(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 734 404**

(51) Int. CI.:

H04L 29/14 (2006.01)
G07C 9/00 (2006.01)
H04W 12/08 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **14.06.2016 PCT/EP2016/063599**

(87) Fecha y número de publicación internacional: **22.12.2016 WO16202780**

(96) Fecha de presentación y número de la solicitud europea: **14.06.2016 E 16729883 (5)**

(97) Fecha y número de publicación de la concesión europea: **01.05.2019 EP 3308532**

(54) Título: **Caché de credenciales**

(30) Prioridad:

15.06.2015 EP 15172069

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
05.12.2019

(73) Titular/es:

ASSA ABLOY AB (100.0%)
P.O. Box 70340
107 23 Stockholm, SE

(72) Inventor/es:

WAGSTAFF, RUSSELL

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Caché de credenciales

Campo técnico

La invención se refiere a un método, un dispositivo de control de acceso, un programa de ordenador y un producto de programa de ordenador con relación a una caché de credenciales para derechos de acceso.

Antecedentes

Las cerraduras y las llaves están evolucionando desde las cerraduras mecánicas puras tradicionales. En estos días, hay interfaces inalámbricas para dispositivos de control de acceso de cerraduras electrónicas, por ejemplo, interactuando con una llave electrónica. Tales interfaces inalámbricas mejoran la usabilidad, al tiempo que la gestión de llaves electrónicas es significativamente más flexible con respecto a la gestión de derechos de acceso en comparación con las cerraduras mecánicas puras.

El dispositivo de control de acceso se comunica con un servidor de control de acceso para obtener derechos de acceso para una llave electrónica en particular. De esa forma, el acceso para una llave electrónica en particular se puede gestionar de manera central gestionando los derechos de acceso almacenados en el servidor de control de acceso.

Sin embargo, algunas veces ocurre que la comunicación entre el dispositivo de control de acceso y el servidor de control de acceso falla durante un período de tiempo. Durante tal período, el dispositivo de control de acceso es incapaz de comprobar los derechos de acceso de una llave electrónica que se le presenta.

El documento WO2015/010218 A1 describe un sistema de control de acceso distribuido a prueba de fallos. El documento US 2014/282993 A1 describe un sistema y un método para el control de acceso físico. El documento EP 2 821 970 describe un dispositivo de comunicación, un método, un programa de ordenador y un producto de programa de ordenador de control de acceso. En el URL http://www.cse.hut.fi/fi/opinnot/T-110.5241/2012/luennot-files/Network%20Security%2007%20-%20NFC.pptx está disponible una presentación realizada en la Universidad de Aalto el 20 de noviembre 2012 por Sandeep Tamrakar. El título de la presentación es “NFC Application Security”.

Compendio

Es un objeto de las realizaciones presentadas en la presente memoria proporcionar una forma mejorada para gestionar la gestión de derechos de acceso cuando el dispositivo de control de acceso es incapaz de comunicarse con un servidor de control de acceso.

Según un primer aspecto, se presenta un método realizado para controlar el acceso a un espacio físico. El método se realiza en un dispositivo de control de acceso y comprende los pasos de: comunicarse con una llave electrónica para autenticar la llave electrónica; realizar una búsqueda de un derecho de acceso usando una identidad de la llave electrónica en una caché de credenciales cuando el dispositivo de control de acceso es incapaz de comunicarse con un servidor de control de acceso; enviar una señal de desbloqueo cuando el derecho de acceso indica que se debería conceder acceso a la llave electrónica; recuperar, del servidor de control de acceso, un derecho de acceso que indica si la llave electrónica debería tener acceso o no, cuando el dispositivo de control de acceso es capaz de comunicarse con el servidor de control de acceso; y actualizar la caché de credenciales con el derecho de acceso recuperado del servidor de control de acceso. Esto implica un relleno basado en extracción de la caché de credenciales, es decir, una entrada iniciada por el dispositivo de control de acceso. De esta forma, la caché de credenciales se rellena automáticamente siempre que se presenta una credencial al dispositivo de control de acceso.

El método comprende además los pasos de: recibir, iniciado desde el dispositivo remoto, un derecho de acceso que indica si la llave electrónica debería tener acceso o no; y actualizar la caché de credenciales con el derecho de acceso recibido desde el servidor de control de acceso. Esto implica un relleno basado en extracción de la caché de credenciales, es decir, una entrada iniciada por el dispositivo remoto, que permite un gran control de la caché de credenciales.

El paso de comunicación puede comprender la comunicación con la llave electrónica usando un protocolo de comunicación inalámbrica.

La caché de credenciales puede formar parte del dispositivo de control de acceso.

El paso de realización de la búsqueda puede comprender encontrar una entrada de derechos de acceso en la caché de credenciales para la llave electrónica.

La entrada puede comprender un tiempo de validez. En tal caso, el paso de enviar una señal de desbloqueo comprende enviar la señal de desbloqueo sólo cuando la hora actual está dentro del tiempo de validez de la entrada.

El paso de comunicación con la llave electrónica puede comprender realizar un procedimiento de respuesta al desafío con la llave electrónica.

Según un segundo aspecto, se presenta un dispositivo de control de acceso para controlar el acceso a un espacio físico. El dispositivo de control de acceso comprende: un procesador; y una memoria que almacena instrucciones que, cuando se ejecutan por el procesador, hacen que el dispositivo de control de acceso: se comunique con una llave electrónica para autenticar la llave electrónica; realice una búsqueda de un derecho de acceso usando una identidad de la llave electrónica en una caché de credenciales cuando el dispositivo de control de acceso es incapaz de comunicarse con un servidor de control de acceso; envíe una señal de desbloqueo cuando el derecho de acceso indique que se debería conceder acceso a la llave electrónica; recupere, desde el servidor de control de acceso, un derecho de acceso que indique si la llave electrónica debería tener acceso o no, cuando el dispositivo de control de acceso es capaz de comunicarse con el servidor de control de acceso; y actualice la caché de credenciales con el derecho de acceso recuperado desde el servidor de control de acceso.

El dispositivo de control de acceso comprende además instrucciones que, cuando se ejecutan por el procesador, hacen que el dispositivo de control de acceso: reciba, iniciado desde un dispositivo remoto, un derecho de acceso que indique si la llave electrónica debería tener acceso o no; y actualice la caché de credenciales con el derecho de acceso recibido desde el dispositivo remoto.

La caché de credenciales puede formar parte del dispositivo de control de acceso.

Las instrucciones para realizar la búsqueda pueden comprender instrucciones que, cuando se ejecutan por el procesador, hacen que el dispositivo de control de acceso encuentre una entrada de derechos de acceso en la caché de credenciales para la llave electrónica.

La entrada puede comprender un tiempo de validez. En tal caso, las instrucciones para enviar una señal de desbloqueo comprenden instrucciones que, cuando se ejecutan por el procesador, hacen que el dispositivo de control de acceso envíe la señal de desbloqueo sólo cuando la hora actual esté dentro del tiempo de validez de la entrada.

Las instrucciones para comunicarse con la llave electrónica pueden comprender instrucciones que, cuando se ejecutan por el procesador, hacen que el dispositivo de control de acceso realice un procedimiento de respuesta al desafío con la llave electrónica.

Según un tercer aspecto, se presenta un programa de ordenador para controlar el acceso a un espacio físico. El programa de ordenador que comprende un código de programa de ordenador que, cuando se ejecuta en un dispositivo de control de acceso, hace que el dispositivo de control de acceso: se comunique con una llave electrónica para autenticar la llave electrónica; realice una búsqueda de un derecho de acceso usando una identidad de la llave electrónica en una caché de credenciales cuando el dispositivo de control de acceso es incapaz de comunicarse con un servidor de control de acceso; envíe una señal de desbloqueo cuando el derecho de acceso indique que se debería conceder acceso a la llave electrónica; recupere, desde el servidor de control de acceso, un derecho de acceso que indique si la llave electrónica debería tener acceso o no, cuando el dispositivo de control de acceso es capaz de comunicarse con el servidor de control de acceso; y actualice la caché de credenciales con el derecho de acceso recuperado desde el servidor de control de acceso, en donde el programa de ordenador que comprende un código de programa de ordenador que, cuando se ejecuta en un dispositivo de control de acceso, hace que el dispositivo de control de acceso:

reciba, iniciado desde un dispositivo remoto, un derecho de acceso que indique si la llave electrónica debería tener acceso o no; y

actualice la caché de credenciales con el derecho de acceso recibido desde el dispositivo remoto.

Según un cuarto aspecto, se presenta un producto de programa de ordenador que comprende un programa de ordenador según el tercer aspecto y un medio legible por ordenador en el que se almacena el programa de ordenador.

En general, todos los términos usados en las reivindicaciones se han de interpretar según su significado habitual en el campo técnico, a menos que se defina explícitamente de otro modo en la presente memoria. Todas las referencias a “un/el elemento, aparato, componente, medio, paso, etc.” se han de interpretar abiertamente como que se refieren a al menos un ejemplo del elemento, aparato, componente, medio, paso, etc., a menos que se exprese explícitamente de otro modo. Los pasos de cualquier método descrito en la presente memoria no tienen que ser realizados en el orden exacto descrito, a menos que se exprese explícitamente.

Breve descripción de los dibujos

La invención se describe ahora, a modo de ejemplo, con referencia a los dibujos adjuntos, en los que:

La Figura 1 es un diagrama esquemático que muestra un entorno en el que se pueden aplicar las realizaciones presentadas en la presente memoria;

Las Figuras 2A-B son diagramas de flujo que ilustran métodos para controlar el acceso a un espacio físico, realizados en el dispositivo de control de acceso de la Figura 1;

La Figura 3 es un diagrama esquemático que ilustra algunos componentes de un dispositivo de control de acceso según la Figura 1;

La Figura 4 muestra un ejemplo de un producto de programa de ordenador que comprende medios legibles por ordenador.

Descripción detallada

La invención se describirá ahora más plenamente de aquí en adelante con referencia a los dibujos adjuntos, en los que se muestran ciertas realizaciones de la invención. Sin embargo, esta invención se puede encarnar de muchas formas diferentes y no se debería interpretar como limitada a las realizaciones expuestas en la presente memoria; en su lugar, estas realizaciones se proporcionan a modo de ejemplo de modo que esta descripción sea minuciosa y completa, y transmita plenamente el alcance de la invención a los expertos en la técnica. Números similares se refieren a elementos similares a lo largo de la descripción.

La Figura 1 es un diagrama esquemático que muestra un entorno en el que se pueden aplicar las realizaciones presentadas en la presente memoria. El acceso a un espacio 16 físico está restringido por una barrera 15 física que se puede desbloquear selectivamente. La barrera 15 física se encuentra entre el espacio 16 físico restringido y un espacio 14 físico accesible. Obsérvese que el espacio 14 físico accesible puede ser un espacio físico restringido en sí mismo, pero en relación con esta barrera 15 física particular, el espacio 14 físico accesible es accesible. La barrera 15 puede ser una puerta, un portón, una trampilla, una ventana, un cajón, etc. Con el fin de desbloquear la barrera 15, se proporciona un dispositivo 1 de control de acceso. El dispositivo 1 de control de acceso está conectado (o combinado con) un dispositivo 12 de bloqueo físico, que es controlable por el dispositivo 1 de control de acceso para ser establecido en un estado desbloqueado o un estado bloqueado. El dispositivo 1 de control de acceso está montado cerca del dispositivo 12 de bloqueo físico. La barrera 15 se proporciona en una estructura fija circundante, tal como una pared o una valla.

El dispositivo 1 de control de acceso es capaz de recibir y enviar señales desde/hacia una llave 2 electrónica sobre un canal 3 de comunicación que puede ser una interfaz inalámbrica de corto alcance o una conexión conductora (es decir, galvánica/eléctrica). La llave 2 electrónica es cualquier dispositivo adecuado portable por un usuario, que se puede usar para la autenticación sobre el canal 3 de comunicación. La llave 2 electrónica se transporta o usa típicamente por un usuario y se puede implementar como una llave física, un llavero, dispositivo que se puede llevar puesto, teléfono inteligente, etc. La interfaz inalámbrica de corto alcance es una interfaz inalámbrica de radiofrecuencia y podría, por ejemplo, estar usando Bluetooth, Bluetooth Low Energy (BLE), ZigBee, Identificación por Radiofrecuencia (RFID), cualquiera de los estándares IEEE 802.11, cualquiera de los estándares IEEE 802.15, Bus Serie Universal (USB) inalámbrico, etc. La llave electrónica también se puede considerar que es una credencial. Usando el canal 3 de comunicación, se puede comprobar la autenticidad de la llave 2 electrónica, por ejemplo, usando un esquema de desafío y respuesta. En cualquier caso, se obtiene una identidad de la llave 2 electrónica, que se usa para conceder o denegar acceso como se explica con más detalle a continuación con referencia a la Figura 2A. Se proporciona un servidor 18 de control de acceso para controlar el sistema de control de acceso que puede comprender un gran número de barreras 15 y dispositivos 12 de bloqueo conectados respectivamente y dispositivos 1 de control de acceso. En esta realización, el dispositivo de control de acceso puede comunicarse con el servidor 18 de control de acceso a través de un concentrador 17. De esta forma, un primer enlace 20 de comunicación entre el dispositivo 1 de control de acceso y el concentrador 17 puede ser inalámbrico para simplificar los requisitos de instalación del dispositivo 1 de control de acceso y del dispositivo 12 de bloqueo. Por ejemplo, el primer enlace 20 de comunicación puede usar Bluetooth, BLE, ZigBee, RFID, cualquiera de los estándares IEEE 802.11, cualquiera de los estándares IEEE 802.15, USB inalámbrico, etc. En una realización, el primer enlace 20 de comunicación se basa en IEEE 802.15.4.

El concentrador 17 puede comunicarse con varios dispositivos de control de acceso, incluso aunque sólo se muestre uno en la Figura 1, y se comunica con el servidor 18 de control de acceso a través de un segundo enlace 21 de comunicación. El segundo enlace 21 de comunicación puede ser cableado, inalámbrico o una combinación de ambos. En una realización, el segundo enlace 21 de comunicación se basa (al menos parcialmente) en RS-485 y/o Wiegand. Tanto el primer enlace 20 de comunicación como el segundo enlace 21 de comunicación pueden utilizar el Protocolo de Internet (IP).

Como con todos los enlaces de comunicación, el primer enlace 20 de comunicación y/o el segundo enlace 21 de comunicación pueden fallar en ocasiones, dando como resultado que el dispositivo 1 de control de acceso sea

incapaz de comunicarse con el servidor 18 de control de acceso. Sin embargo, usando las realizaciones presentadas en la presente memoria, el dispositivo 1 de control de acceso aún puede funcionar cuando el dispositivo 1 de control de acceso es incapaz de comunicarse con el servidor 18 de control de acceso. Esto funciona mediante el dispositivo 1 de control de acceso que usa una caché 10 de credenciales que se almacena en la memoria local. La caché 10 de credenciales contiene un subconjunto de los derechos de acceso para llaves electrónicas. Cuando la llave 2 electrónica se presenta al dispositivo 1 de control de acceso, los derechos de acceso se comprueban primero con el servidor 18 de control de acceso. Sin embargo, si el dispositivo 1 de control de acceso es incapaz de comunicarse con el servidor 18 de control de acceso, los derechos de acceso para la llave 2 electrónica se comprueban frente a la caché 10 de credenciales en la memoria local. De esta forma, bajo algunas circunstancias, el dispositivo 1 de control de acceso puede conceder acceso a llaves electrónicas válidas incluso cuando el dispositivo 1 de control de acceso sea incapaz de comunicarse con el servidor 18 de control de acceso.

Cuando se concede el acceso, el dispositivo 1 de control de acceso envía una señal de desbloqueo al dispositivo 12 de bloqueo, por lo que el dispositivo 12 de bloqueo se establece en un estado desbloqueado. En esta realización, por ejemplo, esto puede implicar una señal sobre una interfaz de comunicación basada en cable, por ejemplo, usando un Bus Serie Universal (USB), Ethernet, una conexión en serie (por ejemplo, RS-485 o RS-232) o incluso una conexión eléctrica simple, o alternativamente una señal sobre una interfaz de comunicación inalámbrica.

Cuando el dispositivo 12 de bloqueo está en estado desbloqueado, la barrera 15 se puede abrir y cuando el dispositivo 12 de bloqueo está en un estado bloqueado, la barrera 15 no se puede abrir. De esta forma, el acceso a un espacio 16 cerrado se controla por el dispositivo 1 de control de acceso. Se ha de observar que el dispositivo 1 de control de acceso y/o el dispositivo 12 de bloqueo se pueden montar en la estructura 16 fija mediante la barrera 15 física (como se muestra) o en la barrera 15 física en sí misma (no mostrada). Opcionalmente, el dispositivo 12 de bloqueo y el dispositivo 1 de control de acceso se combinan en una unidad.

Opcionalmente, la recolección de energía de las acciones mecánicas de usuario y/o la energía ambiental (energía solar, viento, etc.) se puede utilizar para prolongar la vida útil de la batería o incluso para permitir que se omita una batería para el dispositivo 1 de control de acceso y/o el dispositivo 12 de bloqueo.

El sistema de control de acceso presentado de la Figura 1 se puede implementar en cualquier entorno adecuado, por ejemplo, en hoteles, dormitorios, hospitales, edificios comerciales, para acceso a servidores en bastidores de servidores, etc.

Las Figuras 2A-B son diagramas de flujo que ilustran métodos para controlar el acceso a un espacio físico, realizados en el dispositivo de control de acceso de la Figura 1. En primer lugar, se describirán las realizaciones ilustradas por la Figura 2A.

Opcionalmente, antes de que se inicie este método, la caché de credenciales se ha rellenado previamente, por ejemplo, en el despliegue o usando una interfaz remota. Opcionalmente, las entradas rellenadas previamente pueden tener un tiempo de validez infinito, por ejemplo, para personal de mantenimiento de alta seguridad. Esto se describe con más detalle con referencia a la Figura 2B a continuación.

En un paso 40 de comunicar con dispositivo de llave, el dispositivo de control de acceso se comunica con la llave electrónica para autenticar la llave electrónica. Como se ha explicado anteriormente, la comunicación con la llave electrónica puede ocurrir usando un protocolo de comunicación inalámbrica que permita una experiencia de usuario simple. Alternativamente, la comunicación puede ocurrir usando una conexión galvánica/eléctrica con la llave electrónica.

La autenticación, por ejemplo, puede ocurrir usando un procedimiento de respuesta al desafío con la llave electrónica. De esta forma, un atacante no puede emular la llave electrónica sólo observando la comunicación entre el dispositivo de control de acceso y la llave electrónica.

En un paso 41 de enlazar con el servidor condicional, se determina si el dispositivo de control de acceso es capaz de comunicarse con el servidor de control de acceso, por ejemplo, en un escenario mostrado en la Figura 1, a través de un concentrador 17 o sin un concentrador 17. Si el dispositivo de control de acceso es incapaz de comunicarse con el servidor de control de acceso, el método pasa a un paso 42 de búsqueda para comprobar los derechos de acceso en la caché de credenciales.

En el paso 42 de búsqueda, se realiza una búsqueda de un derecho de acceso en la caché de credenciales usando una identidad de la llave electrónica. La caché de credenciales es una base de datos almacenada localmente en el dispositivo de control de acceso (tal como parte del dispositivo de control de acceso) que contiene un subconjunto de los derechos de acceso almacenados en el sistema de control de acceso central.

La búsqueda puede dar como resultado una entrada encontrada en la caché de credenciales para la llave electrónica. La entrada corresponde a un derecho de acceso, por lo que la entrada también se denomina entrada de derecho de acceso. El derecho de acceso puede ser un derecho de acceso positivo (se permite el acceso) o un derecho de acceso negativo (se deniega el acceso).

Opcionalmente, la entrada comprende un tiempo de validez. Como se explica a continuación, la caché de credenciales se rellena automáticamente cuando se presenta una llave electrónica al dispositivo de control de acceso en un momento cuando el dispositivo de control de acceso es capaz de comunicarse con el servidor 18 de control de acceso.

Opcionalmente, cada entrada se actualiza con una última marca de tiempo accedida cuando se realiza una búsqueda para la entrada.

En un paso 43 de acceso condicional, se comprueba el derecho de acceso para ver si se ha de conceder el acceso. Cuando no se ha encontrado ningún derecho de acceso, esto implica acceso denegado. Cuando el derecho de acceso comprende un tiempo de validez, el acceso se concede sólo cuando una hora actual está dentro del tiempo de validez de la entrada. También, cuando el paso anterior fue el paso de búsqueda (comprobación de la caché de credenciales), el acceso sólo se concede cuando hay una entrada para la llave electrónica en la caché de credenciales. Cuando se concede el acceso, el método pasa a un paso 44 de desbloqueo. Cuando se deniega el acceso, el método pasa opcionalmente a un paso 49 de indicar acceso denegado. De otro modo, el método finaliza cuando se deniega el acceso.

En el paso 44 de desbloqueo, el dispositivo de control de acceso envía una señal de desbloqueo para establecer la barrera en un estado que se puede abrir.

En el paso 49 de indicar acceso denegado opcional, el dispositivo de control de acceso indica al usuario que se deniega el acceso usando señales visuales y/o audibles, por ejemplo, una luz roja y un pitido.

Volviendo al paso 41, cuando el dispositivo de control de acceso es capaz de comunicarse con el servidor de control de acceso, el método pasa al paso 46 de recuperar derecho de acceso.

En el paso 46 de recuperar derecho de acceso, el dispositivo 1 de control de acceso recupera, desde el servidor de control de acceso, un derecho de acceso que indica si la llave electrónica debería tener acceso o no. El derecho de acceso recuperado puede ser una concesión de acceso o una denegación de acceso. Si se recibe una respuesta vacía o ninguna respuesta, esto implica una denegación de acceso.

En un paso 48 de actualizar caché de credenciales, la caché de credenciales se actualiza con el derecho de acceso recuperado desde el servidor de control de acceso. De esta forma, la caché de credenciales se actualiza automáticamente. Por lo tanto, cuando el derecho de acceso desde el servidor de control de acceso indica acceso concedido, entonces la caché de credenciales se actualiza para reflejar esto. De manera análoga, cuando el derecho de acceso desde el servidor de control de acceso indica acceso denegado, entonces la caché de credenciales se actualiza para reflejar esto, por ejemplo, eliminando una entrada previamente válida o modificando la entrada para indicar que se ha de denegar el acceso a esa llave electrónica en particular.

En otras palabras, la decisión de control de acceso realizada por el servidor de control de acceso en el paso 46 se almacena en la caché de credenciales en el paso 48. De esta forma, la caché de credenciales se actualiza automáticamente cada vez que se presenta un dispositivo de llave al dispositivo de control de acceso.

Opcionalmente, se puede limitar el tamaño de la caché de credenciales (en número de entradas). En tal caso, cuando la caché de credenciales está llena en el momento de este paso, el comienzo de este paso comprende la eliminación de una entrada para permitir la actualización de la caché de credenciales con la nueva entrada. Por ejemplo, se puede eliminar una entrada para la que la última marca de tiempo accedida es la más antigua.

Opcionalmente, se establece un tiempo de validez siempre que se actualiza un derecho de acceso válido. Por ejemplo, si la llave electrónica con id x ya está en la caché de credenciales y se ha de realizar una actualización de un derecho de acceso de acceso concedido para la llave electrónica con id x, la entrada correspondiente en la caché de credenciales se puede actualizar con un nuevo tiempo de validez. El tiempo de validez se puede configurar en cualquier tiempo adecuado, por ejemplo, una hora, 24 horas, una semana, etc. desde el momento de la actualización. El tiempo de validez se puede configurar arbitrariamente por el propietario del sistema. Un tiempo de validez más prolongado mejora la comodidad, ya que los derechos de acceso más antiguos del acceso concedido permiten que la misma llave electrónica tenga acceso durante un fallo de comunicación. Sin embargo, un tiempo de validez más largo también aumenta el riesgo de que un derecho de acceso cancelado no tenga efecto en caso de un fallo de comunicación entre el dispositivo de control de acceso y el servidor de control de acceso. Por lo tanto, el tiempo de validez se puede configurar por el propietario del sistema para lograr el equilibrio deseado entre comodidad y seguridad.

Después del paso 48 de actualizar caché de credenciales, el método pasa al paso 43 de acceso condicional, usando el derecho de acceso recuperado desde el servidor de control de acceso.

Opcionalmente, la funcionalidad de caché de credenciales se puede activar o desactivar de manera remota. Alternativamente, la funcionalidad de caché de credenciales está configurada para estar activa según una programación. Por ejemplo, la caché de credenciales puede estar activa durante las horas de oficina, pero inactiva

en otros momentos. De esta forma, no se compromete la seguridad en horas de descanso, mientras que el acceso durante las horas de oficina se mejora incluso durante fallos de comunicación.

Usando este método, la caché de credenciales se rellena automáticamente siempre que se presenta una llave electrónica al dispositivo de control de acceso. En comparación con la gestión manual de una lista de derechos de acceso local por un operador, este método es mucho más cómodo. Además, el método es escalable a un gran número de dispositivos de control de acceso, dado que cada dispositivo de control de acceso gestiona automáticamente su propia caché de credenciales. El método presentado tampoco requiere ninguna integración con el concentrador o con el servidor de control de acceso, dado que el dispositivo de control de acceso gestiona la caché de credenciales de manera autónoma.

Mirando ahora a la Figura 2B, ésta muestra pasos que se pueden realizar opcionalmente antes del método mostrado en la Figura 2A y descrito anteriormente.

En un paso 50 de recibir datos de derecho de acceso, el dispositivo 1 de control de acceso recibe datos de derecho de acceso desde un dispositivo remoto, tal como el servidor 18 de control de acceso o un terminal de gestión de sistema remoto de control de acceso.

En un paso 52 de actualizar caché de credenciales, el dispositivo 1 de control de acceso actualiza la caché de credenciales con los datos de derecho de acceso recibidos en el paso 50.

Estos pasos permiten la gestión remota de la caché de credenciales sobre una interfaz remota. Las entradas añadidas de esta forma se denotan aquí entradas remotas, incluso aunque estén almacenadas localmente en el dispositivo de control de acceso. La interfaz remota se puede usar por un operador manual que controla un dispositivo remoto (tal como un terminal de gestión del sistema de control de acceso o el servidor de control de acceso) o se puede usar por un programa de ordenador ejecutado por el servidor de control de acceso u otro dispositivo remoto.

Se pueden usar los pasos de la Figura 2B, por ejemplo, antes de las realizaciones ilustradas en la Figura 2A, para rellenar previamente la caché de credenciales, por ejemplo, en el despliegue o usando una interfaz remota. Opcionalmente, las entradas rellenadas previamente pueden tener un tiempo de validez infinito, por ejemplo, para personal de mantenimiento de alta seguridad.

En el paso 42 de búsqueda descrito anteriormente, la caché de credenciales puede contener entonces entradas rellenadas dinámicamente (a partir del paso 48 de actualizar caché de credenciales) y/o entradas rellenadas de manera remota (a partir del paso 52 de actualizar caché de credenciales). Opcionalmente, las entradas rellenadas dinámicamente y las entradas rellenadas de manera remota se almacenan en la misma base de datos. Opcionalmente, estos dos tipos de entradas se pueden diferenciar por un indicador en cada entrada. Por ejemplo, la Tabla 1 muestra un ejemplo de entradas en una caché de credenciales.

Tabla 1: Ejemplo de tabla de caché de credenciales

Id de credencial	Dinámica/remota	Válida hasta	Positivo/negativo
132	remota	infinita	positivo
532	dinámica	20-06-2016 15:00	positivo
254	dinámica	21-06-2016 08:00	negativo
840	remota	infinita	negativo
342	dinámica	22-06-2016 17:00	positivo

La primera columna es el identificador de credencial. Opcionalmente, cada entrada es un valor de comprobación aleatoria del identificador de credencial. El valor de comprobación aleatoria se calcula por el dispositivo de control de acceso a partir del identificador de credencial original usando cualquier función unidireccional adecuada, por ejemplo, SHA256 (Algoritmo de Comprobación Aleatoria Seguro 256), MDA6 (Algoritmo de Asimilación de Mensaje 6), etc. De esta forma, el tamaño de la entrada en la primera columna es siempre el mismo y la seguridad se aumenta dado que la tabla no almacena los identificadores de credenciales reales. Opcionalmente, el valor de comprobación aleatoria también depende de una llave de bloqueo única, por lo que un valor de comprobación aleatoria para una credencial para un bloqueo no se puede usar para otro bloqueo.

El identificador de credencial (o su valor de comprobación aleatoria) se hace coincidir, en el paso de búsqueda 42, con un identificador (o su valor de comprobación aleatoria) recibido en el paso 40 de comunicar con dispositivo de llave. La segunda columna indica la fuente de la entrada, que puede ser dinámica (desde el paso 48) o remota (desde el paso 52). La tercera columna define la validez de la entrada, aquí indicada en el formato ‘día-mes-año hora:minuto’ o ‘infinita’ para una validez infinita. La última columna indica si la entrada indica un derecho de acceso

positivo o un derecho de acceso negativo. Se ha de observar que puede haber columnas adicionales en la tabla de caché de credenciales no mostradas en este ejemplo, tales como una marca de tiempo de cuándo fue añadida (o actualizada) la entrada, etc. Opcionalmente, a las entradas remotas (indicadas en la segunda columna) se les da prioridad sobre las entradas dinámicas, para permitir el control remoto completo de la operación de acceso del dispositivo de control de acceso.

Opcionalmente, la profundidad, es decir, el número de entradas, en la caché de credenciales se puede configurar sobre la interfaz remota al dispositivo de control de acceso. Además, una pista de auditoría que indique el historial de acceso (que comprende eventos de acceso con éxito e intentados sin éxito) del dispositivo de control de acceso, se puede recuperar desde el dispositivo de control de acceso al servidor de control de acceso o terminal de gestión usando la interfaz remota.

Opcionalmente, la interfaz remota se puede usar para configurar el dispositivo de control de acceso para ignorar cualquier entrada dinámica en la caché, es decir, deshabilitar o habilitar la funcionalidad de caché dinámica. Opcionalmente, la interfaz remota se puede usar para configurar el dispositivo de control de acceso para ignorar cualquier entrada remota en la caché, es decir, deshabilitar o habilitar la funcionalidad de caché remota. Se ha de observar que las entradas pueden permanecer en la tabla de caché de credenciales en caso de que la funcionalidad de caché se habilite de nuevo en una etapa posterior.

Opcionalmente, las entradas remotas (y/o dinámicas) se almacenan en la memoria persistente del dispositivo de control de acceso, por ejemplo, memoria rápida, de modo que las entradas configuradas de manera remota todavía están allí y se apliquen después de un fallo de alimentación. Cuando se inicia el dispositivo de control de acceso, las entradas de la caché de credenciales se pueden cargar en la Memoria de Acceso Aleatorio (RAM) para mejorar el rendimiento durante la operación. Cualquier actualización de la caché de credenciales se puede escribir entonces tanto en la caché de credenciales en la RAM como en la caché de credenciales de la memoria persistente para asegurar la sincronización.

Usando este sistema, el operador del sistema de control de acceso se provee de una gran seguridad y flexibilidad. Dado que la tabla de caché de credenciales se almacena localmente en el dispositivo de control de acceso, está disponible incluso si hay un fallo de comunicación de red en algún punto entre el dispositivo de control de acceso y el servidor de control de acceso. Las entradas dinámicas proporcionan un mantenimiento automático de la tabla de caché de credenciales. Al mismo tiempo, las entradas remotas proporcionan un gran control para el operador del sistema de control de acceso para conceder o denegar el acceso a credenciales particulares. En otras palabras, usando este sistema, las entradas en la tabla se pueden rellenar tanto usando un mecanismo de extracción, para las entradas dinámicas, como usando un mecanismo de inserción, para las entradas remotas. Además, las entradas remotas permiten que la caché de credenciales sea llenada en la instalación, cuando puede que no haya ninguna (o sólo unas pocas) entradas dinámicas en la caché de credenciales.

Un uso de la interfaz remota es configurar el acceso de superusuario, por ejemplo, para el personal de mantenimiento, de manera que siempre se pueda conceder acceso a los superusuarios, incluso si hay un fallo de comunicación e incluso aunque nunca se haya concedido acceso anteriormente al superusuario en cuestión por el dispositivo de control de acceso particular (y de este modo puede no tener una entrada dinámica en la caché de credenciales). Esto puede ser de uso crítico, por ejemplo, en caso de incendio u otro desastre cuando la comunicación puede estar inactiva, pero los superusuarios pueden necesitar acceder al espacio físico controlado por el dispositivo de control de acceso.

La Figura 3 es un diagrama esquemático que muestra algunos componentes del dispositivo 1 de control de acceso de la Figura 1. Un procesador 60 se proporciona usando cualquier combinación de uno o más de una unidad central de procesamiento (CPU), multiprocesador, microcontrolador, procesador de señales digitales (DSP), circuito integrado de aplicaciones específicas, etc., adecuado capaz de ejecutar las instrucciones 66 de software almacenadas en una memoria 64, que de este modo puede ser un producto de programa de ordenador. El procesador 60 se puede configurar para ejecutar el método descrito con referencia a las Figuras 2A-B anteriores.

La memoria 64 puede ser cualquier combinación de memoria de lectura y escritura (RAM) y memoria de sólo lectura (ROM). La memoria 64 también comprende almacenamiento persistente, que, por ejemplo, puede ser uno cualquiera o una combinación de memoria magnética, memoria óptica, memoria de estado sólido o incluso memoria montada de manera remota.

También se proporciona una memoria de datos 65 para leer y/o almacenar datos durante la ejecución de instrucciones de software en el procesador 60. La memoria 65 de datos puede ser cualquier combinación de memoria de lectura y escritura (RAM) y memoria de sólo lectura (ROM) que puede ser memoria persistente y/o volátil. La memoria 65 de datos puede formar parte del dispositivo 1 de control de acceso o ser externa, pero local al dispositivo 1 de control de acceso. La memoria 65 de datos puede almacenar la caché 10 de credenciales descrita anteriormente. La caché de credenciales se puede almacenar en una parte persistente de la memoria 65 de datos, por ejemplo, en una memoria rápida.

El dispositivo 1 de control de acceso comprende además una interfaz 67 de I/O para comunicarse con otras entidades externas tales como el dispositivo 12 de bloqueo y la llave 2 electrónica. La interfaz 67 de I/O también puede comprender un lector para leer tarjetas de llave con una banda magnética o una tarjeta inteligente. La interfaz 67 de I/O puede soportar comunicación basada en cable, por ejemplo, usando un Bus Serie Universal (USB), Ethernet o incluso una conexión eléctrica simple (por ejemplo, al dispositivo 12 de bloqueo) o una conexión galvánica/eléctrica para comunicarse con la llave 2 electrónica.

De manera alternativa o adicional, la interfaz 67 de I/O soporta comunicación inalámbrica, por ejemplo, usando Bluetooth, BLE, ZigBee, RFID, cualquiera de los estándares IEEE 802.11, cualquiera de los estándares IEEE 802.15, USB inalámbrico, etc., por ejemplo, para comunicación con la llave 2 electrónica.

Otros componentes del dispositivo 1 de control de acceso se omiten con el fin de no oscurecer los conceptos presentados en la presente memoria.

Opcionalmente, el dispositivo 12 de bloqueo de la Figura 1 forma parte del dispositivo 1 de control de acceso.

La Figura 4 muestra un ejemplo de un producto de programa de ordenador que comprende medios legibles por ordenador. En este medio legible por ordenador, se puede almacenar un programa 91 de ordenador, cuyo programa de ordenador que puede hacer que un procesador ejecute un método según las realizaciones descritas en la presente memoria. En este ejemplo, el producto de programa de ordenador es un disco óptico, tal como un CD (disco compacto) o un DVD (disco versátil digital) o un disco Blu-Ray. Como se ha explicado anteriormente, el producto de programa de ordenador también se podría encarnar en una memoria de un dispositivo, tal como el producto de programa de ordenador 64 de la Figura 3.

Mientras que el programa 91 de ordenador se muestra aquí esquemáticamente como una pista en el disco óptico representado, el programa de ordenador se puede almacenar de cualquier forma que sea adecuada para el producto de programa de ordenador, tal como una memoria de estado sólido extraíble, por ejemplo, una unidad de Bus Serie Universal (USB).

Aquí ahora sigue una lista de realizaciones desde otra perspectiva, enumeradas con números romanos.

i. Un método realizado para controlar el acceso a un espacio (16) físico, el método que se realiza en un dispositivo (1) de control de acceso y que comprende los pasos de:

comunicar (40) con una llave (2) electrónica para autenticar la llave (2) electrónica;

realizar (42) una búsqueda de un derecho de acceso usando una identidad de la llave (2) electrónica en una caché (10) de credenciales cuando el dispositivo (1) de control de acceso es incapaz de comunicarse con un servidor (18) de control de acceso; y

enviar (44) una señal de desbloqueo cuando el derecho de acceso indica que se debería conceder acceso a la llave (2) electrónica.

ii. El método según la realización i, que comprende además los pasos de:

recuperar (46), desde el servidor (18) de control de acceso, un derecho de acceso que indica si la llave (2) electrónica debería tener acceso o no, cuando el dispositivo (1) de control de acceso es capaz de comunicarse con el servidor (18) de control de acceso; y

actualizar (48) la caché (10) de credenciales con el derecho de acceso recuperado desde el servidor (18) de control de acceso.

iii. El método según una cualquiera de las realizaciones anteriores, en donde el paso de comunicación (40) comprende la comunicación con la llave electrónica usando un protocolo de comunicación inalámbrica.

iv. El método según una cualquiera de las realizaciones anteriores, en donde la caché (10) de credenciales forma parte del dispositivo (1) de control de acceso.

v. El método según una cualquiera de las realizaciones anteriores, en donde el paso de realizar (42) la búsqueda comprende encontrar una entrada de derechos de acceso en la caché de credenciales para la llave (2) electrónica.

vi. El método según la realización v, en donde la entrada comprende un tiempo de validez y en donde el paso de enviar (44) una señal de desbloqueo comprende enviar la señal de desbloqueo sólo cuando la hora actual está dentro del tiempo de validez de la entrada.

vii. El método según una cualquiera de las realizaciones anteriores, en donde el paso de comunicación (40) con la llave (2) electrónica comprende realizar un procedimiento de respuesta al desafío con la llave (2) electrónica.

viii. Un dispositivo (1) de control de acceso para controlar el acceso a un espacio (16) físico que comprende:

un procesador (60); y

una memoria (64) que almacena instrucciones (66) que, cuando se ejecutan por el procesador, hacen que el dispositivo (1) de control de acceso:

se comunique con una llave (2) electrónica para autenticar la llave (2) electrónica;

realice una búsqueda de un derecho de acceso usando una identidad de la llave (2) electrónica en una caché (10) de credenciales cuando el dispositivo (1) de control de acceso es incapaz de comunicarse con un servidor (18) de control de acceso; y

envíe una señal de desbloqueo cuando el derecho de acceso indique que se debería conceder acceso a la llave (2) electrónica.

ix. El dispositivo (1) de control de acceso según la realización viii, que comprende además instrucciones (66) que, cuando se ejecutan por el procesador, hacen que el dispositivo (1) de control de acceso:

recupere, desde el servidor (18) de control de acceso, un derecho de acceso que indica si la llave (2) electrónica debería tener acceso o no, cuando el dispositivo (1) de control de acceso es capaz de comunicarse con el servidor (18) de control de acceso; y

actualice la caché (10) de credenciales con el derecho de acceso recuperado del servidor (18) de control de acceso.

x. El dispositivo (1) de control de acceso según la realización viii o ix, en donde la caché (10) de credenciales forma parte del dispositivo (1) de control de acceso.

xi. El dispositivo (1) de control de acceso según cualquiera de las realizaciones viii a x, en donde las instrucciones para realizar la búsqueda comprenden instrucciones (66) que, cuando se ejecutan por el procesador, hacen que el dispositivo (1) de control de acceso encuentre una entrada de derecho de acceso en la caché de credenciales para la llave (2) electrónica.

xii. El dispositivo (1) de control de acceso según la realización xi, en donde la entrada comprende un tiempo de validez y en donde las instrucciones para enviar una señal de desbloqueo comprenden instrucciones (66) que, cuando se ejecutan por el procesador, hacen que el dispositivo (1) de control de acceso envíe la señal de desbloqueo sólo cuando una hora actual esté dentro del tiempo de validez de la entrada.

xiii. El dispositivo (1) de control de acceso según una cualquiera de las realizaciones viii a xii, en donde las instrucciones para comunicarse con la llave (2) electrónica comprenden instrucciones (66) que, cuando se ejecutan por el procesador, hacen que el dispositivo (1) de control de acceso realice un procedimiento de respuesta al desafío con la llave (2) electrónica.

xiv. Un programa (91) de ordenador para controlar el acceso a un espacio (16) físico, el programa de ordenador que comprende un código de programa de ordenador que, cuando se ejecuta en un dispositivo (1) de control de acceso, hace que el dispositivo (1) de control de acceso:

se comunique con una llave (2) electrónica para autenticar la llave (2) electrónica;

realice una búsqueda de un derecho de acceso usando una identidad de la llave (2) electrónica en una caché (10) de credenciales cuando el dispositivo (1) de control de acceso es incapaz de comunicarse con un servidor (18) de control de acceso; y

envíe una señal de desbloqueo cuando el derecho de acceso indique que se debería conceder acceso a la llave (2) electrónica.

xv. Un producto (90) de programa de ordenador que comprende un programa de ordenador según la realización xiv y un medio legible por ordenador en el que se almacena el programa de ordenador.

La invención se ha descrito principalmente anteriormente con referencia a unas pocas realizaciones. Sin embargo, como se apreciará fácilmente por un experto en la técnica, otras realizaciones distintas de las descritas anteriormente son igualmente posibles dentro del alcance de la invención, como se define en las reivindicaciones de patente adjuntas.

REIVINDICACIONES

1. Un método realizado para controlar el acceso a un espacio (16) físico, el método que se realiza en un dispositivo (1) de control de acceso y que comprende los pasos de:

comunicar (40) con una llave (2) electrónica para autenticar la llave (2) electrónica;

realizar (42) una búsqueda de un derecho de acceso usando una identidad de la llave (2) electrónica en una caché (10) de credenciales cuando el dispositivo (1) de control de acceso es incapaz de comunicarse con un servidor (18) de control de acceso;

enviar (44) una señal de desbloqueo cuando el derecho de acceso indique que se debería conceder acceso a la llave (2) electrónica;

recuperar (46), desde el servidor (18) de control de acceso, un derecho de acceso que indique si la llave (2) electrónica debería tener acceso o no, cuando el dispositivo (1) de control de acceso es capaz de comunicarse con el servidor (18) de control de acceso; y

actualizar (48) la caché (10) de credenciales con el derecho de acceso recuperado desde el servidor (18) de control de acceso;

en donde el método comprende además los pasos, antes del paso de comunicación (40), de:

recibir (50), iniciado desde un dispositivo remoto, un derecho de acceso que indique si la llave (2) electrónica debería tener acceso o no; y

actualizar (52) la caché (10) de credenciales con el derecho de acceso recibido desde el dispositivo remoto.

2. El método según la reivindicación 1, en donde el paso de comunicación (40) comprende la comunicación con la llave electrónica usando un protocolo de comunicación inalámbrica.

3. El método según una cualquiera de las reivindicaciones anteriores, en donde la caché (10) de credenciales forma parte del dispositivo (1) de control de acceso.

4. El método según una cualquiera de las reivindicaciones anteriores, en donde el paso de realizar (42) la búsqueda comprende encontrar una entrada de derechos de acceso en la caché de credenciales para la llave (2) electrónica.

5. El método según la reivindicación 4, en donde la entrada comprende un tiempo de validez y en donde el paso de envío (44) de una señal de desbloqueo comprende enviar la señal de desbloqueo sólo cuando la hora actual está dentro del tiempo de validez de la entrada.

6. El método según una cualquiera de las reivindicaciones anteriores, en donde el paso de comunicación (40) con la llave (2) electrónica comprende realizar un procedimiento de respuesta al desafío con la llave (2) electrónica.

7. Un dispositivo (1) de control de acceso para controlar el acceso a un espacio (16) físico que comprende:

un procesador (60); y

una memoria (64) que almacena instrucciones (66) que, cuando se ejecutan por el procesador, hacen que el dispositivo (1) de control de acceso:

se comunique con una llave (2) electrónica para autenticar la llave (2) electrónica;

realice una búsqueda de un derecho de acceso usando una identidad de la llave (2) electrónica en una caché (10) de credenciales cuando el dispositivo (1) de control de acceso es incapaz de comunicarse con un servidor (18) de control de acceso;

envíe una señal de desbloqueo cuando el derecho de acceso indique que se debería conceder acceso a la llave (2) electrónica;

recupere, desde el servidor (18) de control de acceso, un derecho de acceso que indique si la llave (2) electrónica debería tener acceso o no, cuando el dispositivo (1) de control de acceso es capaz de comunicarse con el servidor (18) de control de acceso; y

actualice la caché (10) de credenciales con el derecho de acceso recuperado desde el servidor (18) de control de acceso;

en donde el dispositivo de control de acceso que comprende además instrucciones (66) que, cuando se ejecutan por el procesador, hacen que el dispositivo (1) de control de acceso:

reciba, iniciado desde un dispositivo remoto, un derecho de acceso que indique si la llave (2) electrónica debería tener acceso o no; y

actualice la caché (10) de credenciales con el derecho de acceso recibido desde el dispositivo remoto.

8. El dispositivo (1) de control de acceso según la reivindicación 7, en donde la caché (10) de credenciales forma parte del dispositivo (1) de control de acceso.

9. El dispositivo (1) de control de acceso según la reivindicación 7 u 8, en donde las instrucciones para realizar la búsqueda comprenden instrucciones (66) que, cuando se ejecutan por el procesador, hacen que el dispositivo (1) de control de acceso encuentre una entrada de derecho de acceso en la caché de credenciales para la llave (2) electrónica.

10. El dispositivo (1) de control de acceso según la reivindicación 9, en donde la entrada comprende un tiempo de validez y en donde las instrucciones para enviar una señal de desbloqueo comprenden instrucciones (66) que, cuando se ejecutan por el procesador, hacen que el dispositivo (1) de control de acceso envíe la señal de desbloqueo sólo cuando la hora actual esté dentro del tiempo de validez de la entrada.

11. El dispositivo (1) de control de acceso según una cualquiera de las reivindicaciones 7 a 10, en donde las instrucciones para comunicarse con la llave (2) electrónica comprenden instrucciones (66) que, cuando se ejecutan por el procesador, hacen que el dispositivo (1) de control de acceso realice un procedimiento de respuesta al desafío con la llave (2) electrónica.

12. Un programa de ordenador (91) para controlar el acceso a un espacio (16) físico, el programa de ordenador que comprende un código de programa de ordenador que, cuando se ejecuta en un dispositivo (1) de control de acceso, hace que el dispositivo (1) de control de acceso:

se comunique con una llave (2) electrónica para autenticar la llave (2) electrónica;

realice una búsqueda de un derecho de acceso usando una identidad de la llave (2) electrónica en una caché (10) de credenciales cuando el dispositivo (1) de control de acceso es incapaz de comunicarse con un servidor (18) de control de acceso;

envíe una señal de desbloqueo cuando el derecho de acceso indique que se debería conceder acceso a la llave (2) electrónica; y

recupere, desde el servidor (18) de control de acceso, un derecho de acceso que indique si la llave (2) electrónica debería tener acceso o no, cuando el dispositivo (1) de control de acceso es capaz de comunicarse con el servidor (18) de control de acceso; y

actualice la caché (10) de credenciales con el derecho de acceso recuperado del servidor (18) de control de acceso,

en donde el programa de ordenador que comprende un código de programa de ordenador que, cuando se ejecuta en un dispositivo (1) de control de acceso, hace que el dispositivo de control de acceso:

reciba, iniciado desde un dispositivo remoto, un derecho de acceso que indique si la llave (2) electrónica debería tener acceso o no; y

actualice la caché (10) de credenciales con el derecho de acceso recibido desde el dispositivo remoto.

13. Un producto de programa de ordenador (90) que comprende un programa de ordenador según la reivindicación 12 y un medio legible por ordenador en el que está almacenado el programa de ordenador.

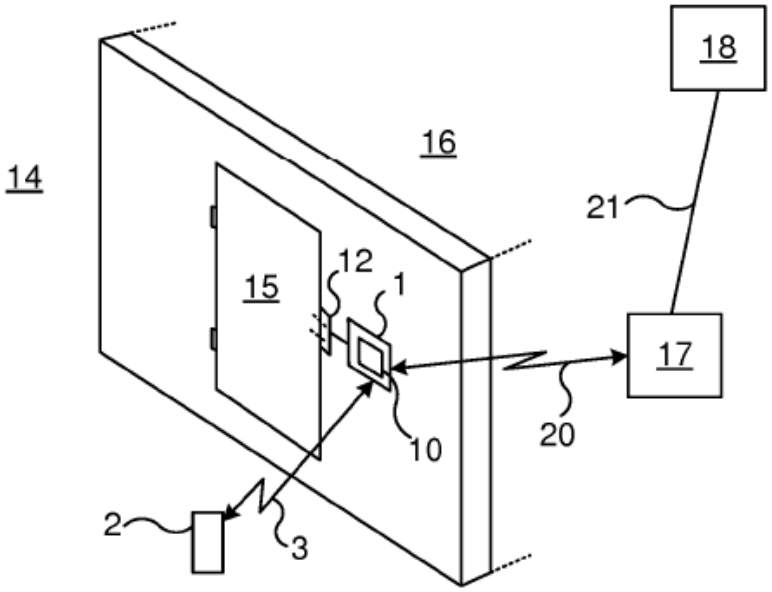
18
16
14
21
15
12
1
17
20
10
2
3

Fig. 1

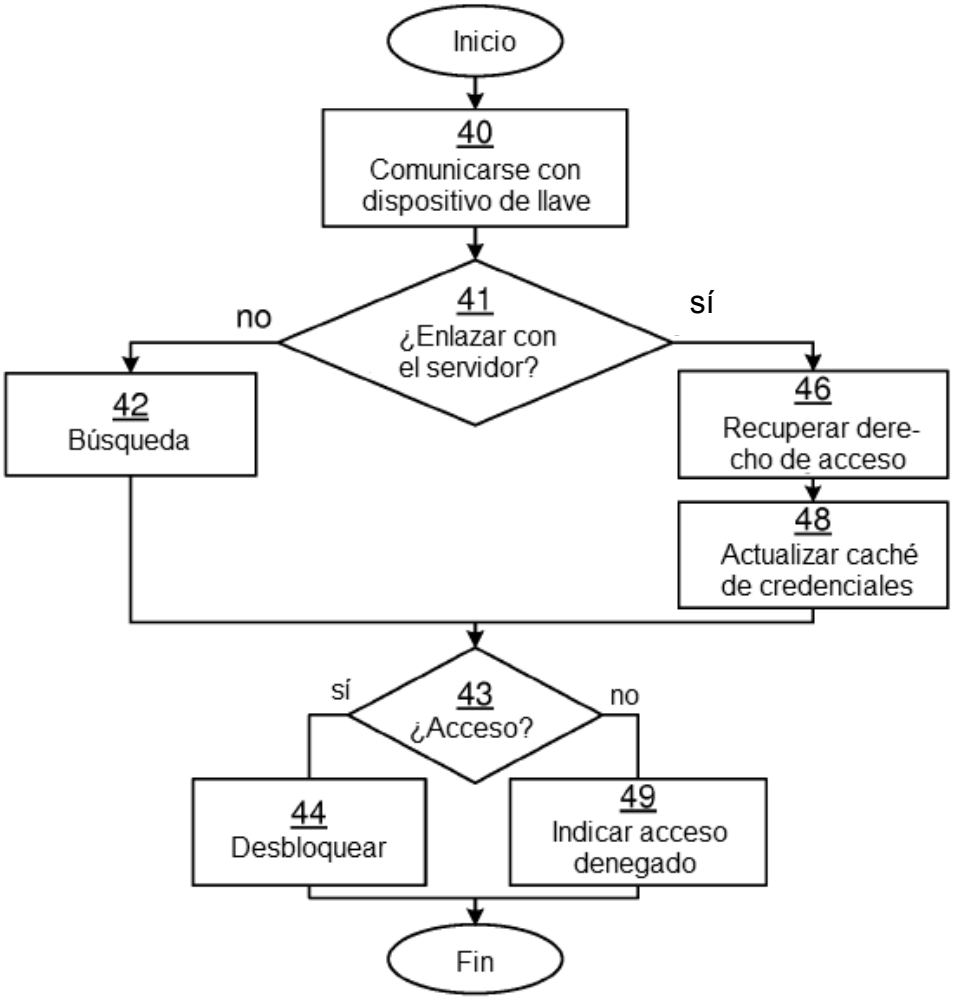
Inicio
40
Comunicarse con dispositivo de llave
41
¿Enlazar con el servidor?
no
sí
42
Búsqueda
46
Recuperar derecho de acceso
48
Actualizar caché de credenciales
43
¿Acceso?
sí
no
44
Desbloquear
49
Indicar acceso denegado
Fin

Fig. 2A

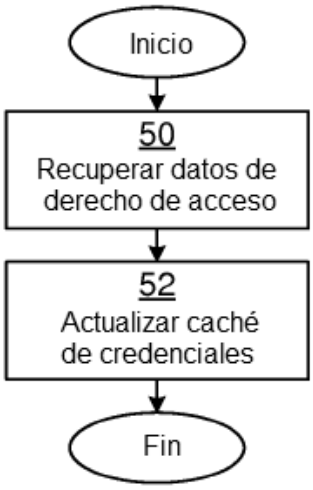

Fig. 2B

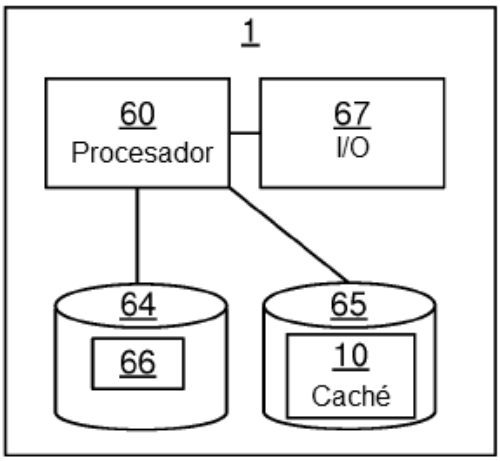

Fig. 3

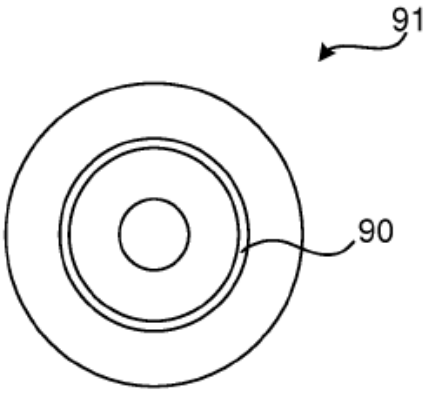

Fig. 4