerradura inteligente 1 descifra los datos clave que se envían desde el dispositivo móvil M e identifica la lista de permisos en la base de datos 512. Si la información/datos descifrados coinciden perfectamente con una de las informaciones listadas en la base de datos 512, en una etapa de desbloqueo 908, la estructura de cerradura inteligente 1 envía una señal electrónica, como un comando de desbloqueo, al mecanismo de cierre 50 para conceder el acceso a recursos específicos o activos para el usuario. Después, la estructura de cerradura inteligente 1 vuelve a la etapa inicial 901 para permanecer en modo de espera y esperar una próxima solicitud de cualquier dispositivo móvil M.

Se activa un mecanismo de protección si la información desencriptada no coincide con ninguna identidad de la lista de permisos de la base de datos 512. Mientras los datos no coincidan, la estructura de cerradura inteligente 1 cuenta el tiempo de fallo e informa al usuario mostrando mensajes de fallo en el dispositivo móvil M para negar la solicitud del usuario. En caso de que el fallo ocurra por debajo de un valor límite, la cerradura inteligente volverá a la etapa de comunicación 903, permitiendo otra prueba.

En un intento de detener el ataque de transmisión de un intruso malintencionado, que probablemente genera señales de radio masivas mediante un dispositivo inalámbrico programable, en una etapa de comprobación 909, la estructura de cerradura inteligente 1 cuenta los fallos de solicitud desbloqueo a través del dispositivo de interrogación por radiofrecuencia 105. En caso de que la estructura de cerradura inteligente 1 detecte que los fallos aumentan anormalmente por encima del límite preestablecido durante un período de tiempo preestablecido, la estructura de cerradura inteligente 1 acumula intervalos de tiempo para retrasar el procesamiento de una próxima solicitud enviada por el dispositivo móvil M.

Aún peor, cuando la invasión maliciosa ocurre continuamente en un cierto período de tiempo, en una etapa de apagado 911, la estructura de cerradura inteligente 1 apaga su mecanismo de desbloqueo inalámbrico y sólo las llaves físicas pueden abrir la puerta. La realización de las etapas 909 y 911 se considera como un Sistema de Prevención de Intrusiones, o "IPS" para la estructura de cerradura inteligente 1.

Instalado por ordenadores o descargado de cualquier plataforma APP móvil, el software de la llave inteligente en el dispositivo móvil M está diseñado para configurar y desbloquear la estructura de cerradura inteligente 1, cifrar las comunicaciones entre el dispositivo interrogador de radiofrecuencia 105, identificar la autenticación del usuario,

seleccionar claves, leer registros de entrada, o monitorizar el estado de la batería de la estructura de cerradura inteligente 1.

En el modo normal/operativo, el cifrado y descifrado de las señales de radiofrecuencia (RF) a través de la comunicación por radiofrecuencia 204 como se muestra en la FIG. 5 es realizado por el software de la llave inteligente en el dispositivo móvil M y la estructura de cerradura inteligente 1. El detalle del cifrado y los procedimientos de descifrado de la comunicación por radiofrecuencia se ilustran a continuación.

Durante un procedimiento abierto de la operación/modo normal, después de que el dispositivo móvil M confirma una respuesta de la estructura de cerradura inteligente 1, el software de la llave inteligente identifica entonces la estructura de cerradura inteligente 1 en una base de datos del dispositivo móvil M, descubre y cifra la información de autenticación correspondiente para evitar que se espíe o se modifiquen los datos.

Para evitar el espionaje, mediante el cual el intruso simplemente graba y copia la frecuencia de radio para confundir al dispositivo de interrogación 105 de la estructura de cerradura inteligente 1, el cifrado del dispositivo de interrogación 105 tal como un dispositivo de interrogación adopta la permutación temporal de las secuencias de datos.

En la etapa de comunicación 903 y la etapa de respuesta 904, el dispositivo móvil M y la estructura de cerradura inteligente 1 sincronizan el tiempo entre sí. El tiempo sincronizado se convierte en parte de un valor inicial para el cifrado entrante. En la etapa de envío 905, el software de la llave inteligente encapsula los nombres de cuentas, la información de autenticación y las contraseñas en diferentes bloques y llena el espacio vacío con datos pseudo aleatorios. Una función, que predefine un tiempo determinado en el valor inicial correspondiente a una secuencia relativa de estos bloques de datos, se incorpora con antelación tanto en el software de la llave inteligente como en el dispositivo de interrogación 105 de la estructura de cerradura inteligente 1. Basándose en la función predefinida, el software de la llave inteligente permuta la secuencia de estos bloques de datos. Por consiguiente, es poco probable que la frecuencia de radio correspondiente al desbloqueo exitoso en diferentes momentos sea idéntica en un determinado intervalo de tiempo, por lo que un intruso no autorizado no puede obtener ningún acceso simplemente copiando la frecuencia de radio de un desbloqueo exitoso en un corto período de tiempo.

Si un intruso no autorizado sigue enviando la copia de las señales de radio de un desbloqueo/entrada previamente exitosa, el dispositivo de interrogación 105 de la estructura de cerradura inteligente 1 se bloquea automáticamente por el "Mecanismo de Prevención de Intrusiones" como se ha descrito anteriormente desde la etapa de comprobación 909 hasta la etapa de apagado 911 después de que el tiempo de fallo sea superior a un valor límite preestablecido.

Para prevenir cualquier modificación de datos, la comunicación inalámbrica entre el dispositivo móvil M y la estructura de cerradura inteligente 1 puede aplicar cifrado de clave simétrica o asimétrica para cifrar su transmisión datos como un segundo o siguiente paso en el cifrado.

Durante la etapa de guardado 808 del modo de configuración, el software de la llave inteligente genera un par de claves privadas para el cifrado y descifrado guardadas en el dispositivo móvil M y en la estructura de cerradura inteligente 1 utilizando un método de cifrado en flujo. Ningún otro dispositivo móvil M o usuario comparte una misma clave criptográfica utilizada en una estructura de cerradura inteligente 1 o en el dispositivo de interrogación 105 de la misma. En caso de que también se aplique un método de cifrado por bloques bajo criptografía simétrica, se guardan múltiples pares de claves para los respectivos bloques de datos de autenticación tanto en el dispositivo móvil M como en la estructura de cerradura inteligente 1.

La criptografía de clave simétrica incluye Twofish, Serpent, Blowfish, Data Encryption Standard, 3DES, CAST5, RC4, IDEA, Advanced Encryption Standard, o cualquier algoritmo conocido como criptografía de clave simétrica.

En algunas realizaciones comerciales, hay demasiados usuarios que comparten un dispositivo de interrogación 105 o la distribución de una clave criptográfica privada es técnica o comercialmente difícil. Alternativamente, se aplica la criptografía de clave asimétrica en estas realizaciones. Se establecen de antemano un par de claves públicas criptográficas para el cifrado y una clave privada para el descifrado. La clave privada está instalada en el dispositivo de interrogación 105 para descifrar los datos del dispositivo móvil M. La correspondiente llave pública está incrustada en el software de llave inteligente descargado en el dispositivo móvil M para cifrar los datos de transmisión.

Una vez que un usuario es autorizado por cualquier autoridad a entrar en un área especial custodiada por el dispositivo de interrogación 105 de la estructura de cerradura inteligente 1, obtiene datos encriptados leídos sólo por el software de la llave inteligente a través del correo electrónico y/o el Servicio de Mensajes Cortos. Para verificar la autenticación, el software de la llave inteligente del dispositivo móvil M comprueba dos veces la información recibida, incluidos los números de teléfono móvil, las contraseñas, los números de serie del dispositivo móvil M, los números MAC del dispositivo móvil M, el ICCID del dispositivo móvil M, o el IMEI de las tarjetas SIM con los del dispositivo móvil M recibido. Mientras que el dispositivo móvil M concedido se presenta en un rango efectivo del dispositivo de interrogación 105, el software de llave inteligente cifra la información de autenticación mediante la clave pública criptográfica y la envía al dispositivo de interrogación 105 en las etapas 905 a 907 para su identificación.

La clave privada criptográfica del dispositivo de interrogación 105 y cualquier nuevo software que incluya la correspondiente clave pública pueden actualizarse regularmente.

La criptografía de clave asimétrica incluye RSA, El Gamal, el protocolo de intercambio de claves Diffie-Hellman, DSS (Digital Signature Standard), varias técnicas de curva elíptica, varias técnicas de clave autenticada con contraseña, criptosistema Paillier, criptosistema Cramer- Shoup, o cualquier algoritmo conocido como criptografía de clave asimétrica.

A la inversa, el dispositivo de interrogación 105 en la estructura de cerradura inteligente 1 decodifica los datos transmitidos por las claves criptográficas simétricas o asimétricas previamente guardadas en la base de datos 512, como se muestra en la etapa de guardado 808, compara los datos decodificados con la información de autenticación original y las contraseñas, e interroga a los datos recibidos dentro de la lista de permisos de los mismos. Este descifrado se realiza mediante el procesador 511 o el chipset de descifrado/encriptación 518.

El dispositivo de Interrogación 105 con los métodos de cifrado descritos anteriormente está instalado no sólo en la estructura de cerradura inteligente 1, sino también en una máquina expendedora, sistema de tickets o sistemas de control de acceso público. Con el acceso autorizado desde el software en un dispositivo móvil, el usuario puede acceder a determinados bienes, áreas o recursos controlado por el dispositivo de interrogación 105.

Un dispositivo móvil M se almacena con juegos de llaves plurales en el software de la llave inteligente para desbloquear las respectivas estructuras de la cerradura inteligente 1. Como se presenta cerca de la estructura 1 de la cerradura inteligente, una de las llaves establecidas en el dispositivo móvil M para la respectiva estructura de cerradura inteligente 1 es capaz de elegirse manualmente, vocalmente o automáticamente de acuerdo con los datos de identificación proporcionados por la estructura de cerradura inteligente 1 en particular, o de acuerdo con los servicios de localización a través de GPS, puntos de acceso Wi-Fi de la multitud o ubicaciones de torres celulares.

La pérdida del teléfono móvil M con el software de la llave inteligente probablemente abre el acceso a cualquier descubridor no autorizado que se haga pasar por una entidad de autenticación. Para mejorar la seguridad, el software de la llave inteligente puede ser configurado para solicitar contraseñas o autenticación biométrica, como el reconocimiento de voz o de rostro, para activar el software de la llave inteligente o para desbloquear la estructura de cerradura inteligente 1.

Con la debida autorización, el usuario puede usar el software de la llave inteligente para leer los registros de acceso en la estructura de cerradura inteligente. La alarma o la actualización instantánea de la entrada no autorizada/incorrecta desde la estructura de cerradura inteligente 1 puede ser enviada a un teléfono móvil de los administradores por Internet o GSM. Además, el usuario puede ser informado del estado de la batería de la estructura de cerradura inteligente 1 desde el software de la llave inteligente del dispositivo móvil M

REIVINDICACIONES

1. Una estructura de cerradura inteligente (1), en la que la estructura de cerradura inteligente comprende:

un agujero para llaves (101) para que las llaves de acceso desbloqueen la estructura de cerradura inteligente (1) para el acceso a las áreas aseguradas;

un dispositivo de interrogación (105) para configurar una lista de permisos de los usuarios para el acceso asegurado por la estructura de la cerradura inteligente (1) y para usar la tecnología de radiofrecuencia para comunicarse con un dispositivo móvil (M) y aceptar las solicitudes de acceso del dispositivo móvil (M) para desbloquear la estructura de cerradura inteligente (1) sin utilizar las llaves de acceso en el agujero para llaves (101); y

un mecanismo de bloqueo (50) que reacciona a una interacción entre el agujero para llaves (101) y el acceso o que reacciona a la comunicación entre el dispositivo de interrogación (105) y el dispositivo móvil (M) para desbloquear la estructura de cerradura inteligente (1) y obtener un privilegio de acceso;

donde el dispositivo de interrogación (105) de la estructura de cerradura inteligente (1) comprende:

un lector de radiofrecuencia (513) para transmitir y recibir datos de radiofrecuencia de la comunicación entre el lector de radiofrecuencia (513) y el dispositivo móvil (M), en el que el lector de radiofrecuencia (513) utiliza la tecnología de radiofrecuencia para recibir una solicitud enviada desde el dispositivo móvil (M) y, en consecuencia, responder al dispositivo móvil (M) enviando un valor de semilla al dispositivo móvil (M), y entonces el dispositivo móvil (M) devuelve una información de autenticación después de recibir el valor de semilla del lector de radiofrecuencia (513), en el que la información de autenticación en el dispositivo móvil (M) está cifrada por un dispositivo criptográfico que se elige, utilizando el valor de la semilla, de una base de datos del dispositivo móvil (M), de tal manera que ningún otro usuario comparta una misma clave criptográfica utilizada en la respectiva estructura de cerradura inteligente (1); y

un procesador (511) para desencriptar y encriptar la información de autenticación recibida desde el dispositivo móvil (M) para evitar la lectura/escritura no autorizada, en la que el procesador (511) descifra y verifica la información de autenticación del dispositivo móvil (M) según una primera base de datos preestablecida de la estructura de la cerradura inteligente (1), en la que durante el descifrado de la información de autenticación realizado por la estructura de cerradura inteligente (1), la estructura de cerradura inteligente (1) utiliza diferentes claves criptográficas de acuerdo con diferentes usuarios que poseen el acceso protegido por la estructura de cerradura inteligente (1), y en el que se recupera la información de autenticación desde el dispositivo móvil (M) a través del lector de radiofrecuencia (513), y el procesador (511) guarda la información de autenticación cifrada durante un modo de configuración de la estructura de cerradura inteligente (1), y el procesador (511) encripta y desencripta además los datos recibidos del dispositivo móvil (M) a través del lector de radiofrecuencia (513) durante un modo de funcionamiento normal de la estructura de cerradura inteligente (1), e identifica la información de autenticación recuperada de la información de datos recibida, y envía un comando de desbloqueo para desbloquear la estructura de cerradura inteligente (1) basado en un resultado de identificación de la información de autenticación, en la que para

detener un ataque de transmisión por un intruso malintencionado que genera señales de radio masivas por un sistema programable a través de un dispositivo inalámbrico, la estructura de cerradura inteligente (1) cuenta los fallos de la solicitud de desbloqueo a través del dispositivo de interrogación (105) de forma que cuando la estructura de cerradura inteligente (1) detecta que los fallos aumentan anormalmente sobre un valor límite preestablecido durante un período de tiempo preestablecido, la estructura de cerradura inteligente (1) acumula intervalos de tiempo para retrasar la tramitación de una próxima solicitud abierta por el dispositivo móvil (M), o cuando la invasión maliciosa se produce continuamente en un determinado período del tiempo, la estructura de cerradura inteligente (1) cierra la comunicación entre el dispositivo de interrogación (105) y el dispositivo móvil (M) mientras que sólo permite que el agujero para llaves (101) desbloquee el mecanismo de cierre (50); y

una base de datos (512) en forma de memoria para guardar la información de autenticación cifrada

2.- Estructura de cerradura inteligente (1), según la reivindicación 1, que comprende además un dispositivo a prueba de fallos (103) equipado junto al dispositivo de interrogación (105) para prevenir el fallo del dispositivo móvil (M) cuando el dispositivo móvil (M) se utiliza para comunicar con el dispositivo de interrogación (105).

3.- Estructura de cerradura inteligente (1), según la reivindicación 1, **caracterizada porque** se proporciona un valor de semilla al procesador (511) desde el dispositivo móvil (M), se preestablece una función de permutación en la base de datos (512) para que el procesador (511) permute las secuencias de datos de la información de autenticación basada en el valor de semilla y para que el procesador (511) además cifre y descifre la información de autenticación.

4.- Estructura de cerradura inteligente (1), según la reivindicación 1, **caracterizada porque** el dispositivo de interrogación (105) comprende además un modulo (514) para recibir la información de autenticación antes de que se guarde durante la configuración de la estructura de cerradura inteligente.

5.- Estructura de cerradura inteligente (1), según la reivindicación 1, **caracterizada porque** el dispositivo de interrogación (105) comprende además un interruptor de configuración (515) para permitir la configuración de la estructura de cerradura inteligente (1).

6.- Estructura de cerradura inteligente (1), según la reivindicación 1, **caracterizada porque** el dispositivo de interrogación (105) comprende además un interruptor de llave móvil (516) para controlar la ruta del dispositivo de interrogación (105) que envía un comando de desbloqueo al mecanismo de cierre (50).

7.- Estructura de cerradura inteligente (1), según la reivindicación 1, **caracterizada porque** el dispositivo de interrogación (105) comprende además un chipset (518) para cifrar o descifrar los datos transmitidos o recibidos a través del lector de radiofrecuencia (513).

8.- Estructura de cerradura inteligente (1), según la reivindicación 1, **caracterizada porque** la estructura de cerradura inteligente incluye tres modos básicos: un modo de configuración, un modo de operación, y un modo de llave, donde el modo de operación es el modo por defecto de la estructura de cerradura inteligente (1).

9.- Estructura de cerradura inteligente (1), según la reivindicación 1, **caracterizada porque** el valor de semilla comprende al menos una de información de identificación del dispositivo móvil (M), información de identificación de la estructura de cerradura inteligente (1), y una un tiempo de sincronización predeterminado entre el dispositivo móvil (M) y el dispositivo de interrogación (105).

10.- Estructura de cerradura inteligente (1), según la reivindicación 1, **caracterizada porque** cuando el dispositivo móvil (M) devuelve la información de la llave cifrada, el dispositivo móvil (M) permuta la secuencia de datos de la información de la llave.

11.- Estructura de cerradura inteligente (1), según la reivindicación 1, **caracterizada porque** comprende además la configuración de la estructura de cerradura inteligente (1) antes de que la estructura de cerradura inteligente (1) reciba una solicitud de desbloqueo del dispositivo móvil (M), que comprende:

al menos un dispositivo de configuración seleccionado de entre el dispositivo móvil (M) y otros ordenadores de configuración que solicitan la configuración de la estructura de cerradura inteligente (1) para modificar una lista de permisos en la primera base de datos preestablecida de la estructura de cerradura inteligente (1);

la estructura de cerradura inteligente (1) que verifica el acceso de al menos un dispositivo de configuración a la primera base de datos preestablecida;

al menos un dispositivo de configuración que modifica la lista de permisos de la estructura de cerradura inteligente (1); y

la estructura de la cerradura inteligente (1) que guarda la modificación de la lista de permisos en la primera base de datos preestablecida para la autenticación para desbloquear la estructura de cerradura inteligente (1).

12.- Estructura de cerradura inteligente (1), según la reivindicación 1, **caracterizada porque** la modificación de la lista de permisos comprende el crear al menos una de un cuenta y claves en nombres de usuarios, teléfonos móviles, contraseñas, números de serie del dispositivo móvil (M), números MAC del dispositivo móvil (M), ICCID del dispositivo móvil (M), IMEI de las tarjetas SIM, y períodos válidos de autorización para cualquier acceso.

13.- Estructura de cerradura inteligente (1), según la reivindicación 1, **caracterizada porque** cuando se crea una cuenta, la estructura de cerradura inteligente (1) genera automáticamente una clave criptográfica correspondiente de acuerdo con una de las criptografías de clave simétrica y asimétrica que se guardará tanto en el dispositivo móvil (M) como en la estructura de cerradura inteligente (1) para el cifrado y descifrado del uso del dispositivo móvil (M) y la estructura de cerradura inteligente (1).

14.- Estructura de cerradura inteligente (1), según la reivindicación 1, **caracterizada porque** comprende además una etapa del dispositivo de interrogación (105) que cuenta los tiempos de fallo de la información clave verificada que no coinciden en la primera base de datos preestablecida, y que comprueba si los tiempos de fallo contados son mayores que un valor límite durante un período de tiempo preestablecido.

15.- Estructura de cerradura inteligente (1), según la reivindicación 1, **caracterizada porque** comprende además una etapa de bloqueo de la estructura de cerradura inteligente (1) mediante el dispositivo móvil (M), en el que después de desbloquear manualmente la estructura de cerradura inteligente (1) dentro de una puerta, la estructura de cerradura inteligente (1) se bloquea al menos uno de los cierres interactuando el dispositivo de interrogación por radiofrecuencia (105) con el dispositivo móvil (M) en un período de tiempo determinado.

FIG. 1A

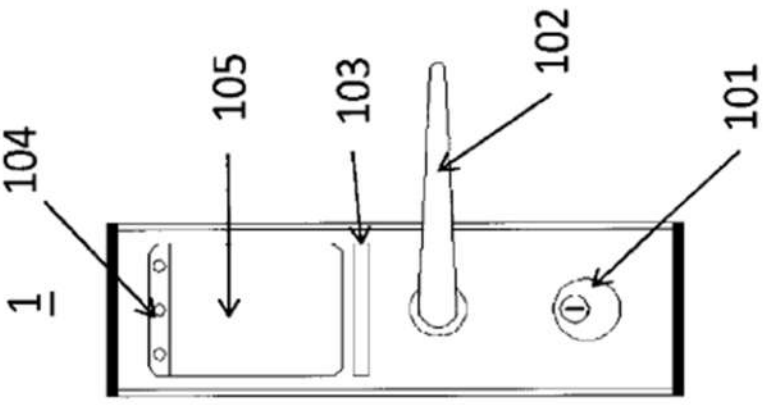


FIG. 1B

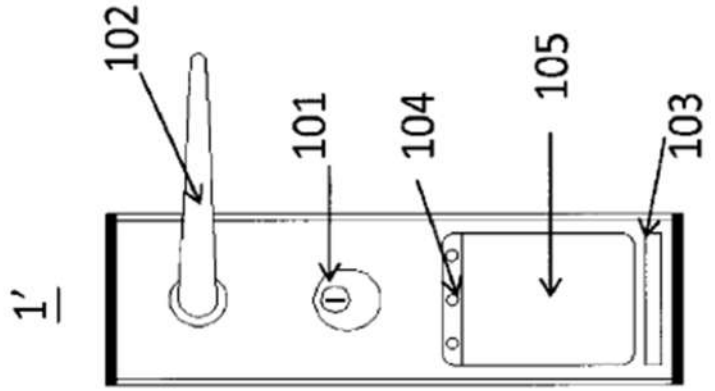


FIG. 1C

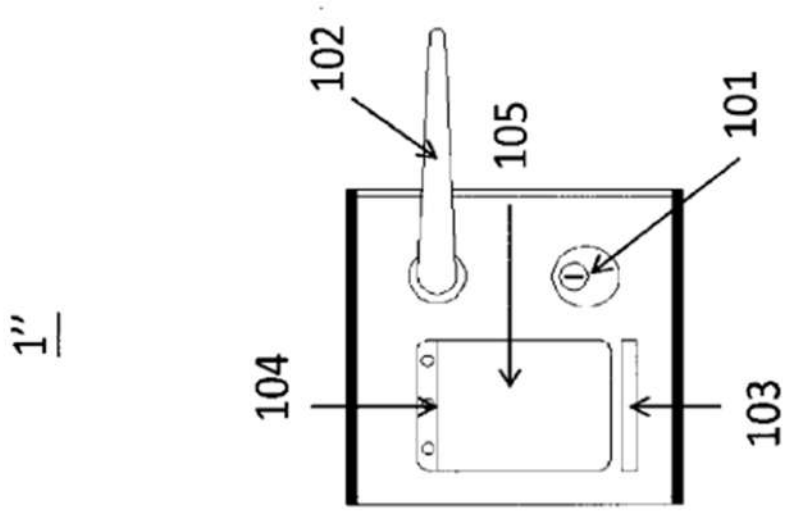


FIG. 2B

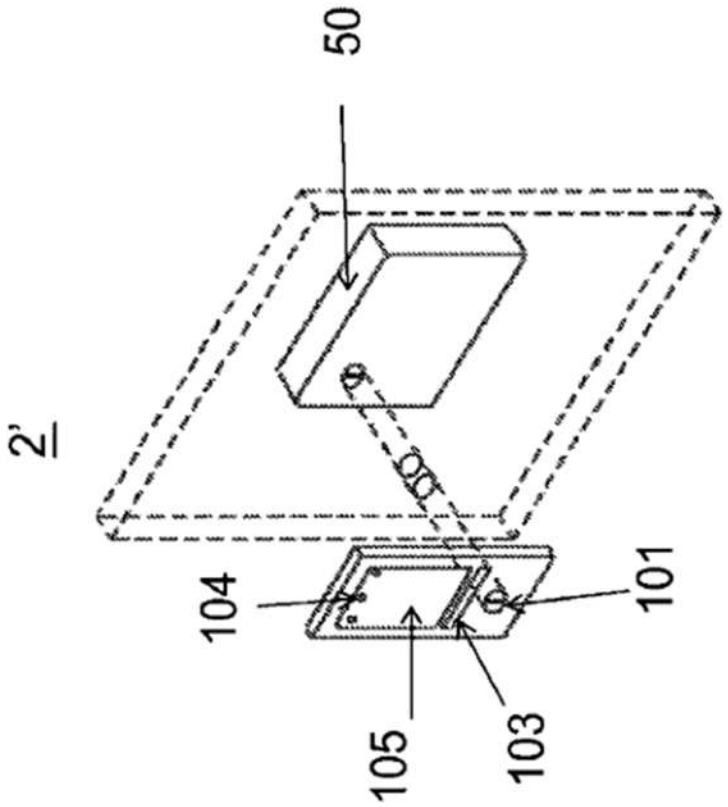


FIG. 2A

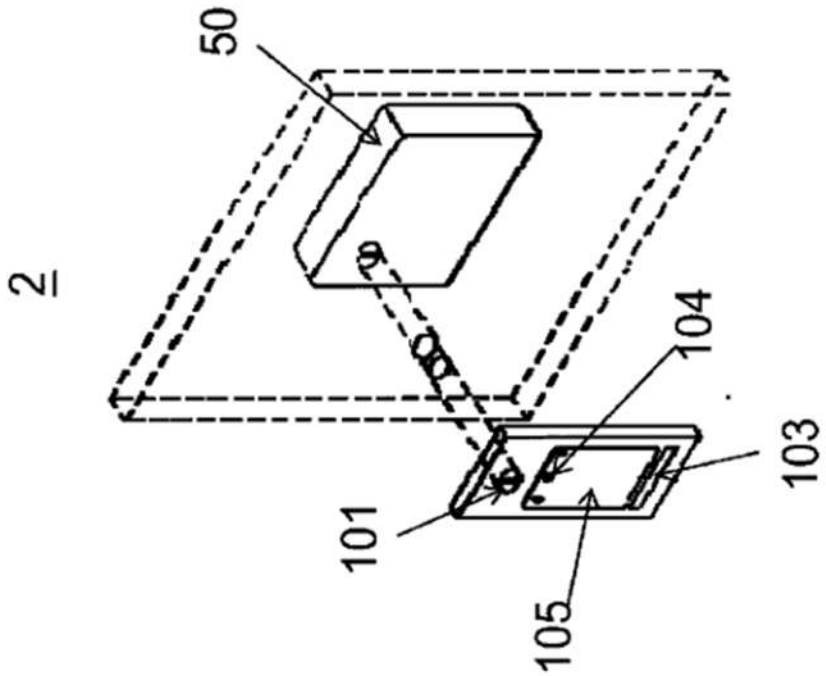


FIG. 3

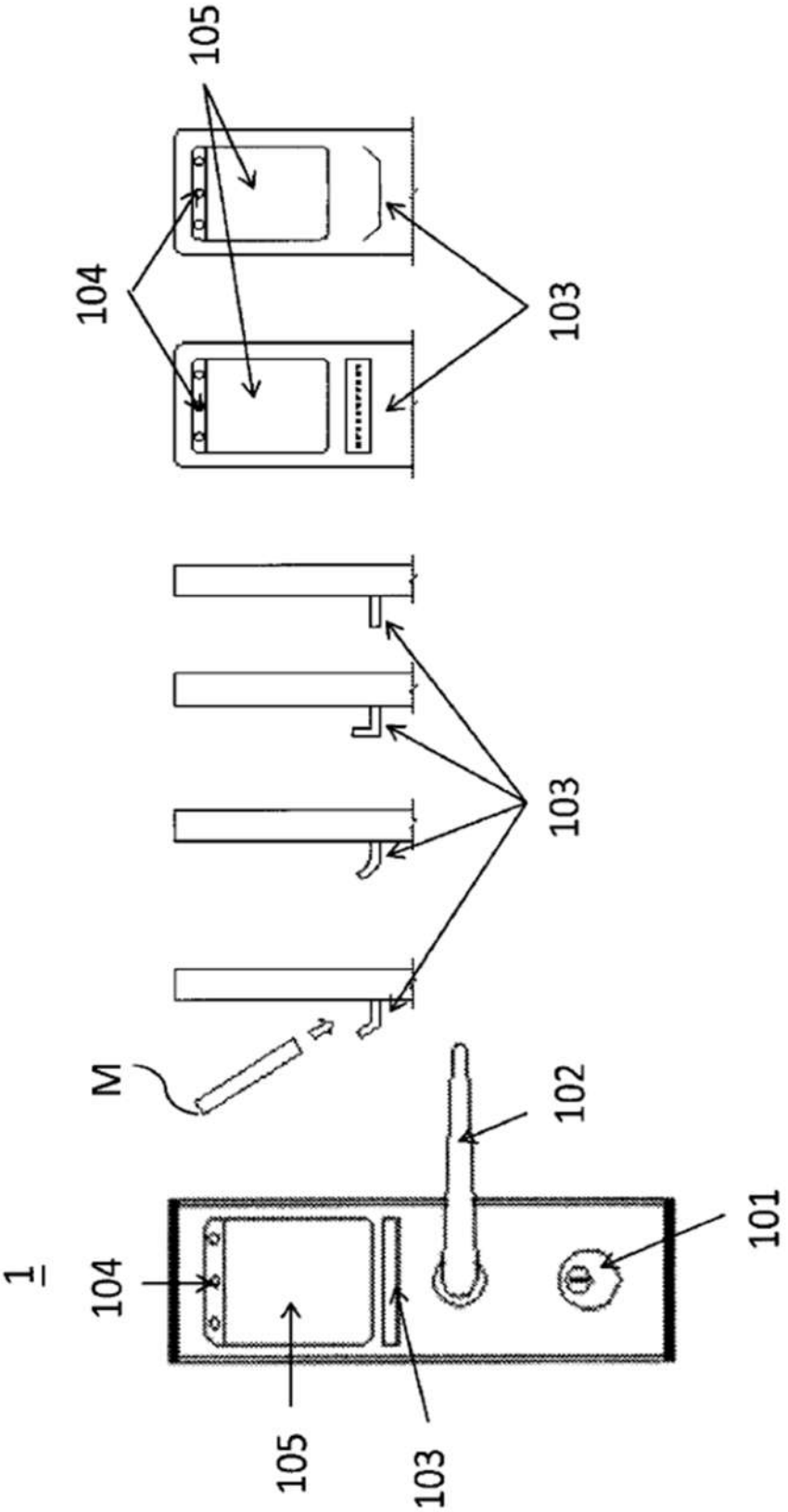


FIG. 4

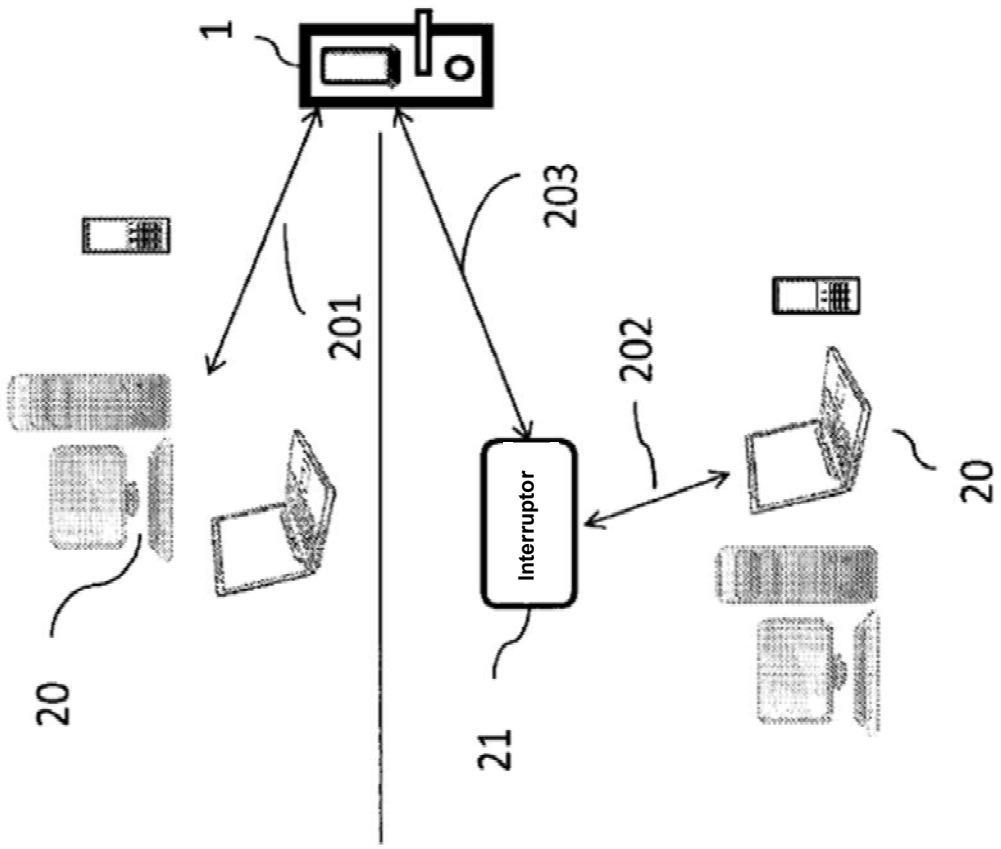


FIG. 5

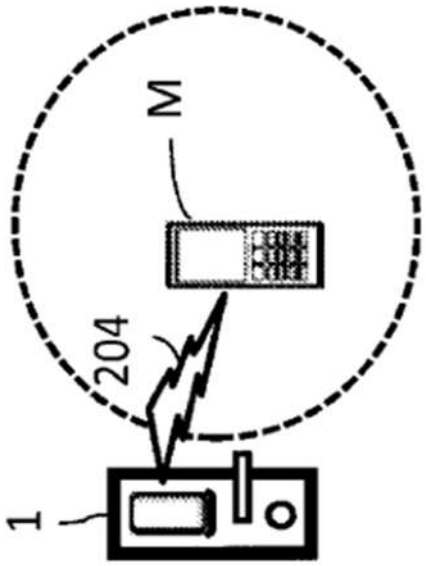


FIG. 6A

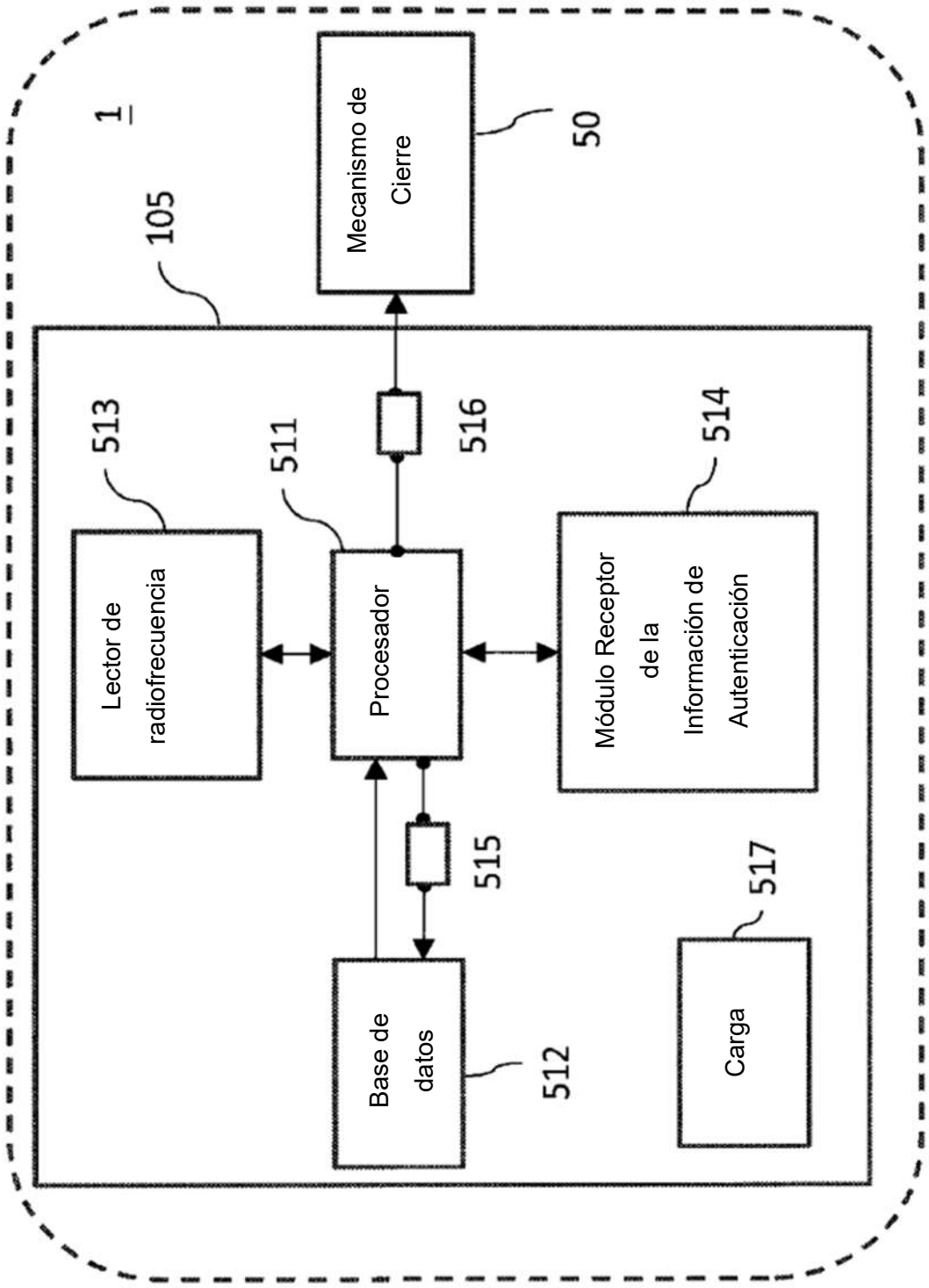

1
105
Mecanismo de Cierre
50
513
511
516
514
Lector de radiofrecuencia
Procesador
Módulo Receptor de la Información de Autenticación
515
517
Base de datos
512
Carga

FIG. 6B

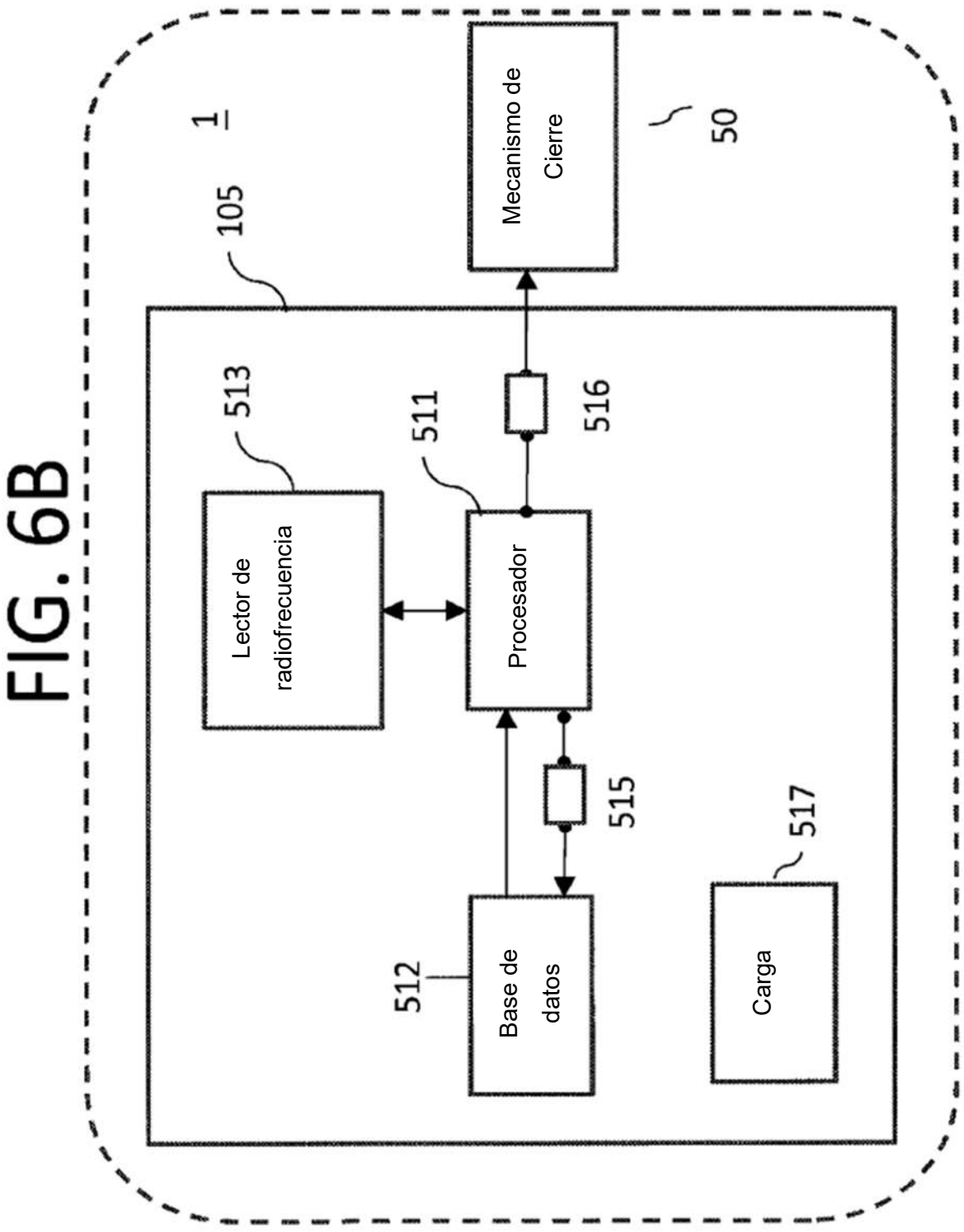

1
105
Mecanismo de Cierre
50
513
511
516
Lector de radiofrecuencia
Procesador
515
517
512
Base de datos
Carga

FIG. 6C

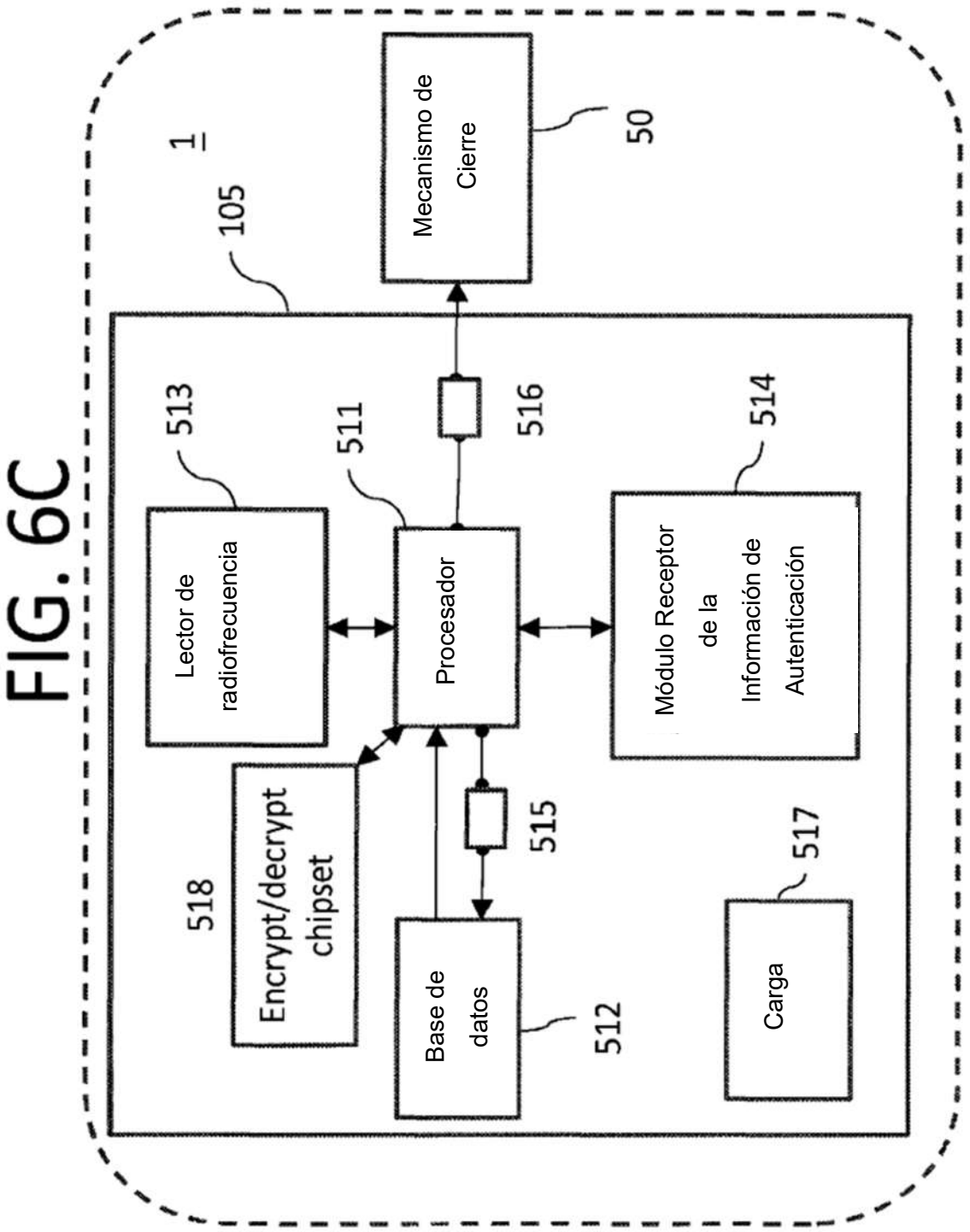

1
105
Mecanismo de Cierre
50
513
511
516
514
Lector de radiofrecuencia
Procesador
Módulo Receptor de la Información de Autenticación
518
Encrypt/decrypt chipset
515
517
Base de datos
512
Carga

FIG. 6D

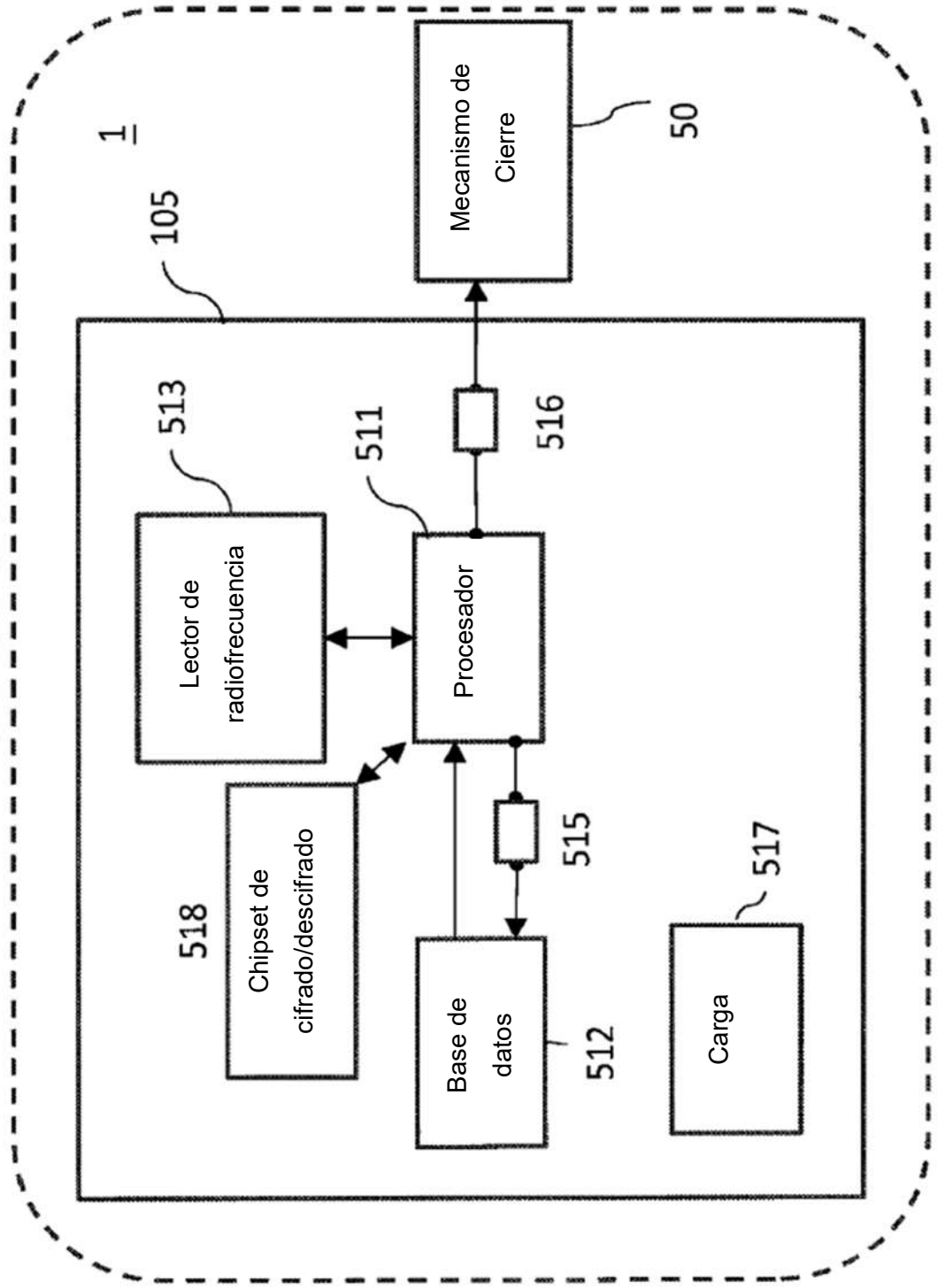

1
105
Mecanismo de Cierre
50
513
511
516
Lector de radiofrecuencia
Procesador
518
Chipset de cifrado/descifrado
515
517
Base de datos
512
Carga

FIG. 7

Modo	Interruptor de configuración 515	Interruptor de llave móvil 516	Configura la lista de permisos	Desbloqueo mediante el dispositivo móvil	Desbloqueo mediante llave física
Configuración	Encendido	Solo Llave	Permitido	No	Si
Operación	Apagado	Llave y Móvil	No Permitido	Si	Si
Solo llave física	Apagado	Solo Llave	No Permitido	No	Si

FIG. 8

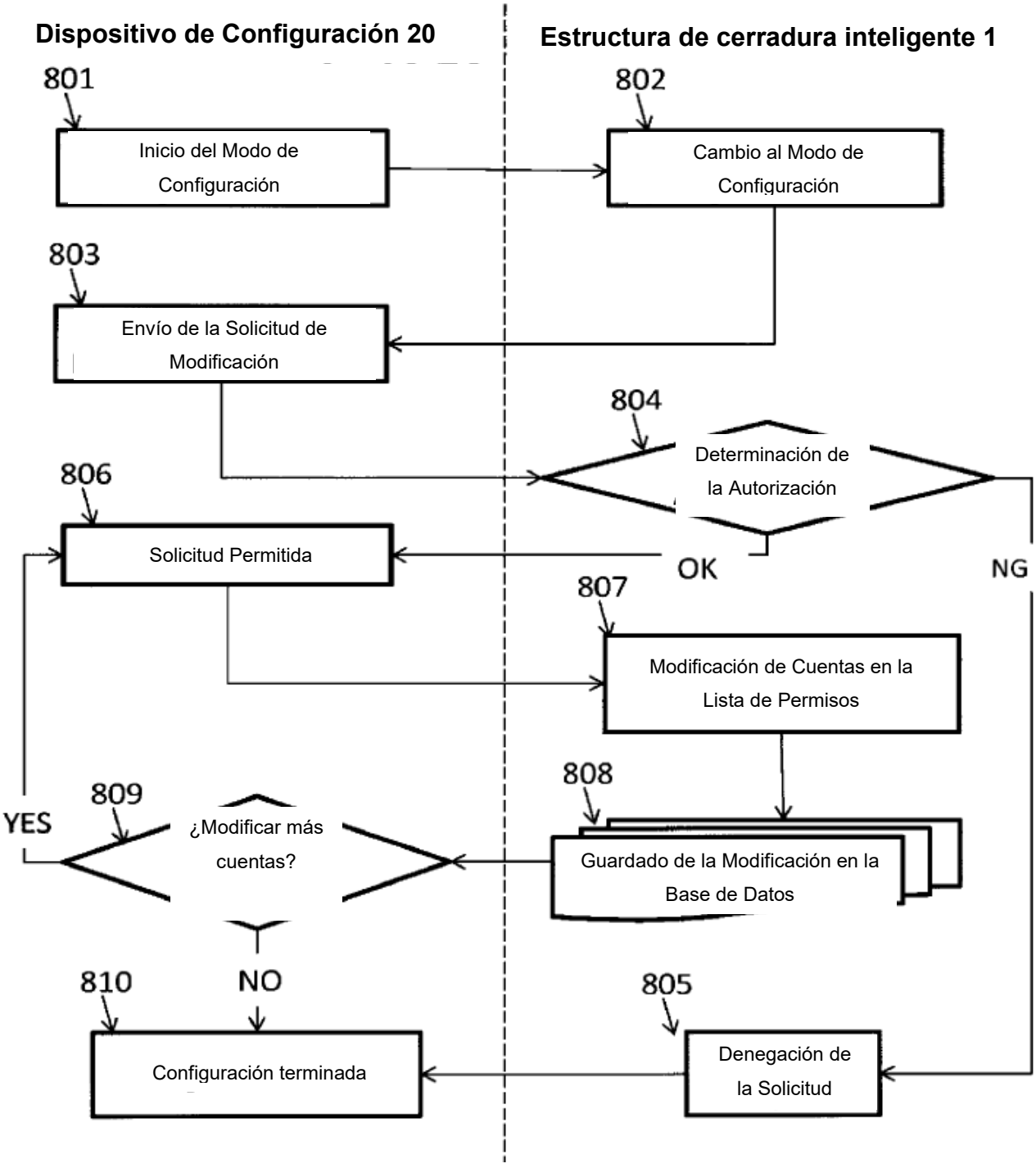
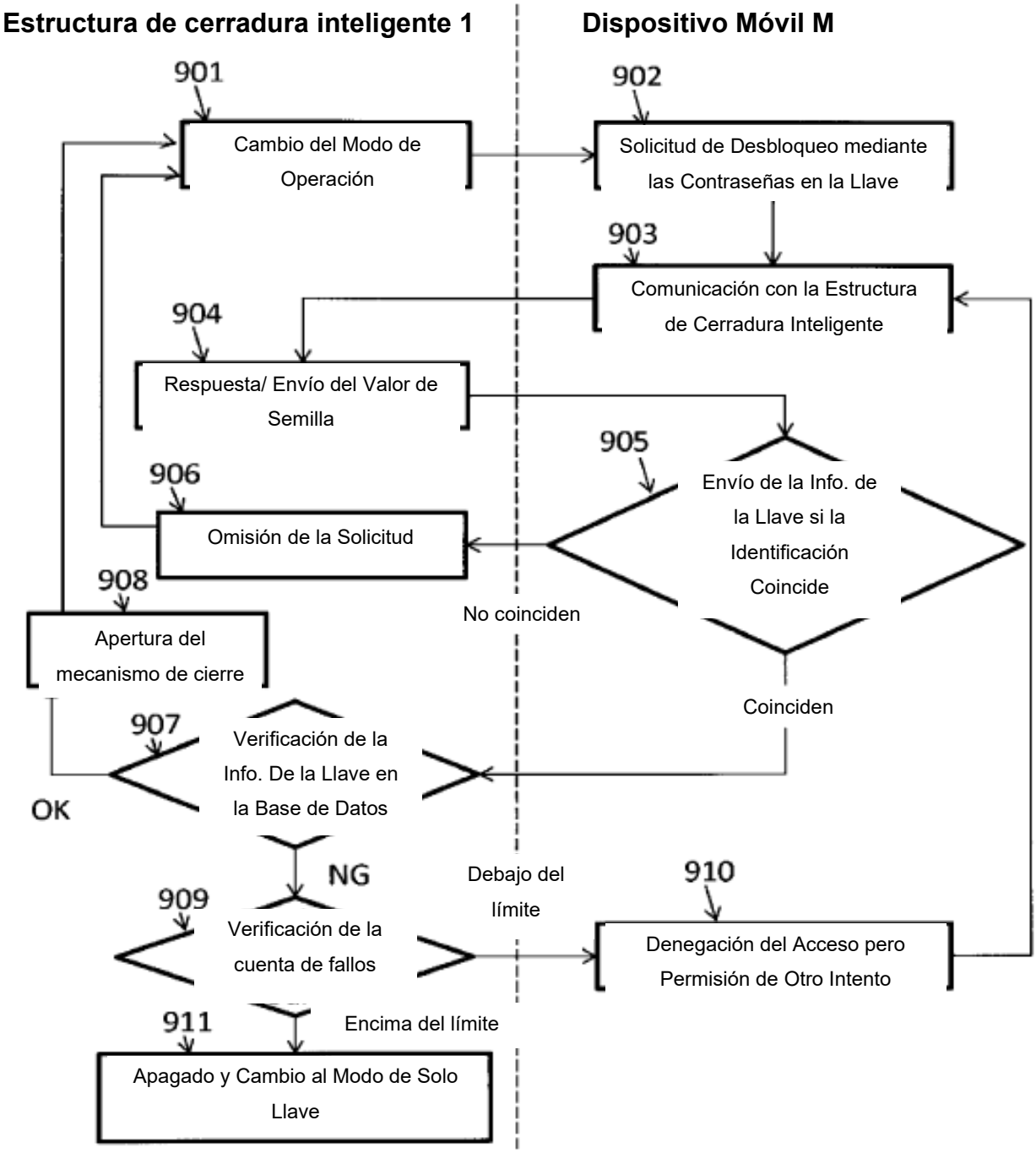

Dispositivo de Configuración 20
Estructura de cerradura inteligente 1
801
Inicio del Modo de Configuración
802
Cambio al Modo de Configuración
803
Envío de la Solicitud de Modificación
804
Determinación de la Autorización
OK
NG
806
Solicitud Permitida
807
Modificación de Cuentas en la Lista de Permisos
808
Guardado de la Modificación en la Base de Datos
809
¿Modificar más cuentas?
YES
NO
810
Configuración terminada
805
Denegación de la Solicitud

FIG. 9


Estructura de cerradura inteligente 1
Dispositivo Móvil M
901
Cambio del Modo de Operación
902
Solicitud de Desbloqueo mediante las Contraseñas en la Llave
903
Comunicación con la Estructura de Cerradura Inteligente
904
Respuesta/ Envío del Valor de Semilla
905
Envío de la Info. de la Llave si la Identificación Coincide
906
Omisión de la Solicitud
No coinciden
908
Apertura del mecanismo de cierre
Coinciden
907
Verificación de la Info. De la Llave en la Base de Datos
OK
NG
909
Verificación de la cuenta de fallos
Debajo del límite
910
Denegación del Acceso pero Permisión de Otro Intento
911
Encima del límite
Apagado y Cambio al Modo de Solo Llave