

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 952 755**

51 Int. Cl.:

G07C 9/00

(2010.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **30.05.2017** **PCT/EP2017/025152**

87 Fecha y número de publicación internacional: **21.12.2017** **WO17215788**

96 Fecha de presentación y número de la solicitud europea: **30.05.2017** **E 17726543 (6)**

97 Fecha y número de publicación de la concesión europea: **28.06.2023** **EP 3469558**

54 Título: **Método y dispositivos para configurar dispositivos de control de acceso en un sitio de instalación**

30 Prioridad:

14.06.2016 CH 7572016

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

03.11.2023

73 Titular/es:

DORMAKABA SWITZERLAND LTD (100.0%)
Mühlebühlstrasse, Kempten
8623 Wetzikon, CH

72 Inventor/es:

KUSTER, CHRISTIAN y
ALESSI, PATRIK

74 Agente/Representante:

DIÉGUEZ GARBAYO, Pedro

ES 2 952 755 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

Método y dispositivos para configurar dispositivos de control de acceso en un sitio de instalación

5 Campo de la invención

La presente invención se refiere a un método y dispositivos para configurar dispositivos de control de acceso en un sitio de instalación. Específicamente, la presente invención se refiere a un método y a un sistema informático para configurar e instalar dispositivos de control de acceso en un sitio de instalación.

10 Antecedentes de la invención

Los dispositivos de control de acceso que controlan el acceso a áreas restringidas cerradas por puertas son unidades independientes que están conectadas a las puertas en el sitio donde está instalada la puerta.

Normalmente, los dispositivos de control de acceso incluyen un dispositivo de cierre electromecánico y un controlador de acceso que controla el dispositivo de cierre. El controlador de acceso puede incluir un teclado para introducir un código de acceso y/o un lector de tarjetas para leer información de identificación y/o autorización de la tarjeta de un usuario a través de una interfaz RFID (identificación por radiofrecuencia), magnética o por contacto. Desafortunadamente, los diferentes tipos y tamaños de puertas o portones tienen diferentes interfaces de conexión y requieren diferentes señales de control. A menos que un dispositivo de control de acceso esté preconfigurado para un tipo específico de puerta o portón, el dispositivo de control de acceso debe configurarse *in situ* tras haber sido instalado y conectado a la puerta o portón. Si bien la configuración previa de los dispositivos de control de acceso haría innecesaria la configuración *in situ*, requiere una gestión laboriosa de los dispositivos preconfigurados (el dispositivo en concreto debe estar en el momento correcto en el lugar correcto con la configuración correcta y ser asignable a una puerta o portón específico) y es inflexible y propensa a errores. Por otro lado, la configuración ad-hoc *in situ* de dispositivos de control de acceso individuales es extremadamente ineficaz, particularmente en edificios que tienen muchas áreas restringidas con diferentes tipos de puertas y portones.

El documento EP 2701124 describe un método para configurar una unidad de control de cierre de un sistema de control de acceso. La unidad de control de cierre está asociada con una llave electrónica y está configurada para comunicación inalámbrica con una unidad de usuario móvil. De acuerdo con el documento EP 2701124, antes de instalar la unidad de control de cierre en una ubicación concreta, la unidad de control de cierre y la ubicación concreta se registran en el sistema de control de acceso. La unidad de control de cierre envía su identificador de unidad de control de cierre a la unidad móvil. Se solicita una llave electrónica al sistema de control de acceso. La unidad móvil se comunica con la unidad de control de cierre y envía a la unidad de control de cierre la llave electrónica y opcionalmente uno o más parámetros.

El documento WO 2014/044832 describe un método y un sistema para la configuración de sistemas de bloqueo con cerraduras electrónicas que se comunican con tarjetas RFID pasivas. Según el documento WO 2014/044832, las cerraduras electrónicas y las tarjetas RFID se configuran mediante teléfonos inteligentes. Una aplicación de administración del teléfono inteligente accede a un servicio en la nube para almacenar de forma centralizada en la nube los datos del sistema de cierre y solicitar datos de la llave y la programación. A continuación, el teléfono inteligente se utiliza para transferir los datos de la llave y los datos de programación al sistema de cierre y las tarjetas RFID.

El documento WO 2015/177020 divulga un dispositivo terminal electrónico que se puede configurar utilizando un identificador de dispositivo que se introduce en el dispositivo. El dispositivo terminal envía el identificador de dispositivo a un servidor de configuración. El servidor de configuración responde enviando información de configuración al dispositivo terminal en función del identificador del dispositivo.

Sumario de la invención

Es un objeto de esta invención proporcionar un método y dispositivos para configurar dispositivos de control de acceso en un sitio de instalación, cuyo método y dispositivos no tienen al menos algunas de las desventajas de la técnica anterior. En particular, es un objeto de la presente invención proporcionar un método y dispositivos para configurar dispositivos de control de acceso en un sitio de instalación, cuyo método y dispositivos hacen posible una configuración eficiente y flexible de los dispositivos de control de acceso.

De acuerdo con la presente invención, estos objetos se logran a través de las características de las reivindicaciones independientes. Además, de las reivindicaciones dependientes y de la descripción se derivan realizaciones ventajosas adicionales.

De acuerdo con la presente invención, los objetos antes mencionados se logran particularmente de acuerdo con la reivindicación 1.

En una realización, almacenar los datos de configuración incluye almacenar información de conectividad para los dispositivos de control de acceso y para los componentes de hardware conectados a los dispositivos de control de acceso.

- 5 En otra realización, almacenar los datos de configuración incluye almacenar información de temporización para los dispositivos de control de acceso y para controlar los componentes de hardware conectados a los dispositivos de control de acceso.

- 10 En una realización, se dispone una representación visual del identificador de medios en una superficie del dispositivo de medios de configuración. Generar el registro incluye leer la representación visual del identificador de medios en la superficie del dispositivo de medios de configuración.

- 15 En una realización adicional, leer el identificador de medios almacenado en el dispositivo de medios de configuración incluye colocar el dispositivo de medios de configuración dentro de un alcance de recepción de un lector RFID y el lector de RFID lee el identificador de medios del dispositivo de medios de configuración.

- 20 En una realización, asignar el dispositivo de control de acceso concreto a uno de los dispositivos de control de acceso no identificados incluye recibir en el sistema informático basado en la nube instrucciones de usuario que vinculan el identificador de dispositivo del dispositivo de control de acceso concreto a uno de los dispositivos de control de acceso no identificados del sitio de instalación asignado al identificador de medios.

- 25 En otra realización, la información de ubicación se recibe en el dispositivo de control de acceso concreto desde un dispositivo de comunicación móvil, y asignar el dispositivo de control de acceso concreto a uno de los dispositivos de control de acceso no identificados incluye recibir en el sistema informático basado en la nube la información de ubicación del dispositivo de control de acceso concreto y usar la información de ubicación para la asignación del dispositivo de control de acceso concreto a uno de los dispositivos de control de acceso no identificados.

- 30 En una realización, el dispositivo de control de acceso concreto recibe los datos de configuración del sistema informático basado en la nube y realiza un proceso de configuración utilizando los datos de configuración.

- 35 En otra realización, se almacena un código de instalación en el dispositivo de medios de configuración. El identificador de medios y el código de instalación del dispositivo de medios de configuración se almacenan en el sistema informático basado en la nube. El código de instalación se transmite desde el sistema informático basado en la nube a una puerta de enlace del controlador de dispositivos en el sitio de instalación. El acceso de un dispositivo de control de acceso inalámbrico a la puerta de enlace del controlador de dispositivos se controla utilizando el código de instalación almacenado en el dispositivo de medios de configuración y el código de instalación recibido en la puerta de enlace del controlador de dispositivos.

- 40 Además de un método para configurar e instalar dispositivos de control de acceso en un sitio de instalación, la presente invención también se refiere a un sistema informático para configurar los dispositivos de control de acceso en el sitio de instalación de acuerdo con la reivindicación 9.

- 45 En una realización, los datos de configuración incluyen información de conectividad para los dispositivos de control de acceso y para los componentes de hardware conectados a los dispositivos de control de acceso.

En otra realización, los datos de configuración incluyen información de temporización para los dispositivos de control de acceso y para controlar los componentes de hardware conectados a los dispositivos de control de acceso.

- 50 En una realización, los procesadores del sistema informático están configurados para recibir, con el fin de asignar el dispositivo de control de acceso concreto a uno de los dispositivos de control de acceso no identificados, instrucciones de usuario que vinculan el identificador de dispositivo del dispositivo de control de acceso concreto a uno de los dispositivos de control de acceso no identificados del sitio de instalación asignado al identificador de medios. En otra realización, los procesadores del sistema informático están configurados para recibir, con el fin de asignar el dispositivo de control de acceso concreto a uno de los dispositivos de control de acceso no identificados, información de ubicación del dispositivo de control de acceso concreto y usar la información de ubicación para asignar el dispositivo de control de acceso concreto a uno de los dispositivos de control de acceso no identificados.

- 60 En una realización, los procesadores están configurados para almacenar el identificador de medios y un código de instalación almacenado en el dispositivo de medios de configuración; y para transmitir el código de instalación a una puerta de enlace del controlador de dispositivos en el sitio de instalación, para habilitar el control de acceso de un dispositivo de control de acceso inalámbrico a la puerta de enlace del controlador de dispositivos, utilizando el código de instalación almacenado en el dispositivo de medios de configuración y el código de instalación transmitido al puerta de enlace del controlador de dispositivo.

65

Breve descripción de los dibujos

La presente invención se explicará con más detalle, a modo de ejemplo, con referencia a los dibujos, en los que:

- Figura 1: muestra un diagrama de bloques que ilustra esquemáticamente un sitio de instalación con un dispositivo de control de acceso conectado a través de una red de comunicación a un sistema informático (basado en la nube).
- Figura 2: muestra un diagrama de bloques que ilustra esquemáticamente un sitio de instalación con varios dispositivos de control de acceso conectados a través de una puerta de enlace y una red de comunicación a un sistema informático (basado en la nube).
- Figura 3: muestra un diagrama de flujo que ilustra una secuencia de ejemplo de pasos para configurar e instalar dispositivos de control de acceso en un sitio de instalación.

Descripción detallada de las realizaciones preferidas

En las Figuras 1 y 2, el número de referencia 3 se refiere a un sitio de instalación para los dispositivos de control de acceso 4, 4'. El sitio de instalación 3 es un local o un edificio, por ejemplo, un edificio público, privado o industrial, con áreas restringidas como salas, pisos, ascensores, etc., que están cerrados por puertas, portones, etc. Las puertas o portones pueden ser de diferentes tipos, por ejemplo, puertas batientes, puertas giratorias, puertas correderas, puertas dobles correderas, etc., y de diferente tamaño, fabricación y marca. Las áreas restringidas o sus puertas o portones, respectivamente, están protegidas, cada una, con un dispositivo de control de acceso 4, 4'.

Como se ilustra en las Figuras 1 y 2, los dispositivos de control de acceso 4, 4' incluyen, cada uno, un dispositivo de cierre 40, un lector 41 y un controlador de acceso 42. El dispositivo de cierre 40 está en una carcasa separada del lector 41 y el controlador de acceso 42.

Los dispositivos de cierre 40 son dispositivos electromecánicos de varios tipos que están conectados a través de conexiones cableadas al controlador de acceso 42 del respectivo dispositivo de control de acceso 4, 4'.

Los controladores de acceso 42 incluyen circuitos electrónicos configurados para realizar varias funciones, como se describe más adelante con más detalle. Los circuitos electrónicos de los controladores de acceso 42 incluyen procesadores programables con datos y memoria de programa para almacenar datos de configuración y módulos de software programados para controlar los procesadores.

Los lectores 41 están conectados al controlador de acceso 42 del respectivo dispositivo de control de acceso 4, 4'. Los lectores 41 incluyen circuitos electrónicos y una antena configurada para leer datos a través de una interfaz de comunicación de datos inalámbrica desde un dispositivo multimedia 5. Los lectores 41 están configurados como lectores RFID para leer datos almacenados en un almacenamiento de datos 50 de dispositivos de medios 5 que se implementan como tarjetas o transpondedores RFID (identificador por radiofrecuencia).

Usando el lector conectado 41, el controlador de acceso 42 está configurado para leer y recibir datos del almacenamiento de datos 50 de un dispositivo de medios 5 colocado dentro de su alcance de recepción. Si el dispositivo multimedia 5 es una tarjeta de identificación de usuario, el controlador de acceso 42 procesa la información de identificación del usuario almacenada en el almacenamiento de datos 50 para determinar si el usuario respectivo está autorizado para acceder al área restringida protegida por el dispositivo de control de acceso respectivo 4, 4' (por ejemplo, basado en derechos de acceso, listas blancas y/o listas negras almacenadas en el controlador de acceso 42). Si el usuario está autorizado, el controlador de acceso 42 genera señales de control para que el dispositivo de cierre 40 abra la puerta o portón respectivo. De lo contrario, el controlador de acceso 42 genera señales de control para indicar al usuario que el acceso está denegado, por ejemplo, a través de una interfaz de señalización óptica y/o acústica.

En la realización de la figura 1, el dispositivo de control de acceso 4 comprende además un controlador de dispositivo remoto 44 conectado al controlador de acceso 42. El controlador de dispositivo remoto 44 comprende un circuito electrónico configurado para intercambiar datos con un sistema informático remoto 1 a través de una red de comunicación 2. Específicamente, la red de comunicación 2 incluye Internet y el sistema informático 1 es un sistema informático basado en la nube. Dependiendo de la realización y/o configuración, la red de comunicación 2 incluye además una LAN (Red de área local), WLAN (LAN inalámbrica) y/o una red de radio móvil, como GSM (Sistema global para comunicación móvil) o UMTS (Sistema universal de telecomunicaciones móviles), para acceder al sistema informático basado en la nube 1 a través de Internet. En una realización, la comunicación entre el controlador de dispositivo remoto 44 y el sistema informático basado en la nube 1 se implementa como una pila de IoT (Internet de las cosas) sobre TCP/IP (Protocolo de control de transmisión/Protocolo de Internet).

El sistema informático basado en la nube 1 comprende una pluralidad de ordenadores, teniendo cada ordenador uno o más procesadores, conectados a un sistema de almacenamiento de datos (por ejemplo, una matriz de discos). El sistema informático basado en la nube 1 comprende además una aplicación de planificación e instalación del sitio 10. La aplicación de planificación e instalación del sitio 10, de forma abreviada "aplicación del sitio" 10, es un programa de software configurado para controlar los procesadores del sistema informático basado en la nube 1 para realizar varias funciones que se describen a continuación con más detalle.

En la realización de la figura 2, el sitio de instalación 3 comprende además un controlador de dispositivo remoto 46 que está configurado como una puerta de enlace inalámbrica entre los dispositivos de control de acceso inalámbrico 4' y el sistema informático basado en la nube 1. En consecuencia, en la realización de la figura 2, los dispositivos de control de acceso 4' comprenden además un módulo inalámbrico 45 configurado para la comunicación inalámbrica de datos con la puerta de enlace del controlador de dispositivo remoto 46. Por ejemplo, el módulo inalámbrico 45 y el controlador de dispositivo remoto (puerta de enlace) 46 están configurados para la comunicación de datos según la especificación ZigBee (basada en I EEE 802.15.4) o Bluetooth. El controlador de dispositivo remoto (puerta de enlace) 46 está configurado además para la comunicación de datos con el sistema informático remoto 1 a través de una red de comunicación 2, como se ha descrito anteriormente en el contexto del controlador de dispositivo remoto 44 de la figura 1.

En las figuras 1 y 2, el número de referencia 6 se refiere a un dispositivo terminal conectado a la red de comunicación 2. Por ejemplo, el dispositivo terminal 6 es un ordenador personal, una tableta, un teléfono inteligente u otro dispositivo de comunicación móvil configurado para la comunicación de datos con el sistema informático remoto 1 a través de la red de comunicación 2. El dispositivo terminal 6 está configurado para acceder e interactuar con la aplicación del sitio 10, como se describe con más detalle a continuación. Para interactuar con la aplicación del sitio 10, el dispositivo terminal 6 comprende una aplicación de programa local, por ejemplo, un navegador, una aplicación de cliente y/o lo que se conoce como una *app*.

En los siguientes párrafos, descritos con referencia a la figura 3, se encuentran posibles secuencias de pasos para configurar e instalar dispositivos de control de acceso 4, 4' en un sitio de instalación 3.

En el paso S1, un usuario usa un dispositivo terminal 6 para acceder y usar la aplicación del sitio 10 en el sistema informático basado en la nube 1. Específicamente, el usuario utiliza la aplicación del sitio 10 para planificar y configurar un sitio de instalación 3 con uno o más dispositivos de control de acceso 4, 4'. Como se ilustra esquemáticamente en la figura 3, en el paso S1, los datos de planificación y configuración para un sitio de instalación específico 3 se transmiten desde el dispositivo terminal 6 al sistema informático basado en la nube 1. Los datos de configuración determinan la ubicación de uno o más dispositivos de control de acceso 4, 4' con respecto a un plano de planta del sitio de instalación 3. Los dispositivos de control de acceso 4, 4' se definen con respecto a sus tipos particulares y en contexto con sus componentes de hardware respectivamente conectados, por ejemplo, tipo, tamaño, marca de puerta o portones, etc. Sin embargo, los dispositivos de control de acceso 4, 4' permanecen sin identificar, es decir, los datos de planificación y configuración no definen una unidad física específica por medio de un número de equipo único o identificador de unidad. En otras palabras, los datos de configuración o plano del sitio de instalación 3 incluyen representaciones lógicas de los dispositivos de control de acceso 4, 4'.

En el paso S10, la aplicación del sitio 10 almacena en el sistema informático basado en la nube 1 los datos recibidos de planificación y configuración para el respectivo sitio de instalación 3. En una realización, la finalización de los datos de planificación y configuración para un sitio de instalación concreto 3 desencadena un proceso de pedido o fabricación para producir los tipos requeridos de dispositivos de control de acceso 4, 4'. Aparte de los tipos y números de unidades requeridos, la fabricación de estos dispositivos de control de acceso 4, 4' se ejecuta sin tener en cuenta ningún dato de configuración especificado por el usuario en el paso S1; en otras palabras, los dispositivos de control de acceso 4, 4' se fabrican de forma genérica, sin ninguna personalización.

En el paso S2, el dispositivo de medios de configuración 5, que se utilizará en el sitio de instalación 3 real para instalar y configurar el sistema de control de acceso, se registra en la aplicación del sitio 10 del sistema informático basado en la nube 1. Específicamente, un identificador de medios almacenado en el almacenamiento de datos 50 del dispositivo de medios de configuración 5 se comunica con la aplicación de sitio 10 del sistema informático basado en la nube 1 en conexión con el sitio de instalación 3. Para ello, el identificador de medios almacenado en el dispositivo de medios de configuración 5 se lee por medio de un lector RFID o una representación visual del identificador de medios provisto y dispuesto en la superficie del dispositivo de medios de configuración 5 se lee y comunica a la aplicación del sitio 10 en el sistema informático basado en la nube 1. Dependiendo de la realización y/o configuración, la representación visual del identificador de medios es un código alfanumérico que el usuario introduce manualmente o un código de barras o código QR que el usuario escanea mediante un escáner o una aplicación de escaneo del dispositivo terminal 6.

En el paso S20, la aplicación del sitio 10 registra el dispositivo de medios de configuración 5 almacenando en el sistema informático basado en la nube 1 el identificador de medios recibido asignado al sitio de instalación especificado 3.

En el paso S3, un usuario instala físicamente los tipos especificados de dispositivos de control de acceso 4, 4' en el sitio de instalación 3 real según el plano y la configuración definidos. Específicamente, los dispositivos de cierre 40 determinados se conectan a sus puertas o portones respectivos, se montan los controladores de acceso 42 y los lectores 41, los controladores de acceso 42 se cablean a sus dispositivos de cierre 40 y se establecen conexiones a una fuente de alimentación. Además, los controladores de dispositivos remotos 44 y las puertas de enlace del controlador de dispositivos remotos 46 están conectados a la red de comunicación 2.

En el paso S4, un usuario comienza a configurar los dispositivos de control de acceso 4, 4' instalados físicamente en el sitio de instalación 3. Específicamente, el usuario presenta el dispositivo de medios de configuración 5 registrado para el sitio de instalación 3 a un lector 41 de uno de los dispositivos de control de acceso 4, 4' instalados'.

5 En el paso S40, el lector 41 realiza una operación de lectura y el identificador de medios del dispositivo de medios de configuración 5 registrado se transmite al lector 41 del respectivo dispositivo de control de acceso 4, 4'.

10 En el paso S5, el identificador de medios del dispositivo de medios de configuración 5 registrado se transmite desde el respectivo dispositivo de control de acceso 4, 4' a través de la red de comunicación 2 al sistema informático basado en la nube 1. Como se indica esquemáticamente en la figura 3, el respectivo dispositivo de control de acceso 4, 4' transmite además al sistema informático basado en la nube 1 un identificador de dispositivo único del dispositivo de control de acceso 4, 4' o su dispositivo de cierre 40, respectivamente (no necesariamente en el mismo tiempo que el identificador de medios). En la realización según la figura 1, la comunicación entre el dispositivo de control de acceso 4 y el sistema informático basado en la nube 1 es ejecutada por el controlador de dispositivo remoto 44 a través de la red de comunicación 2. En la realización según la figura 2, la comunicación entre el dispositivo de control de acceso 4' y el sistema informático basado en la nube 1 se ejecuta a través de la puerta de enlace del controlador de dispositivo remoto 46. Por lo tanto, el identificador de medios leído por el lector 41 y el identificador de dispositivo único del dispositivo de control de acceso 4' o su dispositivo de cierre 40, respectivamente, son transmitidos por el módulo inalámbrico 45 a la puerta de enlace del controlador de dispositivo remoto 46; desde la puerta de enlace del controlador de dispositivo remoto 46, el identificador de medios y el identificador de dispositivo único se transmiten al sistema informático basado en la nube 1.

25 En la realización según la figura 2, se realizan pasos adicionales para autorizar la comunicación entre el módulo inalámbrico 45 del respectivo dispositivo de control de acceso 4' y la puerta de enlace del controlador de dispositivo remoto 46. Para ello, además del identificador de medios, el dispositivo de medios de configuración 5 también tiene almacenado de forma segura un código de instalación (no legible por una unidad externa). El código de instalación se genera como un código aleatorio secreto y se almacena en el almacenamiento de datos 50 del dispositivo de medios de configuración 5 como parte del proceso de fabricación. El código de instalación del dispositivo de medios de configuración 5 también se almacena en el sistema informático basado en la nube 1. Cuando la puerta de enlace del controlador de dispositivo remoto 46 recibe el identificador de medios del módulo inalámbrico 45 (paso S5), la puerta de enlace del controlador de dispositivos remotos 46 obtiene del sistema informático basado en la nube 1 el código de instalación asignado al identificador de medios recibido. Para verificar la autenticidad del dispositivo de control de acceso 4', la puerta de enlace del controlador de dispositivo remoto 46 verifica que el código de instalación recibido del sistema informático basado en la nube 1 corresponde (coincide) con el código de instalación almacenado en los medios de configuración 5 presentados al lector 41 de el respectivo dispositivo de control de acceso 4', antes de que se permita cualquier otra comunicación. Por ejemplo, se realiza la verificación del código de instalación utilizando algoritmos criptográficos conocidos, como un par de claves asimétricas (PKI) almacenadas en los medios de configuración 5.

40 En el paso S6, la aplicación del sitio 10 en el sistema informático basado en la nube 1 determina el sitio de instalación 3 asignado y definido por el identificador de medios recibido en el paso S5.

45 En el paso S7 o S7', respectivamente, la aplicación del sitio 10 en el sistema informático basado en la nube 1 recibe información de asignación que permite la asignación del dispositivo de control de acceso 4, 4' físico real a un dispositivo de control de acceso no identificado correspondiente incluido en el plano del sitio de instalación 3 específico identificado en el paso S5. En la realización del paso S7, la información de asignación se transmite desde el dispositivo terminal 6 a la aplicación del sitio 10 en el sistema informático basado en la nube 1. En la realización del paso S7', la información de asignación se transmite desde el respectivo dispositivo de control de acceso 4, 4' a la aplicación del sitio 10 en el sistema informático basado en la nube 1. Por lo tanto, el dispositivo de control de acceso 4, 4' físico real se asigna a su representación lógica correspondiente (hasta ahora no identificada) en el plano del sitio de instalación 3 respectivo. La asignación o coincidencia del dispositivo de control de acceso 4, 4' físico real con su representación lógica correspondiente en el plano del sitio de instalación 3 respectivo se realiza a través de un proceso de emparejamiento. Por ejemplo, la información de asignación incluye información de ubicación relacionada con la ubicación del dispositivo de control de acceso 4, 4' físico real en el sitio de instalación 3. La aplicación de sitio 10 en el sistema informático basado en la nube 1 usa la información de ubicación para asignar el dispositivo de control de acceso 4, 4' físico real a su representación lógica correspondiente en el plano del sitio de instalación 3 respectivo. Por ejemplo, en una realización del paso S7, el usuario usa el dispositivo terminal 6 para comunicar a la aplicación del sitio 10 una selección o indicación de la representación lógica del dispositivo de control de acceso en el plano que coincide con el dispositivo de control de acceso 4, 4' real que el usuario está configurando actualmente. Por ejemplo, cuando el usuario está configurando el dispositivo de control de acceso 4, 4' ubicado en una determinada posición/ubicación del edificio, el usuario indicará o seleccionará en una representación gráfica del plano del sitio de instalación 3 la representación lógica del dispositivo de control de acceso que se muestra en la misma posición/ubicación. Como alternativa, en la realización del paso S7', el usuario usa un elemento operativo del dispositivo de control de acceso 4, 4', por ejemplo, un botón, para comunicar o señalar a la aplicación del sitio 10 que el dispositivo de control de acceso 4, 4' real que el usuario está configurando actualmente coincide con la

representación lógica del dispositivo de control de acceso que actualmente está resaltado por la aplicación del sitio 10 en la representación gráfica del plano del lugar de instalación 3 mostrado al usuario en el dispositivo terminal 6. En otra realización, cuando está cerca del dispositivo de control de acceso 4, 4', el dispositivo terminal 6 transmite al dispositivo de control de acceso 4, 4' (a través del lector 41 o el módulo inalámbrico 45) información de ubicación actual del dispositivo terminal 6. La información de ubicación se obtiene de un receptor GPS del dispositivo terminal 6 y/o mediante la entrada de datos (descriptivos) por parte del usuario. La información de ubicación se almacena en el dispositivo de control de acceso 4, 4' y se transmite desde el dispositivo de control de acceso 4, 4' al sistema informático basado en la nube 1, donde se utiliza para asignar el respectivo dispositivo de control de acceso 4, 4' a la representación lógica del dispositivo de control de acceso, usando información de ubicación almacenada en el sistema informático basado en la nube 1 para la representación lógica del dispositivo de control de acceso.

En el paso S70, la aplicación del sitio 10 en el sistema informático basado en la nube 1 realiza la asignación del dispositivo de control de acceso 4, 4' físico real a la representación lógica correspondiente del dispositivo de control de acceso en el plano del sitio de instalación 3. Específicamente, la aplicación del sitio 10 en el sistema informático basado en la nube 1 almacena el identificador de dispositivo único del dispositivo de control de acceso 4, 4' o su dispositivo de cierre 40, respectivamente, asignado a la representación lógica correspondiente del dispositivo de control de acceso en el plano del sitio de instalación 3.

En el paso S8, la aplicación del sitio 10 determina los datos de configuración almacenados en el sistema informático basado en la nube 1 para el dispositivo de control de acceso que está ahora identificado y asignado al dispositivo de control de acceso físico 4, 4' real en el sitio de instalación 3.

En el paso S80, la aplicación del sitio 10 transmite los datos de configuración al dispositivo de control de acceso físico real 4, 4' en el sitio de instalación 3.

En la realización según la figura 1, los datos de configuración se transmiten desde el sistema informático basado en la nube 1 a través de la red de comunicación 2 al controlador de dispositivo remoto 44 del respectivo dispositivo de control de acceso 4. En la realización según la figura 2, los datos de configuración se transmiten desde el sistema informático basado en la nube 1 a través de la red de comunicación 2 a la puerta de enlace del controlador de dispositivos remotos 46 del sitio de instalación 3 respectivo, y desde la puerta de enlace del controlador de dispositivos remotos 46 de forma inalámbrica al módulo inalámbrico 45 del respectivo dispositivo de control de acceso 4'. Por lo tanto, los datos de configuración se transmiten desde el sistema informático basado en la nube 1 a la puerta de enlace del controlador de dispositivo remoto 46 del respectivo sitio de instalación 3; desde la puerta de enlace del controlador de dispositivo remoto 46, los datos de configuración se transmiten al módulo inalámbrico 45 del respectivo dispositivo de control de acceso 4'.

En el paso S9, el controlador de acceso 42 del respectivo dispositivo de control de acceso 4, 4' completa la configuración del dispositivo de control de acceso 4, 4' realizando un proceso de configuración utilizando los datos de configuración recibidos. Los datos de configuración recibidos son almacenados e implementados por el controlador de acceso 42. Específicamente, dependiendo del tipo especificado de dispositivo de control de acceso 4, 4', dispositivo de cierre respectivo 40 y componentes de hardware conectados especificados, los datos de configuración incluyen información de conectividad y temporización. La información de conectividad indica qué puertos de conexión del controlador de acceso 42 están conectados a qué puertos de conexión correspondientes del dispositivo de cierre 40, actuadores de puerta o portón, dispositivos de señalización y otros elementos de hardware de la puerta o portón especificado. La información de temporización define la temporización de las señales de control generadas por el controlador de acceso 42 para controlar elementos de hardware conectados al controlador de acceso 42, por ejemplo, tiempos de señalización, duraciones de tiempo y temporización de señales de control para el dispositivo de cierre 40, relés electromecánicos, actuadores de puertas o portones, unidades de señalización óptica y/o acústica, etc.

Además, los datos de configuración incluyen firmware, es decir, instrucciones de programa ejecutables, para el controlador de acceso 42, el lector 41 y/o el módulo inalámbrico 45 del dispositivo de control de acceso 4, 4'. El firmware incluye módulos de programa con actualizaciones de firmware ya instaladas en el dispositivo de control de acceso 4, 4' y/o módulos de programa adicionales necesarios para controlar los elementos de hardware especificados en la configuración del dispositivo de control de acceso 4, 4'.

Además, los datos de configuración pueden incluir información de control de acceso. La información de control de acceso incluye listas blancas, listas negras y/o derechos de acceso para usuarios identificados y períodos de tiempo definidos.

En este punto, debe señalarse que los datos de configuración para un sitio de instalación 3 concreto incluyen además datos de configuración, como firmware y parámetros de configuración, para el controlador de dispositivo remoto 44 y/o la puerta de enlace del controlador de dispositivo remoto 46, respectivamente. Los datos de configuración se almacenan y utilizan en un proceso de configuración en el controlador de dispositivo remoto 44 y/o en la puerta de enlace del controlador de dispositivo remoto 46, respectivamente.

Se debería hacer notar que, en la descripción, el código de programa informático se ha asociado con módulos funcionales específicos y la secuencia de los pasos se ha presentado en un orden específico, un experto en la materia entenderá, sin embargo, que el código de programa informático se puede estructurar de manera diferente y que el orden de al menos algunos de los pasos se podría alterar sin apartarse del alcance de las reivindicaciones adjuntas.

5

REIVINDICACIONES

1. Un método para configurar e instalar dispositivos de control de acceso (4, 4') en un sitio de instalación (3), comprendiendo el método:

5 almacenar (S10) en un sistema informático basado en la nube (1) datos de configuración para dispositivos de control de acceso (4,4') no identificados del sitio de instalación;
 recibir (S2) en el sistema informático basado en la nube (1) un registro que asigna el sitio de instalación a un identificador de medios almacenado en un dispositivo de medios de configuración (5);
 10 leer (S40) por uno de los dispositivos de control de acceso (4, 4') concreto en el sitio de instalación el identificador de medios almacenado en el dispositivo de medios de configuración (5);
 recibir (S5) en el sistema informático basado en la nube desde el dispositivo de control de acceso concreto el identificador de medios y un identificador de dispositivo único del dispositivo de control de acceso concreto;
 15 recibir (S7, S7') en el sistema informático basado en la nube (1) información de asignación que permite asignar el dispositivo de control de acceso concreto a uno de los dispositivos de control de acceso no identificados del sitio de instalación;
 asignar (S70) en el sistema informático basado en la nube (1) el dispositivo de control de acceso concreto a uno de los dispositivos de control de acceso no identificados del sitio de instalación asignado al identificador de medios, y almacenar el identificador de dispositivo único del dispositivo de control de acceso concreto en el
 20 sistema informático basado en la nube (1) asignado al dispositivo de control de acceso no identificado asignado al dispositivo de control de acceso concreto; y
 transmitir (S80) los datos de configuración del dispositivo de control de acceso no identificado asignado al dispositivo de control de acceso concreto desde el sistema informático basado en la nube (1) al dispositivo de control de acceso concreto.

25 2. El método de la reivindicación 1, en donde almacenar los datos de configuración incluye almacenar información de conectividad para los dispositivos de control de acceso (4,4') y para los componentes de hardware conectados a los dispositivos de control de acceso (4,4').

30 3. El método de una de las reivindicaciones 1 o 2, en donde almacenar los datos de configuración incluye almacenar información de temporización para los dispositivos de control de acceso (4,4') y para controlar los componentes de hardware conectados a los dispositivos de control de acceso (4,4').

35 4. El método de una de las reivindicaciones 1 a 3, en donde el método comprende además disponer una representación visual del identificador de medios en una superficie del dispositivo de medios de configuración; y generar el registro incluye leer la representación visual del identificador de medios en la superficie del dispositivo de medios de configuración.

40 5. El método de una de las reivindicaciones 1 a 4, en donde leer el identificador de medios almacenado en el dispositivo de medios de configuración incluye colocar el dispositivo de medios de configuración dentro de un alcance de recepción de un lector RFID, y el lector de RFID lee el identificador de medios del dispositivo de medios de configuración.

45 6. El método de una de las reivindicaciones 1 a 5, en donde asignar el dispositivo de control de acceso concreto a uno de los dispositivos de control de acceso no identificados incluye recibir en el sistema informático basado en la nube instrucciones de usuario que vinculan el identificador de dispositivo del dispositivo de control de acceso concreto a uno de los dispositivos de control de acceso no identificados del sitio de instalación asignado al identificador de medios.

50 7. El método de una de las reivindicaciones 1 a 6, en donde el método comprende además recibir en el dispositivo de control de acceso concreto información de ubicación desde un dispositivo de comunicación móvil; y asignar el dispositivo de control de acceso concreto a uno de los dispositivos de control de acceso no identificados incluye recibir en el sistema informático basado en la nube la información de ubicación del dispositivo de control de acceso concreto, y usar la información de ubicación para la asignación del dispositivo de control de acceso concreto a uno
 55 de los dispositivos de control de acceso no identificados.

8. El método de una de las reivindicaciones 1 a 7, en donde el método comprende además almacenar un código de instalación en el dispositivo de medios de configuración; almacenar en el sistema informático basado en la nube el identificador de medios y el código de instalación del dispositivo de medios de configuración; transmitir el código de
 60 instalación desde el sistema informático basado en la nube a una puerta de enlace del controlador de dispositivos en el sitio de instalación; y controlar el acceso de un dispositivo de control de acceso inalámbrico a la puerta de enlace del controlador de dispositivos, usando el código de instalación almacenado en el dispositivo de medios de configuración y el código de instalación recibido en la puerta de enlace del controlador de dispositivos.

65 9. Un sistema informático para configurar dispositivos de control de acceso (4, 4') en un sitio de instalación (3), comprendiendo el sistema informático (1) uno o más procesadores configurados para almacenar (S10) en el sistema

- informático (1) datos de configuración para dispositivos de control de acceso no identificados del sitio de instalación; recibir (S2) en el sistema informático (1) un registro que asigna el sitio de instalación a un identificador de medios almacenado en un dispositivo de medios de configuración (5);
- 5 recibir (S5) en el sistema informático (1) desde uno de los dispositivos de control de acceso (4, 4') concreto en el sitio de instalación el identificador de medios y un identificador de dispositivo único del dispositivo de control de acceso concreto;
- 10 recibir (S7, S7') en el sistema informático (1) información de asignación que permite asignar el dispositivo de control de acceso concreto a uno de los dispositivos de control de acceso no identificados del sitio de instalación; asignar (S70) en el sistema informático (1) el dispositivo de control de acceso concreto a uno de los dispositivos de control de acceso no identificados del sitio de instalación asignado al identificador de medios, y almacenar en el sistema informático (1) el identificador de dispositivo único del dispositivo de control de acceso concreto asignado al dispositivo de control de acceso no identificado asignado al dispositivo de control de acceso concreto; y
- 15 transmitir (S80) los datos de configuración del dispositivo de control de acceso no identificado asignado al dispositivo de control de acceso concreto desde el sistema informático (1) al dispositivo de control de acceso concreto.
10. El sistema informático de la reivindicación 9, en donde los datos de configuración incluyen información de conectividad para los dispositivos de control de acceso y componentes de hardware conectados a los dispositivos de control de acceso (4, 4').
- 20 11. El sistema informático de una de las reivindicaciones 9 o 10, en donde los datos de configuración incluyen información de temporización para los dispositivos de control de acceso y para controlar componentes de hardware conectados a los dispositivos de control de acceso (4, 4').
- 25 12. El sistema informático de una de las reivindicaciones 9 a 11, en donde los procesadores están configurados para recibir, con el fin de asignar el dispositivo de control de acceso concreto a uno de los dispositivos de control de acceso no identificados, instrucciones de usuario que vinculan el identificador de dispositivo del dispositivo de control de acceso concreto a uno de los dispositivos de control de acceso no identificados del sitio de instalación asignados al identificador de medios.
- 30 13. El sistema informático de una de las reivindicaciones 9 a 12, en donde los procesadores están configurados para recibir, con el fin de asignar el dispositivo de control de acceso concreto a uno de los dispositivos de control de acceso no identificados, información de ubicación del dispositivo de control de acceso concreto, y para usar la ubicación información para asignar el dispositivo de control de acceso concreto a uno de los dispositivos de control de acceso no identificados.
- 35 14. El sistema informático de una de las reivindicaciones 9 a 13, en donde los procesadores están configurados para almacenar el identificador de medios y un código de instalación almacenado en el dispositivo de medios de configuración; y para transmitir el código de instalación a una puerta de enlace del controlador de dispositivos en el sitio de instalación, para habilitar el control de acceso de un dispositivo de control de acceso inalámbrico a la puerta de enlace del controlador de dispositivos, utilizando el código de instalación almacenado en el dispositivo de medios de configuración y el código de instalación transmitido al puerta de enlace del controlador de dispositivo.
- 40

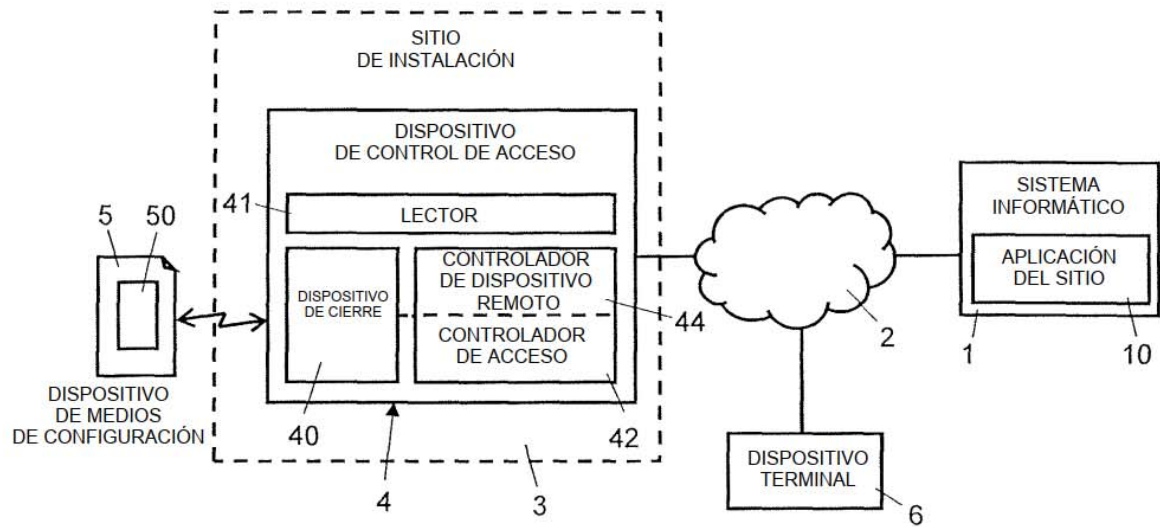


Fig. 1

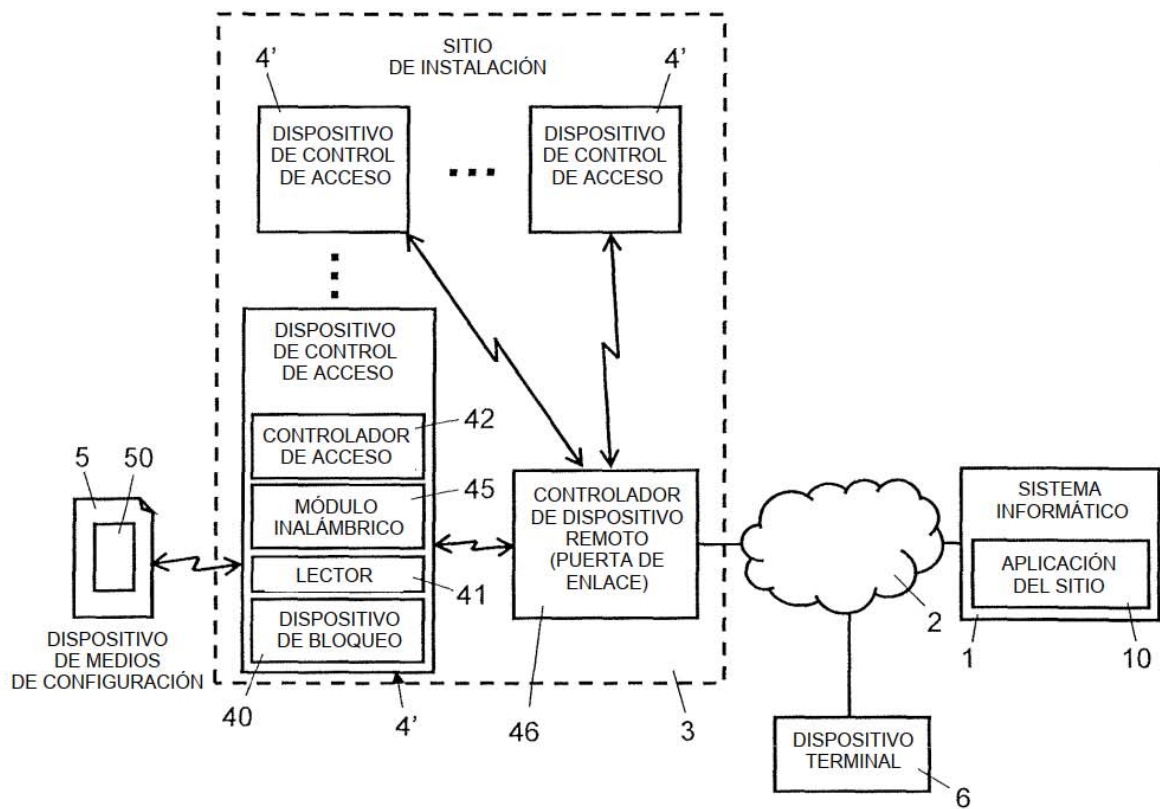


Fig. 2

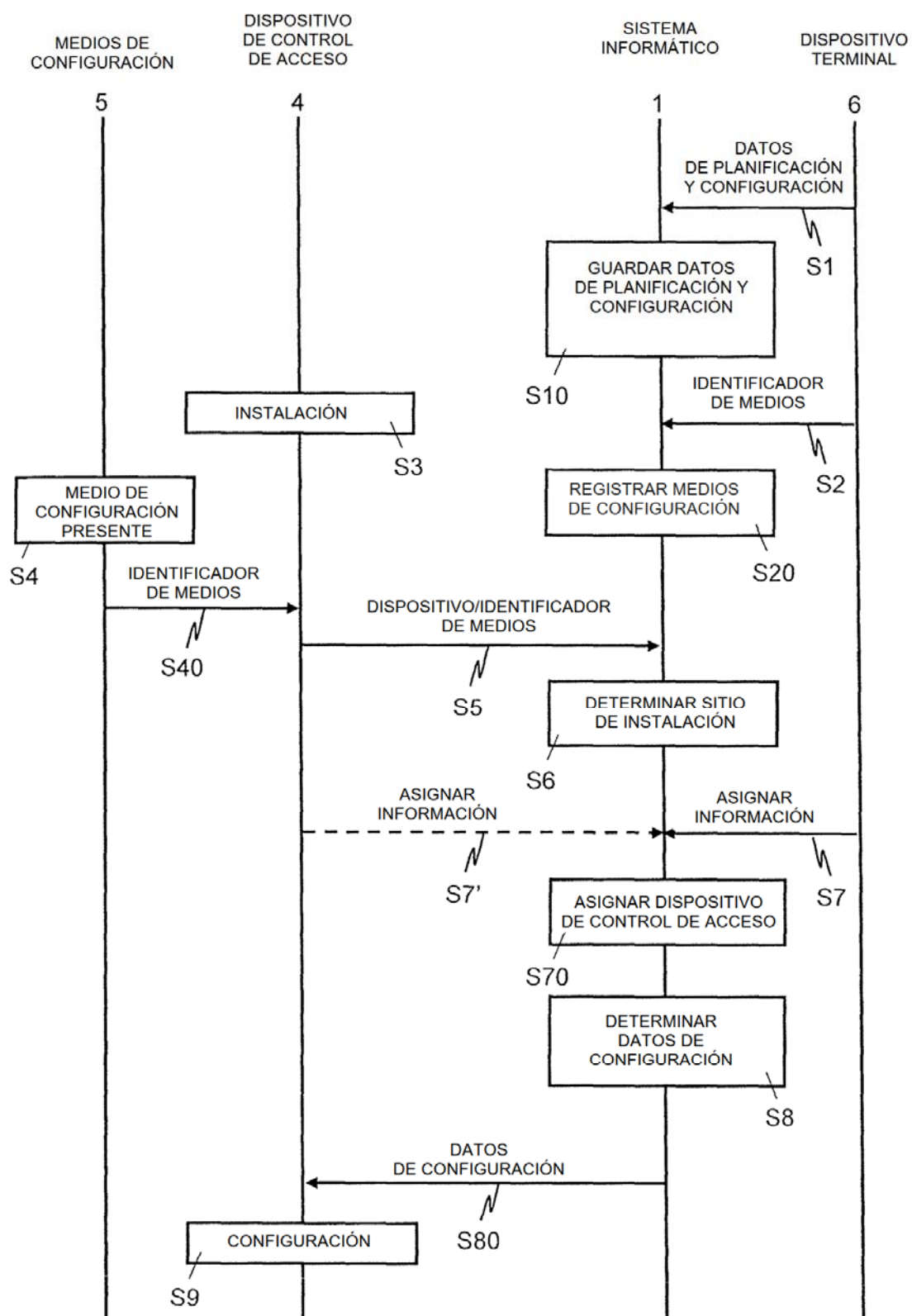


Fig. 3