(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 760 301**

(51) Int. CI.:

G07C 9/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **06.10.2016 E 16450026 (6)**

(97) Fecha y número de publicación de la concesión europea: **04.09.2019 EP 3156980**

(54) Título: **Método para la programación de medios de identificación de un sistema de control de acceso**

(30) Prioridad:

08.10.2015 AT 6532015

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
13.05.2020

(73) Titular/es:

EVVA SICHERHEITSTECHNOLOGIE GMBH (100.0%)
Wienerbergstrasse 59-65
1120 Wien, AT

(72) Inventor/es:

ULLMANN, JOHANNES

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Método para la programación de medios de identificación de un sistema de control de acceso

La invención se refiere a un método para la programación de medios de identificación de un sistema de control de acceso, comprendiendo el sistema de control de acceso al menos un dispositivo de control de acceso y una unidad central de cálculo, en la que se almacenan y administran datos de derechos de acceso, comprendiendo la programación del medio de identificación el envío de datos de derechos de acceso a través de una red de telecomunicaciones inalámbrica a un aparato de telecomunicaciones móvil y la transmisión de los datos de derechos de acceso recibidos por el aparato de telecomunicaciones móvil a una memoria del medio de identificación.

La invención también se refiere a un dispositivo de control de acceso para la realización de un método de este tipo.

En sistemas de cierre modernos se presentan diversas necesidades. Los sistemas de cierre entran en aplicación, generalmente, en edificios más grandes, en los que debe controlarse de manera individual el acceso a una pluralidad de espacios o secciones del edificio. Para cubrir la necesidad de autorizaciones a menudo cambiantes, los sistemas de cierre a menudo se equipan con dispositivos de control de acceso, que presentan medios electrónicos de consulta de autorización. Las informaciones de autorización están almacenadas en medios de identificación electrónicos. Las informaciones de autorización existen, por ejemplo, como código electrónico, que puede leerse electrónicamente por las unidades de lectura del dispositivo de control de acceso y puede evaluarse con respecto a la autorización de acceso. En este caso, no es obligatoriamente necesario que de hecho se transmita el código electrónico. Más bien, la autorización de acceso también puede determinarse por medio de un protocolo de autenticación y/o de identificación entre el dispositivo de control de acceso y el medio de identificación, es decir, con procesos criptográficos, con los que sin transmisión del código sensible se puede determinar si el medio de identificación y el dispositivo de control de acceso disponen del mismo secreto, el cual corresponde a una autorización de acceso.

Bajo dispositivos de control de acceso o unidades de cierre, en el marco de la invención deben entenderse unidades de cierre eléctricas, electrónicas o mecatrónicas, en particular, cerraduras. En este caso, las unidades de cierre pueden comprender diferentes componentes como, p. ej., dispositivos de lectura para medios de identificación, una electrónica de cierre y similares. Los dispositivos de control de acceso o bien unidades de cierre, sirven, en este caso, para bloquear o habilitar el acceso a espacios en función de la autorización de acceso y, por lo tanto, está previstos para la instalación en puertas, ventanas y similares. Bajo unidades de cierre mecánicas debe entenderse, p. ej., cierres de cilindro. Las unidades de cierre mecatrónicas son, p. ej., dispositivos de bloqueo, cilindros de motor, cilindros electrónicos, herrajes electrónicos y similares accionados de manera electromotriz. Las unidades de cierre eléctricas son, p. ej., porteros automáticos eléctricos.

Bajo medios de identificación se entienden medios de identificación electrónicos o dispositivos, que tienen almacenado un código electrónico o bien informaciones de autorización, p. ej., en forma de tarjetas, llaveros y combinaciones de llaves mecánicas y electrónicas, o teléfonos inteligentes.

Bajo informaciones de autorización, deben entenderse, p. ej., códigos de identificación o bien de acceso y/o condiciones de acceso como, p. ej., hora de acceso autorizada, día de acceso autorizado, fecha de acceso autorizada de un usuario y similares. En particular, las informaciones de autorización están compuestas por una llave individual de dispositivo de control de acceso, es decir, una identificación que identifica el dispositivo de control de acceso y, opcionalmente, una restricción temporal de autorización.

En el documento WO 2009/094683 A1 está descrito un método del tipo mencionado al principio. En el método ahí descrito, la programación de los medios de identificación electrónicos con datos de derechos de acceso tiene lugar a través de una red de telecomunicaciones inalámbrica, de modo que los datos de derechos de acceso se envían por la unidad central de cálculo a un aparato de telecomunicaciones móvil inalámbrico del usuario o bien del propietario de la tarjeta respectivamente deseado. Los datos de derechos de acceso recibidos por el aparato de telecomunicaciones móvil, se pueden poner a disposición de un medio de identificación adecuado, el cual, de esta manera, obtiene una función de llave. De esta forma, se crea un tipo de “llave-en-línea”, dado que el medio de identificación puede reprogramarse a través de la red de telecomunicaciones móvil y el correspondiente dispositivo terminal móvil para, de esta manera, modificar los datos de derechos de acceso y, por lo tanto, la autorización de acceso del propietario de la tarjeta.

A causa de la posibilidad de la programación remota de medios de identificación, para la modificación de las autorizaciones de acceso ya no es necesario obtener un acceso directo a las unidades de cierre o bien dispositivos de control de acceso individuales. Los dispositivos de control de acceso, después de la instalación y la inicialización, pueden trabajar como unidades autónomas y, en particular, no necesitan una conexión de red. Esto es una ventaja particular, cuando a causa de las circunstancias locales no se desea una interconexión de unidades de cierre, por ejemplo, cuando en sistemas de cierre más pequeños el coste de interconexión sería demasiado costoso o cuando no se desean intervenciones de construcción en la puerta y en la zona de la puerta.

Como se describe en el documento WO 2009/094683 A1, los datos de derechos de acceso, después de la transmisión al aparato de telecomunicaciones móvil, con utilización de un dispositivo de escritura/de lectura, se escriben en el medio de identificación externo separado del aparato de telecomunicaciones. Esto, por su naturaleza, requiere un proceso de escritura adicional y un correspondiente dispositivo de escritura. En el caso de medios de identificación que trabajan de forma pasiva, dado que no presentan un suministro eléctrico propio, la comunicación entre el aparato de telecomunicaciones móvil y el medio de identificación tiene lugar por medio de comunicación de campo cercano que, en particular, se realiza según el estándar de RFID o bien de NFC. Sin embargo, esto requiere que el teléfono móvil disponga de un módulo de envío/de recepción para la comunicación de campo cercano.

Por ello, la presente invención aspira a hacer posible la programación de medios de identificación por medio de aparatos de telecomunicaciones móviles, en particular, teléfonos móviles, también cuando el correspondiente aparato no dispone de un módulo de comunicación de campo cercano.

Para la solución de esta misión, la invención prevé en un método del tipo mencionado al principio esencialmente, que la transmisión de los datos de derechos de acceso tiene lugar desde el aparato de telecomunicaciones a la memoria del medio de identificación a través de al menos un dispositivo de control de acceso, transmitiéndose los datos de derechos de acceso desde el aparato de telecomunicaciones a una primera interfaz de comunicaciones inalámbrica del dispositivo de control de acceso y desde una segunda interfaz de comunicaciones inalámbrica del dispositivo de control de acceso a la memoria del medio de identificación. El intercambio de datos entre el dispositivo terminal de telecomunicaciones móvil y el medio de identificación con el fin de la programación del medio de identificación no tiene lugar, por lo tanto, directamente, sino con interconexión de un dispositivo de control de acceso. El dispositivo de control de acceso puede, en este caso, de manera sencilla estar equipado con una primera interfaz de comunicaciones, que permite un intercambio de datos con teléfonos móviles comunes. La comunicación de datos entre el dispositivo de control de acceso y el medio de identificación puede tener lugar, fundamentalmente, a través de estándares cualesquiera que prevé el fabricante del sistema de cierre. Puesto que los dispositivos de control de acceso y los medios de identificación de un sistema de cierre, habitualmente, se ponen a disposición por el fabricante del sistema, la compatibilidad de las interfaces de comunicaciones en la transmisión de datos entre el dispositivo de control de acceso y el medio de identificación no representa una dificultad. La compatibilidad del sistema de cierre con el aparato de telecomunicaciones móvil, en particular, el teléfono móvil del respectivo usuario, por el contrario, se representa difícil, ya que teléfonos móviles presentan diferentes y, en el transcurso del tiempo, también equipamientos cambiantes con interfaces de comunicaciones. Cuando el teléfono móvil del usuario no soporta la comunicación de campo cercano utilizada generalmente para la programación del medio de identificación, la invención posibilita la utilización de otra interfaz de comunicaciones del teléfono móvil, teniendo lugar la programación entonces con intermediación del dispositivo de control de acceso, el cual está equipado con una interfaz compatible con el teléfono móvil.

Una realización preferida de la invención prevé, en este caso, que los datos de derechos de acceso se transmitan de forma inalámbrica a través radio de corto alcance como, p. ej., Bluetooth, en particular, Bluetooth de baja energía, desde el aparato de telecomunicaciones a la primera interfaz de comunicaciones inalámbrica del dispositivo de control de acceso. En particular, el estándar de Bluetooth 4.0 de LE es ventajoso, dado que éste presenta un consumo eléctrico sumamente bajo. La tecnología de Bluetooth está muy extendida y, prácticamente, incorporada en todos los teléfonos móviles modernos, de modo que la transmisión de datos entre teléfono móvil y el dispositivo de control de acceso se garantiza independientemente del respectivo modelo del teléfono móvil. Preferiblemente, el dispositivo terminal de telecomunicaciones y el dispositivo de control de acceso están acoplados electrónicamente (p. ej., con Bluetooth) entre sí, de modo que solo es posible una conexión de datos entre las unidades acopladas. La comunicación de datos entre el dispositivo de control de acceso y el medio de identificación tiene lugar, preferiblemente, por medio de comunicación de campo cercano, en particular, según el estándar de RFID, de NFC, de JCOP (Java Card OpenPlatform) o de MIFARE DESFire. La comunicación del medio de identificación con el dispositivo de control de acceso y aquella del dispositivo de control de acceso con el aparato de telecomunicaciones tiene lugar, por lo tanto, según protocolos de transmisión diferentes entre sí, de modo que el dispositivo de control de acceso dispone de al menos dos unidades de envío/de recepción o bien dos interfaces de comunicaciones. Las dos unidades de envío/de recepción o bien interfaces de comunicaciones, están, p. ej., configuradas como unidades de hardware separadas entre sí, o contenidas en un único módulo.

Ventajoso en la utilización de comunicación de campo cercano entre el dispositivo de control de acceso y el medio de identificación es, que el medio de identificación puede estar configurado como componente pasivo sin suministro eléctrico propio. Un modo de proceder preferido prevé en este contexto, que el suministro de energía de la unidad de envío/de recepción del medio de identificación tiene lugar a través de un campo alterno electromagnético, en particular, esencialmente magnético, de la segunda interfaz de comunicaciones inalámbrica del dispositivo de control de comunicación.

Para reducir el peligro de una lectura o una escucha no autorizada de datos sensibles, puede estar previsto de manera preferida, que el dispositivo terminal de telecomunicaciones y/o el medio de identificación y/o el dispositivo de control de acceso presenten un módulo de hardware de seguridad, en el que se almacena al menos un certificado digital para posibilitar una autenticación de los socios de comunicación. La transmisión de datos entre el dispositivo terminal de telecomunicaciones y el dispositivo de control de acceso y/o entre el dispositivo de control de

acceso y el medio de identificación comprende, preferiblemente, la utilización de un protocolo de intercambio de clave o protocolo de derivación de clave, con lo cual, se hace accesible a los respectivos socios de comunicación al menos una clave de sesión secreta, común, después de lo cual, la al menos una clave de sesión se utiliza para el establecimiento de un canal de transmisión seguro entre los respectivos socios de comunicación y transmitiéndose los datos de derechos de acceso a través del canal seguro. Preferiblemente, las operaciones necesarias para el intercambio de clave o el protocolo de derivación de clave en el medio de identificación, en el dispositivo de control de acceso o bien en el dispositivo terminal de telecomunicaciones, se realizan en el respectivo módulo de hardware de seguridad. El al menos un certificado digital puede, en este caso, preferiblemente, firmarse por la unidad central de cálculo.

Preferiblemente, la al menos una clave de derivación en el módulo de hardware de seguridad del medio de identificación o bien del dispositivo terminal de telecomunicaciones y en el dispositivo de control de acceso, se genera en base a un código de acceso individual del dispositivo de control de acceso, preferiblemente, además, en base a un número aleatorio generado por los respectivos socios de comunicación y/o un número consecutivo generado por los respectivos socios de comunicación.

El método de programación de acuerdo con la invención para la programación de un medio de identificación puede entrar en aplicación, preferiblemente, en un método de control de acceso. La invención prevé en este contexto, preferiblemente, un método para el control de acceso, en particular, en estructuras de construcción como, p. ej., edificios, en los que tiene lugar una transmisión de datos bidireccional entre un medio de identificación electrónico, que almacena datos de derechos de acceso, y un dispositivo de control de acceso, y en el dispositivo de control de acceso se realiza una comprobación de derecho de acceso, controlándose un medio de bloqueo para la habilitación o el bloqueo opcional del acceso en función del derecho de acceso determinado, almacenándose y administrándose los datos de derechos de acceso en una unidad central de cálculo y programándose el medio de identificación con datos de derechos de acceso con un método con un método según una de las reivindicaciones 1 a 4.

De acuerdo con otro aspecto, la presente invención se refiere a un dispositivo de control de acceso que comprende una interfaz de comunicaciones inalámbrica para la transmisión de datos, en particular, datos de derechos de acceso, desde un y/o a un aparato de telecomunicaciones y una segunda interfaz de comunicaciones inalámbrica para la transmisión de datos, en particular, datos de derechos de acceso desde un y/o a un medio de identificación, comprendiendo el dispositivo de control de acceso una memoria intermedia y una unidad de control, interactuando la unidad de control con la primera y la segunda interfaz de comunicaciones, de modo que datos que llegan a través de la primera interfaz de comunicaciones se suministran a la memoria intermedia, y para el reenvío al medio de identificación se entregan desde la memoria intermedia a la segunda interfaz de comunicaciones.

La primera interfaz de comunicaciones está configurada, preferiblemente, para la comunicación de datos por medio de radio de corto alcance. En particular, la primera interfaz de comunicaciones está configurada para la comunicación de datos a través del estándar de Bluetooth, en particular, Bluetooth de baja energía.

La segunda interfaz de comunicaciones está configurada, preferiblemente, para la comunicación de datos inalámbrica por medio de comunicación de campo cercano, en particular, según un estándar de RFID, de NFC, de JCOP o de MIFARE DESFire. El medio de identificación puede, en este caso, estar configurado como unidad de RFID, de NFC, de JCOP o de MIFARE DESFire que trabaja pasiva.

El dispositivo de control de acceso es, preferiblemente, una unidad de cierre de un sistema de cierre, en particular, una unidad de cierre eléctrica, electrónica o mecatrónica como, p. ej., cierres de cilindro, cilindros electrónicos, porteros automáticos eléctricos, herrajes o lectores de pared.

Básicamente, la presente invención no está limitada a una configuración determinada del aparato de telecomunicaciones. El aparato de telecomunicaciones debe ser capaz de realizar únicamente una comunicación de datos, por un lado, con la unidad central de cálculo y, por otro lado, con el dispositivo de control de acceso. El aparato de telecomunicaciones presenta, por ello, preferiblemente, dos interfaces de transmisión de datos diferentes entre sí. Una de las interfaces de transmisión de datos está configurada con el fin de la comunicación con la unidad central de cálculo, preferiblemente, para la comunicación a través de una red de telecomunicaciones. La otra interfaz de transmisión de datos está configurada con el fin de la comunicación con el dispositivo de control de acceso a través de radio de corto alcance, p. ej., Bluetooth. Preferiblemente, en el caso del aparato de telecomunicaciones se trata de un teléfono móvil, en particular, un teléfono móvil de GSM/UMTS, en particular, teléfono inteligente, tableta, reloj inteligente o de un ordenador personal, en particular, portátil. El aparato de telecomunicaciones, sin embargo, también puede estar configurado como dispositivo estacionario, p. ej., como nodo de Bluetooth, que transforma los datos obtenidos a través de la red de telecomunicaciones al protocolo de Bluetooth.

La transmisión de datos ente la unidad central de cálculo y el aparato de telecomunicaciones, puede tener lugar a través de una red de telecomunicaciones móvil como, p. ej., una red de GSM, de GPRS, de UMTS y/o de LTE, o a través de una conexión a Internet inalámbrica como, p. ej., WLAN o similar.

El aparato de telecomunicaciones puede asumir la función de una unidad de retransmisión o de proxy entre la unidad central de cálculo y el dispositivo de control de acceso. En este caso, los datos de derechos de acceso no se almacenan de forma intermedia en el aparato de telecomunicaciones, sino que se crea una conexión de datos extremo a extremo entre la unidad central de cálculo y el dispositivo de control de acceso, de modo que los datos únicamente se conducen a través del aparato de telecomunicaciones. En el aparato de telecomunicaciones tiene lugar, entonces, únicamente una transformación de los datos desde el protocolo de transmisión utilizado para la conexión entre la unidad central de cálculo y el aparato de telecomunicaciones al protocolo de transmisión utilizado para la conexión entre el aparato de telecomunicaciones y el dispositivo de control de acceso.

Bajo un medio de bloqueo, debe entenderse en el marco de la invención, p. ej., un elemento de bloqueo que actúa mecánicamente, que puede moverse entre una posición de bloqueo y una de habilitación, un elemento de acoplamiento mecánico o magnético, que acopla o desacopla un elemento de accionamiento como, p. ej., una manija, con un miembro de bloqueo, o un elemento de bloqueo bloqueable y/o habilitable eléctricamente como, p. ej., un portero automático eléctrico.

A continuación, se explica la invención más en detalle mediante un ejemplo de realización representado esquemáticamente en el dibujo. En éste, la Fig. 1 muestra la construcción esquemática de un sistema de control de acceso y la Fig. 2 la programación de un medio de identificación mediante un diagrama de bloques.

En la Fig. 1, una unidad central de cálculo está designada con 1. Los objetos, a los que debe controlarse el acceso con ayuda del sistema de control de acceso, están designados con 2 y, en el presente caso, representados esquemáticamente como casas. Los objetos 2 presentan, respectivamente, una puerta con una unidad de cierre basada en RFID o en NFC. Un administrador 3 administra la unidad 1 central de cálculo y puede conceder autorizaciones de acceso. La unidad 1 central de cálculo está conectada a una red 4 de telecomunicaciones inalámbrica móvil como, por ejemplo, una red móvil de GSM, y puede enviar datos de derechos de acceso a aparatos 5 de telecomunicaciones móviles a través de la red 4 de telecomunicaciones. En el caso de los aparatos 5 de telecomunicaciones móviles se trata de teléfonos móviles, que están dotados con una aplicación de software, la cual controla el intercambio de datos entre la unidad 1 central de cálculo y un medio 6 de identificación. La aplicación de software, o bien el aparato 5 de telecomunicaciones, funciona como enrutador, que reenvía los datos de derechos de acceso obtenidos por la unidad 1 central de cálculo al medio 6 de identificación a través de la conexión 7 de comunicaciones. Los datos de derechos de acceso a ser transmitidos, en este caso, se cifran en la unidad 1 central de cálculo y se descifran en el medio 6 de identificación. En el aparato 5 de telecomunicaciones no tiene lugar un descifrado de los datos de derechos de acceso. En el caso más sencillo, los datos de derechos de acceso se envían al aparato 5 de telecomunicaciones móvil como identificación de cerradura. Cuando ahora, en un ejemplo considerablemente simplificado, las unidades de cierre de los objetos 2 representados en la Fig. 1, presentan la identificación 100, 101 y 102, de esta manera, la transmisión de los datos de derechos de acceso a un aparato 5 de telecomunicaciones en forma de la identificación 101, significa que esto corresponde a una autorización de acceso para la unidad de cierre con la identificación 101. Cuando ahora, el medio 6 de identificación utilizado como llave, se lleva a la cercanía de una unidad de cierre con la identificación 101 y, en el curso de la comprobación de autorización de acceso, los datos de derechos de acceso, es decir, la identificación “101” de cerradura, se transmiten a la unidad de cierre, de esta manera, la unidad de cierre, a causa de una comparación de la identificación de cerradura transmitida por la llave con la propia identificación de cerradura, en caso de coincidencia de las mismas, reconoce la existencia de una autorización de acceso, después de lo cual, se habilita la cerradura.

De acuerdo con la invención, la transmisión 7 de los datos de derechos de acceso desde el aparato 5 de telecomunicaciones a un medio 6 de identificación no tiene lugar directamente, sino a través de una unidad 8 de cierre provista para ello, como está representado en la Fig. 2. La unidad 8 de cierre dispone, para este fin, de una primera interfaz 13 de comunicaciones, en la que se trata de una interfaz para radio de corto alcance como, p. ej., una interfaz de Bluetooth 4.0 de baja energía. La unidad 8 de cierre dispone, además, de una segunda interfaz 15 comunicaciones, en la que se trata de una interfaz para comunicación de campo cercano, p. ej., a través de RFID o bien NFC.

Para el control del proceso de programación, el aparato de telecomunicaciones, en el que se puede tratar, p. ej., de un teléfono inteligente, una tableta o un reloj inteligente, dispone de una interfaz 12 gráfica de usuario y una aplicación 11 de software. Los datos de derechos de acceso transmitidos por la unidad 1 central de cálculo al aparato 5 de telecomunicaciones a través de la conexión 4, se transmiten a la unidad 9 de cierre a través de la conexión 9 de radio (p. ej., conexión de Bluetooth) y la primera interfaz 13 de comunicaciones. Los datos de derechos de acceso se transmiten junto con informaciones de cabecera, de modo que un microcontrolador 14 de la unidad 8 de cierre reconoce los datos como datos determinados para el medio 6 de identificación y se encarga del reenvío de los datos al medio 6 de identificación a través de la segunda interfaz 15 de comunicaciones y la conexión 10 de comunicación de campo cercano. En el medio de identificación, los datos se escriben en una memoria y se utilizan para consultas de autorización futuras, para poder comprobar la autorización de acceso, en relación con un deseo de acceso, en el intercambio de datos con una unidad de cierre.

De acuerdo con un ejemplo de aplicación, para la programación de un medio 6 de identificación se puede proceder como a continuación:

1. El usuario selecciona la función “actualizar medio de identificación a través de componente de cierre” en la aplicación 11 en el dispositivo 5 terminal móvil.
2. La aplicación 11 comprueba primero si existe una conexión 4 de datos al servidor 1.
3. La aplicación 11 comprueba si se puede establecer una conexión 9 a un componente 9 de cierre.
4. Se solicita al usuario que mantenga el medio 6 de identificación en el correspondiente componente 8 de cierre.
5. Se establece una conexión entre:

a. Medio 6 de identificación y componente 7 de cierre a través de RFID/NFC 10,
b. Componente 8 de cierre y dispositivo 5 terminal móvil a través de radio/Bluetooth 9 de LE,
c. Dispositivo 5 terminal móvil y servidor 1 a través de conexión 4 de datos.

6. Se informa al usuario del proceso de actualización a través de la interfaz 12 de usuario de la aplicación 11.
7. El componente 8 de cierre y la aplicación 11 señalizan al usuario si el proceso se completó correctamente o, alternativamente, un mensaje de error.

Alternativamente, también podría omitirse el paso 2 y el paso 5c, siempre y cuando la aplicación 11 haya almacenado de forma intermedia ya antes los datos necesarios para la actualización. Para ello, sin embargo, el usuario debe preseleccionar los medios 6 de identificación a ser actualizados de una lista en la aplicación 11. Este proceso alternativo podría parecer como sigue:

1. El usuario selecciona la función “almacenar datos de medios” en la aplicación 11 en el dispositivo 5 terminal móvil.

a. La aplicación 11 comprueba primero si existe una conexión 4 de datos al servidor 1.
b. El usuario selecciona los medios 6 de identificación a ser actualizados.
c. Los datos necesarios se transmiten desde el servidor 1 a la aplicación 11 y ahí se almacenan.

2. El usuario selecciona la función “actualizar medio a través de componente de cierre” en la aplicación 11 en el dispositivo 5 terminal móvil.
3. La aplicación 11 comprueba si se puede establecer una conexión 9 a un componente 8 de cierre.
4. Se solicita al usuario que mantenga el medio 6 de identificación en el correspondiente componente 8 de cierre.
5. Se establece una conexión entre:

a. Medio 6 de identificación y componente 8 de cierre a través de comunicación de campo cercano, p. ej., RFID/NFC 10,
b. Componente 8 de cierre y dispositivo 5 terminal móvil a través de radio 9, p. ej., Bluetooth de LE.

6. Se informa al usuario acerca del proceso de actualización a través de la interfaz 12 de usuario de la aplicación 11.
7. El componente 8 de cierre y la aplicación 11 señalizan al usuario si el proceso se completó correctamente o, alternativamente, un mensaje de error.
8. Tan pronto como la aplicación 11 tenga de nuevo conexión 4 de datos al servidor 1, los datos actualizados de los medios 6 de identificación se transmiten de vuelta al servidor 1.

En el marco de la presente invención, la conexión 9 de radio de corto alcance no puede utilizarse para la transmisión de datos de derechos de acceso. A través de la conexión de radio también pueden transmitirse datos de configuración de los componentes de cierre, una lista negra de medios de identificación sin autorización de derechos de acceso, a partir de los datos de eventos leídos de los componentes de cierre, así como datos de estado. La transmisión de datos puede tener lugar, básicamente, también sin orden activa mediante el usuario. Más bien, la transmisión de datos puede tener lugar automáticamente, tan pronto como el dispositivo terminal móvil se encuentre al alcance del correspondiente componente de cierre. Mediante programación adecuada de la aplicación 11, puede determinarse en qué momento tiene lugar la transmisión de datos, con qué componente de cierre y con qué frecuencia. En este caso, pueden tenerse en cuenta, p. ej., estrategias de gestión de energía y estrategias de información. De manera análoga, también pueden notificarse datos, a partir de los componentes de cierre, de vuelta al servidor central.

A continuación, se mencionan ejemplos para los datos a ser transmitidos a través de la conexión 9: datos para un medio de identificación, en particular, su actualización (actualización de software o de firmware), datos para diferentes medios de identificación para la actualización de estos, datos de estado acerca de un proceso de actualización exitoso, datos de estado acerca de un estado de carga de batería así como acerca de un próximo cambio de batería, ajuste de hora con el servidor, datos de estado acerca de un ajuste de hora exitoso, datos de estado acerca de la conservación de la lista negra, datos de estado acerca de la apertura (p. ej., cerradura actualmente en apertura permanente), datos de contacto de puerta y datos de contacto de cerrojo (si existen),

alarmas de manipulación y de forzado (cuando se soporta por el componente de cierre), informaciones de versión de firmware, actualizaciones de firmware, horómetros del componente de cierre, bloqueos realizados del componente de cierre, datos de configuración, datos de estado acerca de la lectura de la lista de eventos del componente de cierre, listas de zonas, informaciones de zonas horarias, calendario de días festivos, calendario de apertura permanente, habilitaciones.

REIVINDICACIONES

1. Método para la programación de medios de identificación de un sistema de control de acceso, comprendiendo el sistema de control de acceso al menos un dispositivo (8) de control de acceso y una unidad (1) central de cálculo, en la que se almacenan y administran datos de derechos de acceso, comprendiendo la programación del medio (6) de identificación el envío de datos de derechos de acceso a un aparato (5) de telecomunicaciones móvil a través de una red (4) de telecomunicaciones inalámbrica, y la transmisión a una memoria del medio (6) de identificación de los datos de derechos de acceso recibidos por el aparato de telecomunicaciones móvil, **caracterizado por que** la transmisión de los datos de derechos de acceso desde el aparato (5) de telecomunicaciones a la memoria del medio (6) de identificación, tiene lugar a través de al menos un dispositivo (8) de control de acceso, transmitiéndose los datos de derechos de acceso desde el aparato (5) de telecomunicaciones a una primera interfaz (13) de comunicaciones inalámbrica y desde una segunda interfaz (15) de comunicaciones inalámbrica del dispositivo de control de acceso a la memoria del medio (6) de identificación.

2. Método según la reivindicación 1, **caracterizado por que** los datos de derechos de acceso se transmiten de forma inalámbrica a través de radio de corto alcance como, p. ej., a través de Bluetooth, en particular, Bluetooth de baja energía, desde el aparato (5) de telecomunicaciones a la primera interfaz (13) de comunicaciones inalámbrica del dispositivo de control de acceso.

3. Método según la reivindicación 1 ó 2, **caracterizado por que** la comunicación de datos entre la segunda interfaz (13) de comunicaciones inalámbrica y una unidad de envío/de recepción del medio (6) de identificación, se realiza por medio de comunicación de campo cercano, en particular, según el estándar de RFID, de NFC, de JCOP o de MIFARE DESFire.

4. Método según la reivindicación 3, **caracterizado por que** el suministro de energía de la unidad de envío/de recepción del medio (6) de identificación tiene lugar a través de un campo alterno electromagnético, de manera preferida, esencialmente magnético, de la segunda interfaz (15) de comunicaciones inalámbrica del dispositivo de control de acceso.

5. Método para el control de acceso, en particular, en edificios, en el que tiene lugar una transmisión de datos bidireccional entre un medio (6) de identificación electrónico, que almacena datos de derechos de acceso, y un dispositivo (8) de control de acceso, y en el dispositivo de control de acceso se realiza una comprobación de autorización de acceso, controlándose, en función de la autorización de acceso determinada, un medio de bloqueo para la habilitación o el bloqueo opcional del acceso, almacenándose y administrándose datos de derechos de acceso en una unidad (1) central de cálculo, y el medio (6) de identificación se programa con datos de derechos de acceso con un método según una de las reivindicaciones 1 a 4.

6. Dispositivo (8) de control de acceso para la realización de un método según una de las reivindicaciones 1 a 5, que comprende una primera interfaz (13) de comunicaciones inalámbrica para la transmisión de datos, en particular, datos de derechos de acceso, desde un y/o a un aparato (5) de telecomunicaciones móvil, y una segunda interfaz (15) de comunicaciones inalámbrica para la transmisión de datos, en particular, datos de derechos de acceso, desde un y/o a un medio (6) de identificación, **caracterizado por que** el dispositivo de control de acceso comprende una memoria intermedia y una unidad (14) de control, estando la unidad (14) de control configurada para la interacción con la primera (13) y la segunda (15) interfaz de comunicaciones, de modo que datos, que llegan a través de la primera interfaz (13) de comunicaciones, se suministran a la memoria intermedia y, para el reenvío al medio (6) de identificación, se entregan desde la memoria intermedia a la segunda interfaz (15) comunicaciones.

7. Dispositivo de control de acceso según la reivindicación 6, **caracterizado por que** la primera interfaz (13) de comunicaciones está configurada para la comunicación de datos por medio de radio de corto alcance.

8. Dispositivo de control de acceso según la reivindicación 7, **caracterizado por que** la primera interfaz (13) de comunicaciones está configurada para la comunicación de datos a través del estándar de Bluetooth, en particular, Bluetooth de baja energía.

9. Dispositivo de control de acceso según una de las reivindicaciones 6 a 8, **caracterizado por que** la segunda interfaz (15) de comunicaciones está configurada para la comunicación de datos inalámbrica por medio de comunicación de campo cercano, en particular, según el estándar de RFID, de NFC, de JCOP o de MIFARE DESFire.

10. Dispositivo de control de acceso según la reivindicación 9, **caracterizado por que** el medio (6) de identificación está configurado como unidad de RFID, de NFC, de JCOP o de MIFARE DESFire que trabaja pasiva.

11. Dispositivo de control de acceso según una de las reivindicaciones 6 a 10, **caracterizado por que** el dispositivo de control de acceso es una unidad de cierre de un sistema de cierre, en particular, una unidad de cierre eléctrica, electrónica o mecatrónica como, p. ej., cierres de cilindro, cilindros electrónicos, porteros automáticos eléctricos, herrajes electrónicos o lectores de pared.

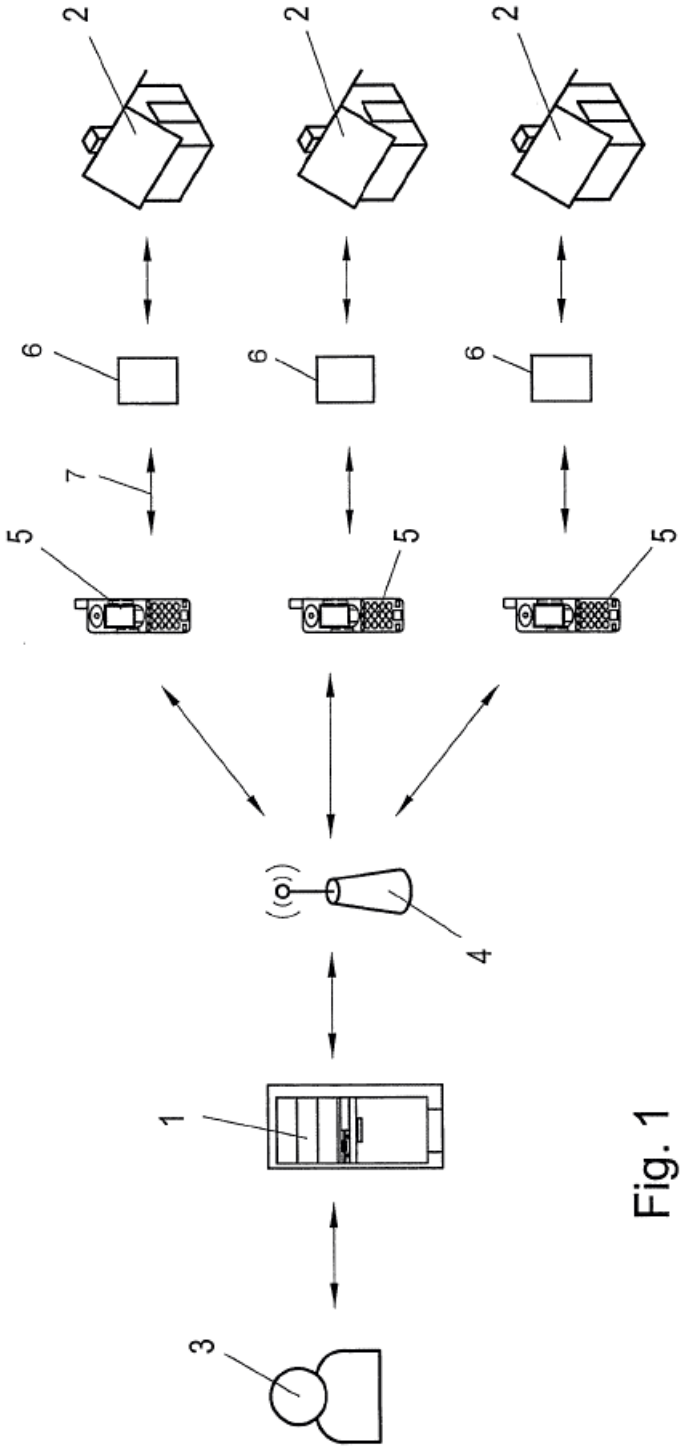

Fig. 1

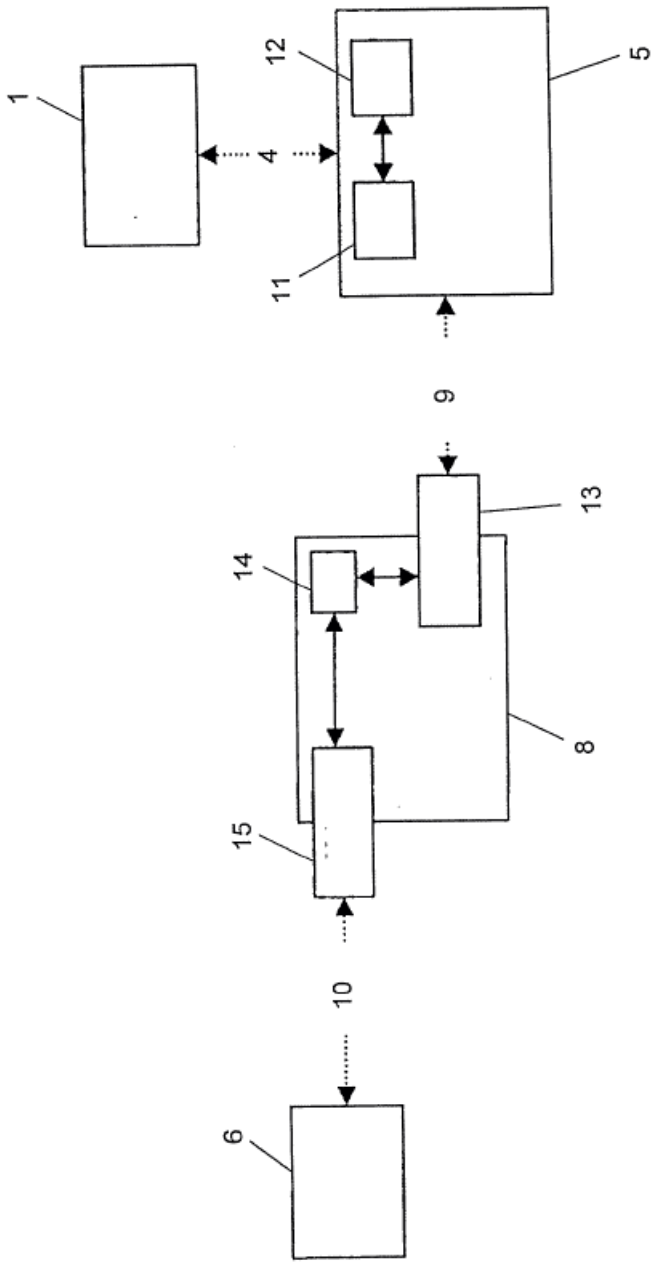

FIG. 2