

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 948 892**

51 Int. Cl.:

G07C 9/00

(2010.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **29.09.2014** **PCT/EP2014/070726**

87 Fecha y número de publicación internacional: **09.04.2015** **WO15049187**

96 Fecha de presentación y número de la solicitud europea: **29.09.2014** **E 14777080 (4)**

97 Fecha y número de publicación de la concesión europea: **07.06.2023** **EP 3053148**

54 Título: **Control de acceso usando dispositivos electrónicos portátiles**

30 Prioridad:

01.10.2013 EP 13186976

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

21.09.2023

73 Titular/es:

INVENTIO AG (100.0%)
Seestrasse 55
6052 Hergiswil, CH

72 Inventor/es:

TROESCH, FLORIAN

74 Agente/Representante:

ELZABURU, S.L.P

ES 2 948 892 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Control de acceso usando dispositivos electrónicos portátiles

Esta descripción se refiere a sistemas de control de acceso.

- 5 Los sistemas de control de acceso requieren normalmente que un usuario presente al sistema algo que está destinado a servir como evidencia de que el usuario está autorizado para recibir acceso del sistema. Por ejemplo, algunos sistemas conceden acceso a un usuario basándose en un testigo (por ejemplo, una tarjeta de identificación o un llavero transmisor) en posesión del usuario. El testigo puede ser una etiqueta de RFID (identificación por radiofrecuencia) u otro dispositivo de almacenamiento de información. En otros sistemas, se concede acceso a un usuario basándose en información que el usuario proporciona al sistema, tal como una contraseña. Algunos sistemas requieren múltiples elementos de un usuario, por ejemplo, tanto un testigo como una contraseña.

- 10 El documento US20110291798A1 describe un sistema en el que un dispositivo electrónico, tal como un teléfono inteligente, almacena un archivo de derechos de acceso físico firmado digitalmente. Un individuo usa este archivo de derechos para acceder a una zona restringida solo después de autenticarse por sí mismo en el dispositivo. Un sistema de control de acceso físico recibe el archivo de derechos, lo valida y determina si permitir el paso a través de una barrera física. Una pasarela de control de acceso puede transmitir un código de autorización al dispositivo electrónico y al sistema de barrera física, de modo que solo se permite el paso si el sistema de barrera recibe posteriormente el código de autorización del dispositivo electrónico usando comunicaciones de campo cercano.

- 15 El documento US 2012/068818 A1 describe un método de control de acceso en el que se envía un código de identificación a un nodo de acceso usando un teléfono móvil. Si el código de identificación se reconoce como válido, se envía un código de acceso desde el nodo de acceso al teléfono móvil y se presenta en la pantalla del teléfono móvil. El código de acceso se detecta usando una cámara y, si el código de acceso se reconoce como válido, se concede el acceso.

- 20 El documento US 2009/324025 A1 describe el control de acceso a una instalación segura, en donde una determinación de si se permite el acceso se basa en una imagen digital de características predeterminadas de la instalación segura. Un dispositivo de usuario capta una imagen de una característica predeterminada de la instalación segura y se compara con datos de seguridad almacenados correspondientes a la instalación segura. Se realiza una determinación de si se permite el acceso a la instalación segura, basándose en los resultados de la comparación.

- 25 El documento US 2013/210406 A1 describe un teléfono que puede detectar o determinar que un usuario del teléfono está sentado en un asiento de conductor de un vehículo móvil. Tras dicha determinación, el teléfono puede bloquear una o más características o aplicaciones, tales como texto o mensajería. Opciones adicionales para sistemas de control de acceso pueden resultar ventajosas. Esto se aborda en las reivindicaciones independientes; en las reivindicaciones dependientes se especifican realizaciones adicionales. Un sistema de control de acceso puede estar configurado para detectar la presencia de un dispositivo electrónico portátil portado por un usuario en una primera zona. El sistema de control de acceso envía un código de acceso al dispositivo. En una segunda zona, el usuario presenta el dispositivo electrónico portátil a un terminal de acceso, que lee el código de acceso del dispositivo. Si el código de acceso leído del dispositivo coincide con el código de acceso que fue enviado al dispositivo por el sistema, entonces el sistema de control de acceso concede acceso al usuario.

- 30 Los siguientes ejemplos/aspectos/realizaciones que no están cubiertos por las reivindicaciones no son según la invención y se presentan únicamente con fines ilustrativos.

La descripción se refiere a las siguientes figuras, en las que:

- La figura 1 muestra una vista en planta de una realización a modo de ejemplo de una zona que usa un sistema de control de acceso.
- 45 La figura 2 muestra un diagrama de bloques de una realización a modo de ejemplo de un sistema de control de acceso.
- La figura 3 muestra un diagrama de bloques de una realización a modo de ejemplo de un método de control de acceso.
- La figura 4 muestra un diagrama de bloques de otra realización a modo de ejemplo de un método de control de acceso.
- 50 La figura 5 muestra un diagrama de bloques de otra realización a modo de ejemplo de un método de control de acceso.
- La figura 6 es un diagrama de señales que muestra a modo de ejemplo un intercambio de señales entre diferentes componentes, incluyendo componentes de un sistema de control de acceso.
- La figura 7 muestra un diagrama de bloques de una realización a modo de ejemplo de un ordenador.

La figura 1 muestra una vista en planta de una realización a modo de ejemplo de una zona que usa un sistema de control de acceso. Se pueden usar una o más de las tecnologías descritas en un entorno como el de la figura 1; sin embargo, al menos algunas realizaciones también pueden usarse en otros entornos. La figura 1 muestra una zona 110 y una zona 112. En este caso, el acceso a la zona 110, al menos parte del tiempo, generalmente no está regulado por un sistema de control de acceso. Un ejemplo posible de la zona 110 es un vestíbulo de edificio que es generalmente accesible para el público desde una puerta exterior del edificio. Por otro lado, el acceso a la zona 112 está generalmente regulado por un sistema de control de acceso. Por lo tanto, la zona 112 se considera una zona "segura". Un posible ejemplo es una zona de oficinas que está destinada a ser accesible solo para empleados y sus invitados. En el caso particular mostrado en la figura 1, la zona 112 está separada de la zona 110 por un conjunto de barreras 120, 122 físicas y por una barrera 130 móvil. En otras realizaciones, las barreras físicas y móviles no están presentes, en vez de eso, uno o más límites entre las zonas 110, 112 se controlan electrónicamente. Si una parte no autorizada atraviesa un límite o barrera, el sistema de control de acceso no abre una puerta o barrera, o el sistema inicia una contramedida (por ejemplo, se notifica al personal de seguridad). Aunque no se muestra en la figura 1, la zona 112 puede conducir a otras zonas de edificio (por ejemplo, salas, escaleras, ascensores, escaleras mecánicas, zonas de almacenamiento u otros lugares). En al menos algunos casos, la zona 110 incluye una entrada 140 a través de la cual un usuario 150 puede entrar o salir de la zona 110. La figura 1 también muestra un sensor 160 para detectar un dispositivo 170 electrónico portátil portado por el usuario 150. Aunque la figura 1 representa que el sensor 160 está en la zona 110, también puede estar ubicado en otra parte (por ejemplo, en la zona 112) y configurado para detectar actividad en la zona 110. La figura 1 también muestra un terminal 180 de acceso, cuyas funciones se explicarán con más detalle a continuación. Generalmente, el terminal 180 de acceso está situado en o cerca de un límite entre las zonas 110, 112.

La figura 2 muestra un diagrama de bloques de una realización a modo de ejemplo de un sistema 200 de control de acceso. El sistema 200 incluye una unidad 210 de control basada en ordenador. La unidad 210 de control comprende, por ejemplo, un procesador configurado para realizar una o más acciones del método descritas en esta solicitud. El procesador lee instrucciones correspondientes para las acciones del método de un componente de memoria.

La unidad 210 de control está acoplada a un primer sensor 220, que puede corresponder al sensor 160 de la figura 1. El sensor 220 puede detectar la presencia de, y comunicarse con, un dispositivo 230 electrónico portátil. El dispositivo 230 electrónico portátil es, por ejemplo, un teléfono inteligente, un teléfono móvil, un ordenador de tipo tableta, un reloj inteligente u otro dispositivo móvil. El sensor 220 detecta y se comunica con el dispositivo 230 usando una tecnología basada en radio, por ejemplo, Bluetooth, Bluetooth LE (Bluetooth de baja energía), Wi-Fi (red inalámbrica), ZigBee, GPRS (servicio general de radio por paquetes) u otra tecnología. La unidad 210 de control también está acoplada a un segundo sensor 240, que también puede detectar la presencia de, y comunicarse con, el dispositivo 240 electrónico portátil.

En algunas realizaciones, se omite el segundo sensor 240 y solo está presente el primer sensor 220. En algunos sistemas que tienen tanto el primer como el segundo sensor, ambos sensores 220, 240 pueden usar la misma tecnología de comunicación (por ejemplo, ambos usan Bluetooth LE). Sin embargo, en otros sistemas, cada uno de los sensores usa una tecnología de comunicación diferente. En realizaciones con tan solo un sensor, el sensor puede usarse para detectar el dispositivo electrónico portátil en múltiples zonas. Por ejemplo, haciendo referencia a la figura 1, un sensor puede estar configurado para detectar el dispositivo electrónico portátil tanto en una zona inmediatamente cerca del terminal 180 de acceso como en una zona más alejada del terminal 180 de acceso. Por ejemplo, el sensor puede detectar el dispositivo 170 electrónico portátil en la ubicación mostrada en la figura 1 y en el terminal 180 de acceso. Específicamente, el sensor puede determinar en cuál de estas ubicaciones está actualmente ubicado el dispositivo 170. La monitorización de dos zonas con un sensor puede realizarse usando, por ejemplo, software o electrónica que controla en consecuencia el funcionamiento del sensor.

La unidad 210 de control está acoplada además a un terminal 250 de acceso, que puede corresponder al terminal 180 de acceso de la figura 1. En algunos casos, el sensor 240 y el terminal 250 están integrados en una única unidad; en otros casos, son componentes independientes. En realizaciones particulares, el terminal 250 es un dispositivo terminal PORT del Grupo Schindler de Suiza. La unidad 210 de control también está acoplada a una red 260 de comunicación inalámbrica que puede comunicarse con el dispositivo 230 electrónico portátil. La red 260 de comunicación inalámbrica comprende, por ejemplo: una red de comunicación celular de largo alcance (por ejemplo, 1G, 2G, 3G, 4G u otro tipo); una red Wi-Fi; una red de Bluetooth; u otro tipo de red inalámbrica. La unidad 210 de control se comunica con los diversos componentes del sistema 200 a través de una red 270 (por ejemplo, Internet, una red de área local u otro tipo de red).

En realizaciones adicionales, la unidad 210 de control también está acoplada a uno o más componentes 280 del sistema de seguridad. Dichos componentes pueden incluir, por ejemplo, alarmas, cámaras, sensores, cerraduras, barreras (por ejemplo, la barrera 130 móvil) u otros componentes.

En realizaciones adicionales, la unidad 210 de control también está acoplada a un sistema 290 de control de ascensor. El sistema 290 de control de ascensor puede usar información proporcionada por la unidad 210 de control para hacer funcionar un sistema de ascensor. Por ejemplo, el sistema 290 de control de ascensor puede usar dicha información para realizar llamadas de ascensor, incluyendo llamadas de destino.

La figura 3 muestra un diagrama de bloques de una realización a modo de ejemplo de un método 300 de control de acceso. Aunque el método 300 se describe aquí en el contexto del sistema 200 de la figura 2, el método 300 también

puede usarse con otras realizaciones del sistema. En una acción 310 de método, el sistema 200 detecta en una primera zona (por ejemplo, la zona 110) la presencia de un dispositivo electrónico portátil, tal como el dispositivo 230 electrónico portátil. El dispositivo se detecta usando un sensor, tal como el primer sensor 220. Como parte de la detección, el sensor determina un primer identificador de dispositivo para el dispositivo electrónico portátil. Como se usa en esta solicitud y en las reivindicaciones, el primer identificador de dispositivo es un fragmento de información que permite al sistema distinguir el dispositivo electrónico portátil de uno o más de otros dispositivos. Por ejemplo, si el sensor es un sensor de Bluetooth o Bluetooth LE, entonces el sensor puede obtener la dirección de dispositivo de MAC de Bluetooth del dispositivo electrónico portátil y usar la dirección como el primer identificador de dispositivo. En realizaciones particulares, el primer identificador de dispositivo comprende un identificador único asignado por el sistema 200 cuando se registró anteriormente el dispositivo electrónico portátil en el sistema 200. Otros ejemplos de primeros identificadores de dispositivo pueden incluir: una dirección MAC (control de acceso a medios) para el dispositivo; una dirección Wi-Fi para el dispositivo; un testigo para el dispositivo; un número de teléfono para el dispositivo; un número IMEI (identidad de equipo de estación móvil internacional) para el dispositivo; u otro fragmento de información.

En algunas realizaciones, el primer identificador de dispositivo se lee directamente del dispositivo electrónico portátil. En otras realizaciones, el primer identificador de dispositivo se determina basándose en otra información recibida del dispositivo electrónico portátil.

En realizaciones particulares, el dispositivo electrónico portátil emite por radiodifusión periódicamente un identificador, que se denomina identificador inicial en la presente memoria. Para implementaciones de Bluetooth o Wi-Fi, el identificador inicial puede ser una dirección MAC. Este identificador se recibe por el sistema de control de acceso usando un sensor. En los casos en los que el identificador inicial para un dispositivo rara vez cambia o nunca cambia, el identificador inicial puede usarse como el primer identificador de dispositivo. Alternativamente, el identificador inicial puede usarse para buscar el primer identificador de dispositivo en una base de datos. Por lo tanto, el primer identificador de dispositivo no se lee explícitamente del dispositivo, sino que, en vez de eso, se recibe de manera pasiva del dispositivo (en forma de identificador inicial) o se determina basándose en información que se recibe de manera pasiva del dispositivo.

En realizaciones adicionales, el dispositivo emite por radiodifusión un identificador inicial, que cambia con frecuencia. En dichas realizaciones, el sistema de control de acceso puede reconocer la presencia del dispositivo tras recibir de manera pasiva el identificador inicial. Entonces, el sistema puede usar el identificador inicial para crear una conexión con el dispositivo, a través de la cual el sistema lee entonces el primer identificador de dispositivo del dispositivo. Posiblemente, esta lectura se realiza usando un programa de software de control de acceso que está ejecutándose en el dispositivo.

En realizaciones adicionales, el dispositivo emite por radiodifusión un identificador, que cambia de manera ocasional. Tras recibir de manera pasiva el identificador inicial, el sistema de control de acceso puede determinar si el identificador inicial ya se conoce por el sistema. Si ya se conoce el identificador inicial, entonces se puede usar como el primer identificador de dispositivo para el dispositivo. En dichos casos, no es necesario que el sistema lea un primer identificador de dispositivo del dispositivo. Si el sistema no conoce el identificador inicial (quizás porque el identificador inicial ha cambiado recientemente), el sistema puede crear una conexión con el dispositivo y leer el primer identificador de dispositivo del dispositivo. En futuras conexiones con este dispositivo, el sistema puede usar entonces el identificador inicial como el primer identificador de dispositivo.

Usar un identificador inicial recibido de manera pasiva puede resultar útil en situaciones donde el sensor solo puede mantener un número limitado de conexiones activas simultáneas con dispositivos dentro de su zona de detección.

Basándose en el primer identificador de dispositivo, el sistema puede consultar una base de datos (por ejemplo, la base de datos 212) y determinar si el dispositivo está asociado con un usuario conocido por el sistema y que está autorizado para usar el sistema. Si el dispositivo está asociado con un usuario autorizado conocido, entonces en una acción 320 del método el sistema de control de acceso envía un código de acceso al dispositivo electrónico portátil. Dependiendo de la realización, el código de acceso se genera por la base de datos 212, por un servidor acoplado al sistema 200 (por ejemplo, un servidor web, un servidor de seguridad) o por otro dispositivo. El sistema envía el código de acceso al dispositivo electrónico portátil basándose en un segundo identificador de dispositivo, que puede obtenerse a través de la base de datos. El segundo identificador de dispositivo es otro fragmento de información que permite al sistema distinguir el dispositivo electrónico portátil de uno o más de otros dispositivos. También permite al sistema dirigir información al dispositivo. En algunas realizaciones, el segundo identificador de dispositivo es un identificador globalmente único. Dependiendo de las tecnologías particulares usadas, el segundo identificador de dispositivo puede comprender, por ejemplo: una dirección de dispositivo de Bluetooth; una dirección de correo electrónico para una cuenta de correo electrónico a la que se puede acceder a través del dispositivo electrónico portátil; un número telefónico asociado con el dispositivo; una dirección para un servicio de notificación automática; u otro fragmento de información. En al menos algunos casos, el segundo identificador de dispositivo es un identificador global para un sistema de comunicación que es externo al sistema de control de acceso.

Usando el segundo identificador de dispositivo, se envía el código de acceso a través de una red de comunicación inalámbrica, tal como la red 260 de la figura 2. En diversas realizaciones, el código de acceso comprende, por ejemplo: un número; una cadena de caracteres; una imagen; un conjunto de imágenes (que incluye posiblemente imágenes variables en el tiempo, tales como una película); o un código óptico. El código de acceso puede enviarse al dispositivo

electrónico portátil como información de usuario. La información de usuario puede comprender, por ejemplo, un mensaje de texto (SMS), una notificación automática, un mensaje de correo electrónico o un mensaje enviado usando otra tecnología de mensajería. El código de acceso se almacena por un programa de control de acceso que está ejecutándose en el dispositivo. En algunos casos, se genera una notificación de mensaje por el programa para informar al usuario de que el dispositivo ha recibido el código de acceso, o de que el usuario puede autenticar o “desbloquear” el dispositivo (el concepto de desbloqueo de un dispositivo se explica a continuación). El programa puede ejecutarse como parte de un sistema operativo para el dispositivo o como una aplicación independiente (por ejemplo, una “app” de teléfono móvil).

Según la invención, el primer identificador de dispositivo es para un primer canal de comunicaciones, y el segundo identificador de dispositivo es para un segundo canal de comunicaciones. En esta solicitud y en las reivindicaciones, “canal de comunicaciones” se refiere a una tecnología o medios para transmitir información entre dos componentes, por ejemplo, entre el sistema de control de acceso y el dispositivo electrónico portátil. Los ejemplos posibles de un canal de comunicación pueden incluir: una conexión de Bluetooth o Bluetooth LE; una conexión Wi-Fi; una conexión de telefonía celular; una conexión para un sistema de mensajería automática; u otro tipo de conexión. En algunas realizaciones que no son según la invención, los canales de comunicaciones primero y segundo son el mismo canal o el mismo tipo de canal. Por ejemplo, cada uno es una conexión de Bluetooth o Bluetooth LE entre el dispositivo electrónico portátil y un sensor del sistema de control de acceso.

Según la invención, los canales primero y segundo son diferentes tipos de canales de comunicación. En un ejemplo, el primer canal de comunicaciones es una conexión de Bluetooth o Bluetooth LE entre el dispositivo electrónico portátil y un sensor del sistema de control de acceso; el segundo canal de comunicaciones es una conexión de telefonía celular entre el dispositivo electrónico portátil y la red de comunicaciones inalámbricas.

En una acción 330 del método, el usuario presenta el dispositivo en un terminal de acceso, tal como el terminal 250, en una segunda zona (por ejemplo, la zona 112).

En una acción 340 del método, el sensor en o cerca del terminal (por ejemplo, el segundo sensor 240) detecta el dispositivo electrónico portátil. El sensor lee el código de acceso del dispositivo electrónico portátil. El sensor también puede leer datos adicionales del dispositivo, por ejemplo: un certificado digital; el primer identificador de dispositivo; la dirección Wi-Fi para el dispositivo; la dirección MAC para el dispositivo; información de identificación de usuario; información del historial para el dispositivo o para el usuario (por ejemplo, en qué otro lugar ha estado el dispositivo, cuándo estuvo el dispositivo por última vez en esta ubicación); u otra información. En realizaciones particulares, el sensor lee esta información comunicándose con el programa de control de acceso que está ejecutándose en el dispositivo.

Si el código de acceso leído del dispositivo coincide con el código que se envió anteriormente al dispositivo, entonces el sistema concede acceso al usuario en una acción 350 del método.

En algunas realizaciones, cuando el sistema lee el primer identificador de dispositivo del dispositivo electrónico portátil en la acción 310 del método, el dispositivo está en un estado “bloqueado”. El dispositivo también está en un estado bloqueado cuando el sistema envía el código de acceso al dispositivo en la acción 320 del método. Cuando el usuario presenta el dispositivo al terminal en la acción 330 del método, el dispositivo está en un estado “desbloqueado”. En esta solicitud y en las reivindicaciones, el dispositivo está “bloqueado” en el sentido de que al menos alguna funcionalidad del dispositivo o alguna información almacenada en el dispositivo no está disponible a menos que el usuario “desbloquee” el dispositivo autenticándose en el mismo. Por ejemplo, con algunos teléfonos inteligentes, un usuario debe escribir un PIN o introducir otra información en el teléfono para acceder a programas o datos almacenados en el teléfono. Otros dispositivos pueden desbloquearse usando datos biométricos (por ejemplo, una huella dactilar), un gesto en una zona sensible al tacto o una combinación de tipos de entrada. En realizaciones particulares, el terminal puede determinar que el dispositivo electrónico móvil está en un estado desbloqueado basándose en información recibida de una aplicación que está ejecutándose en el dispositivo. Por ejemplo, la aplicación puede indicar que el usuario está actualmente usando la aplicación. En realizaciones adicionales, si el dispositivo está bloqueado o desbloqueado es irrelevante para el funcionamiento de la tecnología.

La figura 3 proporciona un ejemplo de una “visión general” de una realización particular de las tecnologías descritas. Por otro lado, la figura 4 muestra un diagrama de bloques de una realización a modo de ejemplo de un método 400 de control de acceso que se realiza mediante un sistema de control de acceso, tal como el sistema 200 de la figura 2. En una acción 410 del método, el sistema detecta un dispositivo electrónico portátil usando un primer sensor, tal como el primer sensor 220. Como parte de la detección, el sensor determina un primer identificador de dispositivo para el dispositivo electrónico portátil. De manera similar al método 300, basándose en el primer identificador, el sistema puede consultar a una base de datos para determinar si el dispositivo está asociado con un usuario conocido por el sistema y que está autorizado para usar el sistema. Si el dispositivo está asociado con un usuario autorizado conocido, entonces en una acción 420 del método el sistema de control de acceso envía un código de acceso al dispositivo electrónico portátil. El sistema envía el código de acceso al dispositivo electrónico portátil basándose en un segundo identificador de dispositivo, que se obtiene a través de la base de datos. En una acción 430 del método, el sistema usa un segundo sensor para leer el código de acceso del dispositivo electrónico portátil. El segundo sensor puede estar en o cerca de un terminal de acceso. Si el código de acceso leído del dispositivo coincide con el código que se envió anteriormente al dispositivo, entonces el sistema concede acceso al usuario en una acción 440 del método.

En algunas realizaciones del método 400, el dispositivo electrónico portátil está en un estado bloqueado durante las acciones 410 y 420 del método; durante la acción 430 del método, el dispositivo electrónico portátil está en un estado desbloqueado, habiéndose desbloqueado el dispositivo por el usuario antes de que el usuario presente el dispositivo al terminal de acceso.

5 La figura 5 muestra un diagrama de bloques de otra realización a modo de ejemplo de un método de control de acceso, el método 500. El método 500 se realiza por un usuario de un dispositivo electrónico portátil. En una acción 510 del método, el usuario pone el dispositivo electrónico portátil dentro del alcance de un sensor en una primera zona. A modo de ejemplo, la primera zona puede ser el vestíbulo de un edificio, un pasillo u otra zona. Cuando el dispositivo está dentro del alcance del sensor, el sensor puede determinar un primer identificador de dispositivo para el dispositivo.

10 En una acción 520 del método, el usuario recibe un código de acceso usando el dispositivo electrónico portátil.

En algunas realizaciones, un programa de software de control de acceso que está ejecutándose en el dispositivo notifica al usuario que se ha recibido el código de acceso. La notificación puede comprender, por ejemplo: un indicador visual en una pantalla del dispositivo (por ejemplo, “se ha recibido el código de acceso”, un icono u otro indicador visual); un indicador de vibración; un indicador de audio; u otro indicador, incluido una combinación de varios tipos de indicadores. En algunas realizaciones, la notificación indica que debe desbloquearse el dispositivo.

15 En una acción 530 del método, el usuario presenta el dispositivo en un terminal de acceso. El terminal de acceso lee el código de acceso del dispositivo. En una acción 540 del método, el sistema concede acceso al usuario (por ejemplo, acceso a una zona segura).

20 La figura 6 es un diagrama de señales que muestra, según la invención, un intercambio de señales entre diferentes componentes, incluyendo componentes de un sistema de control de acceso. El sistema puede ser, por ejemplo, una versión del sistema 200 o puede ser otro sistema. En la figura 6, se envía un primer identificador de dispositivo por un dispositivo electrónico portátil de un usuario y se recibe por una unidad de control de sistema de acceso (señal 610). Esta información se desplaza hasta la unidad de control a través de un sensor, tal como el sensor 220. Después de recibir el primer identificador de dispositivo, la unidad de control envía el primer identificador de dispositivo a una base de datos (señal 620). Entre otra posible información, la unidad de control recibe un segundo identificador de dispositivo de la base de datos (señal 630). Basándose en el segundo identificador de dispositivo, la unidad de control determina un código de acceso e indica a la red de comunicación inalámbrica que envíe el código de acceso al dispositivo electrónico portátil (señal 640). Entonces, la red de comunicación inalámbrica envía el código de acceso al dispositivo electrónico portátil (señal 650). El dispositivo electrónico portátil transmite el código de acceso a la unidad de control a través de un sensor, tal como el sensor 240 (señal 660). Después de confirmar que el código de acceso es válido, la unidad de control concede acceso al usuario (señal no mostrada).

En realizaciones particulares, que no son según la invención, el código de acceso se genera por un servidor web (no mostrado en la figura 6). El servidor web envía el código de acceso a la base de datos, a la unidad de control y al dispositivo electrónico portátil. En realizaciones adicionales, el código de acceso se genera por la base de datos, que luego envía el código de acceso a la unidad de control y al dispositivo electrónico portátil. El código de acceso también puede generarse por la unidad de control.

35 Por claridad, la figura 6 muestra una representación de alto nivel de señales intercambiadas entre diferentes componentes. Por consiguiente, la figura 6 no muestra todas las señales posibles que pueden intercambiarse entre los componentes mostrados. Por ejemplo, los protocolos de establecimiento de comunicación entre el dispositivo electrónico portátil y otros componentes, tales como la red de comunicación inalámbrica, no se muestran en detalle.

40 En cualquiera de las realizaciones descritas, la validez del código de acceso puede estar limitada a una cierta cantidad de tiempo después de enviarse el código al dispositivo electrónico portátil (por ejemplo, 1 minuto, 2 minutos, 5 minutos, 10 minutos), limitada a un cierto periodo de tiempo (por ejemplo, miércoles entre 9 AM y 10 AM) o a un cierto número de usos (por ejemplo, el código de acceso solo se puede usar una vez, dos veces, cinco veces, diez veces u otro número de veces).

45 En algunos casos, el tiempo de validez del código de acceso se basa en una distancia entre la primera zona y la segunda zona. Por ejemplo, si las zonas primera y segunda están cerca, el tiempo de validez es más corto que para un sistema donde las dos zonas están alejadas. En otros casos, el tiempo de validez se basa en un tiempo de desplazamiento previsto para el usuario entre la primera zona y la segunda zona. El tiempo de desplazamiento previsto puede personalizarse para diferentes usuarios. Por ejemplo, a los usuarios que se mueven lentamente, quizás debido a la edad o a una discapacidad, se les puede asignar más tiempo para desplazarse desde la primera zona hasta la segunda zona.

50 Al menos algunas versiones de las tecnologías descritas pueden usarse en entornos donde diversas zonas dentro de una región tienen diferentes niveles de seguridad o requisitos. Por ejemplo, en una realización, a un usuario se le concede acceso a una zona segura al presentar a un terminal de acceso un dispositivo electrónico portátil en el que está almacenado un código de acceso correspondiente, habiendo desbloqueado previamente el usuario el dispositivo. La validez del código de acceso está limitada a una cierta cantidad de tiempo después de enviarse el código al dispositivo (por ejemplo, 1 minuto, 2 minutos, 5 minutos, 10 minutos, medio día, un día u otra cantidad de tiempo).

En una realización adicional, a un usuario se le concede acceso a una zona segura al presentar a un terminal de acceso un dispositivo electrónico portátil en el que está almacenado un código de acceso. Se puede conceder acceso aunque el usuario no haya desbloqueado el dispositivo. Aunque el código de acceso puede ser válido durante una cantidad de tiempo limitada, el límite de tiempo puede ser un periodo relativamente largo (por ejemplo, una hora, medio día, un día, varios días u otra cantidad de tiempo). Esta realización puede permitir que un usuario entre en una zona segura (así como que se mueva entre diferentes zonas seguras) simplemente poniendo el dispositivo electrónico portátil dentro del alcance del terminal de acceso. El usuario no necesita desbloquear el dispositivo para acceder a la zona segura. Esto puede ser más conveniente para el usuario que una realización que requiere desbloquear el dispositivo cada vez que el usuario desea acceder a otra zona. Esta realización puede combinarse con una realización que requiere inicialmente presentar un dispositivo desbloqueado con el código de acceso, después de lo cual la presentación de un dispositivo bloqueado con el código de acceso es suficiente. La presentación del dispositivo desbloqueado puede ser suficiente para obtener acceso únicamente dentro de una zona específica (por ejemplo, dentro de un piso particular de un edificio). Después de un periodo de tiempo seleccionado (por ejemplo, medio día, un día u otro periodo de tiempo), el sistema de control de acceso puede requerir que el usuario presente nuevamente un dispositivo electrónico portátil desbloqueado a un terminal de acceso, aunque el usuario no haya salido de la zona específica.

En una realización particular, a un usuario se le concede acceso a una zona segura después de desbloquear un dispositivo electrónico portátil y presentar el dispositivo a un terminal de acceso. El código de acceso está almacenado en el dispositivo y, por tanto, al usuario se le concede acceso a la zona segura. Por lo tanto, para obtener acceso a la zona segura, el usuario debe estar en posesión del dispositivo electrónico portátil (con el código de acceso) y debe desbloquear el dispositivo. Sin embargo, dentro de la zona segura, al usuario se le concede acceso a zonas seguras adicionales basándose únicamente en una o más características del dispositivo. Dicho de otro modo, para obtener acceso a las zonas seguras adicionales, el usuario no necesita desbloquear el dispositivo. En cambio, el sistema de control de acceso obtiene un identificador del dispositivo (por ejemplo, una dirección MAC, una dirección Wi-Fi, un número IMEI, un testigo, un número de teléfono u otro fragmento de información) y concede acceso basándose en este identificador. Esta disposición puede proporcionar un nivel algo más bajo de control de acceso seguro con la zona segura, a la vez que se mejora la comodidad para el usuario dentro de la zona segura.

La figura 7 muestra un diagrama de bloques de una realización a modo de ejemplo de un ordenador 700 (por ejemplo, parte de una unidad de control de sistema de control de acceso, parte de un dispositivo electrónico portátil, parte de un terminal de acceso, parte de una unidad de control de ascensor, parte de una base de datos, parte de una red de comunicación inalámbrica) que puede usarse con una o más tecnologías descritas en la presente memoria. El ordenador 700 comprende uno o más procesadores 710. El procesador 710 está acoplado a una memoria 720, que comprende uno o más medios de almacenamiento legibles por ordenador que almacenan instrucciones 730 de software. Cuando se ejecutan por el procesador 710, las instrucciones 730 de software hacen que el procesador 710 realice una o más de las acciones del método descritas en la presente memoria. Realizaciones adicionales del ordenador 700 pueden comprender uno o más componentes adicionales. El ordenador 700 puede estar conectado a uno o más de otros ordenadores o dispositivos electrónicos a través de un componente de entrada/salida (no mostrado). En al menos algunas realizaciones, el ordenador 700 puede estar conectado a otros ordenadores o dispositivos electrónicos a través de una red 740. En realizaciones particulares, el ordenador 700 funciona con uno o más de otros ordenadores, que están ubicados de manera local, remota o ambos. Por lo tanto, uno o más de los métodos descritos pueden realizarse usando un sistema informático distribuido.

Al menos algunas de las realizaciones descritas pueden proporcionar un control de acceso más conveniente y fácil de usar. Por ejemplo, para acceder a una zona segura, un usuario no necesita portar un testigo además del dispositivo electrónico portátil, que puede ser algo que el usuario lleva consigo con fines adicionales, tal como un teléfono inteligente. Además, durante el funcionamiento del sistema, el usuario no necesita introducir manualmente o incluso conocer el código de acceso.

Al menos algunas de las realizaciones descritas pueden proporcionar una mayor seguridad en comparación con métodos de autenticación de un solo factor donde, por ejemplo, solo se requiere un testigo o solo una contraseña. Las realizaciones que requieren que un usuario esté en posesión de un dispositivo electrónico portátil y que pueda desbloquear el dispositivo pueden servir como métodos de autenticación de múltiples factores.

La invención proporciona una mayor seguridad usando diferentes tipos de canales de comunicaciones primero y segundo. Se puede usar cualquier combinación de tecnologías para los canales de comunicaciones. Por ejemplo, el primer identificador de dispositivo puede leerse a partir de un dispositivo electrónico portátil usando una conexión de Bluetooth o Bluetooth LE, mientras el código de acceso se envía al dispositivo usando una conexión telefónica (por ejemplo, como un mensaje de texto). Si la dirección de dispositivo de Bluetooth o Bluetooth LE se ha falseado por un tercero (por ejemplo, para que parezca que el dispositivo del tercero es el dispositivo del usuario), el sistema de acceso seguirá enviando el código de acceso al dispositivo del usuario a través del segundo canal de comunicación. El dispositivo del usuario recibirá el código de acceso, aunque el dispositivo del usuario no esté cerca de un sensor del sistema de control de acceso. El usuario puede reconocer entonces que el tercero está intentando emular el dispositivo del usuario.

En un ejemplo no limitativo, un usuario entra en un edificio y camina hacia el vestíbulo portando un teléfono inteligente. A través de un sensor, un sistema de control de acceso detecta que el teléfono inteligente ha entrado en el vestíbulo y que un programa de software de control de acceso particular está ejecutándose en el teléfono inteligente. El teléfono

- inteligente está en un estado bloqueado. El sistema de control de acceso determina un primer identificador de dispositivo para el teléfono inteligente, que en este caso es una dirección de dispositivo de Bluetooth o un identificador universal (UID). El sistema de acceso usa el primer identificador de dispositivo para determinar si, según una base de datos, el dispositivo pertenece a un usuario autorizado. Después de determinar que el dispositivo pertenece a un
- 5 usuario autorizado, el sistema de acceso recupera, de la base de datos, un segundo identificador de dispositivo para el teléfono inteligente. En este caso, el segundo identificador de dispositivo es una dirección de notificación automática. Usando la dirección de notificación automática, el sistema de control de acceso indica a una red de comunicación inalámbrica (en este caso, la red de telefonía celular) que envíe un código de acceso al teléfono inteligente en una notificación automática. El teléfono inteligente recibe la notificación automática. Como resultado, el programa de
- 10 software que está ejecutándose en el teléfono inteligente visualiza una notificación de que el teléfono inteligente ha recibido el código de acceso. El usuario se desplaza por el vestíbulo y se aproxima a un terminal de control de acceso ubicado en una barrera en el vestíbulo. El usuario desbloquea el teléfono inteligente escribiendo un PIN en el teléfono. El usuario mantiene el teléfono inteligente cerca del terminal de control de acceso. Un sensor de Bluetooth en el terminal detecta el teléfono inteligente, determina que el teléfono inteligente está en un estado desbloqueado, y se
- 15 comunica con el programa de software para leer el código de acceso del teléfono inteligente. El sensor también lee un certificado digital del teléfono inteligente. El sistema de control de acceso confirma que el código de acceso leído del teléfono inteligente es el mismo código que el sistema anteriormente enviado usando la notificación automática, y que el código de acceso corresponde al certificado digital. Entonces, el sistema de control de acceso abre la barrera de vestíbulo para conceder al usuario acceso a una zona segura.
- 20 Aunque muchas de las realizaciones del sistema de acceso descritas se describen de manera general como control de acceso a una zona física, cualquiera de las realizaciones puede adaptarse para controlar el acceso a información (por ejemplo, información almacenada en un ordenador).
- A menos que se indique lo contrario, una expresión que hace referencia a “al menos uno de” una lista de elementos se refiere a cualquier combinación de esos elementos, incluyendo elementos individuales. Como ejemplo, “al menos uno de: a, b o c” se pretende que abarque: a; b; c; a y b; a y c; b y c; y a, b y c. Como otro ejemplo, “al menos uno de: a, b y c” se pretende que abarque: a; b; c; a y b; a y c; b y c; y a, b y c. Tal como se usa en la presente memoria, un
- 25 “usuario” puede ser una persona, un grupo de personas, una máquina, un objeto o un animal.

REIVINDICACIONES

1. Un método, que comprende:

5 determinar un primer identificador de dispositivo para un dispositivo (170) electrónico portátil de un usuario (150), realizándose la determinación en respuesta a entrar el dispositivo (170) electrónico portátil en una primera zona (110) y enviarse el primer identificador de dispositivo usando un primer canal de comunicaciones por el dispositivo (170) electrónico portátil y recibirse a través de un sensor (160, 220) mediante una unidad (210) de control de sistema de acceso, en donde el primer identificador de dispositivo es para el primer canal de comunicación;

como resultado de determinar el primer identificador de dispositivo del dispositivo (170) electrónico portátil,

10 enviar el primer identificador de dispositivo desde la unidad (210) de control de sistema de acceso a una base de datos (212) y recibir por la unidad (210) de control de sistema de acceso un segundo identificador de dispositivo para el dispositivo (170) electrónico portátil de la base de datos (212), habiéndose determinado el segundo identificador de dispositivo basándose en el primer identificador de dispositivo y siendo para un segundo canal de comunicaciones, en el que los canales de comunicación primero y segundo son diferentes tipos de canales de comunicación;

y

20 enviar un código de acceso determinado por la unidad (210) de control de acceso basándose en el segundo identificador de dispositivo para el dispositivo (170) electrónico portátil desde la unidad (210) de control de acceso al dispositivo (170) electrónico portátil usando el segundo canal de comunicaciones, en donde enviar el código de acceso incluye indicar por la unidad (210) de control de sistema de acceso a una red (260) de comunicación inalámbrica que envíe el código de acceso al dispositivo (170) electrónico portátil, y enviar por la red (260) de comunicación inalámbrica el código de acceso al dispositivo (170) electrónico portátil;

leer el código de acceso del dispositivo (170) electrónico portátil en una segunda zona (112) usando un terminal (180, 250) de acceso; y

25 conceder acceso al usuario (150) como resultado de leer el código de acceso del dispositivo (170) electrónico portátil.

30 2. El método según la reivindicación 1, estando el dispositivo (170) electrónico portátil en un estado bloqueado cuando se determina el primer identificador de dispositivo para el dispositivo (170) y cuando se envía el código de acceso al dispositivo (170), y estando el dispositivo (170) electrónico portátil en un estado desbloqueado cuando se lee el código de acceso del dispositivo (170) usando el terminal (180) de acceso.

3. El método según la reivindicación 2, siendo la segunda zona (112) una zona de mayor seguridad, comprendiendo el método, además:

35 leer el código de acceso del dispositivo (170) electrónico portátil en una tercera zona usando otro terminal de acceso mientras el dispositivo (170) está en un estado bloqueado, siendo la tercera zona una zona de menor seguridad y estando dentro de la segunda zona (112); y

conceder al usuario (150) acceso a la tercera zona.

4. El método según cualquier reivindicación anterior, comprendiendo el segundo identificador de dispositivo un identificador global para un sistema de comunicación, siendo el sistema de comunicación externo a un sistema de control de acceso.

40 5. El método según cualquier reivindicación anterior, comprendiendo el envío del código de acceso al dispositivo (170) electrónico portátil enviar información de usuario al dispositivo (170) electrónico portátil.

6. El método según cualquier reivindicación anterior, obteniéndose el primer identificador de dispositivo usando una señal de radio del dispositivo (170) electrónico portátil, o leyéndose el código de acceso del dispositivo (170) electrónico portátil usando una señal de radio del dispositivo (170) electrónico portátil.

45 7. El método según cualquier reivindicación anterior, teniendo el código de acceso un tiempo de validez limitado.

8. El método según la reivindicación 7, basándose el tiempo de validez del código de acceso en un tiempo de desplazamiento previsto para el usuario (150) desde la primera zona (110) hasta la segunda zona (112), en una distancia entre la primera zona (110) y la segunda zona (112), o en un nivel de seguridad para una zona.

50 9. El método según cualquier reivindicación anterior, que comprende además determinar, usando el terminal (180) de acceso, que un programa de control de acceso está ejecutándose en el dispositivo (170) electrónico portátil.

10. El método según cualquier reivindicación anterior, comprendiendo la determinación del primer identificador de dispositivo recibir, usando el sensor (160), un identificador de dispositivo transmitido periódicamente del dispositivo (170) electrónico portátil.
- 5 11. El método según la reivindicación 10, en donde se determina que el primer identificador de dispositivo es el identificador de dispositivo transmitido periódicamente, o en donde el identificador de dispositivo transmitido periódicamente se usa para crear una conexión de comunicación con el dispositivo (170) electrónico portátil, leyéndose el primer identificador de dispositivo del dispositivo a través de la conexión de comunicación.
12. El método según la reivindicación 11, que comprende además determinar si el identificador de dispositivo transmitido periódicamente es un identificador de dispositivo transmitido periódicamente conocido.
- 10 13. Un sistema (200), que comprende:
- un sensor (220);
 - un terminal (180, 250) de acceso;
 - una red (260) de comunicación inalámbrica;
 - una base de datos (212); y
- 15 una unidad (210) de control basada en ordenador acoplada al sensor (220), al terminal (250) de acceso, a la red (260) de comunicación inalámbrica y a la base de datos (212), comprendiendo la unidad (210) de control un procesador (710) y un medio (720) de almacenamiento legible por ordenador, comprendiendo el medio (720) de almacenamiento legible por ordenador instrucciones (730) que hacen que el procesador (710)
- 20 determine un primer identificador de dispositivo para un dispositivo (230) electrónico portátil de un usuario (150) usando el sensor (220), realizándose la determinación en respuesta a entrar el dispositivo (230) electrónico portátil en una primera zona (110) y enviarse el primer identificador de dispositivo usando un primer canal de comunicación por el dispositivo (230) electrónico portátil y recibirse a través del sensor (220), en donde el primer identificador de dispositivo es para el primer canal de comunicaciones,
- como resultado de determinar el primer identificador de dispositivo del dispositivo (230) electrónico portátil,
- 25 enviar el primer identificador de dispositivo a la base de datos (212) y recibir un segundo identificador de dispositivo para el dispositivo (230) electrónico portátil de la base de datos (212), habiéndose determinado el segundo identificador de dispositivo basándose en el primer identificador de dispositivo y siendo para un segundo canal de comunicaciones, en el que los canales de comunicación primero y segundo son diferentes tipos de canales de comunicación;
- 30 enviar, usando el segundo canal de comunicación, un código de acceso al dispositivo (230) electrónico portátil basándose en el segundo identificador de dispositivo para el dispositivo (230) electrónico portátil, en donde enviar el código de acceso incluye indicar a la red (230) de comunicación inalámbrica que envíe el código de acceso al dispositivo (230) electrónico portátil, y enviar el código de acceso al dispositivo (230) electrónico portátil;
- 35 leer el código de acceso del dispositivo (230) electrónico portátil usando el terminal (180, 250) de acceso, estando el terminal (180, 250) de acceso en una segunda zona (112), y
- conceder acceso al usuario (150) como resultado de leer el código de acceso del dispositivo (230) electrónico portátil.

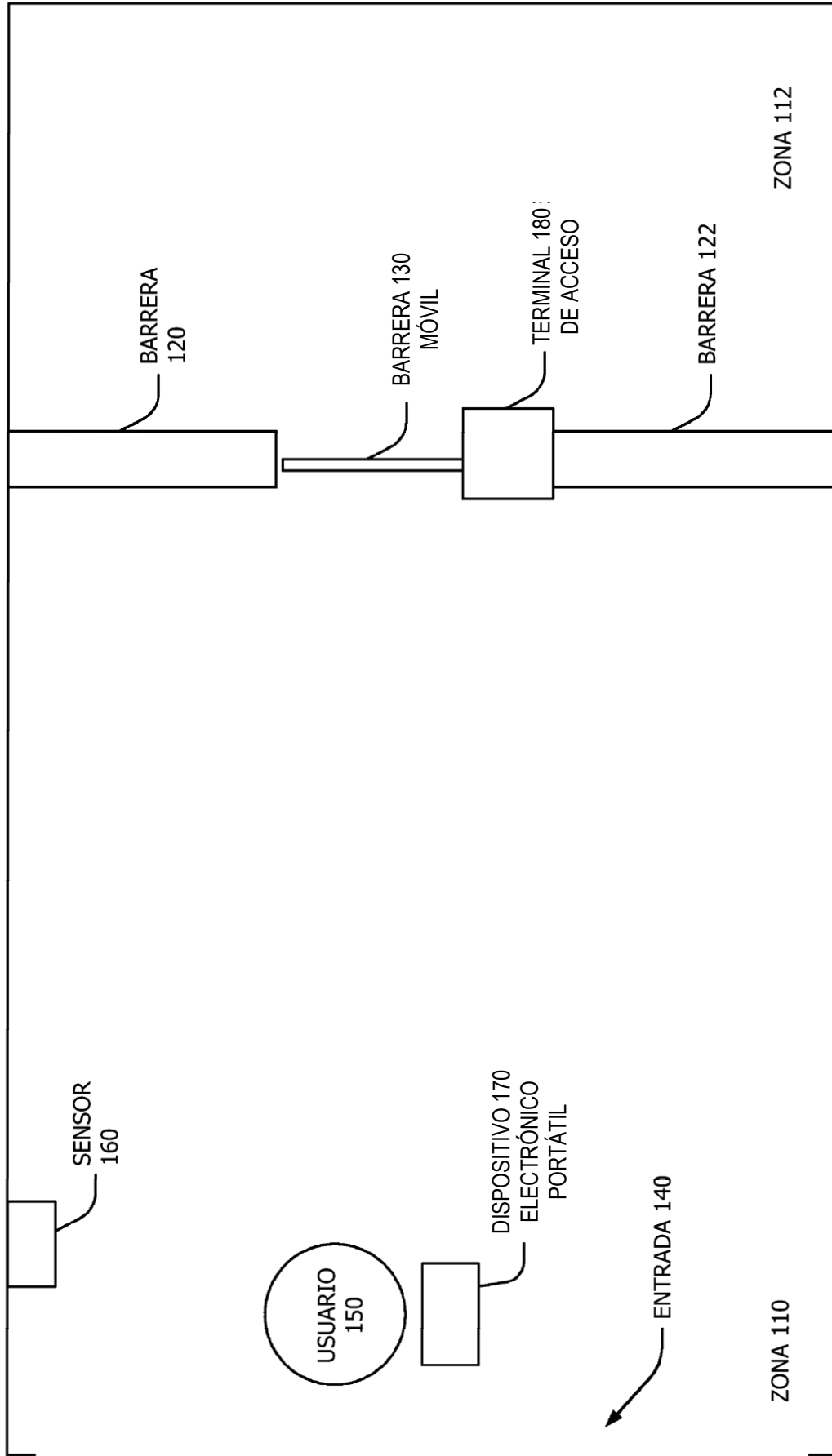


Figura 1

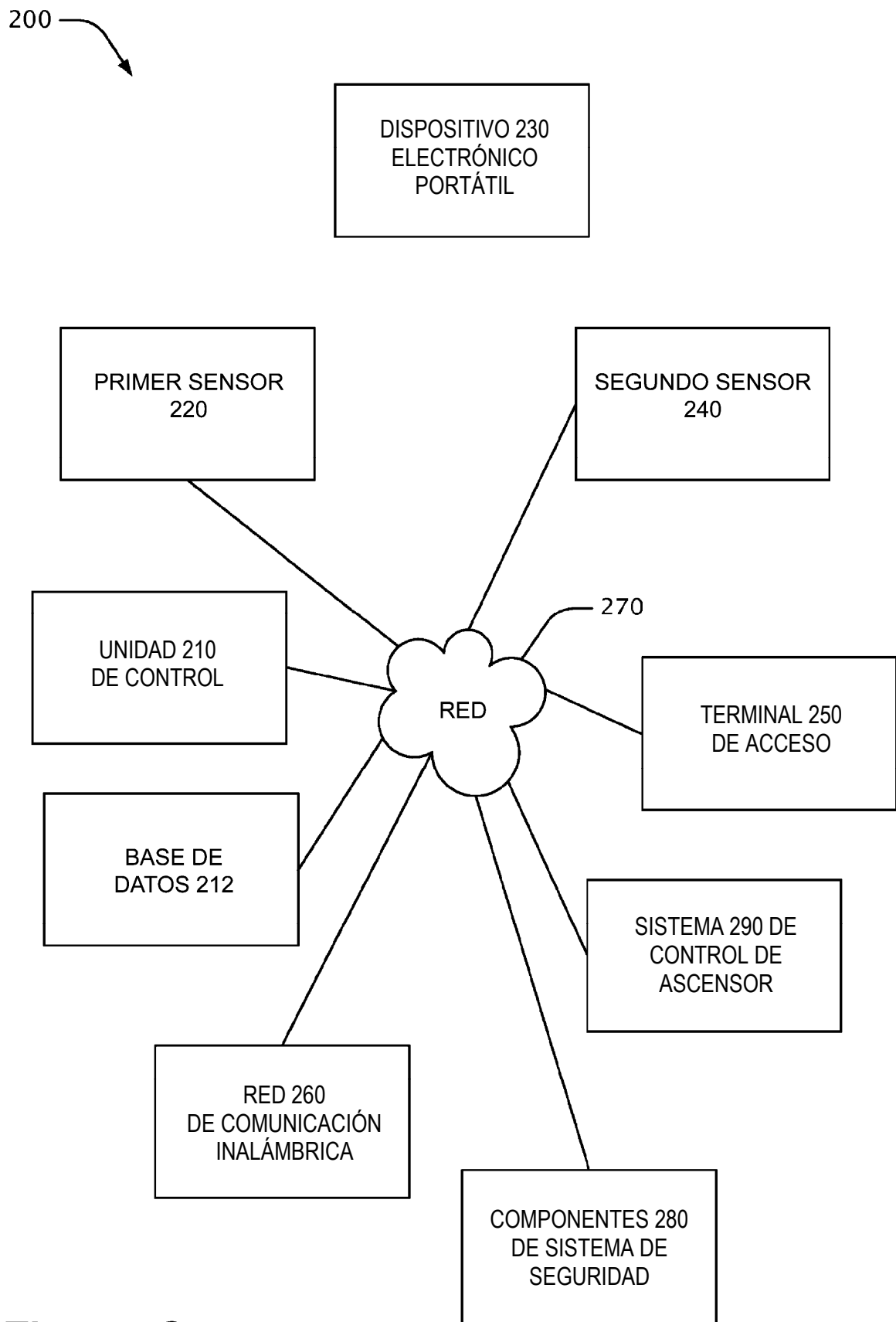


Figura 2

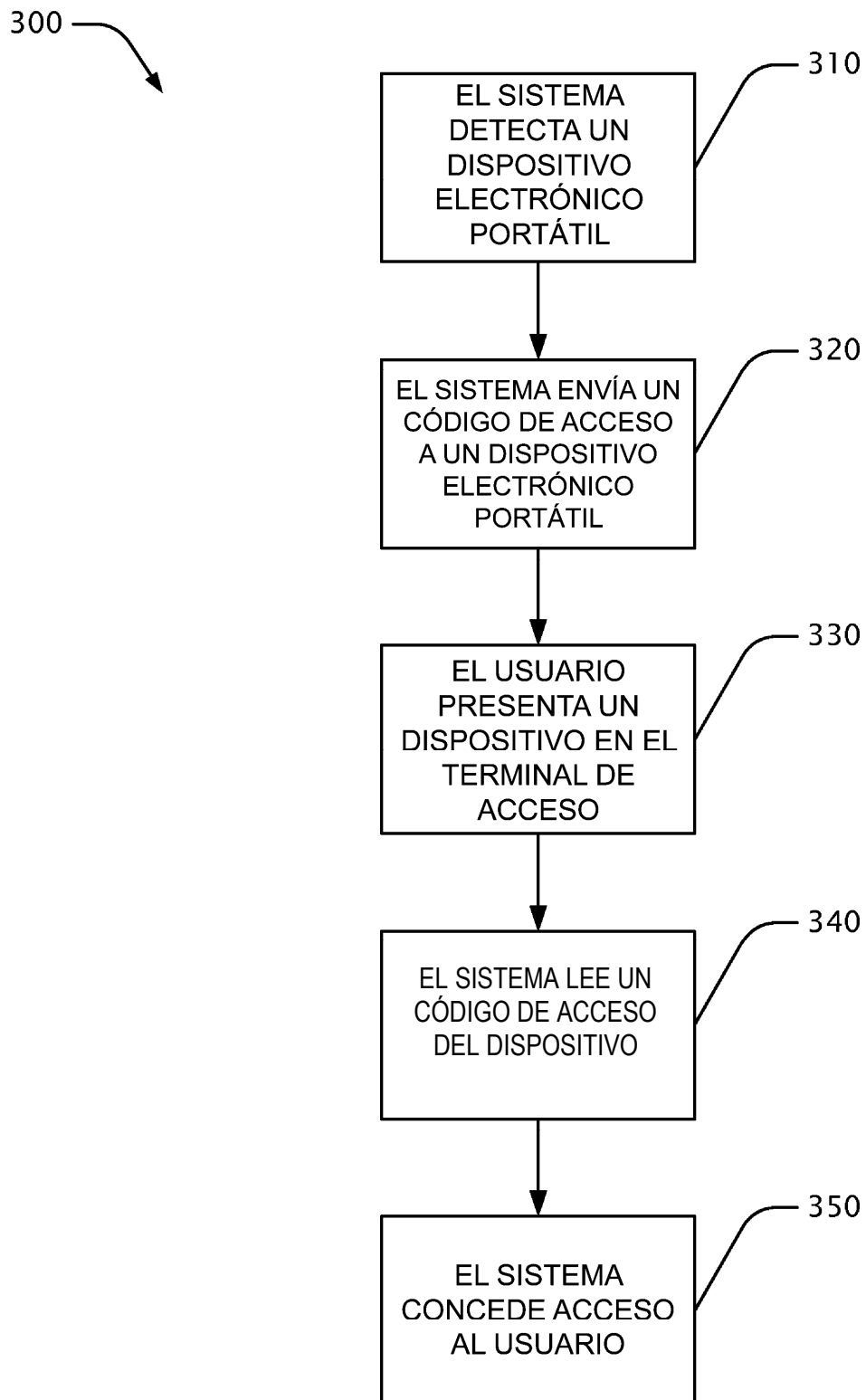


Figura 3

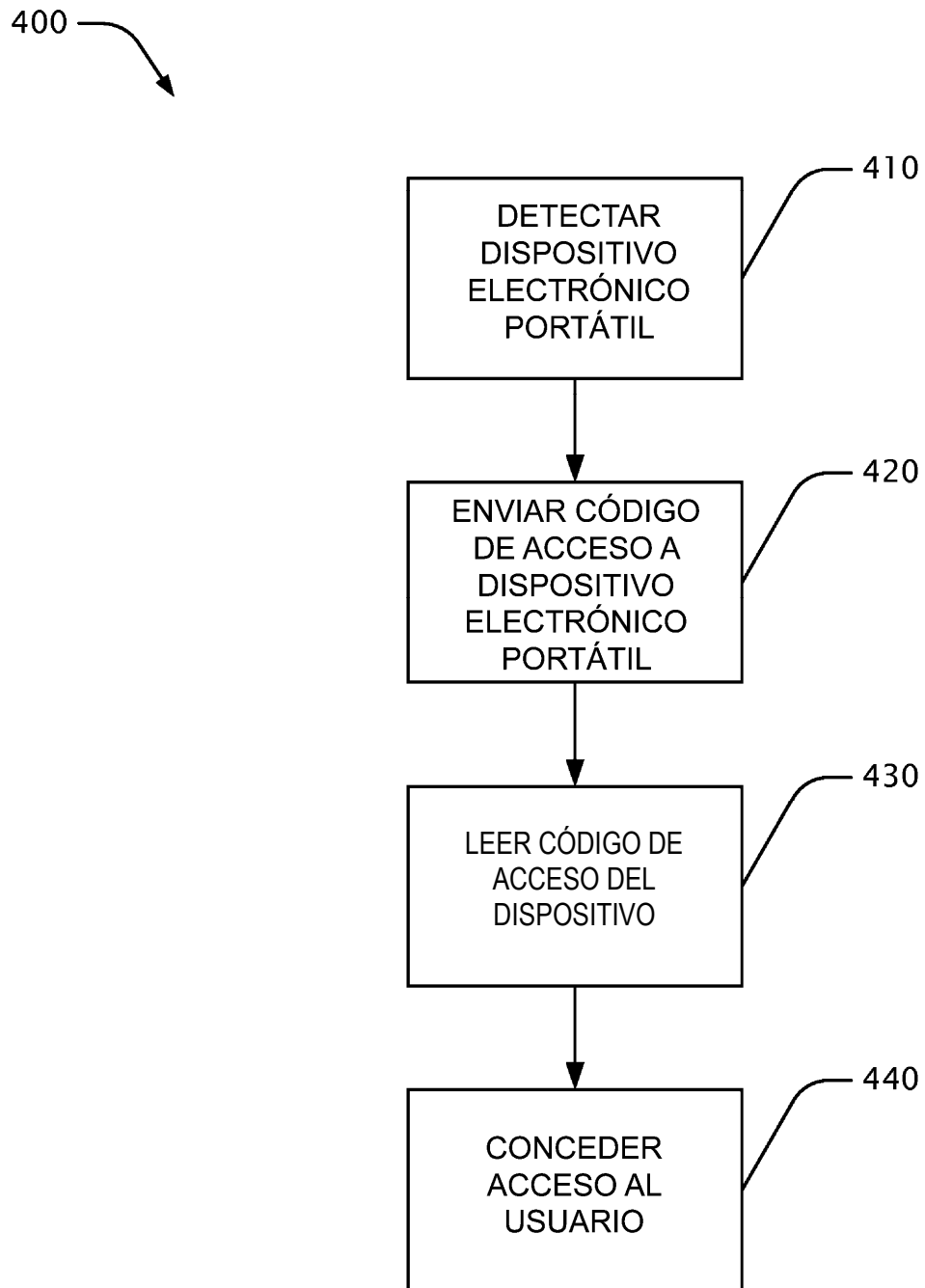


Figura 4

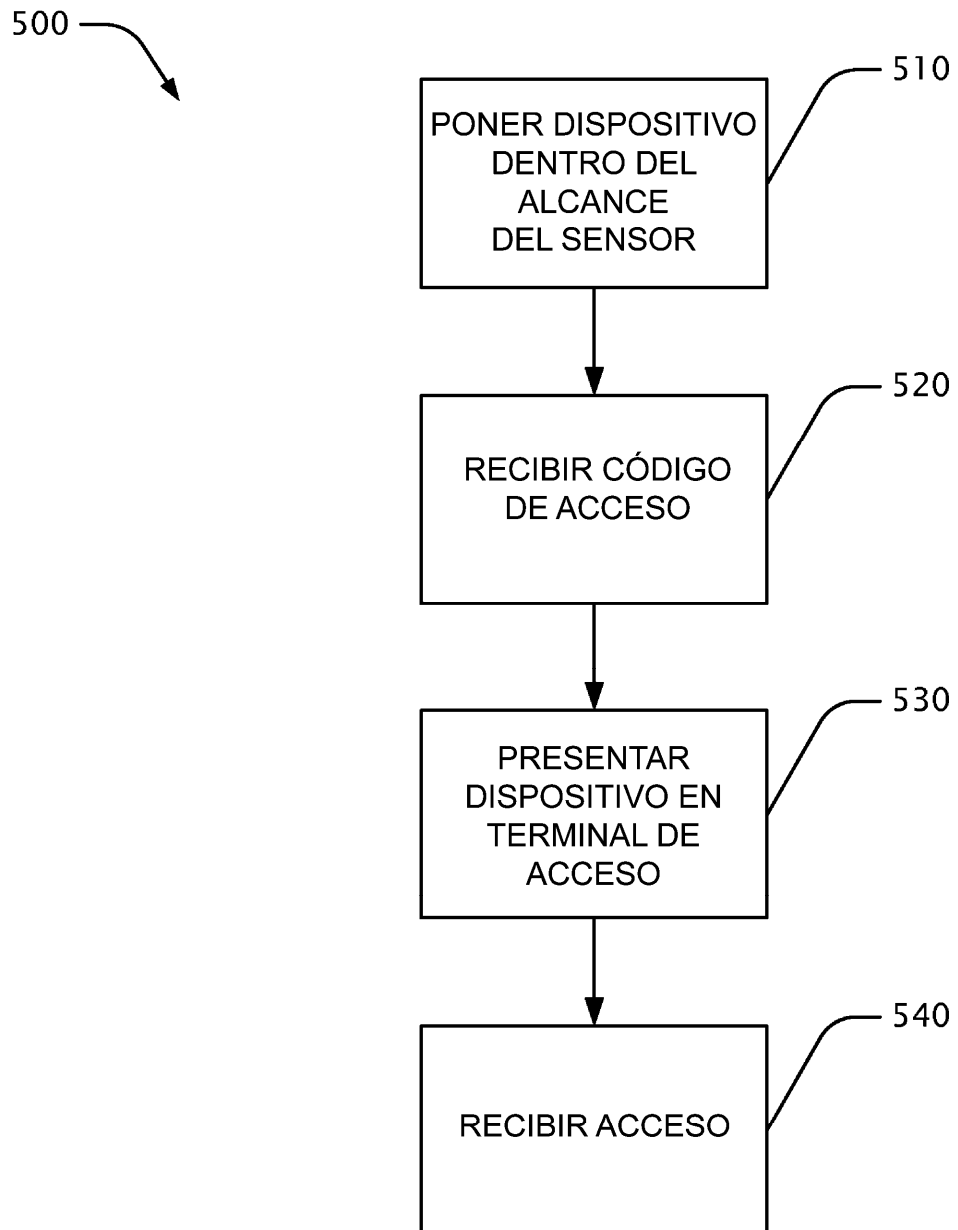


Figura 5

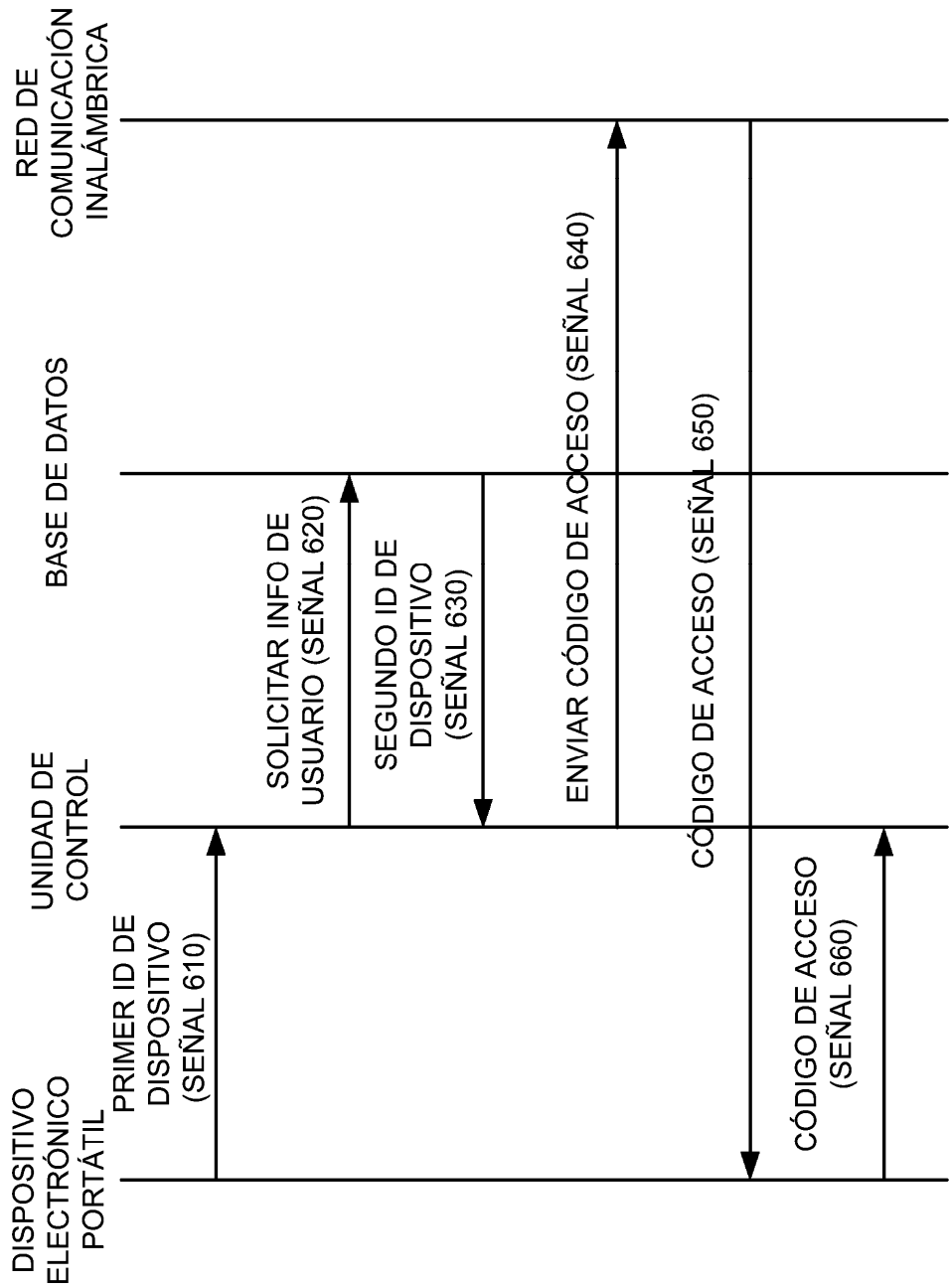


Figura 6

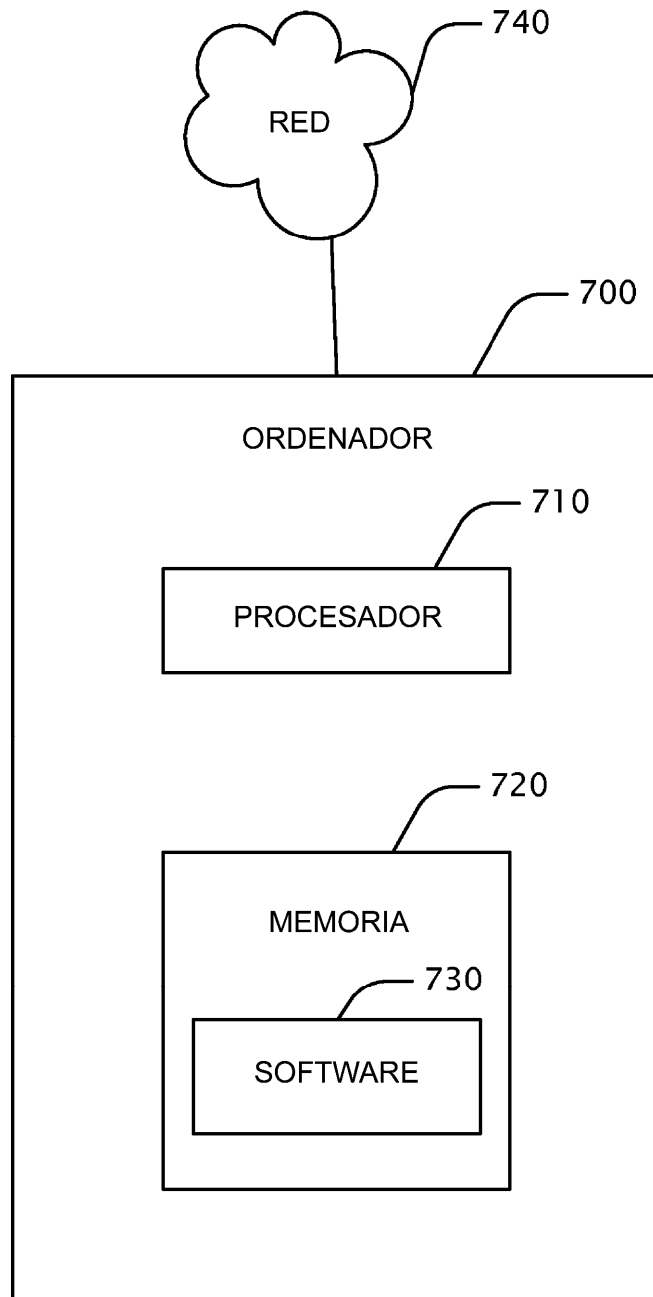


Figura 7