

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 991 892**

51 Int. Cl.:

H04W 12/08 (2011.01)

G06F 21/35 (2013.01)

G07C 9/00 (2010.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **26.11.2018 E 18208415 (2)**

97 Fecha y número de publicación de la concesión europea: **09.10.2024 EP 3489916**

54 Título: **Dispositivo de control de acceso, sistema de control de acceso y procedimiento**

30 Prioridad:

27.11.2017 EP 17203912

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

05.12.2024

73 Titular/es:

DORMAKABA SCHWEIZ AG (50.0%)

MühlebühlstrasseKempten

8623 Wetzikon, CH y

DORMA DEUTSCHLAND GMBH (50.0%)

72 Inventor/es:

WOLF, MARTIN;

FANARJI, ALEXANDER;

SCHMIDT, ANDREAS;

RAIANO, ADRIANO;

MEIER, TOM;

BORMUTH, PHILLIP y

GRAF, FABIEN

74 Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

ES 2 991 892 T3

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

DESCRIPCIÓN

Dispositivo de control de acceso, sistema de control de acceso y procedimiento

5 La invención se refiere a un dispositivo de control de acceso para un sistema de control de acceso de acuerdo con el preámbulo de la reivindicación 1. El dispositivo de control de acceso está diseñado para asignarse a un área física. El acceso al área física puede concederse mediante el dispositivo de control de acceso. El dispositivo de control de acceso comprende una interfaz de programación. La invención se refiere además a un sistema de control de acceso con un dispositivo de control de acceso de acuerdo con la invención de acuerdo con la reivindicación 10 y un procedimiento para transmitir datos desde un dispositivo móvil a un dispositivo de control de acceso de acuerdo con la reivindicación independiente 13

15 El documento US 2002/0204167 A1 divulga un dispositivo de control de acceso con un sensor biométrico de huellas dactilares. El dispositivo de control de acceso comprende una interfaz de programación para recibir la transmisión de datos de control por cable a través de un token para compararlos con los datos capturados por el sensor de huellas dactilares. La conexión por cable del token al dispositivo de control de acceso es compleja de establecer para el usuario.

20 El documento WO2016/185008 A1 divulga un dispositivo de control de acceso que puede recibir una actualización de software o firmware de forma inalámbrica mediante un dispositivo móvil. El documento DE 10 2016 104 530 A1 divulga un dispositivo de control de acceso a un vehículo que puede reprogramarse mediante un dispositivo móvil. El documento US 2017/0098335 A1 divulga un dispositivo de control de acceso según el preámbulo de la reivindicación 1, en donde un dispositivo móvil dispone de una interfaz de programación.

25 Por lo tanto, el objetivo de la invención es proporcionar un dispositivo de control de acceso, un sistema de control de acceso y un procedimiento para transmitir datos desde un dispositivo móvil a un dispositivo de control de acceso, que superen la desventaja anterior, en particular que esté diseñado para ser fácil de usar.

30 El objetivo se resuelve mediante un dispositivo de control de acceso de acuerdo con la reivindicación independiente 1. En las reivindicaciones dependientes, la descripción y en las figuras se indican perfeccionamientos ventajosos del dispositivo de control de acceso. Además, el objetivo también se resuelve mediante un sistema de control de acceso de acuerdo con la reivindicación 10 y mediante un procedimiento de acuerdo con la reivindicación independiente 13. En las reivindicaciones dependientes 11 y 12, la descripción y en las figuras se indican perfeccionamientos ventajosos del sistema de control de acceso. En particular, el sistema de control de acceso de acuerdo con la invención comprende un dispositivo de control de acceso de acuerdo con la invención, tal como se describe el dispositivo de control de acceso en una de las reivindicaciones 1 a 9 de la descripción y las figuras. Otros perfeccionamientos ventajosos del procedimiento de acuerdo con la invención se indican en la descripción y en las figuras. Las características y detalles descritos en relación con el dispositivo de control de acceso de acuerdo con la invención también se aplican a este respecto en relación con el sistema de control de acceso de acuerdo con la invención y el procedimiento de acuerdo con la invención y viceversa. A este respecto, las características mencionadas en la descripción y en las reivindicaciones pueden ser esenciales para la invención en cada caso individualmente por sí mismas o en cualquier combinación. En particular, se proporciona protección para un dispositivo de control de acceso y un sistema de control de acceso en los que se puede llevar a cabo el procedimiento de acuerdo con la invención, en particular el procedimiento según la reivindicación 13, así como un procedimiento que se puede llevar a cabo con el dispositivo de control de acceso de acuerdo con la invención, en particular con un dispositivo de control de acceso de acuerdo con una de las reivindicaciones 1 a 9, o con el sistema de control de acceso de acuerdo con la invención, en particular con un sistema de control de acceso según una de las reivindicaciones 10 a 12.

50 De acuerdo con la invención está previsto que la interfaz de programación se utilice para comunicarse de forma inalámbrica con un dispositivo móvil.

55 El hecho de que el dispositivo móvil y la interfaz de programación (API) se comuniquen entre sí de forma inalámbrica significa que no es necesario establecer una conexión por cable. Esto hace que el dispositivo de control de acceso de acuerdo con la invención sea particularmente fácil de usar. La interfaz de programación también puede denominarse API. Comunicación significa, en particular, que el dispositivo de control de acceso recibe datos a través de la interfaz de programación.

60 El dispositivo de control de acceso está asignado al área física. En particular, un usuario asignará el dispositivo de control de acceso al área física. El dispositivo de control de acceso sirve de vigilante, en particular de vigilante instalado permanentemente en el área física. Preferentemente el dispositivo de control de acceso está previsto cerca del área física. El dispositivo de control de acceso puede comprender un dispositivo electromecánico, p.ej. un motor eléctrico o un solenoide, o un dispositivo electromagnético, mediante el cual el usuario puede acceder al área física. Por ejemplo, el dispositivo de control de acceso puede comprender una manija que puede conectarse operativamente a una cerradura mediante el dispositivo electromecánico. Alternativamente, el dispositivo de control de acceso puede accionar un elemento de bloqueo, en particular un cerrojo y/o un pestillo, mediante el dispositivo electromecánico. En otra alternativa, el dispositivo de control de acceso puede permitir que el obstáculo, en particular la puerta, la barrera

- o el torniquete, se abra mediante el dispositivo electromecánico o electromagnético. En particular, el dispositivo de control de acceso puede estar diseñado como un herraje electromecánico, un cilindro de cierre electromecánico, un abrepuertas electromecánico o una cerradura motorizada. El dispositivo de control de acceso puede comprender un motor eléctrico para mover el obstáculo, en particular la puerta, el torniquete o la barrera. El dispositivo de control de acceso puede constar de varias partes. Por ejemplo, el dispositivo de control de acceso puede comprender un lector. El lector puede comunicarse con el dispositivo electromecánico o electromagnético, en particular con el herraje electromecánico, el cilindro de cierre electromecánico, el electromotor, el electroimán o la cerradura motorizada, de forma inalámbrica o por cable.
- 5
- 10 El dispositivo de control de acceso comprende preferentemente un procesador. El dispositivo de control de acceso comprende preferentemente una memoria.
- El dispositivo de control de acceso puede comprender un generador de sonido para indicar acústicamente que se ha concedido el acceso y/o una fuente luminosa para indicar de forma visual que se ha concedido y/o denegado el acceso.
- 15 El área física está bloqueada preferentemente por un obstáculo. El obstáculo puede diseñarse como una puerta, en particular una puerta de edificio, una tapa, una trampilla, un torniquete o una barrera. La puerta puede diseñarse como una puerta de torniquete, una puerta corredera o una puerta giratoria, por ejemplo.
- 20 El área física en particular es fija. El área física puede diseñarse como una sala o una caja. Por ejemplo, el área física puede ser una sala bloqueada por una puerta. Alternativamente, el área física puede diseñarse como una caja cerrada, en particular un buzón, como taquilla, una zona al aire libre o un área obstaculizada por una barrera, por ejemplo un aparcamiento.
- 25 En particular, el dispositivo móvil y el dispositivo de control de acceso pueden comunicarse entre sí mediante una comunicación inalámbrica de corto alcance. En este sentido, se utiliza en particular la comunicación de corto alcance como Bluetooth, especialmente Bluetooth de baja energía (BLE), RFID o NFC.
- 30 En particular, el dispositivo de control de acceso comprende una unidad emisora y receptora para la comunicación de corto alcance. El dispositivo de control de acceso recibe inalámbricamente a través de una unidad receptora datos que se procesan en el dispositivo de control de acceso mediante la interfaz de programación. La unidad receptora comprende al menos una antena.
- 35 En particular, el dispositivo móvil comprende un procesador y/o una memoria. Preferentemente, el dispositivo móvil comprende una conexión a una red de comunicaciones móviles. La red de comunicaciones móviles puede diseñarse como una red de telecomunicaciones. Por ejemplo, el dispositivo móvil está diseñado preferentemente como un teléfono móvil. El teléfono móvil está configurado preferentemente como un teléfono inteligente. En particular, el dispositivo móvil puede comprender una pantalla. De manera especialmente preferente, el usuario puede introducir comandos a través de la pantalla.
- 40 En particular, el dispositivo móvil comprende un primer dispositivo de emisión y recepción para la red de telecomunicaciones. En particular, el dispositivo móvil comprende un segundo dispositivo de emisión y recepción para la comunicación de corto alcance.
- 45 En particular, el dispositivo de control de acceso comprende otra interfaz de comunicación, en particular una interfaz binaria. El dispositivo de control de acceso recibe de forma inalámbrica datos procesados por la interfaz de comunicación en el dispositivo de control de acceso. Preferentemente, se utiliza para este fin la misma unidad receptora del dispositivo de control de acceso. Por consiguiente pueden transmitirse datos a la interfaz de programación y a la interfaz de comunicación utilizando el mismo hardware.
- 50 Los datos para la interfaz de comunicación y para la interfaz de programación pueden transmitirse a la unidad receptora con la misma frecuencia.
- 55 Preferentemente está previsto que el dispositivo de control de acceso abra la interfaz de programación al menos parcialmente como resultado de la comunicación con el dispositivo móvil. El dispositivo de control de acceso puede abrir, al menos parcialmente, la interfaz de programación como resultado de una comunicación con el dispositivo móvil.
- 60 Por tanto, la interfaz de programación puede estar cerrada como estado inicial. Por consiguiente el dispositivo de control de acceso no puede procesar ningún dato a través de la interfaz de programación. Para que el dispositivo de control de acceso pueda procesar datos a través de la interfaz de programación, primero debe abrir la interfaz de programación. Esto significa que el dispositivo de control de acceso debe permitir primero la recepción de datos a través de la interfaz de programación.
- 65 Un procedimiento para abrir, al menos parcialmente, la interfaz de programación comienza, en particular, con la interfaz de programación cerrada. Si se cumplen los requisitos para la apertura al menos parcial de la interfaz de programación, el procedimiento para la apertura al menos parcial de la interfaz de programación puede terminar con la interfaz de

programación abierta o con la interfaz de programación cerrada de nuevo tras la apertura. Si no se cumple al menos uno de los requisitos para abrir la interfaz de programación, el procedimiento finaliza con la interfaz de programación cerrada.

- 5 La comunicación, que provoca una apertura al menos parcial de la interfaz de programación, tiene lugar en particular a través de la interfaz de comunicación.

10 Es posible que la comunicación, que provoca una apertura al menos parcial de la interfaz de programación se realice para conceder un acceso al área física. Por lo tanto, la comunicación, que provoca una apertura al menos parcial de la interfaz de programación, puede tener lugar dentro de un procedimiento de control de acceso. El procedimiento de control de acceso puede comprender la comunicación a raíz de la cual se abre, al menos parcialmente, la interfaz de programación.

15 El procedimiento de control de acceso tiene lugar, en particular, para conceder a un usuario el acceso al área física. El área física se bloquea al inicio del procedimiento de control de acceso. La comprobación de si se puede conceder el acceso es una parte esencial del procedimiento de control de acceso. El dispositivo móvil y el dispositivo de control de acceso pueden diseñarse para llevar a cabo el procedimiento de control de acceso.

20 El procedimiento de control de acceso se lleva a cabo al menos mediante el dispositivo de control de acceso y el dispositivo móvil, en particular cuando el dispositivo móvil se encuentra en las proximidades del dispositivo de control de acceso. El procedimiento de control de acceso finaliza, en particular, con la concesión del acceso o con la terminación de la concesión del acceso cuando la comprobación de si se puede conceder el acceso concluye positivamente. Si no se cumple una condición previa de acceso, el procedimiento de control de acceso puede finalizar antes, en cuyo caso se denegará el acceso.

25 El dispositivo móvil puede comprender una información de acceso. La información de acceso se utiliza para conceder acceso al área física vigilada por el dispositivo de control de acceso. La información de acceso puede diseñarse específicamente para el dispositivo de control de acceso. La información de acceso puede asignarse al dispositivo de control de acceso. El dispositivo móvil comprende preferentemente al menos una memoria en la que se almacena la información de acceso.

30 La información de acceso puede comprender al menos un atributo de acceso. Preferentemente se utiliza el al menos un atributo de acceso en el procedimiento de control de acceso.

35 La información de acceso puede comprender una parte cifrada. La parte móvil puede ser indescifrable por el dispositivo móvil. La parte cifrada puede comprender el atributo de acceso. La información de acceso, en particular la parte cifrada, es recibida por el dispositivo de control de acceso a través de la interfaz de comunicación.

40 La información de acceso puede comprender una parte legible que no esté cifrada o que pueda ser descifrada por el dispositivo móvil. La parte legible puede comprender información que puede mostrarse al usuario en el dispositivo móvil. En particular, la información que puede visualizarse puede mostrarse en una pantalla del dispositivo móvil.

La información de acceso puede diseñarse como un fichero.

45 Preferentemente, el dispositivo de control de acceso puede recibir el al menos un atributo de acceso a través de la unidad receptora. El dispositivo de control de acceso también puede recibir varios atributos de acceso de la información de acceso. Si a continuación se menciona el atributo de acceso, también puede tratarse de varios atributos de acceso. Preferentemente, el dispositivo de control de acceso puede recibir la parte cifrada a través de la unidad receptora.

50 El dispositivo de control de acceso puede utilizar el al menos un atributo de acceso transmitido en el procedimiento de control de acceso. La comunicación, que también provoca la apertura al menos parcial de la interfaz de programación, puede comprender la transmisión del atributo de acceso desde el dispositivo móvil al dispositivo de control de acceso o corresponder a la transmisión del atributo de acceso desde el dispositivo móvil al dispositivo de control de acceso.

55 Preferentemente está previsto que el dispositivo de control de acceso abra la interfaz de programación al menos parcialmente como consecuencia de un resultado positivo de una comprobación de al menos una regla. El dispositivo de control de acceso puede abrir al menos parcialmente la interfaz de programación como consecuencia de un resultado positivo de una comprobación de al menos una regla.

60 Por tanto, la regla puede definirse como un requisito previo para la apertura, al menos parcial, de la interfaz de programación. Una comprobación de la regla significa que se comprueba si se cumple o no el requisito previo definido en la regla.

La al menos una regla se comprueba preferentemente en el dispositivo de control de acceso.

65 Si el resultado de la comprobación de la regla es negativo, la interfaz de programación permanece cerrada. El resultado

- positivo de la comprobación de la regla es al menos un requisito previo para la apertura, al menos parcial, de la interfaz de programación. Si sólo se comprueba una regla para la apertura al menos parcial de la interfaz de programación o si la regla comprobada corresponde a la última regla que debe comprobarse, la interfaz de programación se abre al menos parcialmente si el resultado de la comprobación de la regla es positivo. Si aún debe comprobarse al menos otra regla para abrir al menos parcialmente la interfaz de programación, se comprueba al menos la al menos otra regla con el objetivo de abrir al menos parcialmente la interfaz de programación. Una apertura al menos parcial de la interfaz de programación sólo se realiza cuando se presenta un resultado positivo de todas las reglas que deben comprobarse para ello.
- 10 Preferentemente la comprobación de la regla al mismo tiempo forma parte del procedimiento de control de acceso. Por lo tanto, la regla puede utilizarse para conceder acceso al área física. Por lo tanto, la regla puede utilizarse para controlar el acceso. La regla puede definir un requisito de acceso. Por lo tanto, un perfil de autorización de acceso puede comprender al menos la regla. Una "comprobación de la regla" significa que se comprueba si se cumple o no el requisito de acceso definido en la regla.
- 15 Si el resultado de la comprobación de la regla es negativo, se denegará el acceso al área física. El resultado positivo de la comprobación de la regla es al menos un requisito previo para conceder el acceso. Si sólo se comprueba una regla para conceder el acceso o si la regla comprobada corresponde a la última regla que debe comprobarse para conceder el acceso, entonces si el resultado de la comprobación de la regla es positivo se concede el acceso. Si es necesario comprobar otra regla para conceder el acceso, se comprueba la otra regla con el fin de conceder el acceso si el resultado de la comprobación de la regla es positivo. El acceso sólo se concede si hay un resultado positivo de todas las reglas que deben comprobarse para ello.
- 20 Por consiguiente no solo mediante la comprobación de la al menos una regla se comprueba si la interfaz de programación puede abrirse. En su lugar, el sistema también comprueba si se cumple una condición para conceder el acceso. Por consiguiente se crea un efecto de sinergia al vincular el procedimiento de control de acceso con la prueba de si la interfaz de programación debe abrirse al menos parcialmente.
- 25 Por ejemplo, puede estar previsto que la al menos una regla que define una condición previa para abrir al menos parcialmente la interfaz de programación defina también un requisito previo para conceder el acceso.
- 30 En este sentido puede ser que también deba comprobarse al menos otra regla para abrir al menos parcialmente la interfaz de programación y/o que además deba comprobarse al menos otra regla para conceder el acceso. Por lo tanto, las reglas que deben comprobarse para la apertura, al menos parcial, de la interfaz de programación y las reglas que deben comprobarse para conceder el acceso se solapan en al menos una regla. Preferentemente, las reglas que deben comprobarse para la apertura al menos parcial de la interfaz de programación y las reglas que deben comprobarse para conceder el acceso se solapan en varias reglas. Es decir, puede ser que deban comprobarse varias reglas tanto para abrir, al menos parcialmente, la interfaz de programación como para conceder el acceso.
- 35 En particular, al menos una regla puede estar situada fuera de la zona de solapamiento. Puede ocurrir que se compruebe al menos una regla para conceder el acceso, pero no para abrir al menos parcialmente la interfaz de programación. Es posible que se compruebe al menos una regla para la apertura al menos parcial de la interfaz de programación, pero no para conceder el acceso.
- 40 Es concebible que el número de reglas que deben comprobarse, que son un requisito previo para abrir la interfaz de programación, y el número de reglas que deben comprobarse, que son un requisito previo para conceder el acceso, difieran entre sí.
- 45 Alternativamente, las reglas que deben comprobarse para abrir la interfaz de programación pueden corresponder a las reglas que deben comprobarse para conceder el acceso.
- 50 La comprobación de la al menos una regla para abrir la interfaz de programación y/o para conceder el acceso tiene lugar preferentemente en el dispositivo de control de acceso.
- 55 El atributo de acceso puede diseñarse como una regla, como datos para una regla, como una instrucción o como datos para una instrucción. La parte cifrada puede comprender una regla, como datos para una regla, como instrucción o como datos para una instrucción. En particular, los datos para una regla pueden estar previstos como un atributo de acceso en lugar de la regla completa. El dispositivo de control de acceso puede utilizar los datos para la regla para comprobar la regla asociada. Si los datos para la regla se transmiten como atributo de acceso, el resto de la regla puede almacenarse en el dispositivo de control de acceso. En este sentido la regla puede completarse utilizando los datos transmitidos por el dispositivo móvil para la regla. El dispositivo de control de acceso puede comprobar la regla asociada utilizando los datos transmitidos para la regla.
- 60 El atributo de acceso puede comprender al menos una instrucción o corresponder a una instrucción. La instrucción define con más detalle la forma en que se concede el acceso al área física. La instrucción no es un requisito previo para conceder el acceso al área física. La instrucción puede comprender cómo se indica visual y/o acústicamente la
- 65

concesión del acceso en el dispositivo de control de acceso. Alternativa o adicionalmente, la instrucción puede comprender cómo se termina la concesión de acceso, por ejemplo, después de un periodo de tiempo predeterminado tras el inicio de la concesión, en un punto predeterminado en el tiempo independiente del inicio de la concesión o después de que se hayan realizado un número especificado de concesiones. La instrucción también puede comprender si la información sobre la concesión de acceso se emite al dispositivo móvil.

En particular, los datos para la al menos una instrucción pueden estar previstos como un atributo de acceso en lugar de la instrucción completa. El dispositivo de control de acceso puede ejecutar la instrucción asociada utilizando los datos para la instrucción. Si los datos de la instrucción se transmiten como atributo de acceso, el resto de la instrucción puede almacenarse en el dispositivo de control de acceso. En este sentido la instrucción puede completarse utilizando los datos transmitidos por el dispositivo móvil para la instrucción.

Preferentemente, el dispositivo de control de acceso puede recibir el al menos un atributo de acceso a través de la unidad receptora. La unidad de control de acceso también puede recibir varios atributos de acceso de la información de acceso.

La regla que debe comprobarse en el dispositivo de control de acceso para abrir al menos parcialmente la interfaz de programación y/o conceder el acceso puede corresponder la regla siguiente o incluir la siguiente regla: Un valor de comparación debe compararse con un valor de comprobación (regla a.). El valor de comparación y/o el valor de comprobación pueden estar diseñados a modo de código, en particular un valor hash o una firma electrónica. La comparación identifica el dispositivo móvil como autorizado en principio. La comparación del valor de comparación con el valor de comprobación se utiliza en particular cuando es necesario garantizar que el dispositivo móvil está autorizado. Si la comparación del valor de comparación con el valor de comprobación arroja un resultado positivo, se cumple al menos una condición previa para abrir al menos parcialmente la interfaz de programación y/o conceder el acceso.

De forma especialmente preferente, el dispositivo móvil transmite primero el valor de comparación al dispositivo de control de acceso para que este pueda comprobar si la interfaz de programación debe abrirse al menos parcialmente y/o si debe concederse el acceso. Es decir, para la comparación se utiliza el valor de comparación transmitido en ese momento. El valor de comparación puede cifrarse. El valor de comparación puede cifrarse de forma que el dispositivo móvil no pueda descifrar el valor de comparación. En particular, la parte cifrada puede contener el valor de comparación.

En particular, el valor de comparación siempre se transmite desde el dispositivo móvil al dispositivo de control de acceso antes de comprobar si la interfaz de programación debe abrirse al menos parcialmente y/o si debe concederse el acceso. En particular, la transmisión del valor de comparación siempre forma parte del procedimiento de control de acceso actual y/o del procedimiento actual para la apertura de la interfaz de programación. Si el valor de comparación no se transmite en el procedimiento en curso, la interfaz de programación permanece cerrada preferentemente y/o el acceso permanece denegado. Es concebible que el valor de comparación no se almacene en el dispositivo de control de acceso después de la comparación.

Preferentemente, el valor de comprobación se transmite desde el dispositivo móvil al dispositivo de control de acceso. El dispositivo móvil contiene el valor de comprobación. El valor de comprobación se pone a disposición en particular del dispositivo móvil mediante el dispositivo de gestión de acceso. El valor de comprobación puede estar contenido en la parte legible. Alternativamente, el valor de comprobación puede, por ejemplo, haberse puesto a disposición del dispositivo móvil mediante el dispositivo de gestión de acceso del dispositivo móvil adicionalmente a la información de acceso.

El valor de comprobación puede estar cifrado.

Preferentemente, el valor de comprobación siempre se transmite desde el dispositivo móvil al dispositivo de control de acceso antes de comprobar si la interfaz de programación debe abrirse al menos parcialmente y/o si debe concederse el acceso. En particular, la transmisión del valor de comprobación siempre forma parte del procedimiento de control de acceso actual y/o del procedimiento actual para la apertura de la interfaz de programación. Si el valor de comprobación no se transmite en el procedimiento en curso, la interfaz de programación permanece cerrada preferentemente y/o el acceso permanece denegado.

Es concebible que el valor de comparación y el valor de comprobación se transmitan siempre en el procedimiento actual antes de que tenga lugar una comparación del valor de comparación con el valor de comprobación, de modo que el dispositivo de control de acceso utilice siempre el valor de comparación transmitido y el valor de comprobación transmitido. Por lo tanto, no es necesario almacenar el valor de comparación y/o el valor de comprobación en el dispositivo de control de acceso. Por el contrario, se deniega el acceso si el dispositivo móvil no transmite el valor de comparación y el valor de comprobación al dispositivo de control de acceso durante el procedimiento actual para la concesión de acceso y/o apertura de la interfaz de programación. De este modo se garantiza siempre el uso de un valor de comparación y de un valor de comprobación actuales, en particular sin tener que realizar grandes actualizaciones en el dispositivo de control de acceso.

5 La regla que debe comprobarse en el dispositivo de control de acceso para abrir al menos parcialmente la interfaz de programación y/o conceder el acceso puede corresponder la regla siguiente o incluir la siguiente regla: Debe comprobarse si una hora actual se encuentra dentro de un intervalo de tiempo especificado (regla b.). El intervalo de tiempo puede comprender horas, días de la semana, días laborables y no laborables, meses y/o años. El intervalo de tiempo puede transmitirse de forma cifrada desde el dispositivo móvil al dispositivo de control de acceso durante el procedimiento de control de acceso y/o el procedimiento de apertura de la interfaz de programación. En particular, la parte cifrada puede comprender el intervalo de tiempo. Si el intervalo de tiempo se transmite siempre en el procedimiento de control de acceso actual y/o en el procedimiento actual para la apertura de la interfaz de programación, no es necesario almacenar el intervalo de tiempo en el dispositivo de control de acceso. Si la hora actual se encuentra dentro del intervalo de tiempo especificado, se cumple al menos una condición previa para abrir, al menos parcialmente, la interfaz de programación y/o conceder el acceso.

15 La regla que debe comprobarse en el dispositivo de control de acceso para abrir al menos parcialmente la interfaz de programación y/o conceder el acceso puede corresponder la regla siguiente o incluir la siguiente regla: Debe realizarse una autenticación adicional, en particular mediante un código o un reconocimiento biométrico (regla c.). Preferentemente, el dispositivo de control de acceso lleva a cabo la autenticación adicional. Para ello, se compara un valor de control con un código o un identificador biométrico. El código y/o el reconocimiento biométrico pueden introducirse o registrarse en el dispositivo móvil y transmitirse al dispositivo de control de acceso. El código y/o reconocimiento biométrico se compara con el valor de control en el dispositivo de control de acceso. Si la comparación es positiva, se presenta una autenticación adicional. Si se presenta la autenticación adicional se cumple al menos un requisito previo para abrir, al menos parcialmente, la interfaz de programación y/o conceder el acceso.

25 El valor de control para la autenticación puede ser recibido por el dispositivo de control de acceso de forma cifrada desde el dispositivo móvil durante el procedimiento de control de acceso y/o durante el procedimiento de apertura de la interfaz de programación. El valor de control puede incluir un código de control y/o un identificador biométrico de control. En particular, la parte cifrada puede comprender el valor de control. Esto elimina la necesidad de almacenar el valor de control en el dispositivo de control de acceso.

30 La regla que debe comprobarse en el dispositivo de control de acceso para abrir al menos parcialmente la interfaz de programación y/o conceder el acceso puede corresponder la regla siguiente o incluir la siguiente regla: Debe comprobarse una identificación que hace distinguible al usuario como vigilante (regla d.). Puede ser deseable que un vigilante se identifique durante una ronda en el dispositivo de control de acceso para registrar la salida adecuada de la ronda. Puede ser deseable que no se conceda acceso al vigilante y/o que la interfaz de programación permanezca cerrada. Por lo tanto, en caso de una identificación positiva como vigilante se deniega el acceso y/o la interfaz de programación permanece cerrada.

40 La identificación positiva o negativa como vigilante puede transmitirse de forma cifrada desde el dispositivo móvil al dispositivo de control de acceso durante el procedimiento de control de acceso. En particular, la parte cifrada puede comprender la identificación positiva o negativa como vigilante. Si la identificación positiva o negativa como vigilante se transmite siempre en el procedimiento de control de acceso actual y/o en el procedimiento actual para la apertura de la interfaz de programación, no es necesario guardar la identificación.

45 La regla que debe comprobarse en el dispositivo de control de acceso para abrir al menos parcialmente la interfaz de programación y/o conceder el acceso puede corresponder la regla siguiente o incluir la siguiente regla: Debe presentarse un resultado positivo de una regla que debe comprobarse en el dispositivo móvil (regla e.). Puede ser conveniente que en el dispositivo móvil se compruebe al menos una regla para conceder el acceso al área física y/o para abrir al menos parcialmente la interfaz de programación. La regla que debe comprobarse en el dispositivo móvil puede, por ejemplo, acceder a este respecto a información que no está disponible para el dispositivo de control de acceso. Por ejemplo, el dispositivo móvil puede comprobar si se ha efectuado un pago o registrado un ingreso, si se ha aceptado una normativa de usuario para el área física o si se ha completado de forma positiva una instrucción de seguridad. También es concebible que se compruebe en el dispositivo móvil otra autenticación, en particular mediante la introducción de un código o un reconocimiento biométrico, en particular si el valor de control está almacenado en el dispositivo móvil.

55 El atributo de acceso puede comprender un valor característico que incluya la necesidad de tener en cuenta el resultado de la verificación de la regla en el dispositivo móvil a la hora de conceder acceso y/o abrir la interfaz de programación. Si una regla debe comprobarse en el dispositivo móvil, el dispositivo de control de acceso espera el resultado positivo de la regla que debe comprobarse en el dispositivo móvil dentro de un plazo. Si el dispositivo de control de acceso no recibe el resultado positivo de la regla que debe comprobarse en el dispositivo móvil dentro del plazo, se deniega el acceso y/o se cierra la interfaz de programación.

65 El valor de comparación, el intervalo de tiempo, el valor de control, la identificación como vigilante y/o el valor característico corresponden así a datos para una regla que puede comprender el atributo de acceso.

La comprobación de una regla del tipo a., c., d. y/o e. sólo puede estar prevista para una ventana de tiempo

especificada en el procedimiento de control de acceso y/o en el procedimiento de apertura de la interfaz de programación. Esto se cumple de manera especialmente preferida a las reglas del tipo c., d. y/o e.. Fuera de la ventana de tiempo, la regla asignada a una ventana de tiempo no se comprueba. Por ejemplo, solo los fines de semana debe realizarse una autenticación adicional mediante un código PIN. No es necesaria una autenticación adicional durante la semana laboral. En este caso, una regla del tipo c. tendría que comprobarse en la ventana de tiempo "fin de semana". Durante la semana laboral no se requiere ninguna otra autenticación como condición previa para conceder el acceso y/o abrir la interfaz de programación.

La información de acceso, en particular la parte cifrada, puede comprender la ventana de tiempo. En la información de acceso, la regla que sólo debe comprobarse en la ventana de tiempo puede comprender la ventana de tiempo correspondiente. El atributo de acceso puede comprender la regla que contiene la ventana de tiempo.

Para abrir la interfaz de programación se comprueba preferentemente al menos la regla a. En particular, la regla a. puede ser la regla que se comprueba tanto para la apertura al menos parcial de la interfaz de programación como para conceder el acceso. Es concebible que un resultado positivo de la comprobación de las reglas b., c. y/o d. no sea un requisito previo para la apertura, al menos parcial, de la interfaz de programación.

Es concebible que el dispositivo de control de acceso reciba datos del dispositivo móvil para la al menos una regla que debe comprobarse en el dispositivo de control de acceso y/o la al menos una regla que debe comprobarse en el dispositivo de control de acceso. De este modo, el dispositivo de control de acceso puede recibir del dispositivo móvil las reglas que debe comprobar el dispositivo de control de acceso para conceder el acceso al área física y/o abrir la interfaz de programación. Por ejemplo, el dispositivo de control de acceso puede recibir el valor de comparación y/o el valor de comprobación del dispositivo móvil. El valor de comparación puede corresponder a los datos de una regla y, por tanto, a un atributo de acceso.

Los datos para la al menos una regla y/o la regla se reciben preferentemente a través de la interfaz de comunicación.

Preferentemente, la regla recibida y/o los datos recibidos se utilizan directamente para una regla en el procedimiento de control de acceso en curso y/o para abrir la interfaz de programación.

De manera especialmente preferente, el dispositivo de control de acceso utiliza los datos recibidos para la al menos una regla y/o la al menos una regla recibida sólo para la concesión actual de acceso al área física y/o para la apertura actual de la interfaz de programación. Preferentemente no tiene lugar un almacenamiento de la regla transmitida o los datos transmitidos para una regla. Por ello una comunicación del dispositivo de control de acceso con el dispositivo móvil y/o las capacidades de memoria del dispositivo de control de acceso pueden mantenerse adecuadamente. Además, se logra siempre usar datos actuales.

Del mismo modo, al menos una instrucción o datos para al menos una instrucción pueden transferirse desde el dispositivo móvil al dispositivo de control de acceso. La al menos una instrucción o los datos para la al menos una instrucción se utilizan preferentemente en el procedimiento de control de acceso actual. De forma especialmente preferente, la instrucción o los datos de la al menos una instrucción sólo se utilizan para la concesión actual de acceso.

El dispositivo de control de acceso puede recibir al menos una versión actualizada de un firmware y/o un firmware adicional a través de la interfaz de programación. Sin embargo, esto sólo puede ser una posibilidad. En particular, también son concebibles formas de realización en las que la interfaz de programación no reciba o no reciba exclusivamente firmware a través de la interfaz de programación.

Adicional o alternativamente, el dispositivo de control de acceso puede recibir al menos una versión actualizada de un identificador de dispositivo de control de acceso a través de la interfaz de programación. El dispositivo de control de acceso está preparado para transmitir el identificador de dispositivo de control de acceso al dispositivo móvil y para recibir del dispositivo móvil la información de acceso o al menos un atributo de acceso para el dispositivo de control de acceso cuyo identificador de dispositivo de control de acceso ha recibido el dispositivo móvil. El dispositivo móvil puede seleccionar la información de acceso adecuada basándose en el identificador de dispositivo de control de acceso.

Adicional o alternativamente, el dispositivo de control de acceso puede recibir al menos una versión actualizada de al menos un atributo preestablecido, preferentemente de varios atributos preestablecidos, a través de la interfaz de programación. El atributo preestablecido puede almacenarse en el dispositivo de control de acceso. El atributo preestablecido puede reemplazar una regla, datos para una regla, una instrucción y/o datos para una instrucción del atributo de acceso. Preferentemente, el atributo de acceso transmitido por el dispositivo móvil anula el atributo preestablecido. El atributo de acceso transmitido por el dispositivo móvil y el atributo preestablecido pertenecen en este sentido a la misma regla o instrucción. En otras palabras, si hay un atributo de acceso transmitido por el dispositivo móvil en el procedimiento de control de acceso actual, el atributo de acceso transmitido por el dispositivo móvil se utiliza en el procedimiento de control de acceso actual, mientras que el atributo preestablecido no se tiene en cuenta en el procedimiento de control de acceso actual. Preferentemente, en el dispositivo de control de acceso se almacena un atributo preestablecido para varios atributos de acceso que pueden ser transmitidos por el dispositivo móvil.

Adicional o alternativamente, el dispositivo de control de acceso puede recibir al menos una versión actualizada de una versión actualizada de datos para poder realizar el descifrado a través de la interfaz de programación.

5 Adicional o alternativamente, el dispositivo de control de acceso puede recibir al menos una lista de bloqueo a través de la interfaz de programación, en la que se enumeran los dispositivos móviles a los que se debe denegar el acceso. En particular, la lista de bloqueo puede ser una versión actualizada.

10 Adicional o alternativamente, el dispositivo de control de acceso puede recibir al menos una versión actualizada de al menos una instrucción para controlar el dispositivo de control de acceso y/o un comando de control para controlar el dispositivo de control de acceso a través de la interfaz de programación.

15 El comando de control puede utilizarse, en particular, para activar una instrucción. Los comandos de control pueden activar instrucciones especiales. Las instrucciones pueden almacenarse en el dispositivo de control de acceso. Los comandos de control pueden, por ejemplo, estar previstos para el generador de sonido acústico y/o la fuente luminosa del dispositivo de control de acceso. El comando de control y/o la instrucción pueden referirse al tipo y modo de la indicación acústica y/o visual, por ejemplo, el volumen, la longitud o la duración o altura de tono, el color, el brillo y/o una frecuencia de parpadeo. Preferentemente, el dispositivo de control de acceso abre la interfaz de programación al menos parcialmente antes de que el dispositivo de control de acceso haya concedido el acceso al área física. Esto hace posible que la interfaz de programación esté disponible para recibir datos para el procedimiento de control de acceso en curso.

25 De este modo, la interfaz de programación puede abrirse con el fin de obtener datos para comprobar una regla, en particular otra regla, para conceder el acceso en el dispositivo de control de acceso. A este respecto un resultado positivo de la comprobación de la regla adicional puede ser un requisito previo para conceder el acceso. Por ejemplo, los datos biométricos de un usuario pueden transmitirse al dispositivo de control de acceso a través de la interfaz de programación. Los datos biométricos pueden recopilarse utilizando el dispositivo móvil.

30 La interfaz de programación puede abrirse para obtener los resultados de una comprobación de una regla para la concesión de acceso que se comprueba en el dispositivo móvil.

La interfaz de programación puede abrirse para recibir un comando de control.

35 El comando de control puede corresponder a un comando sobre cómo conceder el acceso. Por lo tanto, el comando de control puede corresponder a una instrucción o comprender datos para una instrucción. El comando de control puede utilizarse para activar una instrucción almacenada en el dispositivo de control de acceso.

40 El comando de control puede corresponder a un comando de apertura. La interfaz de programación puede abrirse para recibir un comando de apertura. Puede ser que el dispositivo móvil decida si se concede el acceso. Para ello, el dispositivo móvil comprueba en particular una regla de concesión de acceso. Si se concede el acceso, el dispositivo móvil puede enviar el comando de apertura al dispositivo de control de acceso. Si el dispositivo de control de acceso recibe el comando de apertura, el dispositivo de control de acceso concede el acceso sin más comprobación.

45 En particular, el dispositivo de control de acceso recibe la parte cifrada a través de la interfaz de comunicación. Como el operador del dispositivo móvil no puede descifrar la parte cifrada, el operador no tiene ninguna posibilidad de cambiar la parte cifrada.

50 A través de la interfaz de programación (API) puede realizarse una transferencia de datos entre programas de software o partes de programas de software en particular. En este sentido el dispositivo móvil y el dispositivo de control de acceso pueden comprender en cada caso un programa o una parte de programa de software. La interfaz de programación se utiliza para recibir los datos del programa o parte de programa de software del dispositivo móvil con el programa o la parte de programa de software del dispositivo de control de acceso.

55 En particular, el operador del dispositivo móvil puede realizar entradas en el dispositivo móvil para modificar el comando de control recibido del dispositivo de control de acceso a través del dispositivo de programación (API) antes de enviarlo. Por ejemplo, el dispositivo móvil comprende un software, en particular una aplicación, en la que el operador puede configurar una instrucción, es decir, el tipo y la forma de acceso, por ejemplo, la frecuencia de parpadeo de la fuente luminosa o la duración del acceso. El dispositivo móvil genera un comando de control correspondiente de acuerdo con la configuración de la aplicación. También es concebible que la instrucción, es decir, el tipo y la forma de acceso, por ejemplo, la frecuencia de parpadeo de la fuente luminosa o la duración del acceso, pueda controlarse mediante una secuencia de programa de un software del dispositivo móvil. El software puede recibir datos durante la secuencia del programa, a partir de los cuales el software genera o modifica un comando de control correspondiente.

65 El dispositivo de control de acceso recibe el comando de control a través de la interfaz de programación y utiliza el comando de control en el procedimiento de control de acceso en curso. Esto hace que la fuente luminosa del dispositivo de control de acceso, por ejemplo, se encienda con la frecuencia de parpadeo deseada por el operador o

especificada por la secuencia de programa del software del dispositivo móvil. La interfaz de programación (API) facilita especialmente la transmisión segura de órdenes de control complejas.

5 Es concebible que el comando de control anule las instrucciones o los datos de las instrucciones de la parte cifrada. Alternativamente, la parte cifrada puede no contener ninguna instrucción correspondiente o datos correspondientes para instrucciones. Es concebible que el comando de control anule los atributos preestablecidos.

10 Alternativamente, si la interfaz de programación se abre antes de que se conceda el acceso, la interfaz de programación sólo podrá abrirse cuando o después de que se conceda el acceso. Así se consigue un nivel de seguridad especial para permitir la transferencia de datos a través de la interfaz de programación. Esto se cumple en particular en datos especialmente relevantes para la seguridad, como una versión actualizada de un firmware y/o un firmware adicional, una versión actualizada de un identificador de dispositivo de control de acceso, una versión actualizada de al menos un atributo preestablecido, preferentemente varios atributos preestablecidos, una versión actualizada de una lista de bloqueo y/o una versión actualizada de datos para poder realizar el descifrado. En particular, puede ser necesario un comando especial para abrir la interfaz de programación para transferir los datos relevantes para la seguridad.

20 Si la interfaz de programación está abierta cuando se concede el acceso, se puede recibir a través de la interfaz de programación una instrucción o un comando de control sobre cómo conceder el acceso.

25 Puede estar previsto que el dispositivo de control de acceso pueda abrir distintas partes de la interfaz de programación. En otras palabras, el dispositivo de control de acceso sólo puede abrir parcialmente la interfaz de programación. Esto permite la recepción de algunos datos a través de la interfaz de programación, mientras que se impide la recepción de otros datos a través de la interfaz de programación. Esto significa que la interfaz de programación permanece parcialmente cerrada durante la apertura parcial. Por ejemplo, es posible recibir comandos o instrucciones de control a través de la interfaz de programación mientras se impide la recepción de una versión actualizada de un firmware, un firmware adicional, una versión actualizada de un identificador de dispositivo de control de acceso, una versión actualizada de al menos un atributo preestablecido, preferiblemente varios atributos preestablecidos, una lista de bloqueo y/o una versión actualizada de datos para realizar un descifrado.

30 En particular, el dispositivo móvil comprende al menos un comando o datos para al menos un comando. El dispositivo móvil transmite el comando o los datos del comando al dispositivo de control de acceso. El comando puede ser abrir parcialmente la interfaz de programación. El comando puede comprender los datos para los que debe abrirse la interfaz de programación. El comando puede comprender qué parte de la interfaz de programación debe abrirse. El comando puede ser, por ejemplo, abrir la interfaz de programación para al menos uno de los siguientes datos: una versión actualizada de un firmware, un firmware adicional, una versión actualizada de un identificador de dispositivo de control de acceso, una versión actualizada de al menos un atributo preestablecido, preferiblemente varios atributos preestablecidos, una lista de bloqueo, una versión actualizada de datos para realizar un descifrado, una instrucción y/o un comando de control, en particular un comando de apertura.

40 Los comandos o los datos de los comandos pueden transmitirse de forma cifrada desde el dispositivo móvil al dispositivo de control de acceso.

45 Por ejemplo, la información de acceso, en particular la parte cifrada, puede comprender el comando o los datos para el comando.

50 Es concebible que sólo unos pocos dispositivos de control de acceso permitan la transferencia de al menos uno de los datos relevantes para la seguridad antes mencionados. En particular, las diferentes informaciones de acceso pueden permitir la recepción de diferentes datos relevantes para la seguridad en cada caso.

Preferentemente está previsto que el dispositivo de control de acceso cierre la interfaz de programación tras una duración especificada. La duración especificada puede almacenarse en el dispositivo de control de acceso.

55 Puede estar previsto que el dispositivo de control de acceso envíe la salida de un procedimiento de control de acceso para conceder acceso al área física y/o de características del procedimiento de control de acceso, en particular de comandos de control recibidos a través de la interfaz de programación o instrucciones, al dispositivo móvil después de que el dispositivo de control de acceso haya recibido un comando de solicitud para enviar la salida del procedimiento de control de acceso y/o las características del procedimiento de control de acceso del dispositivo móvil, en donde en particular un usuario inicia voluntariamente el comando de solicitud. El flujo de datos puede controlarse conscientemente iniciando deliberadamente el envío de vuelta de información al dispositivo móvil. Si no se solicita la transmisión de la información, la comunicación del dispositivo de control de acceso con el dispositivo móvil puede mantenerse escasa.

65 El objetivo de la invención también se resuelve mediante un sistema de control de acceso de acuerdo con la invención. El sistema de control de acceso de acuerdo con la invención comprende el dispositivo de control de acceso de acuerdo con la invención, tal como se describe el dispositivo de control de acceso dentro de esta divulgación. El sistema de

control de acceso también comprende un dispositivo móvil que está diseñado para la comunicación inalámbrica con el dispositivo de control de acceso a través de la interfaz de programación. El dispositivo móvil puede diseñarse como se ha descrito. El dispositivo móvil y el dispositivo de control de acceso pueden interactuar entre sí como se ha descrito.

5 En particular, el dispositivo móvil puede comprender información de acceso, en donde la información de acceso comprende una parte cifrada que no puede ser descifrada por el dispositivo móvil. En particular, la parte cifrada puede comprender un atributo de acceso que debe transmitirse, en particular una regla que debe comprobarse o los datos de una regla que debe comprobarse. La regla puede utilizarse para conceder acceso y/o abrir la interfaz de programación.

10 Es concebible que el dispositivo móvil compruebe una regla para conceder acceso al área física y que el dispositivo de control de acceso reciba el resultado de la comprobación a través de la interfaz de programación. La regla comprobada por el dispositivo móvil es, en particular, una regla adicional, mientras que en el dispositivo de control de acceso se comprueba al menos otra regla para conceder el acceso.

15 El objetivo de la invención también se resuelve mediante un procedimiento para transmitir datos desde un dispositivo móvil a un dispositivo de control de acceso, en particular según una de las reivindicaciones 1 a 10. El procedimiento puede llevarse a cabo con el sistema de control de acceso de acuerdo con la invención, en particular con un sistema de control de acceso según una de las reivindicaciones 11 a 13.

20 El dispositivo de control de acceso para el procedimiento de acuerdo con la invención está configurado para asignarse a un área física a la que se puede conceder acceso mediante el dispositivo de control de acceso. El dispositivo de control de acceso comprende una interfaz de programación.

25 De acuerdo con la invención está previsto que el dispositivo de control de acceso utilice la interfaz de programación para recibir los datos de forma inalámbrica desde el dispositivo móvil.

30 El procedimiento de acuerdo con la invención puede comprender un procedimiento de control de acceso y/o formar parte de un procedimiento de control de acceso. El procedimiento de acuerdo con la invención puede comprender el procedimiento para abrir la interfaz de programación.

La invención se describe a continuación con mayor detalle mediante ejemplos de realización. Las características técnicas con la misma función están provistas de números de referencia idénticos en las figuras. Muestran:

35 la figura 1 un dispositivo de control de acceso de acuerdo con la invención y un sistema de control de acceso de acuerdo con la invención con un dispositivo de control de acceso de acuerdo con la invención y de acuerdo con un primer ejemplo de realización,

40 la figura 2 muestra el dispositivo de control de acceso y el sistema de control de acceso de la figura 1, en el que se muestra la transferencia de atributos de acceso,

la figura 3 una vista en despiece ordenado de una parte del dispositivo de control de acceso de acuerdo con la invención,

45 la figura 4 un procedimiento de acuerdo con la invención de acuerdo con un primer ejemplo de realización,

la figura 5 un procedimiento de acuerdo con la invención de acuerdo con un segundo ejemplo de realización y

50 la figura 6 un procedimiento de acuerdo con la invención de acuerdo con un tercer ejemplo de realización.

La figura 1 muestra un dispositivo de control de acceso 3 de acuerdo con la invención y un sistema de control de acceso 1 de acuerdo con la invención. El sistema de control de acceso 1 comprende un dispositivo móvil 2 y el dispositivo de control de acceso 3 de acuerdo con la invención. El dispositivo móvil 2 se muestra esquemáticamente. El dispositivo móvil 2 está diseñado como un teléfono inteligente. El dispositivo móvil 2 comprende una pantalla 18. El dispositivo de control de acceso 3 de acuerdo con la invención y el sistema de control de acceso 1 de acuerdo con la invención pueden realizar un procedimiento 100, 200, 300 de acuerdo con la invención. El dispositivo móvil 2 comprende al menos un procesador, no mostrado, para llevar a cabo el procedimiento 100, 200, 300 de acuerdo con la invención. El dispositivo móvil 2 puede utilizar en este sentido un procesador con el que también puede ejercerse otras funciones del dispositivo móvil 2. El dispositivo móvil comprende un primer dispositivo de emisión y recepción para comunicarse a través de una red de telecomunicaciones 4, por ejemplo, con una nube 5.

65 El dispositivo de control de acceso 3 sirve como vigilante instalado permanentemente para un área física bloqueada por un obstáculo, no mostrado. La figura 1 muestra un ejemplo del dispositivo de control de acceso 3 como herraje electromecánico 3. A modo meramente de ejemplo se describe un herraje 3 de este tipo en el documento EP2998484 A1. Alternativamente, el dispositivo de control de acceso 3 puede diseñarse como un cilindro de cierre electromecánico, un abrepuertas o una cerradura motorizada. El dispositivo de control de acceso 3 también puede

estar diseñado de varias piezas (no mostradas). El dispositivo de control de acceso 3 puede comprender, por ejemplo, un lector y una cerradura motorizada (no mostrada). El lector y la cerradura motorizada pueden comunicarse entre sí por cable o de forma inalámbrica.

5 El dispositivo de control de acceso 3 y el dispositivo móvil 2 se comunican entre sí a través de un enlace de comunicación de corto alcance 6, como Bluetooth, BLE, RFID o NFC. Preferentemente se emplea BLE. El enlace de comunicación de corto alcance 6 se muestra esquemáticamente como una flecha doble. Para el enlace de comunicación de corto alcance 6, el dispositivo móvil 2 presenta un segundo dispositivo de emisión y recepción, no
10 mostrado. Para el enlace de comunicación de corto alcance 6, el dispositivo de control de acceso 3 presenta una unidad emisora y receptora 20, que se muestra en la figura 3. La unidad emisora y receptora 20 está situada detrás de una cubierta 21 del dispositivo de control de acceso 3. La unidad emisora y receptora 20 comprende una antena 22 y un circuito de emisión y recepción. El circuito de emisión y recepción puede estar configurado en una placa de circuitos 23.

15 La placa de circuitos 23 incluye un procesador (no representado) y una memoria.

El dispositivo de control de acceso 3 comprende un dispositivo electromecánico 7 que se muestra de forma puramente esquemática en la figura 1 y de forma figurativa en la figura 3. El dispositivo electromecánico 7 está diseñado como un motor eléctrico, por ejemplo. El dispositivo electromecánico 7 está situado dentro del dispositivo de control de acceso 3 y, por lo tanto, sólo se indica mediante una línea discontinua en la figura 1. El dispositivo electromecánico 7
20 puede acoplar una manija 17 del dispositivo de control de acceso 3 con una cerradura no representada para permitir el acceso al área física (véase la figura 1). En el estado acoplado, un usuario puede cambiar la cerradura a un estado desbloqueado accionando la manija 17. En el estado desacoplado, la manija 17 está desacoplada de la cerradura. Por ejemplo, el dispositivo electromecánico 7 puede acoplar y desacoplar un elemento de acoplamiento 24 con un elemento de acoplamiento complementario 25 (véase la figura 3). Esto se describe, por ejemplo, en el documento EP2998484 A1. Alternativamente, el dispositivo electromecánico 7 puede cambiar automáticamente la cerradura a un estado desbloqueado en el que el dispositivo electromecánico 7 retrae un cerrojo y/o un pestillo. En otra alternativa, el dispositivo electromecánico 7 puede liberar un pestillo de un abrepuertas.

30 El dispositivo de control de acceso 3 comprende una guía de luz 16, como se muestra en las figuras 1 y 3. Una fuente luminosa 26 está dispuesta detrás de la guía de luz 16 dentro del dispositivo de control de acceso 3 (véase la figura 3). Mediante la fuente luminosa 26 y la guía de luz 16, el dispositivo de control de acceso 3 puede indicar una denegación de acceso y una concesión de acceso mediante diferentes señales visuales. Por ejemplo, una denegación de acceso puede mostrarse en rojo y una concesión de acceso en verde.

35 El dispositivo de control de acceso 3 comprende un generador de sonido, no representado, que puede utilizarse para indicar una denegación de acceso y/o una concesión de acceso mediante una señal acústica. En particular, sólo se señaliza acústicamente la concesión de acceso.

40 El dispositivo de control de acceso 3 incluye un temporizador, no representado, para medir el tiempo.

De acuerdo con la invención, el dispositivo de control de acceso 3 comprende una interfaz de programación 8, que se indica de forma puramente esquemática en la figura 1. La interfaz de programación se realiza como interfaz de software mediante el procesador y la memoria. Los datos para la interfaz de programación 8 se reciben a través de la unidad emisora y receptora 20. El procesador y la memoria también realizan otra interfaz de comunicación 28, que está
45 diseñada como una interfaz binaria. La interfaz de comunicación 28 se muestra de forma puramente esquemática en la figura 1. Los datos de la interfaz de comunicación 28 también se reciben a través de la unidad emisora y receptora 20. Los datos para la interfaz de programación 8 y para la interfaz de comunicación 28 se envían a este respecto desde el dispositivo móvil 2 al dispositivo de control de acceso 3 con la misma frecuencia de emisión.

50 De acuerdo con la invención, los datos para la interfaz de programación 8 se transfieren de forma inalámbrica desde el dispositivo móvil 2 al dispositivo de control de acceso 3. Esto aumenta la comodidad para el usuario.

La interfaz de programación 8 puede estar abierta al menos parcialmente de forma temporal, de modo que puedan recibirse datos a través de la interfaz de programación 8. La interfaz de programación 8 puede cerrarse temporalmente para que no puedan recibirse datos a través de la interfaz de programación. Preferentemente, la interfaz de programación 8 está siempre cerrada, a menos que se requiera que la interfaz de programación 8 esté al menos
55 parcialmente abierta.

60 La interfaz de programación 8 se abre al menos parcialmente cuando se ha comprobado al menos una regla en el dispositivo de control de acceso 3 y la comprobación se ha completado con un resultado positivo.

La comprobación de la regla no se realiza únicamente con el objetivo de abrir la interfaz de programación 8. Más bien, la regla se comprueba también para comprobar si se puede conceder el acceso al área física. Por lo tanto, la comprobación de la regla también forma parte de un procedimiento de control de acceso 100, 200, 300. Un procedimiento para abrir, al menos parcialmente, la interfaz de programación 8 forma parte del procedimiento de
65

control de acceso 100, 200, 300.

Al inicio del procedimiento de control de acceso 100, 200, 300, el dispositivo de control de acceso 3 deniega el acceso al área física. El procedimiento de control de acceso 100, 200, 300 se utiliza para comprobar si se puede conceder acceso al usuario del dispositivo móvil 2. El procedimiento de control de acceso 100, 200, 300 puede comenzar con una primera comunicación del dispositivo móvil 2 y el dispositivo de control de acceso 3 con el fin de conceder acceso al área física. El procedimiento de control de acceso 100, 200, 300 puede comprender la concesión del acceso si el resultado de la comprobación es positivo. Si el resultado de la comprobación es positivo, el procedimiento de control de acceso puede finalizar con la concesión del acceso o con el fin de la concesión del acceso. En este sentido la forma en que se concede el acceso también forma parte del procedimiento de control de acceso 100, 200, 300.

El dispositivo de control de acceso 3 puede comprobar una o varias reglas para comprobar si debe concederse el acceso y/o si debe abrirse la interfaz de programación 8. Preferentemente, la comprobación de al menos una regla se utiliza tanto para comprobar si debe concederse el acceso como para comprobar si debe abrirse la interfaz de programación 8.

La regla puede incluir que el acceso sólo se conceda tras un resultado positivo de la comparación de un valor de comparación con un valor de comprobación. El valor de comparación y/o el valor de comprobación pueden estar diseñados como un código, en particular un valor hash o una firma electrónica.

La regla puede incluir la comprobación de si la hora actual se encuentra dentro de un intervalo de tiempo especificado. El dispositivo de control de acceso 3 conoce la hora actual mediante el temporizador.

La regla puede requerir que el dispositivo de control de acceso deba efectuar una autenticación adicional. La introducción del PIN para la autenticación tiene lugar tras una solicitud en el dispositivo móvil 2 y se transmite al dispositivo de control de acceso 3, de modo que el dispositivo de control de acceso puede realizar una autenticación adicional comparando un valor de control con el PIN, del mismo modo que el PIN se introdujo en el dispositivo móvil 2 y se transmitió al dispositivo de control de acceso 3.

La regla puede incluir que el dispositivo móvil 2 compruebe una regla. Si el dispositivo móvil transmite el resultado al dispositivo de control de acceso en un plazo especificado, la regla se ha comprobado con un resultado positivo.

Preferentemente, es necesario al menos un resultado positivo de una comparación del valor de comparación con el valor de comprobación como requisito previo para abrir la interfaz de programación 8 y conceder el acceso.

El dispositivo de control de acceso 3 recibe del dispositivo móvil 2 la(s) regla(s) y/o los datos para la(s) regla(s) del procedimiento actual 100, 200, 300. Esto garantiza que siempre se utilicen datos actualizados.

El dispositivo móvil 2 tiene acceso a la nube 5 a través de la red de telecomunicaciones 4. La red de telecomunicaciones 4 se muestra esquemáticamente como una flecha doble. En la nube 5 hay información de acceso 10.

La información de acceso 10 comprende una parte cifrada 11 y una parte legible 12. Si la información de acceso 10 está destinada al dispositivo móvil 2, el dispositivo móvil 2 puede recuperar la información de acceso 10 de la nube 5. La opción de recuperación para el dispositivo móvil 2 se limita en este sentido a la información de acceso 10 proporcionada para el dispositivo móvil 2. La información de acceso 10 también es específica del dispositivo de control de acceso 3. Es decir, la información de acceso 10 contiene información prevista para conceder el acceso al área física vigilada por el dispositivo de control de acceso 3 específico. La información de acceso se asigna al dispositivo de control de acceso 3 mediante un identificador de dispositivo de control de acceso. La información de acceso incluye el identificador de dispositivo de control de acceso. Si puede concederse acceso al usuario a varias áreas físicas vigiladas por diferentes dispositivos de control de acceso 3 mediante el dispositivo móvil 2, el dispositivo móvil 2 contiene varias informaciones de acceso 10. En particular, puede estar prevista una información de acceso 10 y almacenarse en cada caso en el dispositivo móvil 2 para cada uno de los dispositivos de control de acceso 3. La figura 2 muestra una información de acceso 10 puramente esquemática para el dispositivo de control de acceso 3 ilustrado en el dispositivo móvil 2.

La información de acceso 10 se pone a disposición de la nube 5 mediante un dispositivo de gestión de acceso 9, que se muestra de forma puramente esquemática. El dispositivo de gestión de acceso 9 puede formar parte del sistema de control de acceso 1 de acuerdo con la invención. El dispositivo de gestión de acceso 9 o la nube 5 cifra la parte cifrada 11 de la información de acceso 10 de tal forma que el dispositivo móvil 2 no pueda descifrar la parte cifrada 11. La parte cifrada 11 está destinada a transferirse al menos parcialmente, desde el dispositivo móvil 2 al dispositivo de control de acceso 3. El dispositivo de control de acceso 3 puede descifrar la parte cifrada 11.

El dispositivo de gestión de acceso 9 puede comunicarse con la nube 5 a través de un enlace de comunicación 19.

La nube 5 puede formar parte del sistema de control de acceso 1. Alternativamente, la nube 5 no forma parte del

sistema de control de acceso 1 de acuerdo con la invención. Más bien, el dispositivo móvil 2 puede diseñarse de tal manera que la información de acceso 10 pueda ser recuperada por el dispositivo móvil 2 desde la nube 5. El dispositivo de gestión de acceso 9 puede diseñarse de tal manera que la información de acceso 10 pueda almacenarse en la nube 5 por el dispositivo de gestión de acceso 9.

5 En una alternativa no mostrada, el dispositivo de gestión de acceso 9 puede enviar la información de acceso al dispositivo móvil 2 a través de la red de telecomunicaciones 4 sin almacenarse en la nube 5.

10 En particular, el sistema de control de acceso 1 de acuerdo con la invención puede prescindir de una conexión del dispositivo de control de acceso 3 a la red de telecomunicaciones 4 y/o de una conexión por cable al dispositivo de gestión de acceso 9. Por lo tanto, el dispositivo de control de acceso 3 puede diseñarse como un dispositivo autónomo/fuera de línea.

15 La parte cifrada 11 es recibida por el dispositivo de control de acceso 3 mediante la unidad emisora y receptora 20 y a través de la interfaz de comunicación 28.

20 La parte cifrada 11 contiene atributos de acceso 13. Algunos atributos de acceso 13 se diseñan como regla o como datos para una regla 14. Los atributos de acceso 13 diseñados como regla o como datos para una regla 14 están marcados esquemáticamente con un asterisco en la figura 2.

25 Algunos atributos de acceso 13 se diseñan como una instrucción o como datos para una instrucción 15. El modo de acceso está determinado por al menos una instrucción. La instrucción puede comprender cómo se indica visual y/o acústicamente la concesión del acceso en el dispositivo de control de acceso 3. Alternativa o adicionalmente, la instrucción puede comprender cómo se termina la concesión de acceso, por ejemplo, después de un periodo de tiempo predeterminado tras el inicio de la concesión, en un punto predeterminado en el tiempo independiente del inicio de la concesión o después de que se hayan realizado un número de concesiones. La instrucción también puede comprender si la información sobre la concesión de acceso se almacena o se emite al dispositivo móvil 2. Los atributos de acceso diseñados como instrucción o como datos para una instrucción 15 se muestran esquemáticamente como un triángulo en la figura 2. Por razones de claridad, no se muestra ningún atributo de acceso 13 en la parte cifrada 11 que se almacena en la nube 5. Sin embargo, la parte cifrada 11, que se almacena en la nube 5, también contiene los atributos de acceso 13.

35 Los atributos de acceso 13 se utilizan en el actual procedimiento de control de acceso 100. Esto permite atributos de acceso siempre actualizados.

40 Adicionalmente o como alternativa a las instrucciones 15 contenidas en la parte cifrada 11 y recibidas a través de la interfaz de comunicación 28, el dispositivo de control de acceso 3 puede recibir instrucciones sobre cómo conceder el acceso a través de la unidad emisora y receptora 20 y a través de la interfaz de programación 8. También es posible que los comandos de control para activar una instrucción almacenada en el dispositivo de control de acceso 3 se reciban a través de la interfaz de programación 8.

45 Otros datos que pueden recibirse a través de la interfaz de programación 8 son: una versión actualizada de un firmware y/o un firmware adicional, una versión actualizada del identificador del dispositivo de control de acceso, una versión actualizada de al menos un atributo preestablecido, preferentemente varios atributos preestablecidos, una lista de bloqueo y/o una versión actualizada de datos para realizar un descifrado, en particular el descifrado de la parte cifrada 11.

50 También es posible que la interfaz de programación 8 reciba datos para el curso posterior del procedimiento de control de acceso 100, 200, 300 desde el dispositivo móvil 2. Por ejemplo, a través de la interfaz de programación 8 pueden recibirse datos para la autenticación posterior y/o el resultado positivo de la comprobación de una regla que debe comprobarse en el dispositivo móvil 2. Para ello, la interfaz de programación 8 se abre, al menos parcialmente, antes de permitir el acceso al área física.

55 También es concebible que la interfaz de programación 8 reciba un comando de apertura del dispositivo móvil 2. El dispositivo móvil 2 emite el comando de apertura después de que el dispositivo móvil 2 haya decidido conceder el acceso. El comando de apertura provoca el funcionamiento del dispositivo electromecánico 7 para conceder el acceso.

El dispositivo de control de acceso 3 sólo puede abrir parcialmente la interfaz de programación 8.

60 De este modo, el dispositivo de control de acceso 3 puede recibir un comando o los datos de un comando de apertura de la interfaz de programación 8 desde el dispositivo móvil 2. El comando es abrir la interfaz de programación sólo parcialmente. El comando comprende en este sentido los datos para los que debe abrirse la interfaz de programación. El comando o los datos para el comando se envían de forma cifrada desde el dispositivo móvil 2 al dispositivo de control de acceso 3.

65 Alternativamente, en el dispositivo de control de acceso 3 se almacena un algoritmo, según el cual se comprueba una

regla y para qué datos se debe abrir, al menos parcialmente, la interfaz de programación 8. En este caso, no es necesario ningún comando especial para abrir, al menos parcialmente, la interfaz de programación 8.

El dispositivo de control de acceso 3 vuelve a cerrar la interfaz de programación 8 tras una duración especificada.

5 El dispositivo de control de acceso 3 emite la salida del procedimiento de control de acceso para conceder acceso al área física y/o características del procedimiento de control de acceso al dispositivo móvil después de que el dispositivo de control de acceso 3 reciba un comando de solicitud para enviar la salida del procedimiento de control de acceso y/o características del procedimiento de control de acceso del dispositivo móvil 2.

10 Las figuras 4, 5 y 6 muestran varios procedimientos 100, 200, 300 de acuerdo con la invención. En este sentido, el procedimiento 100, 200, 300 de acuerdo con la invención sirve a la vez como procedimiento de transmisión de datos del dispositivo móvil 2 al dispositivo de control de acceso 3 de acuerdo con la invención y como procedimiento de control de acceso 100, 200, 300, de modo que se utilizan los mismos signos de referencia para el procedimiento común 100, 200, 300. El procedimiento de transmisión de datos desde el dispositivo móvil 2 al dispositivo de control de acceso 3 forma parte del procedimiento de control de acceso 100, 200, 300.

La interfaz de programación 8 se cierra al inicio de los procedimientos 100, 200, 300 en cada caso.

20 En una primera etapa de procedimiento 101 del procedimiento de acuerdo con la invención 100, el dispositivo de control de acceso 3 emite al dispositivo móvil 2 un identificador de dispositivo de control de acceso.

25 A continuación, el dispositivo móvil 2 comprueba en una segunda etapa de procedimiento 102 del procedimiento 100 si una información de acceso 10, que puede identificarse como perteneciente al dispositivo de control de acceso 3 mediante el identificador de dispositivo de control de acceso, está almacenada en el dispositivo móvil 2. Si se almacena dicha información de acceso 10, el dispositivo móvil 2 emite al dispositivo de control de acceso 3 la parte cifrada 11 de la información de acceso 10 que se ha identificado como perteneciente al dispositivo de control de acceso 3. Esto se muestra en particular en la figura 2. Si una información de acceso correspondiente 10 para el dispositivo de control de acceso 3 no está almacenada en el dispositivo móvil 2, el procedimiento 100 finaliza. Esto se ilustra con una flecha en la segunda etapa de procedimiento 102 de la figura 3.

30 En la etapa de procedimiento 101, puede estar previsto que el usuario deba efectuar una entrada en el dispositivo móvil 2, por ejemplo, pulsar un botón o iniciar una aplicación con la que el usuario exprese su voluntad de acceder. Si falta la entrada, el procedimiento 100 puede darse por finalizado. Esto se ilustra con una flecha en la primera etapa de procedimiento 101 de la figura 3.

35 Parte de la primera etapa de procedimiento 101 puede consistir, adicional o alternativamente, en que el dispositivo móvil 2 muestre al usuario en la pantalla 18 todos los dispositivos de control de acceso 3 con los que el dispositivo móvil 2 puede comunicarse, en particular cuyo identificador de dispositivo de control de acceso haya recibido el dispositivo móvil 2 y cuya información de acceso 10 esté almacenada en el dispositivo móvil 2. La visualización de los dispositivos de control de acceso 3 se respalda en la información contenida en la respectiva parte legible 12 de la información de acceso 10 relativa a los correspondientes dispositivos de control de acceso 3. Así, la parte legible 12 puede comprender una imagen o descripción de los posibles dispositivos de control de acceso 3, los posibles espacios físicos y/o las barreras vigiladas por los posibles dispositivos de control de acceso 3. Las imágenes y/o descripciones correspondientes pueden mostrarse en la pantalla 18 del dispositivo móvil 2. El usuario puede seleccionar uno de los dispositivos de control de acceso 3 basándose en la información mostrada. En la etapa de procedimiento 102 el dispositivo móvil 2 emite entonces la información de acceso asociada 10, en particular la parte cifrada 11, únicamente al dispositivo de control de acceso 3 seleccionado.

50 La parte cifrada 11 recibida en la etapa de procedimiento 102 es descifrada por el dispositivo de control de acceso 3 en una tercera etapa de procedimiento 103 del procedimiento 100. La parte cifrada 11 contiene un valor de comparación.

55 El dispositivo móvil 2 ha recibido un valor de comprobación del dispositivo de gestión de acceso 9, por ejemplo a través de la nube 5. El valor de comprobación puede estar contenido en la parte legible 12. Asimismo es concebible que el dispositivo móvil 2 reciba el valor de comprobación por separado de la información de acceso 10 del dispositivo de gestión de acceso 9. El valor de comprobación puede descargarse del dispositivo móvil 2 a través de la nube 5, por ejemplo.

60 En una cuarta etapa de procedimiento 104 del procedimiento 100, el dispositivo móvil 2 transmite el valor de comprobación al dispositivo de control de acceso 3.

65 En una quinta etapa de procedimiento 105 del procedimiento 100, el dispositivo de control de acceso 3 compara el valor de comparación con el valor de comprobación. De este modo, el dispositivo de control de acceso 3 comprueba una regla. Si la comparación es positiva, el dispositivo de control de acceso 3 reconoce el dispositivo móvil 2 como autorizado en principio y el procedimiento 100 continúa.

- 5 Si el valor de comparación y/o el valor de comprobación no se transmiten en el procedimiento actual 100 o si la comparación entre el valor de comparación y el valor de comprobación es negativa, se deniega el acceso y se cierra la interfaz de programación 8. El procedimiento 100 termina. Esto se muestra mediante flechas en las etapas de procedimiento 103, 104 y 105 de la figura 4.
- 10 Si la comparación entre el valor de comparación y/o el valor de comprobación es positiva, la interfaz de programación 8 se abre inmediatamente en una etapa de procedimiento 106. Esto permite al dispositivo de control de acceso 3 recibir más datos para el procedimiento de control de acceso 100 a través de la interfaz de programación 8.
- 15 Así, en una séptima etapa de procedimiento 107, el dispositivo de control de acceso 3 puede recibir un código PIN para una autenticación adicional del dispositivo móvil 2 por medio de la interfaz de programación 8 y realizar la autenticación adicional. Si no se recibe el código PIN, el procedimiento 100 finaliza sin conceder el acceso. Esto se muestra con una flecha en las etapas de procedimiento 107 de la figura 4.
- 20 En una octava etapa de procedimiento 108, el dispositivo de control de acceso 3 puede recibir un resultado positivo de una regla que debe comprobarse en el dispositivo móvil 2 dentro de un plazo predeterminado a través de la interfaz de programación 8.
- 25 Como regla que debe comprobarse, el dispositivo móvil 2 puede pedir al usuario que acepte una normativa de uso como "esta es una habitación para no fumadores" introduciéndola en el dispositivo móvil 2. Adicional o alternativamente, el dispositivo móvil 2 puede comprobar la finalización con éxito de una instrucción de seguridad. Para ello, el dispositivo móvil 2 puede realizar y analizar una prueba. Adicional o alternativamente, el dispositivo móvil 2 sólo puede conceder acceso si previamente se concedió otro acceso. En este sentido puede ser que el usuario tenga que pasar primero por otra área física, por ejemplo, una esclusa o una sala blanca, antes de que se le conceda el acceso deseado en ese momento. El dispositivo móvil 2 comprueba así un historial de localización del dispositivo móvil 2. El dispositivo móvil 2 también puede comprobar si se ha efectuado previamente un pago para utilizar el área física. Asimismo, al menos una de las reglas b, c. o d. puede comprobarse en el dispositivo móvil 2 para conceder el acceso.
- 30 Si transcurre el plazo especificado sin que se reciba un resultado positivo de la regla que debe comprobarse en el dispositivo móvil 2, el procedimiento 100 finaliza. Si el dispositivo de control de acceso 8 recibe el resultado positivo dentro del plazo, el procedimiento 100 continúa. Esto se muestra con una flecha en las etapas de procedimiento 108 en la figura 4.
- 35 En una novena etapa de procedimiento 109, el dispositivo de control de acceso 3 determina que todas las reglas que deben comprobarse para conceder el acceso se han comprobado con un resultado positivo y espera una duración especificada para ver si se ha recibido un comando de control o una instrucción a través de la interfaz de programación 8. En este caso, el dispositivo de control de acceso 3 concede el acceso de acuerdo con el comando de control o una instrucción recibida a través de la interfaz de programación 8. Si no se recibe ningún comando de control o instrucción dentro de la duración especificada, el dispositivo de control de acceso 3 concede el acceso de acuerdo con las instrucciones 15 de la parte cifrada 11 y/o de acuerdo con los atributos preestablecidos almacenados en el dispositivo de control de acceso 3 configurados como instrucciones. Para permitir el acceso, el dispositivo electromecánico 7 se activa para el acoplamiento.
- 40
- 45 En una décima etapa de procedimiento 110, el dispositivo de control de acceso 3 cierra la interfaz de programación 8. En una undécima etapa del procedimiento 111, el dispositivo de control de acceso 3 finaliza el procedimiento 100. En este sentido el acceso se deniega de nuevo.
- 50 Para ello, el controlador del dispositivo de control de acceso 3 controla el dispositivo electromecánico 7 para el desacoplamiento.
- Son posibles procedimientos alternativos en los que falten una o dos de las etapas de procedimiento 107, 108 y/o 109.
- 55 La parte cifrada 11 no se almacena en el dispositivo de control de acceso 3 una vez finalizado el procedimiento 100. Esto garantiza que siempre se utilice una parte cifrada actual 11 transferida por el dispositivo móvil 2 durante el procedimiento 100. Si no se transfiere la parte cifrada 11, el procedimiento 100 finaliza.
- 60 La figura 5 muestra otro procedimiento 200 de acuerdo con la invención. El procedimiento 200 puede llevarse a cabo mediante el sistema de control de acceso 1 de acuerdo con la invención y el dispositivo de control de acceso 3 de acuerdo con la invención de las figuras 1, 2 y 3. La primera, segunda y tercera etapa de procedimiento 101, 102 y 103 del procedimiento 100 de la figura 4 corresponden a la primera, segunda y tercera etapa de procedimiento 201, 202 y 203 del procedimiento 200 de la figura 5.
- 65 En una cuarta etapa de procedimiento 204 se comprueban las reglas, en particular las reglas a., b., c. y/o d. en el dispositivo 3 de control de acceso. Si una de las comprobaciones termina con un resultado negativo, el procedimiento 200 finaliza. Esto se ilustra con una flecha en la etapa de procedimiento 204 de la figura 5.

Si todas las reglas que debe comprobarse se comprueban con un resultado positivo, el procedimiento continúa y el dispositivo de control de acceso 3 permite el acceso al área física en una quinta etapa de procedimiento 205 al controlarse el dispositivo electromecánico 7. Además, en la quinta etapa de procedimiento 205, se lleva a cabo una instrucción 15, con la que se indica visualmente la concesión del acceso. Para ello, se controla la fuente luminosa 26 situada detrás de la guía de luz 16. La instrucción 15 está contenida en la parte cifrada 11.

En una sexta etapa de procedimiento 206, la interfaz de programación 8 se abre parcialmente. La interfaz de programación 8 sólo se abre para recibir una versión actualizada de los atributos preestablecidos. De lo contrario, la interfaz de programación 8 permanece cerrada. El dispositivo de control de acceso 3 espera una duración especificada a que los atributos preestablecidos se transmitan de forma cifrada desde el dispositivo móvil 2. Si los atributos preestablecidos se transmiten dentro de la duración especificada, el dispositivo de control de acceso 3 almacena los atributos preestablecidos para su uso en procedimientos futuros. Si los atributos preestablecidos no se transmiten dentro de la duración especificada, la interfaz de programación 8 no recibirá los atributos preestablecidos. El dispositivo de control de acceso 3 cierra la interfaz de programación 8 tras la duración especificada.

En una séptima etapa de procedimiento 207, se termina el acceso al área física. Para ello, la parte cifrada 11 comprende un periodo de tiempo predeterminado. El periodo de tiempo indica cuándo debe denegarse de nuevo el acceso después del comienzo de la concesión del acceso. El periodo de tiempo se transmitió al dispositivo de control de acceso 3 en la parte cifrada 11. Mediante el temporizador, el dispositivo de control de acceso 3 determina el periodo de tiempo que ha transcurrido desde que se concedió el acceso en la etapa 205. Si el periodo de tiempo determinado corresponde al periodo de tiempo predeterminado, el controlador del dispositivo de control de acceso 3 activa el dispositivo electromecánico 7. A continuación, el dispositivo electromecánico 7 deniega el acceso. Por ejemplo, el dispositivo electromecánico 7 desacopla la manija 17 de una cerradura de modo que un par de la manija 17 ya no puede transferirse a la cerradura. Después de eso, el procedimiento termina 200.

La figura 6 muestra otro procedimiento 300 de acuerdo con la invención. El procedimiento 300 puede llevarse a cabo mediante el sistema de control de acceso 1 de acuerdo con la invención y el dispositivo de control de acceso 3 de acuerdo con la invención de las figuras 1, 2 y 3. La primera, segunda, tercera, cuarta, quinta y séptima etapas de procedimiento 201, 202, 203, 204, 205, 207 del procedimiento 200 de la figura 5 corresponden a la primera, segunda, tercera, cuarta, quinta y séptima etapas 301, 302, 303, 304, 305, 307 del procedimiento 300 de la figura 6.

Si se concede el acceso, el dispositivo de control de acceso 3 comprueba en una etapa 306 si hay un comando para abrir parcialmente la interfaz de programación para recibir una versión actualizada de un firmware, el identificador de dispositivo de control de acceso y/o datos para realizar un descifrado. En una forma de realización del procedimiento 300, la parte cifrada 11 comprende el comando correspondiente. En una forma de realización alternativa, el dispositivo móvil 2 transmite el comando que no está contenido en la parte cifrada 11. Si se ha concedido el acceso y se presenta el comando correspondiente, el dispositivo de control de acceso 3 abre la interfaz de programación 8. El dispositivo de control de acceso 3 espera una duración especificada a que se transmita la versión actualizada que debe transmitirse de un firmware, del identificador de dispositivo de control de acceso y/o de los datos para realizar un descifrado en forma cifrada desde el dispositivo móvil 2. Si la versión actualizada que debe transmitirse de un firmware, del identificador de dispositivo de control de acceso y/o de los datos para realizar un descifrado se transmiten dentro de la duración especificada, el dispositivo de control de acceso 3 almacena la versión actualizada que debe transmitirse de un firmware, del identificador del dispositivo de control de acceso y/o de los datos para realizar un descifrado para su uso en procedimientos futuros. Si la versión actualizada que debe transmitirse del firmware, del identificador de dispositivo de control de acceso y/o de los datos para realizar un descifrado no se transmiten dentro de la duración especificada, la interfaz de programación 8 no recibe la versión actualizada que debe transmitirse. El dispositivo de control de acceso 3 cierra la interfaz de programación 8 tras la duración especificada.

En una alternativa a la etapa 306, no es suficiente que el dispositivo móvil 2 envíe el comando al dispositivo de control de acceso 3. En cambio, aunque ya se haya concedido el acceso, hay que comprobar otra regla para abrir la interfaz de programación 8. La interfaz de programación 8 sólo puede abrirse si el resultado de la comprobación de la otra regla es positivo. La otra regla puede comprobarse en el dispositivo móvil 2 o en el dispositivo de control de acceso 3.

REIVINDICACIONES

1. Dispositivo de control de acceso (3) para un sistema de control de acceso (1),

5 en donde el dispositivo de control de acceso (3) está diseñado para asignarse a un área física a la que se puede conceder acceso mediante el dispositivo de control de acceso (3),

caracterizado

10 **por que** el dispositivo de control de acceso (3) comprende una interfaz de programación (8), en donde la interfaz de programación (8) se utiliza para comunicarse de forma inalámbrica con un dispositivo móvil (2) y el dispositivo de control de acceso (3) a través de la interfaz de programación (8) recibe al menos uno, preferiblemente varios, de los siguientes datos:

- i. una versión actualizada de un firmware y/o un firmware adicional
- 15 ii. una versión actualizada de un identificador de dispositivo de control de acceso,
- iii. una versión actualizada de al menos un atributo preestablecido, preferentemente varios atributos preestablecidos,
- iv. una versión actualizada de datos para poder realizar un descifrado,
- v. al menos un comando de control para controlar el dispositivo de control de acceso (3),

20 en donde el dispositivo de control de acceso (3) abre al menos parcialmente, la interfaz de programación (8) como resultado de la comunicación con el dispositivo móvil (2).

2. Dispositivo de control de acceso (3) según la reivindicación 1, **caracterizado por que** la comunicación se realiza para conceder un acceso al área física.

25 3. Dispositivo de control de acceso (3) según la reivindicación 1 o 2, **caracterizado por que** el dispositivo de control de acceso (3) abre al menos parcialmente la interfaz de programación (8) como consecuencia de un resultado positivo de una comprobación de al menos una regla que tiene lugar en el dispositivo de control de acceso (3), en donde en particular tiene lugar la comprobación de la regla para conceder el acceso al área física.

30 4. Dispositivo de control de acceso (3) según la reivindicación 3, **caracterizado por que** la regla que debe comprobarse en el dispositivo de control de acceso (3) para abrir al menos parcialmente la interfaz de programación (8) y/o para conceder el acceso corresponde a, o comprende una de las siguientes reglas:

- a. debe comprobarse un valor de comparación con un valor de comprobación,
- b. debe comprobarse si una hora actual se encuentra dentro de un intervalo de tiempo especificado,
- 40 c. debe efectuarse una autenticación adicional, en particular mediante un código o un reconocimiento biométrico,
- d. debe comprobarse una identificación que hace distinguible al usuario como vigilante,
- e. debe presentarse un resultado positivo de una regla que debe comprobarse en el dispositivo móvil,

45 en donde, en particular, las reglas b., c., d. y/o e. sólo se cumplen en una ventana de tiempo especificada.

5. Dispositivo de control de acceso (3) según la reivindicación 3 o 4, **caracterizado por que** el dispositivo de control de acceso (3) recibe datos para la al menos una regla y/o la al menos una regla desde el dispositivo móvil (2), en particular por que el dispositivo de control de acceso (3) utiliza los datos recibidos para la al menos una regla y/o la al menos una regla recibida únicamente para la concesión actual del acceso al área física y/o para la apertura actual de la interfaz de programación.

6. Dispositivo de control de acceso (3) según una de las reivindicaciones anteriores, **caracterizado por que** el dispositivo de control de acceso (3) abre al menos parcialmente la interfaz de programación (8) antes de que el dispositivo de control de acceso (3) haya concedido acceso al área física.

55 7. Dispositivo de control de acceso (3) según una de las reivindicaciones anteriores, **caracterizado por que** diferentes partes de la interfaz de programación (8) pueden abrirse mediante el dispositivo de control de acceso (3), en particular por que la parte de la interfaz de programación (8) que se abre depende de un comando o de datos para un comando recibidos del dispositivo móvil (2), comprendiendo el comando para qué parte de la interfaz de programación (8) debe abrirse.

60 8. Dispositivo de control de acceso (3) según una de las reivindicaciones anteriores, **caracterizado por que** el dispositivo de control de acceso (3) cierra la interfaz de programación (8) tras una duración especificada.

65 9. Dispositivo de control de acceso (3) según una de las reivindicaciones precedentes, **caracterizado por que** el dispositivo de control de acceso (3) emite al dispositivo móvil (2) la salida de un procedimiento de control de acceso

para conceder el acceso al área física y/o de características del procedimiento de control de acceso, en particular de comandos de control recibidos a través de la interfaz de programación, después de que el dispositivo de control de acceso haya recibido un comando de solicitud para enviar la salida del procedimiento de control de acceso y/o las características del procedimiento de control de acceso del dispositivo móvil, en donde en particular un usuario inicia voluntariamente el comando de solicitud.

5
10. Sistema de control de acceso (1)
con un dispositivo de control de acceso (3) según una de las reivindicaciones anteriores 1 a 9 y con un dispositivo móvil (2) que está diseñado para la comunicación inalámbrica con el dispositivo de control de acceso (3) a través de la interfaz de programación (8).

11. Sistema de control de acceso (1) según la reivindicación 10, **caracterizado por que**
el dispositivo móvil (2) comprende información de acceso (10), en donde la información de acceso (10) comprende una parte cifrada (11) que no puede ser descifrada por el dispositivo móvil (2), en donde en particular la parte cifrada (11) comprende un atributo de acceso (13, 14, 15) que debe transmitirse, en particular una regla (14) que debe comprobarse o datos para una regla (14) que debe comprobarse.

12. Sistema de control de acceso (1) según la reivindicación 10 u 11, **caracterizado por que** el dispositivo móvil (2) comprueba una regla para conceder el acceso al área física, y el dispositivo de control de acceso (3) recibe el resultado de la comprobación a través de la interfaz de programación (8).

13. Procedimiento (100, 200, 300) para transmitir datos desde un dispositivo móvil (2) a un dispositivo de control de acceso (3), en particular según una cualquiera de las reivindicaciones 1 a 9,

25 en donde el dispositivo de control de acceso (3) está diseñado para asignarse a un área física a la que se puede conceder acceso mediante el dispositivo de control de acceso (3), en donde el dispositivo de control de acceso (3) comprende una interfaz de programación (8),

caracterizado porque
el dispositivo de control de acceso (3) utiliza la interfaz de programación (8) para recibir datos de forma inalámbrica desde el dispositivo móvil (2), y el dispositivo de control de acceso (3) a través de la interfaz de programación (8) recibe al menos uno, preferentemente varios, de los siguientes datos:

- 30
- i. una versión actualizada de un firmware y/o un firmware adicional
 - 35 ii. una versión actualizada de un identificador de dispositivo de control de acceso,
 - iii. una versión actualizada de al menos un atributo preestablecido, preferentemente varios atributos preestablecidos,
 - iv. una versión actualizada de datos para poder realizar un descifrado,
 - v. al menos un comando de control para controlar el dispositivo de control de acceso (3), en donde el dispositivo de control de acceso (3) abre al menos parcialmente la interfaz de programación (8) como resultado de una
 - 40 comunicación con el dispositivo móvil (2).

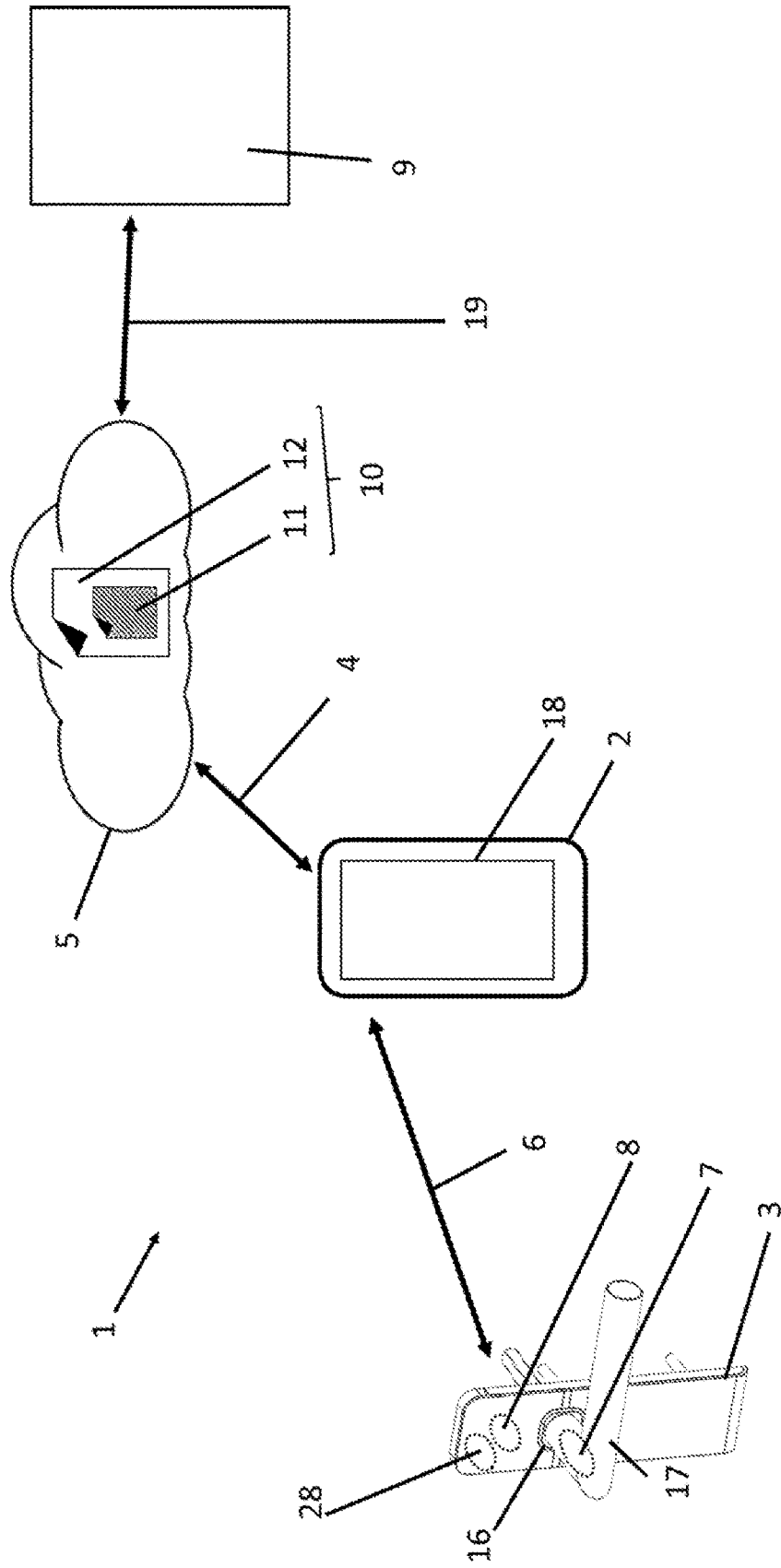


Fig. 1

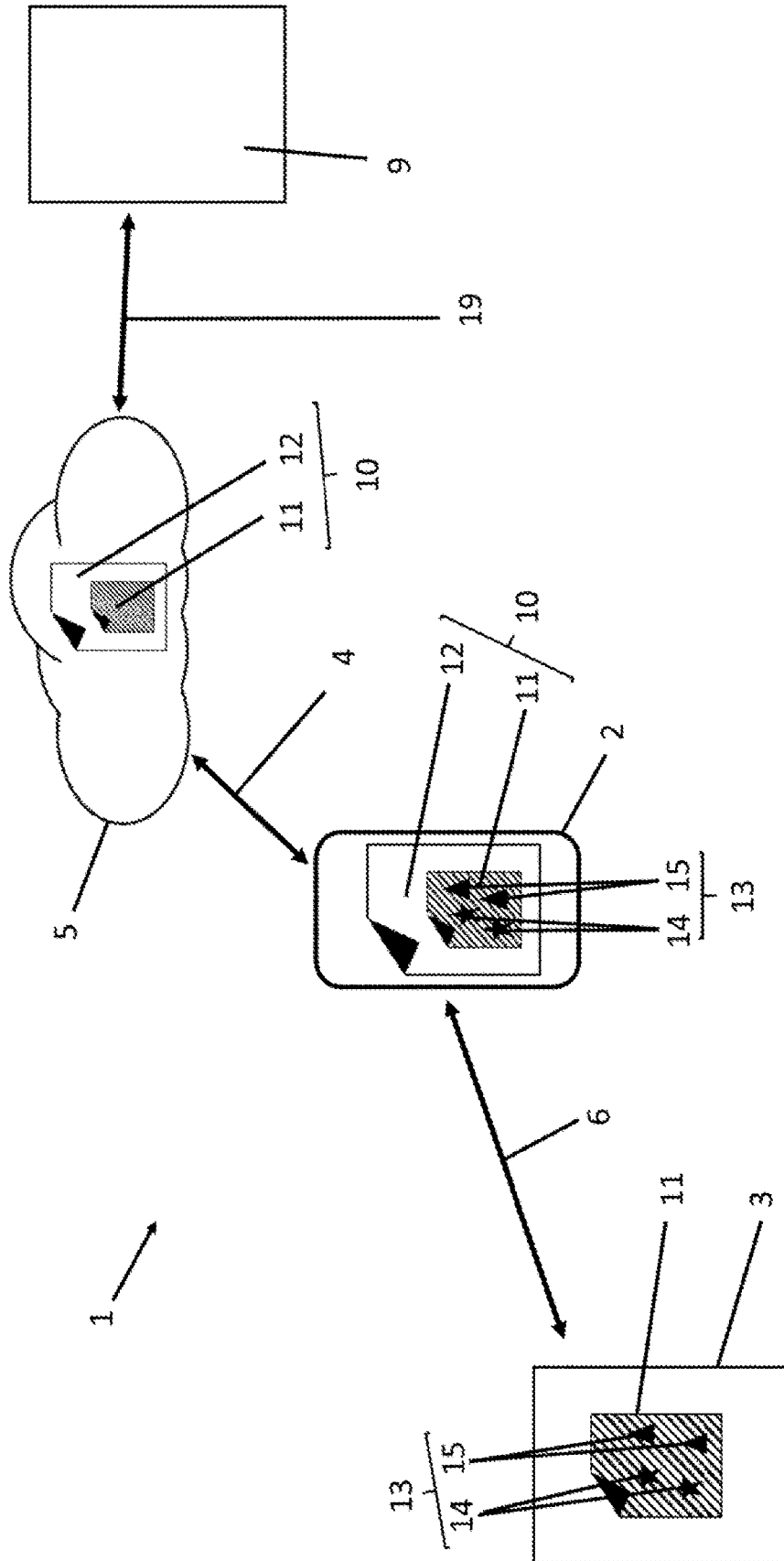


Fig. 2

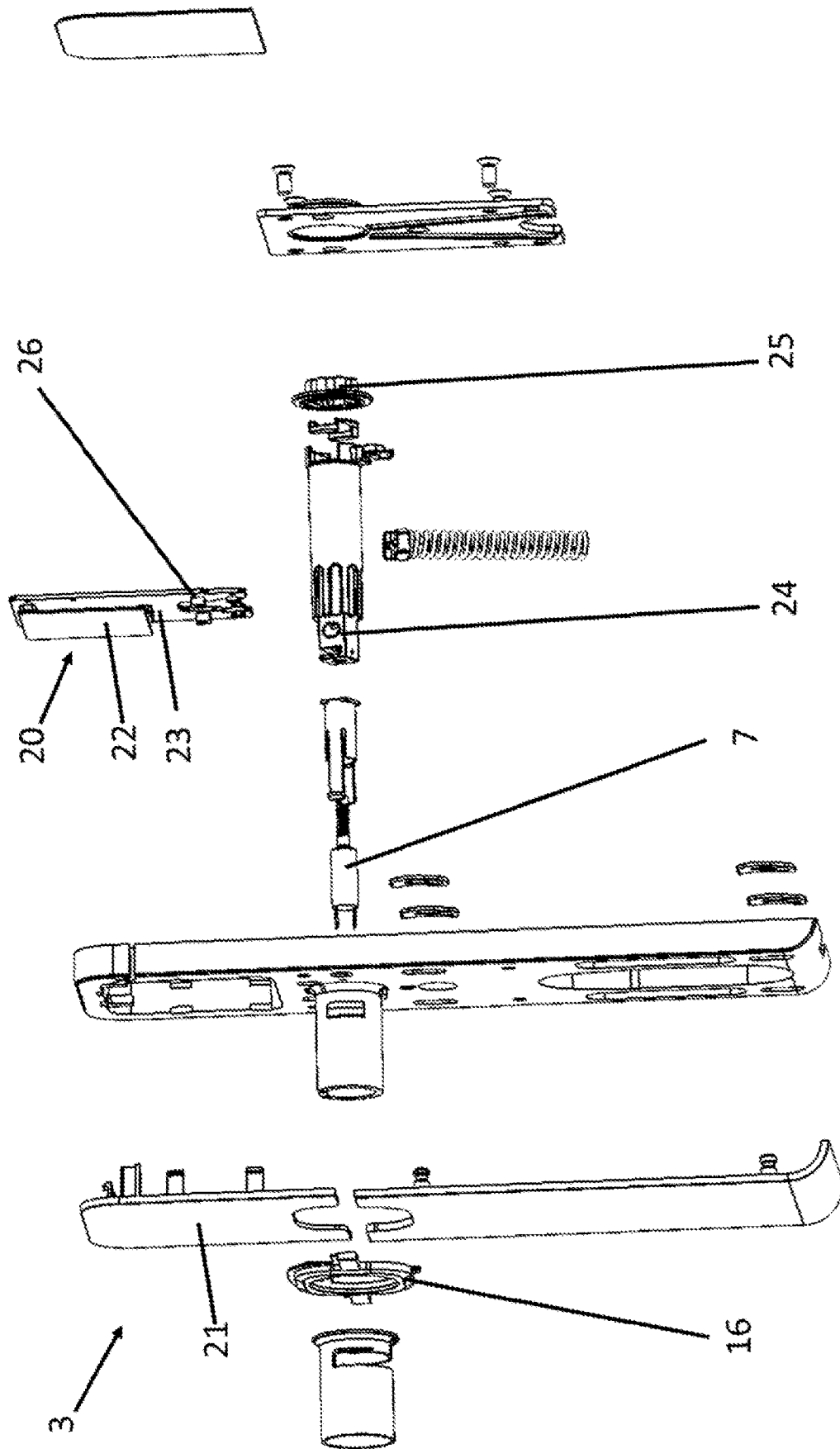


Figura 3

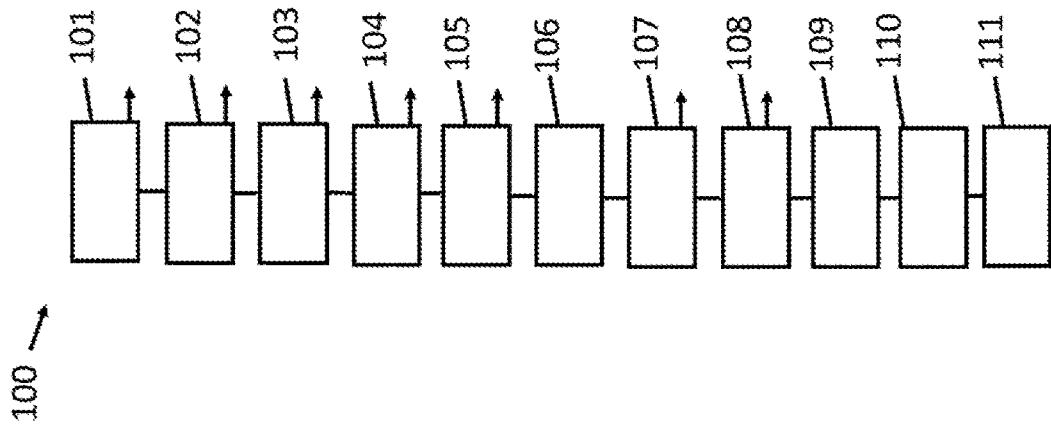


Fig. 4

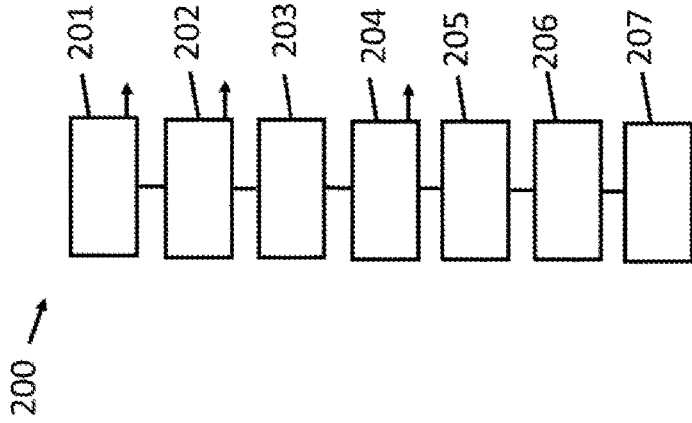


Fig. 5

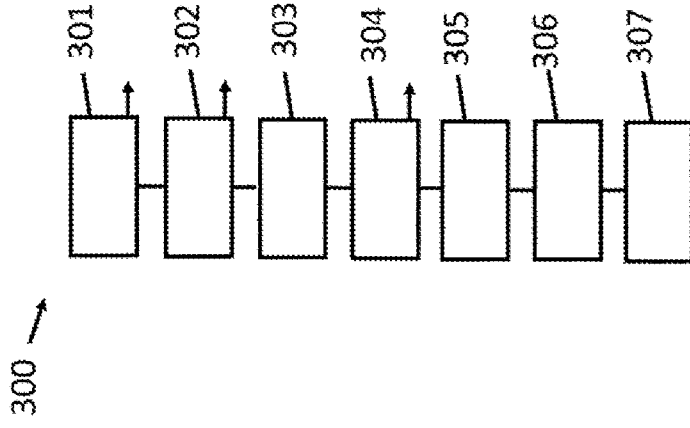


Fig. 6