(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 390 797**

(51) Int. CI.:
G07C 9/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **08162655 .8**
(96) Fecha de presentación: **20.08.2008**
(97) Número de publicación de la solicitud: **2157552**
(97) Fecha de publicación de la solicitud: **24.02.2010**

(54) Título: **Bloqueo electromecánico**

(45) Fecha de publicación de la mención BOPI:
16.11.2012

(45) Fecha de la publicación del folleto de la patente:
16.11.2012

(73) Titular/es:
ILOQ OY (50.0%)
Elektroniikkatie 11
90590 Oulu, FI

(72) Inventor/es:
PUKARI, MIKA

(74) Agente/Representante:
DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Bloqueo electromecánico.

Campo de aplicación

El invento se refiere a los bloqueos electromecánicos.

Antecedentes

Los bloqueos mecánicos tradicionales están siendo sustituidos por diversos tipos de bloqueo electromecánicos. Dichos bloqueos electromecánicos requieren un suministro externo de energía eléctrica, una batería dentro del bloqueo, una batería dentro de la llave, o unos medios para la generación de energía eléctrica dentro de dicho bloqueo, que hacen que el usuario suministre la energía al bloqueo. Los bloqueos electromecánicos tienen muchas ventajas con respecto a los bloqueos tradicionales. Proporcionan una mayor seguridad y el control de las llaves o fichas de seguridad es más fácil.

Además, la mayoría de los bloqueos electromecánicos y/o llaves y fichas de seguridad son programables. Es posible programar el bloqueo para aceptar llaves diferentes y rechazar otras.

Un problema inherente a todos los tipos de sistemas de bloqueo es la distribución de la llave o ficha de seguridad. Las llaves y fichas de seguridad deben ser distribuidas a los usuarios. Por otra parte, los usuarios tienen varias llaves y fichas de seguridad a su disposición, lo cual puede dar lugar a un manejo incómodo de dichas llaves y fichas.

El documento EP 1288841A expone un sistema de control de acceso para un vehículo. Para desbloquear el vehículo, dicho vehículo y un dispositivo transpondedor portátil se comunican por medio de un método pasivo de comunicación de respuesta. El sistema de control de acceso incluye unos sensores acoplados a las manillas de las puertas del vehículo que están conectados a una unidad de control en la estación base, de modo que cuando el usuario tira de la manilla de la puerta del vehículo para abrir una puerta del mismo se envía una señal desde el correspondiente sensor a la unidad de control en la estación base, que responde a esta señal preguntando al dispositivo transpondedor portátil mediante el envío de una señal de activación seguida por una señal de interrogación, que incluye un número aleatorio encriptado y un código de identificación de la estación base. El dispositivo transpondedor portátil recibe la señal de interrogación a través del enlace LF y verifica que la pregunta corresponde a una pregunta válida de su estación base correspondiente. Si la interrogación es válida, el dispositivo transpondedor portátil responde transmitiendo los datos de identificación que tiene guardados en una memoria a través del enlace UHF a la unidad de control de la estación base, estando los datos de identificación encriptados mediante el número aleatorio transmitido por la unidad de control de la estación base. Dicha unidad de control de la estación base desencripta y verifica los datos de identificación transmitidos por el dispositivo transpondedor portátil y, si la identificación es válida, permite el desbloqueo de los bloqueos.

Breve descripción

De acuerdo con un aspecto del presente invento se ha proporcionado un bloqueo electromecánico como el especificado en la reivindicación 1.

De acuerdo con otro aspecto del presente invento se ha proporcionado un método para el funcionamiento de un bloqueo electromecánico como el especificado en la reivindicación 14.

El invento tiene diversas ventajas. El sistema descrito de bloqueo electrónico y de llave así como las soluciones inalámbricas minimizan el consumo de energía en un bloqueo inalámbrico ya que permiten unas soluciones de bloqueo autoalimentado así como un período de tiempo operativo largo en las soluciones de bloqueo alimentado por batería.

En una realización del invento se utiliza una llave electrónica inalámbrica que abre un bloqueo electrónico inalámbrico. La llave es llevada por una persona como una pieza de su dispositivo inalámbrico de comunicación y puede estar provista de un dispositivo de Comunicación de Campo Cercano (NFC).

Las realizaciones del invento pueden aplicarse a bloqueos electromecánicos que tienen un suministro de energía externo, una batería dentro del dispositivo de bloqueo o dentro de la llave o unos bloqueos electromecánicos con energía suministrada por el usuario.

Relación de dibujos

A continuación se describen unas realizaciones del presente invento, a modo de ejemplo solamente, que hacen referencia a los dibujos que se acompañan, en los que:

la Figura 1A ilustra una realización de un sistema electrónico de autentificación;

la Figura 1B ilustra una realización de un sistema electrónico de bloqueo autoalimentado;

la Figura 2 ilustra una realización de una unidad de comunicación;

la Figura 1B ilustra una realización de un sistema electrónico de bloqueo autoalimentado;

la Figura 2 ilustra una realización de una unidad de comunicación;

las Figuras 3A, 3B y 3C son diagramas de flujos que ilustran unas realizaciones; y

las Figuras 4A, 4B, 4C y 4D ilustran unas realizaciones de un sistema electrónico de bloqueo.

Descripción de las realizaciones

Las siguientes realizaciones lo son a modo de ejemplo. Aunque la especificación puede referirse a “una”, o “alguna” realización o realizaciones en algunos lugares, esto no significa necesariamente que cada una de tales referencias lo sean a la misma o mismas realizaciones, o que la característica solamente corresponda a una única realización. Las características únicas de realizaciones diferentes pueden también ser combinadas para proporcionar otras realizaciones.

En una realización del invento se utiliza una llave electrónica para abrir inalámbricamente un bloqueo electromecánico inalámbrico. La llave puede ser llevada por una persona como parte de su dispositivo de comunicación inalámbrica. La Figura 1A muestra una realización de un sistema de bloqueo electrónico. Un usuario 105 va a abrir una puerta 115. El usuario tiene un dispositivo de comunicación 106.

Dicho dispositivo de comunicación 106 es un dispositivo calculador portátil. Tales dispositivos de cálculo incluyen unos dispositivos móviles de comunicación inalámbrica que funcionan con o sin un módulo de identificación de abonado (SIM), que incluyen, aunque no están limitados a, los siguientes tipos de dispositivos: teléfono móvil, teléfono inteligente, asistente digital personal (PDA), microteléfono. El dispositivo de comunicación 106 puede tener una conexión de canal de red inalámbrica 104 a una red inalámbrica 102. La conexión de canal de red inalámbrica 104 y la red inalámbrica 102 pueden ser puestas en práctica de acuerdo con el GSM (Sistema Global de Comunicaciones Móviles), el WCDMA (Acceso Múltiple de Banda Ancha por División de Códigos), la WLAN (Red Inalámbrica de Área Local) o cualquier otro medio de comunicación inalámbrica normalizada / no normalizada.

En una realización el dispositivo de comunicación 106 comprende un Módulo de Identificación de Abonado (SIM) o una Tarjeta Universal de Circuitos Integrados (UICC). El SIM y la UICC se usan en los sistemas de comunicación móvil para la identificación de los abonados. Cada dispositivo de comunicación de un sistema dado comprende tal identificación. El SIM y la UICC tienen un circuito integrado capaz de realizar cálculos y guardar datos.

El dispositivo de comunicación 106 está equipado con una unidad de comunicación inalámbrica de corto alcance configurada para comunicar con otras unidades respectivas tras la detección de tal unidad.

En una realización la comunicación inalámbrica de corto alcance se realiza con una técnica de Comunicación de Campo Cercano (NFC). La NFC es una técnica de comunicación inalámbrica normalizada diseñada para el intercambio de datos entre dispositivos en distancias cortas. Una distancia de trabajo típica es de aproximadamente 0 a 20 cm. La NFC utiliza una frecuencia dada (13,56 MHz). Los transceptores NFC pueden ser activos, semipasivos o pasivos.

Los transceptores activos comprenden una fuente de energía que se usa para dotar de energía a los componentes del transceptor y la transmisión. Los transceptores pasivos comprenden o no un suministro de energía. Reciben la energía de funcionamiento inalámbricamente de un campo magnético generado por una transmisión NFC próxima. De este modo, están activos solamente cuando un transceptor activo transmite dentro del área de cobertura de dicho transceptor. Los transceptores pasivos no consumen energía cuando se encuentran en un estado inactivo. Típicamente, los transceptores pasivos son etiquetas de identificación RFID (Identificación por Radiofrecuencia) que comprenden un circuito de memoria y un transmisor pasivo que está configurado para responder a una consulta de transmisión NFC. Los transceptores semipasivos comprenden un suministro de energía, pero dicho suministro de energía se usa para dar energía a una micropastilla del transceptor pero no para retransmitir una señal. Para transmitir, un dispositivo semipasivo necesita ser dotado de energía por un transceptor activo.

La puerta 115 comprende un dispositivo de bloqueo electromecánico 116. El bloqueo comprende una interfaz 108 de bloqueo, una antena 112 del bloqueo y un pasador de bloqueo 114. La antena 112 del bloqueo está conectada a un circuito electrónico del bloqueo (no mostrado en la Figura 1A). El circuito comprende un dispositivo de comunicación de corto alcance. Dicho dispositivo puede ser un transceptor NFC. En una realización el transceptor NFC del bloqueo es un transceptor pasivo.

Cuando un usuario se aproxima a la puerta que desea abrir coloca el dispositivo de comunicación 106 cerca de la antena 112 del bloqueo. El circuito del bloqueo se activa mediante la transmisión de corto alcance del dispositivo de comunicación y se inicia una transacción. El dispositivo de comunicación lee una pregunta de autentificación

procedente del circuito electrónico del bloqueo. El dispositivo de comunicación 106 calcula una respuesta y transmite dicha respuesta al circuito electrónico del bloqueo. A continuación, el usuario opera la interfaz de usuario 108 del bloqueo. La operación puede comprender el giro de un pomo de puerta o la inserción de una llave física en el bloqueo. La operación activa dicho bloqueo y proporciona la energía operativa para que el bloqueo realice la autentificación. En la autentificación el bloqueo autentifica la respuesta. En una realización la respuesta es autentificada con respecto a la pregunta. Si la autentificación tiene éxito el bloqueo se fija en un estado en el que es posible la apertura y permite que el usuario opere el pasador de bloqueo.

En la realización anteriormente descrita la llave física no lleva a cabo autentificación alguna pero proporciona la activación de la energía operativa del bloqueo. En algunas realizaciones la llave puede proporcionar alguna autentificación adicional.

En una realización el dispositivo de comunicación 106 indica la pregunta leída desde el circuito electrónico del bloqueo a un servicio de autentificación 100 usando el canal 104 de red inalámbrica. El servicio de autentificación 100 puede calcular la respuesta y transmitirla al dispositivo de comunicación 106.

En una realización el servicio de autentificación puede registrar un seguimiento de auditoria de las acciones relacionadas con los elementos de bloqueo de los sistemas de bloqueo. De este modo, cada intento de abrir un bloqueo puede ser visto más tarde. Además, el servicio de autentificación puede utilizar una gestión de los derechos de acceso limitados en tiempo. En una realización el bloqueo puede guardar cada acción en un seguimiento de auditoría. El servicio de autentificación puede ser realizado con uno o más ordenadores, servidores o equipo de cálculo y el soporte lógico asociado.

Se puede usar cualquier técnica de autentificación apropiada en conexión con las realizaciones del presente invento. La selección de la técnica de autentificación depende del nivel de seguridad deseado del bloqueo 106 y posiblemente también del consumo de electricidad permitido para la autentificación (especialmente en elementos electromecánicos activados por el usuario).

En una realización la autentificación es realizada por una función SHA-1 (Algoritmo de Control Seguro) diseñado por la Agencia Nacional de Seguridad (NSA). En el SHA-1 una representación digital condensada (conocida como un resumen del mensaje) es calculada a partir de una secuencia de datos de entrada dados (conocida como el mensaje). El resumen del mensaje es con un alto grado de probabilidad único para el mensaje. El SHA-1 se denomina “seguro” debido, porque para un algoritmo dado, es computacionalmente imposible encontrar un mensaje que corresponda a un resumen de mensaje dado, o encontrar dos mensajes diferentes que produzcan el mismo resumen del mensaje. Cualquier cambio en un mensaje dará, con un grado de probabilidad muy alto, como resultado un resumen de mensaje diferente. Si es necesario aumentar la seguridad se pueden usar otras funciones de dispersión (SHA-224, SHA-256, SHA-384 y SHA-512) en la familia SHA, cada una con resúmenes más largos, conocidas colectivamente como SHA-2.

En una realización la pregunta comprende un identificador del sistema de bloqueo, un sistema de bloqueo, unos datos de acceso y un valor de verificación. El identificador del sistema de bloqueo identifica el sistema de bloqueo al cual pertenece dicho bloqueo. El identificador del bloqueo identifica dicho bloqueo en el sistema de bloqueo. Cada bloqueo en un sistema de bloqueo puede comprender una única identificación. Los datos de acceso pueden ser unos datos numéricos aleatorios. El valor de verificación es un valor de verificación por redundancia cíclica que confirma la identidad de la pregunta.

En una realización el servicio de autentificación o el dispositivo de comunicación que calcula la respuesta puede determinar sobre la base de la respuesta si la autentificación tendrá éxito o no. El dispositivo de comunicación 106 puede informar al usuario si la autentificación tendrá éxito o no.

En una realización un Número de Identificación Personal (PIN) o unos datos de la huella del dedo del usuario del dispositivo de comunicación pueden ser usados al generar una respuesta a la pregunta. El dispositivo de comunicación puede comprender un lector de la huellas del dedo configurado para leer la huella del dedo y generar una presentación numérica sobre la base de la huella del dedo.

La pregunta puede comprender una consulta sobre el PIN o la huella del dedo. El usuario del dispositivo de comunicación puede teclear en el PIN o usar el lector de datos de la huella del dedo del dispositivo de comunicación. Dicho dispositivo de comunicación está configurado para enviar el PIN o la presentación numérica de la huella del dedo como respuesta a la pregunta. El bloqueo puede ser configurado para guardar un conjunto de PINs y de huellas de dedo que permiten la apertura del bloqueo. Los circuitos electrónicos del bloqueo comparan la respuesta con los valores guardados y si se encuentra una coincidencia se considera que la autentificación ha tenido éxito.

La Figura 1B muestra un ejemplo más detallado de un bloqueo electromecánico 116 y de un dispositivo de comunicación 106. Dicho dispositivo de comunicación comprende una unidad de comunicación de corto alcance 140. En una realización dicha unidad de comunicación de corto alcance 140 es un transceptor NFC de tipo activo. El dispositivo de comunicación 106 puede comprender un transceptor inalámbrico 107 para realizar una conexión de

canal de red inalámbrica a una red inalámbrica tal como una red GSM, una red WCDMA o una red WLAN o cualquier otra red de comunicación inalámbrica normalizada / no normalizada.

El bloqueo 116 comprende unos circuitos electrónicos 142. Dicho bloqueo comprende además una interfaz de usuario 108 y un generador 122 el cual está configurado para suministrar energía al bloqueo 116 cuando la interfaz de usuario del bloqueo es operada.

Los circuitos electrónicos 142 pueden estar dispuestos como uno o más circuitos integrados, tal como unos circuitos integrados de aplicación específica ASIC. También son posibles otras realizaciones tales como un circuito constituido por unos componentes lógicos independientes o unas unidades de memoria y uno o más procesadores con soporte lógico. También es factible un híbrido de estas diferentes realizaciones. Al seleccionar el método de puesta en práctica una persona experta en la técnica considerará las exigencias fijadas sobre el consumo de energía del dispositivo, los costes de producción, y los volúmenes de producción, por ejemplo. Los circuitos electrónicos 142 pueden ser configurados para ejecutar las instrucciones del programa informático para ejecutar los procesos de cálculo.

En la realización de la Figura 1B los circuitos electrónicos 142 están compuestos por dos circuitos. Dichos circuitos comprenden una unidad de comunicación 126 y un circuito electrónico 120 del bloqueo que están conectados entre sí con un canal de comunicación 118. En una realización el circuito electrónico 120 del bloqueo está compuesto por un microcontrolador y una unidad de memoria.

El bloqueo comprende además una antena 112 conectada a la unidad de comunicación 126. En una realización la unidad de comunicación 126 es un transceptor NFC de tipo pasivo.

El bloqueo comprende además un actuador 124 que controla un pasador de bloqueo 114. Después de una autentificación con éxito el actuador 124 es configurado para fijar el bloqueo en un estado en el que es posible la apertura. El actuador puede ser activado mediante la energía eléctrica producida por el generador 108. El actuador 110 puede ser fijado en un estado bloqueado mecánicamente, pero no es necesaria una discusión sobre ello para ilustrar las presentes realizaciones.

Cuando el actuador 124 ha fijado el bloqueo en un estado en el que es posible la apertura mecánica el mecanismo 114 del pasador puede ser movido operando la interfaz de usuario 108, por ejemplo. También se pueden usar otros mecanismos operativos apropiados.

La Figura 2 ilustra una realización de la unidad de comunicación 126. Puede constar de una interfaz de comunicación 200 entre la antena 112 y dos unidades de memoria 202, 204. La interfaz de comunicación 200 con las unidades de memoria 202, 204 puede ser un transceptor NFC de tipo pasivo. Cuando la antena 112 se encuentra dentro del alcance operativo de un dispositivo NFC activo (por ejemplo el dispositivo de comunicación 106 de las Figuras 1A y 1B) la unidad de comunicación 126 es suministrada con energía a través de la antena 112 por el campo magnético generado por el dispositivo NFC activo. La unidad de memoria 202 está configurada para guardar una pregunta de autentificación, y la unidad de memoria 204 está configurada para guardar una respuesta de autentificación. El dispositivo NFC activo suministra energía a la interfaz de comunicación 200 con las memorias 202, 204, lee inalámbricamente la pregunta de la unidad de memoria 202 y guarda la respuesta inalámbricamente en la unidad de memoria 204.

Cuando la interfaz de usuario del bloqueo es operada la unidad de comunicación 126 es suministrada de energía por el generador 122 de la Figura 1B a través de la interfaz 206 usando el canal de comunicación 118. La electrónica 120 del bloqueo lee la respuesta procedente de la memoria 204 y escribe una nueva pregunta a la unidad de memoria 202.

La unidad de memoria 202 puede ser una memoria permanente realizada con una tecnología Flash o EEPROM, por ejemplo. La unidad de memoria 204 puede ser una memoria no permanente realizada con una tecnología RAM o DRAM, por ejemplo. La unidad de comunicación 126 está configurada para guardar una respuesta en la unidad de memoria 204 solamente durante un período de tiempo predeterminado, de lo contrario existe un riesgo para la seguridad si un bloqueo no es operado después de escribir la respuesta. La interfaz de comunicación 206 ilustra un ejemplo de una interfaz de comunicación entre las unidades de memoria 202, 204 y la electrónica 120 del bloqueo. Se suministra energía a una operación de lectura de la unidad de memoria 204 y a la operación de escritura de la unidad de memoria 202 por el bloqueo cuando es operado.

Las Figuras 3A a 3C son diagramas de flujos que ilustran unas realizaciones del invento. Aquí se ha supuesto que por defecto el bloqueo electromecánico 116 de la puerta 115 se encuentra en un estado bloqueado y permanece en dicho estado hasta que sea fijado en un estado en el que es posible la apertura.

Las Figuras 3A y 3B ilustran unas realizaciones desde el punto de vista del dispositivo de comunicación 106.

La secuencia de apertura comienza en el paso 300.

En el paso 302 el usuario del dispositivo de comunicación 106 inicia el dispositivo de comunicación. Esto puede comprender la conexión del transceptor NFC del dispositivo de comunicación. Dicho dispositivo de comunicación es situado de modo que la antena de bloqueo se encuentre dentro del área de cobertura del transceptor NFC del dispositivo de comunicación. Por ejemplo, el usuario puede tocar la antena de bloqueo con el dispositivo de comunicación.

En el paso 304 el dispositivo de comunicación 106 transmite una consulta NFC al bloqueo.

En el paso 306 el dispositivo de comunicación recibe la pregunta actual enviada por el bloqueo.

En el paso 308 de la Figura 3A el dispositivo de comunicación 106 calcula una respuesta. En una realización la respuesta es calculada por la unidad de procesamiento del dispositivo de comunicación 106. En otra realización la respuesta es calculada en un Módulo de Identidad de Abonado (SIM) o una Tarjeta Universal de Circuitos Integrados (UICC) situada en el dispositivo de comunicación 106.

La Figura 3B ilustra otra realización en la que el dispositivo de comunicación 106 transmite la pregunta al servicio de autentificación 100 en el paso 320.

En el paso 322 de la Figura 3B el servicio de autentificación 100 calcula una respuesta a la pregunta y la envía al dispositivo de comunicación 106. Esta realización permite una gestión de los derechos de acceso limitados en tiempo y un registro del seguimiento de auditoria al servicio de autentificación 100. A partir de ahí el proceso continúa como en la Figura 3A de la siguiente manera.

En el paso 310 el dispositivo de comunicación 106 transmite la respuesta a la unidad de comunicación del bloqueo 116.

La Figura 3C ilustra unas realizaciones desde el punto de vista del bloqueo electromecánico 116.

La secuencia de apertura comienza en el paso 330.

En el paso 332 la unidad de comunicación 126 es activada mediante la transmisión del dispositivo de comunicación 106 y la unidad recibe una consulta del dispositivo de comunicación.

En el paso 334 se lee la pregunta actual de la memoria 202 y se transmite desde la interfaz 200 al dispositivo de comunicación 106 mediante la antena 112.

En el paso 336 la interfaz RF 200 de la unidad de comunicación recibe una respuesta del dispositivo de comunicación 106. La interfaz guarda la respuesta en la memoria 204. Dicha memoria 204 está configurada para guardar la respuesta durante un período de tiempo predeterminado.

Las anteriores operaciones en la unidad de comunicación 126 son suministradas de energía por la transmisión NFC del dispositivo de comunicación.

En el paso 338 el bloqueo recibe una entrada de usuario procedente de la interfaz de usuario del bloqueo. La entrada activa la energía para el resto de las operaciones de la secuencia de apertura.

En el paso 340 un circuito electrónico 120 lee la pregunta actual procedente de su memoria interna en la que está guardada.

En el paso 342 el circuito electrónico 120 calcula una nueva consulta y la guarda en su memoria interna y en la memoria 202 a través del canal 118 y la interfaz 206.

En el paso 344 el circuito electrónico 120 del bloqueo lee la respuesta de la memoria 204 a través del canal 118 y a través de la interfaz 206.

En el paso 346 el circuito electrónico 120 del bloqueo autentifica la respuesta. En una realización dicho circuito electrónico 120 del bloqueo autentifica la respuesta con respecto a la pregunta.

En el paso 348 se verifica si la autentificación tuvo éxito.

Si lo tuvo, el circuito electrónico 120 del bloqueo envía una orden de apertura al activador 124 del bloqueo en el paso 350. Dicho activador 124 fija el bloqueo en un estado en el que es posible la apertura.

Si falló la autentificación, el circuito electrónico 120 no envía una orden de apertura al activador 124 del bloqueo en el paso 352 y dicho bloqueo permanece en un estado bloqueado.

Antes, el paso 338 comprende la activación de la energía para el bloqueo sobre la base de la entrada del usuario. Las operaciones de entrada en la interfaz de usuario pueden comprender el giro de un pomo de puerta o la inserción

de una llave física en el bloqueo. La operación activa el bloqueo y proporciona energía operativa para que el bloqueo realice la autentificación.

En realizaciones que utilizan la estructura de bloqueo de la Figura 1B la operación de la interfaz de usuario 108 del bloqueo permite que el generador active el bloqueo 116. El generador puede generar electricidad a partir del giro del pomo de una puerta o de una inserción de una llave.

Las Figuras 4A, 4B, 4C y 4D ilustran unos ejemplos de otras realizaciones de un sistema electrónico de bloqueo.

En el ejemplo de la Figura 4A el bloqueo comprende un suministro de energía 130 que está configurado para suministrar energía al bloqueo. El suministro de energía 130 puede ser de una batería interna, de una batería externa o un suministro de energía externo. En una realización el circuito electrónico 120 del bloqueo puede ser configurado para desconectarse él mismo cuando no está en uso para permitir una vida de servicio larga de la batería. Cuando un usuario opera la interfaz de bloqueo 108 se activa un sensor 132. Cuando está activado, el sensor activa el circuito electrónico 120 del bloqueo. Dicho circuito electrónico del bloqueo es activado y es configurado para leer una respuesta de la unidad de comunicaciones 126, genera y escribe una nueva pregunta a la unidad de comunicaciones 126 para una próxima secuencia de apertura y para realizar la autentificación. En caso de una autentificación con éxito el circuito electrónico del bloqueo activa el actuador 124 que fija el bloqueo 116 en un estado en el que es posible la apertura, y escribe una nueva pregunta a la unidad de comunicaciones 126 para una próxima secuencia de apertura.

En el ejemplo de la Figura 4B la antena de bloqueo 112 está incorporada en el pomo 108 de la puerta. En esta realización la secuencia de apertura de la puerta puede comprender los siguientes pasos. Primeramente, un usuario toca el pomo 108 mediante un dispositivo de comunicación 106. En la segunda fase el usuario 105 gira el pomo 108 para activar la energía para la autentificación y fijar el bloqueo 116 en un estado en el que es posible la apertura. En la tercera fase al girar el pomo 108 se opera el pasador 114. Además, se puede usar una interfaz de operación de tipo palanca en lugar de una estructura de pasador. El usuario experimenta la segunda y la tercera fases como un giro continuo del pomo.

En el ejemplo de la Figura 4C la antena 112 del bloqueo está situada en la puerta y se usa una llave 134 para operar un bloqueo 116. La interfaz de usuario del bloqueo comprende un agujero 144 para la llave. En esta realización la secuencia de apertura de la puerta puede comprender los siguientes pasos. Primeramente un usuario toca la antena 112 con el dispositivo de comunicación 106. En la segunda fase se inserta la llave 134 en el agujero 114 de la llave del bloqueo 116 para activar la energía para la autentificación y para fijar el bloqueo 116 en un estado en el que es posible la apertura. En la tercera fase el giro de la llave 134 opera el pasador 114.

El ejemplo de la Figura 4D ilustra un bloqueo 116, el cual es una combinación de las estructuras del bloqueo de las Figuras 4B y 4C. El bloqueo de la Figura 4D puede tener unos modos de operación diferentes. En una realización el bloqueo 116 autentifica la llave 134 y la respuesta recibida del dispositivo de comunicación 106. El bloqueo es fijado en un estado en el que es posible la apertura si ambas autentificaciones tienen éxito.

En otra realización el bloqueo 116 autentifica la respuesta recibida del dispositivo de comunicación 106. La llave 134 se usa solamente para operar el mecanismo de bloqueo.

En otra realización la operación de bloqueo puede ser diferente para usuarios distintos. Algunos usuarios utilizan la llave 134 para la autentificación. Algunos usuarios (usuarios temporales, por ejemplo) utilizan el dispositivo de comunicación 106 para la autentificación y abren el bloqueo 116 girando el pomo 108.

En una realización las características del invento se ejecutan como soporte lógico. Las realizaciones pueden ser ejecutadas como un producto de programa de cálculo que codifica un programa de cálculo de instrucciones para ejecutar un proceso de cálculo que lleva a cabo los pasos anteriormente descritos para operar un bloqueo electromecánico.

Es evidente para una persona experta en la materia que, en cuanto a los avances tecnológicos, el concepto del invento puede ser puesto en práctica de diversas formas. El invento y sus realizaciones no están limitados a los ejemplos antes descritos aunque pueden variar dentro del alcance de las reivindicaciones.

REIVINDICACIONES

1. Un bloqueo electromecánico (116) que comprende:

un circuito electrónico (142) para guardar una pregunta, que proporciona una interfaz inalámbrica (126) para un dispositivo de comunicación (106) para leer la pregunta,

unos medios para recibir una respuesta del dispositivo de comunicación (106) y guardarla en una memoria (204) de la interfaz inalámbrica (126);

en el que los circuitos electrónicos (142) están configurados para recibir inalámbricamente del dispositivo de comunicación (106) la energía operativa para comunicar con el dispositivo de comunicación (106) y para recibir y guardar la respuesta;

unos medios para leer la respuesta de la memoria (204) de la interfaz inalámbrica (126) y unos medios para autentificar la respuesta, y para emitir una orden de apertura siempre que la autentificación tenga éxito;

unos medios de actuación (124) para recibir la orden de apertura y para fijar el bloqueo mecánicamente en un estado en el que es posible la apertura;

en el que una interfaz de usuario (108) está configurada para recibir una entrada de un usuario, y después activar la energía operativa para los medios de lectura, autentificación y actuación.

2. El bloqueo electromecánico (116) de la reivindicación 1, en el que el bloqueo está configurado para obtener la energía operativa para la interfaz de usuario (108) y para recibir y guardar las operaciones de respuesta de un campo de Comunicación Cercano (NFC) generado por el dispositivo de comunicación (106).

3. El bloqueo electromecánico (116) de cualquiera de las reivindicaciones anteriores, en el que dicho bloqueo está configurado para guardar la respuesta en el circuito electrónico (142) durante un período de tiempo predeterminado.

4. El bloqueo electromecánico (116) de cualquiera de las reivindicaciones anteriores, en el que dicho bloqueo (116) está configurado para calcular una nueva pregunta y guardar dicha pregunta en los circuitos (142) después de recibir una entrada de usuario con la interfaz de usuario (108).

5. El bloqueo electromecánico (116) de cualquiera de las reivindicaciones anteriores, en el que los circuitos electrónicos (142) están configurados para realizar la autentificación de la respuesta usando el mismo algoritmo que el usado en el dispositivo de comunicación (106) cuando se genera la respuesta.

6. El bloqueo electromecánico (116) de cualquiera de las reivindicaciones anteriores, en el que la pregunta comprende un identificador del sistema de bloqueo, un identificador del bloqueo, unos datos de acceso y un valor de verificación.

7. El bloqueo electromecánico (116) de cualquiera de las reivindicaciones anteriores, en el que los circuitos electrónicos (142) están configurados para autentificar la respuesta con respecto a la pregunta.

8. El bloqueo electromecánico (116) de cualquiera de las reivindicaciones anteriores, en el que los circuitos electrónicos (142) comprenden:

una unidad de comunicación (126) para guardar una pregunta y proporcionar una interfaz de radiofrecuencia (200) para un dispositivo de comunicación (106) y para recibir y guardar una respuesta del dispositivo de comunicación (106); y

un circuito electrónico (120) del bloqueo para leer la respuesta de la unidad de comunicación (126) y la pregunta de una memoria (204), la autentificación de la respuesta, y para emitir una orden de apertura.

9. El bloqueo electromecánico (116) de la reivindicación 8, en el que la unidad de comunicación (126) comprende una interfaz (206) configurada para comunicar con el circuito electrónico (120) del bloqueo.

10. El bloqueo electromecánico (116) de la reivindicación 8, en el que la unidad de comunicación (126) comprende una memoria (202) para guardar la pregunta, una memoria (204) para guardar la respuesta y una antena (112) conectada a la interfaz de radiofrecuencia (200).

11. El bloqueo electromecánico (116) de cualquiera de las reivindicaciones anteriores, en el que el bloqueo (116) está configurado para autentificar una llave (134) insertada en el bloqueo y para emitir una orden de apertura siempre que la autentificación tenga éxito.

12. El bloqueo electromecánico (116) de cualquiera de las reivindicaciones anteriores, en el que la interfaz de usuario (108) comprende un pomo (108) de la puerta, y el bloqueo (116) está configurado para activar la energía

operativa para las operaciones de autentificación y del actuador cuando el pomo (108) de la puerta es operado por un usuario.

13. El bloqueo electromecánico (116) de cualquiera de las reivindicaciones anteriores, en el que la interfaz de usuario (108) comprende un agujero (144) para la llave, y el bloqueo (116) está configurado para activar la energía operativa para las operaciones de autentificación y del actuador cuando se inserta una llave (134) en el agujero (144) de la llave.

14. Un método para operar un bloqueo electromecánica (116), que comprende:

guardar una pregunta en unos circuitos electrónicos (142) del bloqueo electromecánico (116);

recibir de forma inalámbrica de un dispositivo de comunicación (106) que opera la energía para:

proporcionar una interfaz inalámbrica (126) para el dispositivo de comunicación (106) para leer la pregunta que está guardada en los circuitos electrónicos (142) del bloqueo electromecánico (116); y

para recibir y guardar una respuesta del dispositivo de comunicación (106) en una memoria (204) de la interfaz inalámbrica (126);

recibir con la interfaz de usuario (108) del bloqueo electromecánico (116) una entrada de un usuario, y a continuación activar la energía operativa para:

leer la respuesta de la memoria (204) de la interfaz inalámbrica (126) y para autentificar la respuesta; y

para emitir una orden de apertura siempre que la autentificación tenga éxito; y

para fijar el bloqueo en un estado en el que es posible la apertura mecánica en respuesta a la orden de apertura.

15. El método de la reivindicación 14, que además comprende:

la comunicación con el dispositivo de comunicación (106) usando una Comunicación de Campo Cercano (NFC).

16. El método de cualquiera de las reivindicaciones anteriores, que además comprende:

proporcionar energía para la recepción y almacenamiento de la respuesta por un campo de Comunicación de Campo Cercano (NFC) generada por el dispositivo de comunicación (106).

17. El método de cualquiera de las reivindicaciones anteriores, que además comprende:

guardar la respuesta en los circuitos electrónicos (142) durante un período de tiempo predeterminado.

18. El método de cualquiera de las reivindicaciones anteriores, que además comprende:

autentificar la respuesta con respecto a la pregunta.

19. El método de cualquiera de las reivindicaciones anteriores, que además comprende:

calcular y guardar una nueva pregunta después de recibir la entrada de usuario con la interfaz de usuario (108).

20. El método de cualquiera de las reivindicaciones anteriores, que además comprende:

calcular la respuesta del dispositivo de comunicación (106).

21. El método de cualquiera de las reivindicaciones anteriores 14 a 19, que además comprende:

el envío por el dispositivo de comunicación (106) de una pregunta a un servicio de autentificación (100);

el cálculo de la respuesta por el servicio de autentificación (100);

la recepción por el dispositivo de comunicación (106) de la respuesta del servicio de autentificación (100); y

la transmisión por el dispositivo de comunicación (106) de la respuesta al circuito electrónico (142).

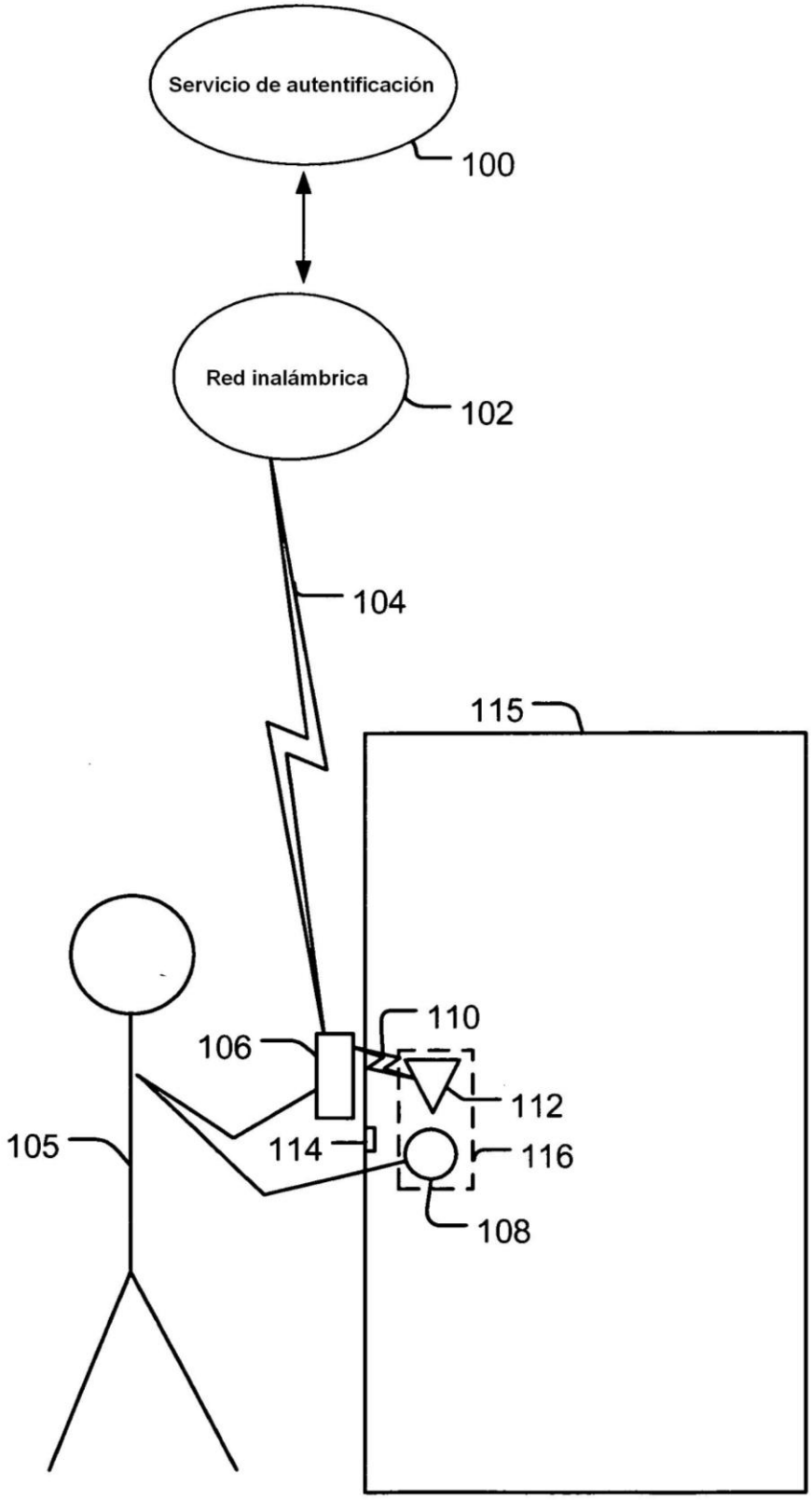
Servicio de autentificación
100
Red inalámbrica
102
104
115
110
106
112
105
114
116
108

FIG. 1A

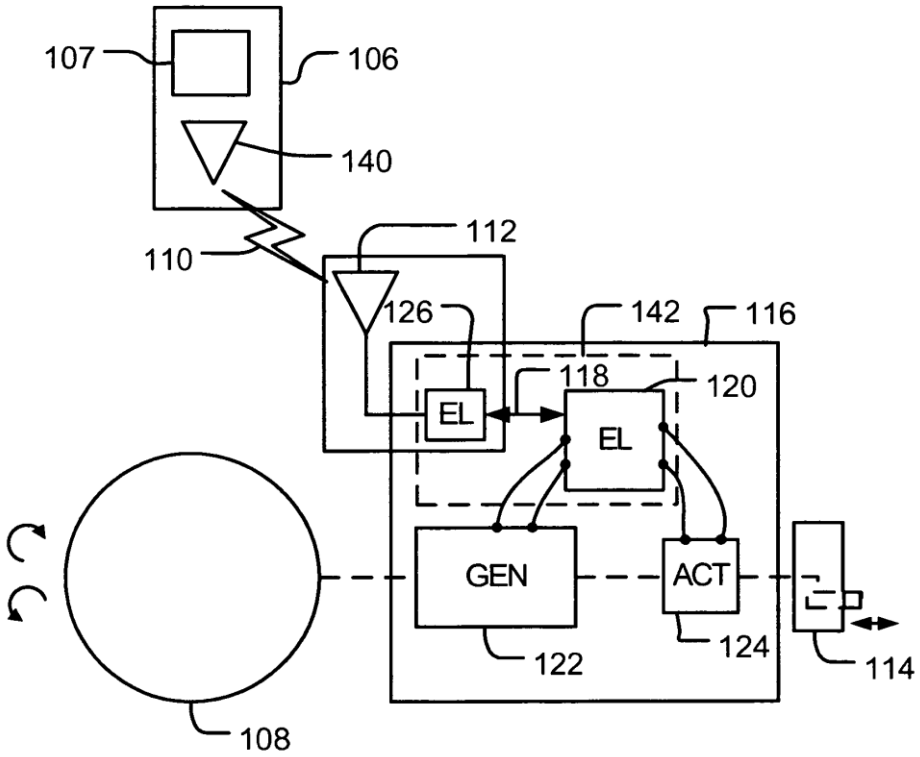
107
106
140
110
112
126
142
116
118
120
EL
EL
GEN
ACT
122
124
114
108

FIG. 1B

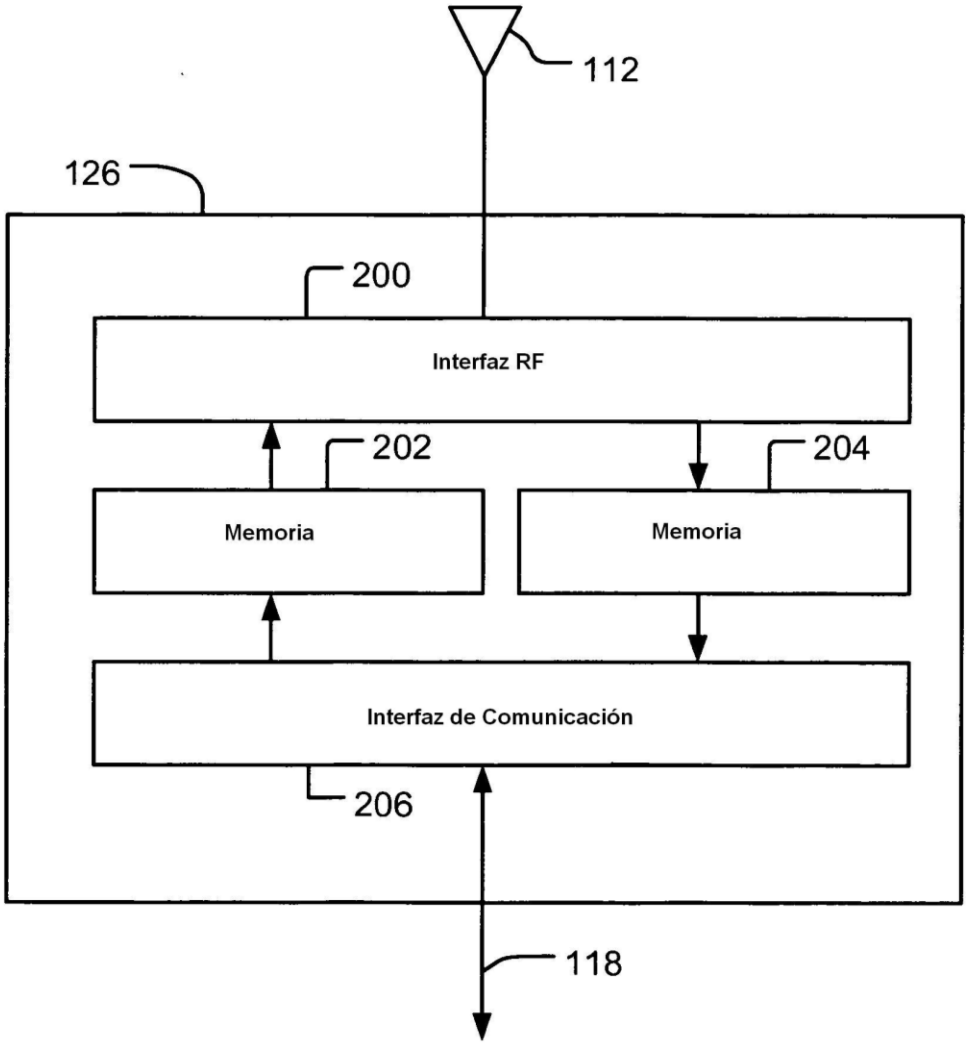
112
126
200
Interfaz RF
202
204
Memoria
Memoria
Interfaz de Comunicación
206
118

FIG. 2

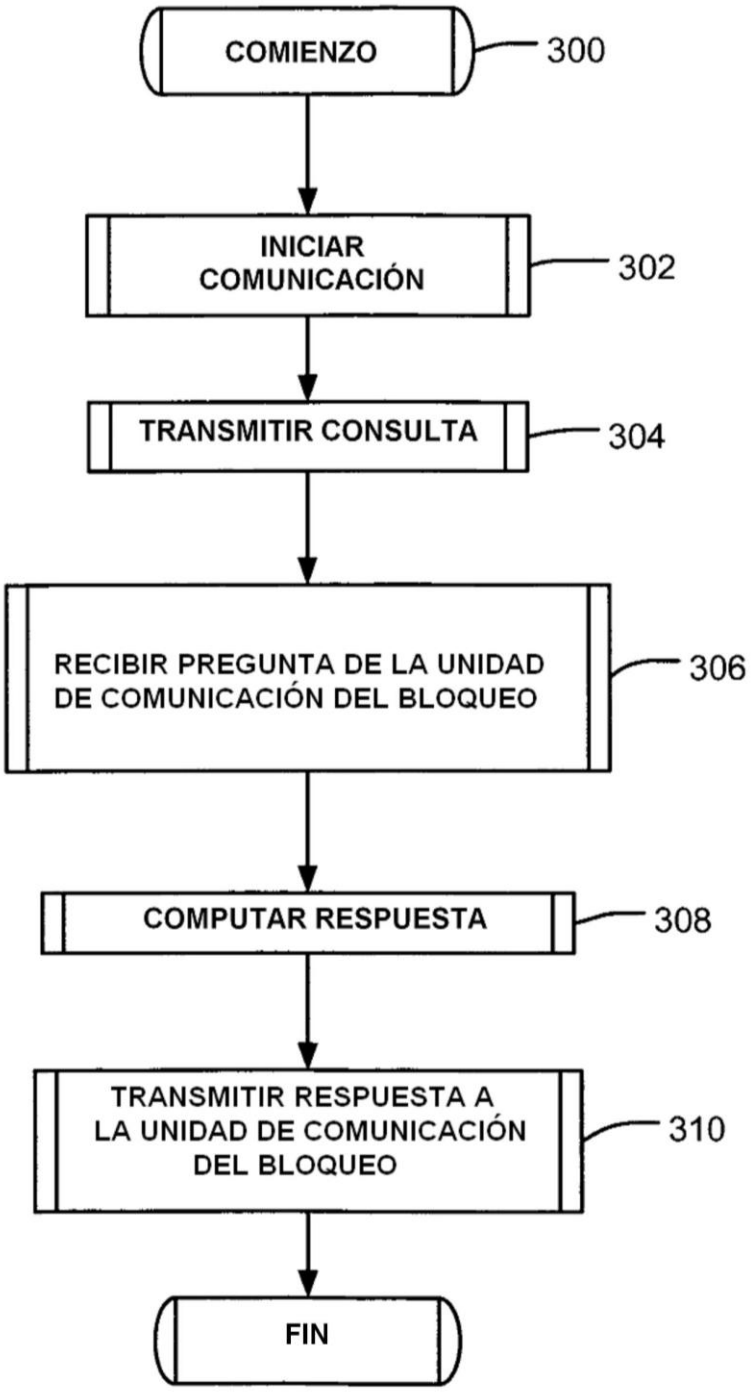
COMIENZO
300
INICIAR COMUNICACIÓN
302
TRANSMITIR CONSULTA
304
RECIBIR PREGUNTA DE LA UNIDAD DE COMUNICACIÓN DEL BLOQUEO
306
COMPUTAR RESPUESTA
308
TRANSMITIR RESPUESTA A LA UNIDAD DE COMUNICACIÓN DEL BLOQUEO
310
FIN

FIG. 3A

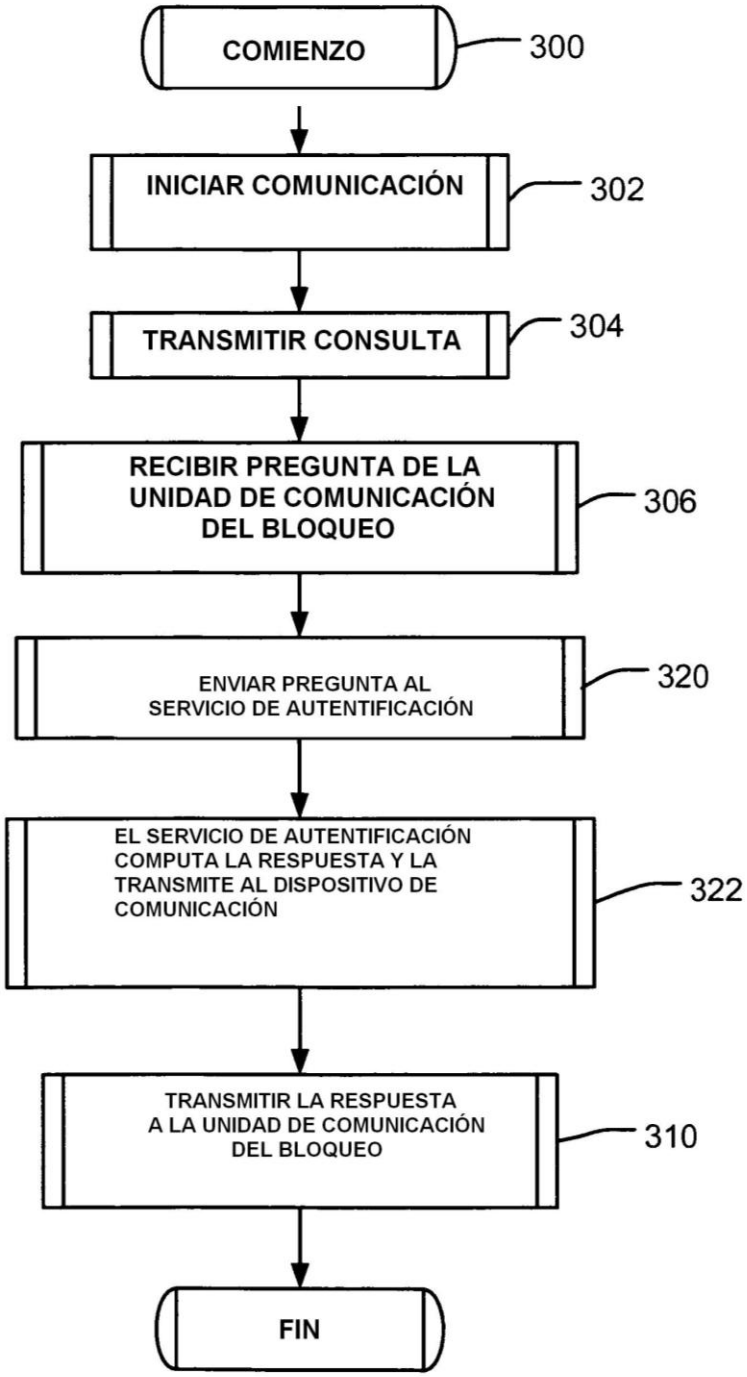
COMIENZO
300
INICIAR COMUNICACIÓN
302
TRANSMITIR CONSULTA
304
RECIBIR PREGUNTA DE LA UNIDAD DE COMUNICACIÓN DEL BLOQUEO
306
ENVIAR PREGUNTA AL SERVICIO DE AUTENTIFICACIÓN
320
EL SERVICIO DE AUTENTIFICACIÓN COMPUTA LA RESPUESTA Y LA TRANSMITE AL DISPOSITIVO DE COMUNICACIÓN
322
TRANSMITIR LA RESPUESTA A LA UNIDAD DE COMUNICACIÓN DEL BLOQUEO
310
FIN

FIG. 3B

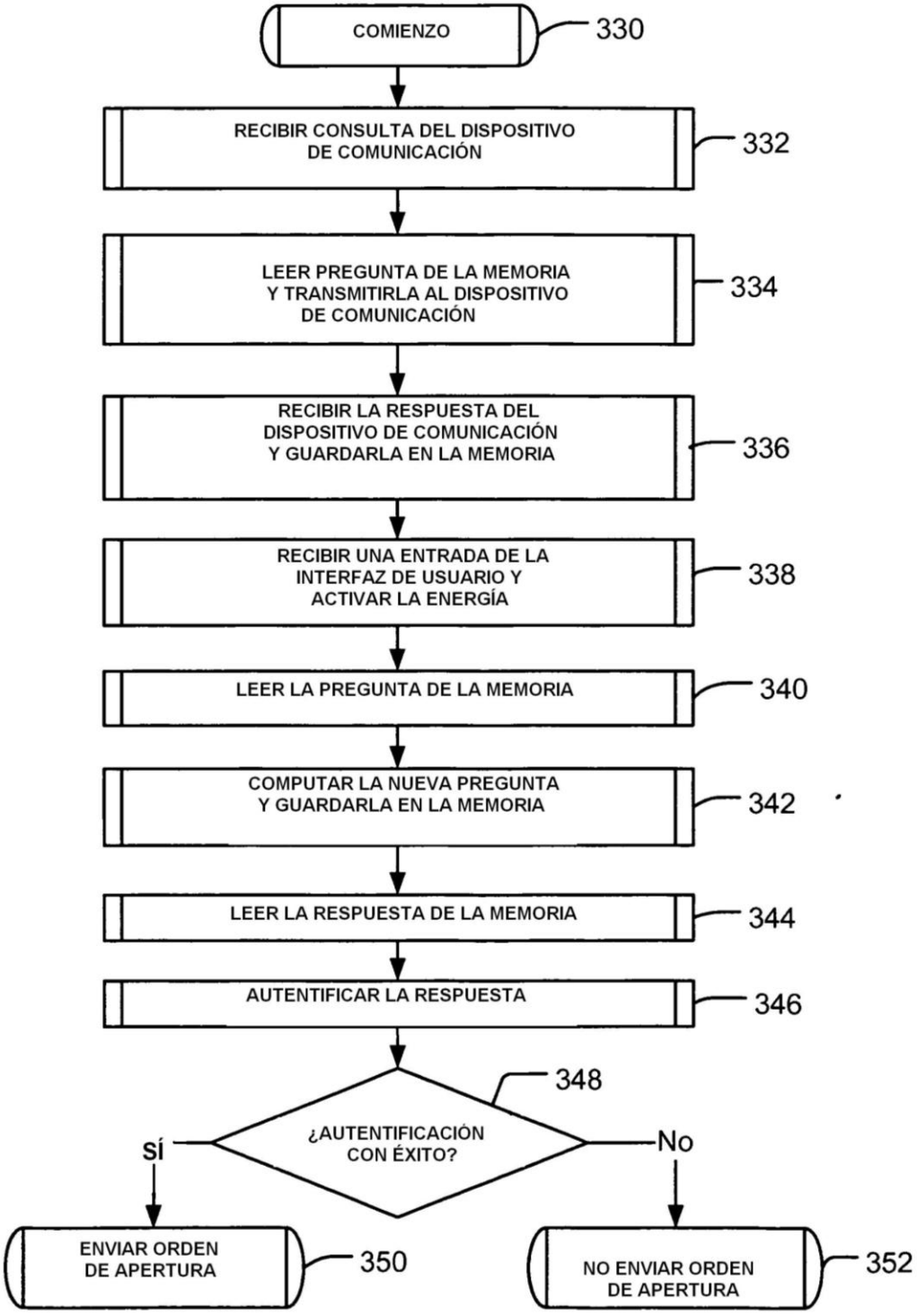
COMIENZO
330
RECIBIR CONSULTA DEL DISPOSITIVO DE COMUNICACIÓN
332
LEER PREGUNTA DE LA MEMORIA Y TRANSMITIRLA AL DISPOSITIVO DE COMUNICACIÓN
334
RECIBIR LA RESPUESTA DEL DISPOSITIVO DE COMUNICACIÓN Y GUARDARLA EN LA MEMORIA
336
RECIBIR UNA ENTRADA DE LA INTERFAZ DE USUARIO Y ACTIVAR LA ENERGÍA
338
LEER LA PREGUNTA DE LA MEMORIA
340
COMPUTAR LA NUEVA PREGUNTA Y GUARDARLA EN LA MEMORIA
342
LEER LA RESPUESTA DE LA MEMORIA
344
AUTENTIFICAR LA RESPUESTA
346
348
¿AUTENTIFICACIÓN CON ÉXITO?
SÍ
No
ENVIAR ORDEN DE APERTURA
350
NO ENVIAR ORDEN DE APERTURA
352

FIG. 3C

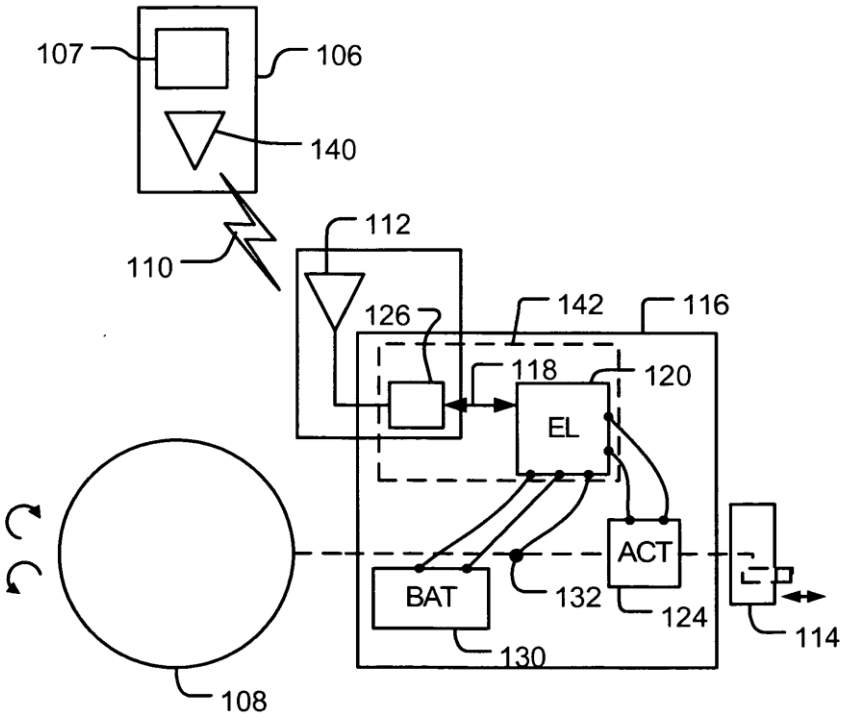
107
106
140
110
112
126
142
116
118
120
EL
ACT
BAT
132
124
114
130
108

FIG. 4A

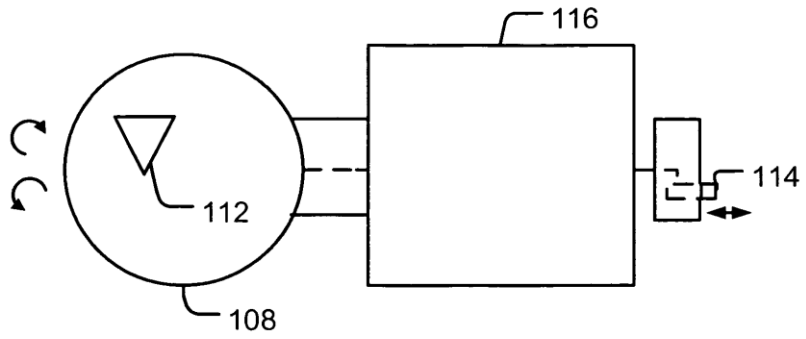

FIG. 4B

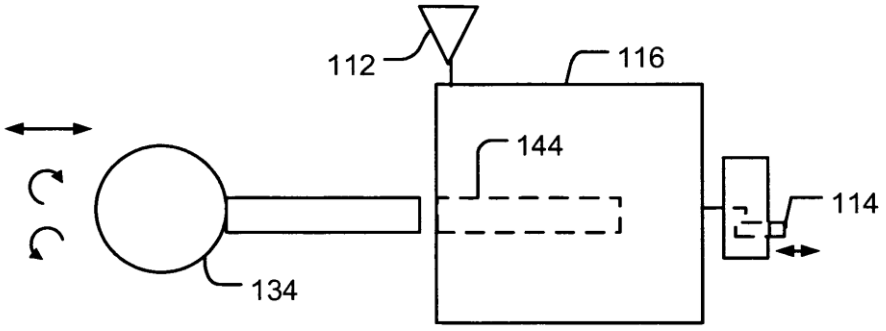

FIG. 4C

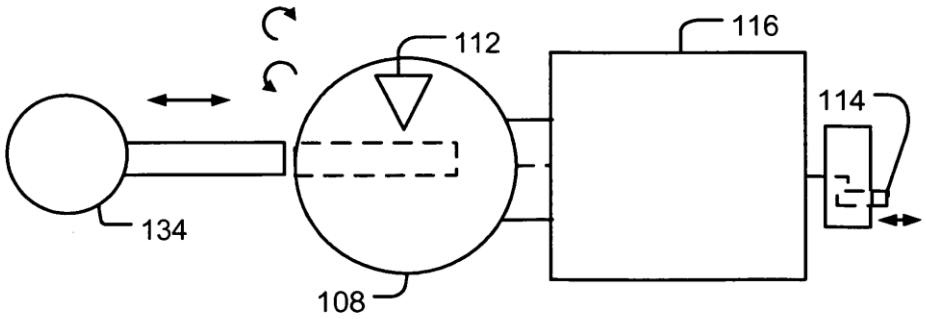

FIG. 4D