(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 847 253**

(51) Int. CI.:

H04W 12/00 (2009.01)
H04L 9/32 (2006.01)
H04W 12/08 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **10.10.2017 PCT/EP2017/075859**

(87) Fecha y número de publicación internacional: **03.05.2018 WO18077610**

(96) Fecha de presentación y número de la solicitud europea: **10.10.2017 E 17784262 (2)**

(97) Fecha y número de publicación de la concesión europea: **02.12.2020 EP 3530023**

(54) Título: **Dispositivo de apertura y/o cierre de cerramiento de edificio o recinto, así como método para el funcionamiento de un cerramiento de edificio o recinto**

(30) Prioridad:

24.10.2016 DE 102016120262
08.11.2016 DE 102016121376

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
02.08.2021

(73) Titular/es:

HÖRMANN KG ANTRIEBSTECHNIK (100.0%)
Michaelisstr. 1
33803 Steinhagen, DE

(72) Inventor/es:

JACOB, FLORIAN y
SCHMALENSTRÖER, JÖRG

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Dispositivo de apertura y/o cierre de cerramiento de edificio o recinto, así como método para el funcionamiento de un cerramiento de edificio o recinto

La invención se refiere a un dispositivo de apertura y/o cierre de cerramiento de edificio o recinto con un aparato de apertura y/o cierre de cerramiento de edificio o recinto, que comprende un actuador, que se puede accionar mediante una señal de accionamiento, para permitir o bloquear un acceso a través de un cerramiento de edificio o recinto, un aparato de comunicación de cerramiento de edificio o recinto para la recepción y/o envío de mensajes cifrados y/o firmados y un aparato de autentificación de cerramiento de edifico o recinto individual por aparato de apertura y/o cierre de cerramiento de edificio o recinto, que debido a la recepción de un código de autentificación válido generado a partir de una o varias claves de código inicia la señal de accionamiento, y al menos un primer terminal de usuario móvil individual, que comprende un dispositivo de comunicación de terminal de usuario para el envío y/o recepción de mensajes cifrados y/o firmados y una memoria para el almacenamiento al menos de una clave de usuario individual, así como un dispositivo de cifrado para el cifrado y/o firma de mensajes por medio de la al menos una clave de usuario individual. Además, la invención se refiere a un método para el funcionamiento de un aparato de apertura y/o cierre de cerramiento de edificio o recinto, que comprende un actuador, que se puede accionar mediante una señal de accionamiento, para abrir y/o cerrar y/o desenclavar y/o enclavar un cerramiento de edificio o recinto, un aparato de comunicación de cerramiento de edificio o recinto para la recepción y/o envío de mensajes cifrados y/o firmados y un aparato de autentificación individual por aparato de apertura y/o cierre de cerramiento de edificio o recinto, que debido a la recepción de un código de autentificación válido generado a partir de una o varias claves de código inicia la señal de accionamiento, utilizando al menos un primer terminal de usuario móvil individual, que comprende un dispositivo de comunicación de terminal de usuario para el envío y/o recepción de mensajes cifrados y/o firmados y una memoria para el almacenamiento al menos de una clave de usuario individual, así como un aparato de cifrado para el cifrado y/o firma de mensajes por medio de la al menos una clave de usuario individual.

Algunos ejemplos para el aparato de apertura y/o cierre de cerramiento de edificio o recinto (no concluyente) son accionamientos de portón, accionamientos de puerta, cerraduras eléctricas, cerraduras a motor y abrepuertas, como abrepuertas de casas. En general el aparato de apertura y/o cierre de cerramiento de edificio o recinto está configurado para asegurar un cerramiento de edificio o cerramiento de recinto, como en particular una puerta o un portón frente al uso no autorizado y permitir una utilización del cerramiento de edificio o recinto en el caso de entrada de una señal de accionamiento válida o iniciar activamente un movimiento de una hoja del cerramiento.

Ejemplos de terminales de usuario son en particular terminales de procesamiento de datos, como teléfonos inteligentes, tablets o similares. Los aparatos de comunicación están configurados en particular para la comunicación inalámbrica, en particular limitada a distancias cortas (por debajo de 50 m, en particular por debajo de 25 m). Preferiblemente los aparatos de comunicación trabajan por medio de un protocolo estándar. De forma especialmente preferida, los aparatos de comunicación capaces de la comunicación por medio de Bluetooth, en particular por medio de un Bluetooth de baja energía (BLE).

La invención se dedica en particular a la necesidad de permitir un acceso a través de cerramientos de edificio o recinto por personas autorizadas por medio de terminales de usuario estándares, como en particular teléfonos inteligentes o equipos de procesamiento de datos móviles similares, y software de aplicación correspondiente (Apps), sin tener que utilizar aparatos individuales separados como llaves mecánicas, en particular chips (chips RFID) o mandos a distancia individuales separados.

Los métodos conocidos por el mercado e implementados, por ejemplo, en instalaciones de cierre adquiribles en el mercado, p. ej. de la empresa Danaiock o de la empresa Nuki, para el control de instalaciones de cierre se basan en una conexión con un servidor, que ayuda en la autentificación de un usuario. De este modo se limita la posibilidad de uso, dado que no se puede manejar la instalación de cierre sin una conexión a internet . Otros métodos permiten el manejo de la instalación de cierre sin conexión a internet, no obstante, el círculo de usuarios está limitado al número máximo de compañeros de emparejamiento (como máx. 8 personas) y la configuración de nuevos usuarios se debe realizar *in situ*.

Las instalaciones de cierre eléctricas son elementos críticos para la seguridad en un edificio, que deben estar preparados contra ataques habituales (p. ej. ataques de repetición). no obstante, las investigaciones actuales muestran que no son seguros muchos equipos disponibles en el mercado.

Lo métodos de cierre basados en servidor requieren un conexión a internet durante o poco antes del proceso de cierre, por lo que por un lado los campos de aplicación claramente la conexión a internet durante o poco antes del proceso de cierre, por lo que por un lado se limitan claramente los campos de aplicación (debido a la falta de accesos a internet en sótanos, cenadores o chalés de vacaciones) y, por otro lado, en el caso de un fallo de servidor el usuario ya no puede entrar en su propia casa. Además, estos enfoques necesitan componentes claramente más potentes. Algunos métodos requieren la presencia del propietario en el portón para la transmisión de la autorización de acceso o registro de un nuevo usuario. Esto es menos cómodo desde el punto de vista del usuario y apenas se puede implementar en determinados escenarios de uso, p. ej. en chalés de vacaciones.

Muchos métodos se basan en información de clave secreta, que es igual en todos los productos o incluso grupos de productos de un fabricante. De este modo, mediante el desensamblado de un producto o de un hueco de seguridad en el fabricante (pérdida de datos por trabajadores o ciberataques) se puede poner en peligro la seguridad de todo un grupo de productos.

El documento DE 10 2014 217899 A1 da a conocer un sistema y un método para el establecimiento de un acceso limitado de un vehículo.

El documento DE 10 2005 057798 A1 describe un método para ofrecerle a un mensajero un acceso temporal a un depósito. A este respecto, las claves públicas del depósito y del portador se intercambian en mensajes cifrados y firmados entre un usuario registrado, el mensajero y el depósito. Los mensajes para el mensajero contienen información sobre el lugar del depósito y el tiempo durante el que se confiere el acceso.

El documento WO 2015/124168 A1 da a conocer un método para la gestión y para la adjudicación de autorizaciones de acceso a cuartos asegurados, donde la comunicación entre una base de datos y una cerradura está asegurada a través de una clave criptográfica y la comunicación entre un equipo móvil y la cerradura está asegurada a través de una segunda clave criptográfica.

Por el documento EP 2 725 823 A1 se conoce un método para la autentificación de usuario entre un teléfono móvil y una cerradura a través de comunicación de campo cercano, donde los datos de usuario se almacenan en un servidor que está conectado con el teléfono móvil a través de una red de comunicación de telefonía móvil.

La invención se ha planteado el objetivo de permitir el acceso a través de cerramientos de edificio o recinto, en particular puertas y portones, de manera más sencilla y cómoda pero segura y de limitarlo a un círculo de personas determinado.

Para la solución de estos objetivos, la invención crea el dispositivo y el método según las reivindicaciones independientes adjuntas.

Configuraciones ventajosas son objeto de las reivindicaciones dependientes.

La invención crea según un aspecto un dispositivo de apertura y/o cierre de cerramiento de edificio o recinto con un aparato de apertura y/o cierre de cerramiento de edificio o recinto,

que comprende un actuador, que se puede accionar mediante una señal de accionamiento, para permitir o bloquear un acceso a través de un cerramiento de edificio o recinto,
un aparato de comunicación de cerramiento de edificio o recinto para la recepción y/o envío de mensajes cifrados y/o firmados y
un aparato de autentificación de cerramiento de edificio o recinto individual por aparato de apertura y/o cierre de cerramiento de edificio o recinto, que debido a la recepción de un código de autentificación válido generado a partir de una o varias claves de código inicia la señal de accionamiento,

y al menos un primer terminal de usuario móvil individual, que comprende un dispositivo de comunicación de terminal de usuario para el envío y/o recepción de mensajes cifrados y/o firmados y una memoria para el almacenamiento al menos de una clave de usuario individual, así como un dispositivo de cifrado para el cifrado y/o firma de mensajes por medio de la al menos una clave de usuario individual,
donde

a) está previsto al menos un segundo terminal de usuario móvil individual, que comprende un aparato de comunicación de terminal de usuario para el envío y/o recepción de mensajes cifrados y/o firmados y una memoria para el almacenamiento al menos de una clave de usuario temporal, así como un aparato de cifrado para el cifrado y/o firma de mensajes por medio de la al menos una clave de usuario temporal, donde el primer terminal de usuario móvil individual está configurado para recibir un mensaje de limitación de tiempo con una información sobre una limitación de tiempo para una autentificación temporal de un segundo usuario o para generarla a partir de especificaciones de usuario y para generar a partir del mensaje de limitación de tiempo y a partir de la clave de usuario temporal una clave de usuario temporal que contiene información sobre la clave de usuario individual y la limitación de tiempo y para transmitirla al al menos un segundo terminal de usuario móvil individual.

La invención crea según otro aspecto un dispositivo de apertura y/o cierre de cerramiento de edificio o recinto con un aparato de apertura y/o cierre de cerramiento de edificio o recinto, que comprende

un actuador, que se puede accionar mediante una señal de accionamiento, para permitir o bloquear un acceso a través de un cerramiento de edificio o recinto,
un aparato de comunicación de cerramiento de edificio o recinto para la recepción y/o envío de mensajes cifrados y/o firmados y

un aparato de autentificación de cerramiento de edificio o recinto individual por aparato de apertura y/o cierre de cerramiento de edificio o recinto, que debido a la recepción de un código de autentificación válido generado a partir de una o varias claves de código inicia la señal de accionamiento,

y

al menos un primer terminal de usuario móvil individual, que comprende un dispositivo de comunicación de terminal de usuario para el envío y/o recepción de mensajes cifrados y/o firmados y una memoria para el almacenamiento al menos de una clave de usuario individual así como un dispositivo de cifrado para el cifrado y/o firma de mensajes por medio de la al menos una clave de usuario individual, donde

b) el aparato de autentificación individual presenta una clave de equipo individual y presenta una memoria, en la que está almacenada una información de identificación de usuario para cada primer terminal de usuario móvil individual,

donde el aparato de autentificación está configurado para calcular una clave de usuario individual para cada primer terminal de usuario móvil individual por medio de un cálculo de código unívoco a partir de la clave de equipo y la información de identificación de usuario, donde el al menos un terminal de usuario móvil individual está configurado para recibir y almacenar en la memoria su clave de usuario individual por aparato de autentificación individual durante una fase de registro.

De forma especialmente preferida, el dispositivo comprende tanto las características según a), como también las características según b).

Es preferible que el al menos un segundo terminal de usuario móvil individual esté configurado para cifrar los mensajes por medio de la clave de usuario temporal y enviarlos opcionalmente a través de un canal cifrado al aparato de comunicación de cerramiento de edificio o recinto.

Es preferible que el aparato de autentificación esté configurado para generar la clave de usuario individual durante la recepción de un mensaje firmado a partir de la información de identificación de usuario y la clave de equipo y verificar por consiguiente el mensaje firmado con la clave de usuario individual o con la clave de usuario temporal generada por la clave de usuario individual.

Es preferible que el aparato de autentificación genere de forma repetida una clave parcial pública temporal válida para un intervalo de tiempo determinado o una acción determinada y la envíe en el caso de contacto con un terminal de usuario a este, donde el terminal de usuario está configurado para firmar los mensajes con la clave de usuario y la clave parcial.

Es preferible que se use HMAC para la firma.

Es preferible que el aparato de autentificación presente un registro, en el que está registrada la información de identificación de usuario de los primeros usuarios autorizados individuales.

Es preferible que el dispositivo de apertura y/o cierre de cerramiento de edificio o recinto esté configurado de manera que el registro de usuarios se pueda modificar o borrar o bloquear o desbloquear por medio de un primer terminal de usuario móvil.

Es preferible que esté configurado de manera que se realice un registro de usuario autorizado por medio de mensajes, que están firmados por medio de una clave de registro, que se puede introducir o escanear en el primer terminal de usuario a autorizar y está depositada en el aparato de autentificación. El aparato de autentificación transmite una clave de usuario individual cifrada con la clave de registro al terminal de usuario del usuario autorizado.

Según otro aspecto, la invención se refiere a un método para el funcionamiento de un aparato de apertura y/o cierre de cerramiento de edificio o recinto, que comprende

un actuador, que se puede accionar mediante una señal de accionamiento, para abrir y/o cerrar y/o desenclavar o enclavar un cerramiento de edificio o recinto,

un aparato de comunicación de cerramiento de edificio o recinto para la recepción y/o envío de mensajes cifrados y/o firmados y

un aparato de autentificación individual por aparato de apertura y/o cierre de cerramiento de edificio o recinto, que debido a la recepción de un código de autentificación válido generado a partir de una o varias claves de código inicia la señal de accionamiento,

usando al menos un primer terminal de usuario móvil individual, que comprende un aparato de comunicación de terminal de usuario para el envío y/o recepción de mensajes cifrados y/o firmados y una memoria para el almacenamiento al menos de una clave de usuario individual, así como un dispositivo de cifrado para el cifrado y/o firma de mensajes por medio de la al menos una clave de usuario individual, con las etapas siguientes a1) a a6):

a1) facilitación de al menos un segundo terminal de usuario móvil individual, que comprende un aparato de

comunicación de terminal de usuario para el envío y/o recepción de mensajes cifrados y/o firmados y una memoria para el almacenamiento al menos de una clave de usuario temporal así como un dispositivo de cifrado para el cifrado y/o firma de mensajes por medio de la al menos una clave de usuario temporal,
a2) recepción o generación de un mensaje de limitación de tiempo con una información sobre una limitación de tiempo para una autentificación temporal de un segundo usuario por medio del primer terminal de usuario móvil
a3) generación de una clave de usuario temporal a partir del mensaje de limitación de tiempo y a partir de la clave de usuario individual, donde la clave de usuario temporal contiene una información sobre la clave de usuario individual y la limitación de tiempo,
a4) transmisión de la clave de usuario temporal del primer terminal de usuario al al menos un segundo terminal de usuario y
a5) generación de un código de autentificación temporal individual a partir de la clave de usuario individual mediante el segundo terminal de usuario móvil, de modo que el código de autentificación temporal contiene una información sobre la clave de usuario individual y la limitación de tiempo y
a6) inicio de la señal de accionamiento mediante el aparato de autentificación, cuando un código de autentificación temporal, que se corresponde con una clave de usuario individual, se recibe dentro de un intervalo de tiempo válido, determinado por la limitación de tiempo.

Según otro aspecto, la invención crea un método para el funcionamiento de un aparato de apertura y/o cierre de cerramiento de edificio o recinto, que comprende

un actuador, que se puede accionar mediante una señal de accionamiento, para abrir y/o cerrar y/o desenclavar o enclavar un cerramiento de edificio o recinto,
un aparato de comunicación de cerramiento de edificio o recinto para la recepción y/o envío de mensajes cifrados y/o firmados y
un aparato de autentificación individual por aparato de apertura y/o cierre de cerramiento de edificio o recinto, que debido a la recepción de un código de autentificación válido generado a partir de una o varias claves de código inicia la señal de accionamiento,

usando al menos un primer terminal de usuario móvil individual, que comprende un aparato de comunicación de terminal de usuario para el envío y/o recepción de mensajes cifrados y/o firmados y una memoria para el almacenamiento al menos de una clave de usuario individual, así como un dispositivo de cifrado para el cifrado y/o firma de mensajes por medio de la al menos una clave de usuario individual, con las etapas siguientes:

b1) registro de una información de identificación de usuario para cada usuario autorizado que utiliza un primer terminal de usuario individual,
b2) cálculo de una clave de usuario individual por usuario autorizado por medio de una clave de equipo secreta asociad al aparato de autentificación individual y de la información de identificación de usuario asignada mediante una rutina de cálculo de código unívoca y
b3) envío de la clave de usuario individual en el curso de una fase de registro al primer terminal de usuario móvil individual asignado. Preferiblemente, la clave de usuario individual se puede cifrar con la clave de registro.

Preferiblemente el método comprende:

Recepción de un mensaje firmado con una clave de usuario individual o temporal mediante el aparato de comunicación de cerramiento de edificio o recinto,
cálculo de la clave de usuario individual a partir de la información de identificación de usuario y la clave de usuario y verificación del mensaje por medio de la clave de usuario individual calculada.

En una configuración preferida, el método comprende tanto las etapas a1 a a6 como también las etapas b1 a b3).

La caracterización de las etapas y características con a), b), a1), a2), b1), b2) sirve solo para referenciar de forma más sencilla y no contiene una limitación con vistas a un orden o preferencia determinados de las etapas o características así caracterizadas.

Preferiblemente el método comprende:

Generación de una clave parcial pública temporal, que es válida para un intervalo de tiempo determinado o una acción determinada y notificación de la clave parcial pública temporal durante o antes del contacto entre los aparatos de comunicación, así como
firma de mensajes por medio de claves de usuario y claves parciales y repetición de estas etapas con una nueva clave parcial temporal después de la expiración del intervalo de tiempo o compleción de la acción.

Preferiblemente el método comprende:

Firma por medio de HMAC. Para el cálculo de las firmas HMAC se usa preferiblemente SHA256.

Preferiblemente el método comprende:

Comunicación por medio de Bluetooth.

Preferiblemente el método comprende:

Registro de la información de identificación de usuario de todos los primeros usuarios autorizados individuales en un registro del aparato de autentificación.

Preferiblemente el método comprende:

Modificación, borrado, bloqueo o desbloqueo de un registro de usuarios por medio de un primer terminal de usuario móvil.

Preferiblemente el método comprende:

Registro de usuarios autorizados por medio de mensajes, que están firmados por medio de una clave de registro, que se puede introducir o escanear en el primer terminal de usuario a autorizar y está depositada en el aparato de autentificación.

Según otro aspecto, la invención se refiere a un programa informático con medios de código de programa almacenados en particular sobre un soporte legible a máquina, establecido para la realización del método según cualquiera de las configuraciones anteriores, cuando el programa informático se ejecuta en un terminal. A este respecto, preferiblemente se trata de una App que se puede cargar en un teléfono inteligente, preferiblemente apto para Bluetooth.

El dispositivo de apertura y/o cierre de cerramiento de edificio o recinto está configurado preferiblemente para la realización del método según una de las configuraciones anteriores. Configuraciones preferidas del método se pueden realizar en un dispositivo de apertura y/o cierre de cerramiento de edificio o recinto según una de las configuraciones descritas anteriormente.

Una configuración preferida de la invención se refiere a en particular una transmisión de clave limitada en tiempo.

Una configuración preferida de la invención se refiere a una transmisión de clave para la transmisión de una clave de código limitada en tiempo para la apertura / cierre de cerramientos de edificio o recinto de un primer usuario individual a un usuario que se debe aceptar de forma limitada en tiempo por la unidad de autentificación.

Preferiblemente, la transmisión de clave se realiza entre la unidad de autentificación y el terminal de los primeros usuarios en base a una conexión de Bluetooth de baja energía y la transmisión de clave de claves limitadas en el tiempo a través de terceras vías de comunicación (códigos QR, correo electrónico, mensaje corto).

En particular, un actuador, que está configurado para apertura / cierre o desenclavamiento/enclavamiento de un cerramiento de edificio o recinto y se puede accionar mediante una señal de accionamiento, está conectado con un equipo de Bluetooth de baja energía, que inicia la señal de accionamiento a la recepción de una clave válida (código de autentificación).

Según una configuración preferida, la invención se refiere a un método para la transmisión de claves limitadas en el tiempo para un método de cierre basado en Bluetooth de baja energía para portones y puertas.

La configuración especialmente preferida de la invención tiene en particular las ventajas siguientes: Un chip de radio de Bluetooth de baja energía se puede usar para la apertura y cierre de portones y puertas. El propietario ventajosamente es capaz de proporcionar un acceso a un cuarto o edificio a otras personas de forma permanente o limitada en el tiempo. El control de accesos funciona preferiblemente independientemente de una conexión a internet. Gracias a la independencia de internet, el equipo se puede usar en cualquier lugar (sótano, cabañas de bosque, chalés de vacaciones, cenadores, cobertizos, almacenes, recintos distantes, etc.). El control de accesos puede estar limitado por motivos de costes con vistas a la memoria y potencia de cálculo. Aun así, preferiblemente se pueden asistir grandes grupos de usuarios con más de 100 personas. La transmisión de claves a terceros es posible preferiblemente a lo largo de grandes distancias (p. ej. por medio de mensaje corto o por teléfono), no obstante, el proceso de cierre mismo es posible preferiblemente sin una conexión a internet .

Las formas de realización preferidas de la invención usan componentes de hardware favorables y métodos criptográficos, conocidos en sí en otros campos, como p. ej. la tecnología de la mensajería o la tecnología de la información para el cifrado de datos y firma, a fin de permitir a grupos de usuarios muy grandes el acceso limitado en el tiempo a edificios, cuartos o recintos. De este modo se produce una buena escalabilidad de los escenarios de aplicación (p. ej. casa privada, propiedad comercial, complejo hotelero, recinto, alojamiento de vacaciones).

Las configuraciones preferidas del método según la invención son muy modestas con vistas a la necesidad de memoria, dado que solo se debe almacenar muy poca información en el mismo equipo respectivo (en particular al equipo de comunicación y autentificación asignado al cerramiento de edificio o recinto). En una configuración preferida, la complejidad de cálculo es baja por el uso de funciones hash.

Ventajosamente se necesita solo una función hash, no se debe utilizar un método de clave pública - privada, que son esencialmente más costosas computacionalmente.

En una configuración preferida, la seguridad de cada equipo (en particular de cada equipo estacionario de comunicación y autentificación) se basa en un secreto determinado al azar, preferiblemente por el hardware, (clave de equipo o código de equipo; individualmente para cada equipo, desconocido al fabricante). Por consiguiente, no será posible poner en peligro la seguridad de un equipo mediante el desensamblado / análisis de otro equipo, o eludir la seguridad por robo de datos en el fabricante.

Preferiblemente, el método prescinde conscientemente del uso de claves específicas al fabricante como secreto y en todos los métodos se basa en números al azar individuales, generados, en particular generados en hardware.

Preferiblemente, el método permite el bloqueo individual de claves o grupos de usuarios dados por usuarios privilegiados. De este modo se pueden minimizar los riesgos de seguridad por pérdidas de claves.

Preferiblemente, un usuario privilegiado que quisiera conferir un acceso al sistema a otra persona, no debe buscar la instalación de cierre, sino que en cualquier lugar a voluntad y en cualquier momento puede generar una clave limitada temporalmente y transmitirla a la persona. No obstante, una persona con una clave limitada temporalmente no puede usar esta clave para conceder acceso a otras personas. Por consiguiente, preferiblemente se puede ver en cualquier momento de forma transparente, qué persona ha concedido a quién acceso al sistema.

Preferiblemente se puede realizar un control (que implementa el método) en un procesador embebido de un chip nrf52 y todavía ofrece espacio para otros componentes de control, por lo que se pueden ahorrar otros módulos y grupos de módulos.

El enfoque permite nuevas funciones para el control de portones y puertas, que superan enfoques actuales por medio del mando a distancia.

Es posible la estructura de un circuito compacto con pocos módulos, de modo que es posible una integración en un cerco de puerta.

La gama de funciones de configuraciones especialmente preferidas comprende una transmisión de claves, la posibilidad de manejar grandes grupos de usuarios con bajo coste de hardware y/o secretos específicos al equipo.

Un ejemplo de realización se explica más en detalle a continuación mediante los dibujos adjuntos. Aquí muestra:

La Figura 1, una representación de bloques esquemática de una forma de realización de un dispositivo de apertura y/o cierre de cerramiento de edificio o recinto en el ejemplo de un control de portón, que se puede accionar de este modo por medio de códigos firmados por medio de HMAC;
la Figura 2, una representación de bloques esquemática de la forma de realización de Figura 1 para la representación de un proceso de registro; y
la Figura 3, una representación de bloques esquemática de la forma de realización de la Figura 2 para la representación de una interacción entre un usuario no privilegiado (como en particular un usuario con autentificación limitada en el tiempo) y el cerramiento de edificio o recinto, aquí con el portón.

En las Figura 1 a 3 está representada una forma de realización de un dispositivo de apertura y/o cierre de cerramiento de edificio o recinto 10 durante las diferentes fases de funcionamiento. En la Figura 1 está representado un funcionamiento normal, donde un usuario autorizado (es decir, un usuario registrado, aquí también denominado “usuario privilegiado”, representa un proceso de mando autorizado, como p. ej. realiza una apertura o cierre de un portón automático. En la Figura 2 está representada una fase de registro para el registro de usuarios autorizados. En la Figura 3 está representado como otro usuario, que se ha autorizado de forma temporal para el mando por un usuario privilegiado autorizado, realiza un proceso de mando.

El dispositivo de apertura y/o cierre de cerramiento de edificio o recinto 10 presenta un aparato de apertura y/o cierre de cerramiento de edificio o recinto 12 y al menos un primer equipo de usuario móvil individual 14.

Bajo un aparato de apertura y/o cierre de cerramiento de edificio o recinto 12 se entiende un aparato por medio del que se puede liberar o bloquear un acceso a través de un cerramiento de edificio 16 o un cerramiento de recinto de forma accionable por señal. Son ejemplos accionamientos de portones o accionamientos de puertas o abrepuertas o abreportones o cerraduras eléctricas o cerraduras a motor. En los ejemplos representados está representado en particular un accionamiento de portón 18 para el accionamiento de un cerramiento de edificio 16 configurado como

portón 20.

El aparato de apertura y/o cierre de cerramiento de edificio o recinto 12 presenta un actuador 21, que se puede accionar por una señal de accionamiento, para permitir o bloquear un acceso a través del cerramiento de edificio o recinto 16, un aparato de comunicación de cerramiento de edificio o recinto 22 para la recepción y/o envío de mensajes cifrados y/o firmados y un aparato de autentificación de cerramiento de edificio o recinto individual 24 por aparato de apertura y/o cierre de cerramiento de edificio o recinto 12, que debido a la recepción de un código de autentificación válido 28 generado a partir de una o varias claves de código inicia la señal de accionamiento.

En la forma de realización representada, el actuador 21 está formado, por ejemplo, por el motor del accionamiento de portón 18. En el caso de un abrepuertas, el actuador puede estar formado, por ejemplo, por un solenoide que libera una puerta, de modo que se puede abrir por tracción o compresión.

El al menos un primer terminal de usuario móvil individual 14 es un terminal de usuario, que está en posesión del usuario registrado. Los ejemplos para los terminales de usuario 14, 30 aquí explicados son en particular equipos de procesamiento de datos móviles como PDAs, tablets y de forma especialmente preferida teléfonos inteligentes. Como primeros terminales de usuario 14 se designan los terminales de usuario en posesión de usuarios registrados. Los usuarios registrados pueden autorizar en el tiempo otros usuarios de forma temporal para el mando, en tanto que las claves temporales (TemporalKey) se envían de sus primeros terminales de usuario 14 a un terminal de usuario en posesión de estos usuarios temporales. Los terminales de usuario de los usuarios a autorizar solo temporalmente se denominan aquí los segundos terminales de usuario móviles 30.

Los terminales de usuario 14, 30 presentan respectivamente un aparato de comunicación de terminal de usuario 32 para el envío y/o recepción de mensajes cifrados y/o firmados y una memoria 34 para el almacenamiento de al menos una clave de usuario 34, 36, así como un aparato de cifrado para el cifrado y/o firma de mensajes por medio de la al menos una clave de usuario 34, 36. Los primeros terminales de usuario 14 utilizan para ello claves de usuario individuales 34, que son específicas para el primer terminal de usuario móvil individual 14 y para el respectivo cerramiento de edificio o recinto a manejar, es decir, en particular para el aparato de autentificación asociado 24. Las claves de usuario individuales 34 se utilizan como secreto individual para la conexión entre los primeros terminales de usuario móviles individuales 14 y los aparatos de autentificación individuales 24 y por ello también se denominan a continuación clave de conexión (ConnectionKey) 24.

Los segundos terminales de usuario 30 utilizan claves de usuario temporales 36 para la firma, que contienen una información sobre el usuario registrado, que ha iniciado la autorización temporal, y sobre la limitación de tiempo (Time Span) 38.

Por lo tanto, preferiblemente está previsto al menos un segundo terminal de usuario móvil individual 30, que comprende igualmente un aparato de comunicación de terminal de usuario 32 para el envío y/o recepción de mensajes cifrados y/o firmados y una memoria para el almacenamiento al menos de una clave de usuario temporal 36, así como un aparato de cifrado para el cifrado y/o firma de mensajes por medio de la al menos una clave de usuario temporal 36, donde el primer terminal de usuario móvil individual 14 está configurado para recibir un mensaje de limitación de tiempo con una información sobre una limitación de tiempo para una autentificación temporal de un segundo usuario o para generarla a partir de especificaciones de usuario y para generar a partir del mensaje de limitación de tiempo y a partir de la clave de usuario temporal una clave de usuario temporal 36 que contiene información sobre la clave de usuario individual 36 y la limitación de tiempo 38 y para transmitirla al al menos un segundo terminal de usuario móvil individual 30.

El aparato de comunicación de terminal de usuario 32 está formado en el ejemplo de realización representado, p. ej. por el aparato de Bluetooth del teléfono inteligente. Como memoria se utiliza la memoria de teléfono inteligente. El aparato de cifrado se implementa por un software de aplicación (p. ej. APP).

El aparato de autentificación individual 24 presenta una clave de equipo individual 40 - denominada a continuación también DeviceKey y una memoria o un registro, en los que está almacenada una información de identificación de usuario (UserID) 42 para cada primer equipo de usuario móvil individual 14.

El aparato de autentificación 24 y el aparato de comunicación de cerramiento de edificio o recinto 22 están implementados, por ejemplo, en un chip BLE. Este presenta en particular un procesador, software de aplicación, un generador aleatorio 41 (en particular implementado en hardware, HW RNG) y una interfaz de Bluetooth para la conexión de Bluetooth con baja energía.

El aparato de autentificación 24 está configurado para calcular una clave de usuario 34 para cada primer terminal de usuario móvil individual 14 por medio de un cálculo de código unívoco a partir de la clave de equipo 40 y la información de identificación de usuario 42.

El al menos un primer terminal de usuario móvil individual 14 está configurado para recibir y almacenar en su memoria su clave de usuario individual 34 por aparato de autentificación individual 24 durante una fase de registro.

El registro se realiza bajo firma con una clave de registro (RegisterKey) 44, que está contenida p. ej. en los documentos adjuntos y se puede introducir por el propietario en el primer terminal de usuario a registrar o se puede registrar p. ej. por medio de un código de escaneo.

Para evitar ataques de repetición, el aparato de autentificación 24 está configurado además para generar un clave parcial 45 válida temporalmente durante un intervalo de tiempo o una acción (un proceso de mando o también serie de procesos de mando), que se pone a disposición de otros equipos 14, 30 configurados para la comunicación y a la que se recurre igualmente para la firma de los mensajes. Un ejemplo para una clave parcial 45 semejante está designado en la descripción siguiente como “Challenge”.

A continuación se explica más en detalle un ejemplo de realización mediante las representaciones en las Figura1 a 3. En las figuras están caracterizadas información pública (Public) e información privada (Privat) con colores o símbolos diferentes.

1.0 Concepto de seguridad para la transmisión de claves

A continuación se describen en detalle los componentes y métodos para la generación de claves y transmisión y se explican las etapas del método prevista para ello.

El mando se realiza mediante la comunicación entre los aparatos de comunicación 22, 32 por medio de los mensajes, que están firmados y/o cifrados por medios de las claves de código 34, 36, 44, 45.

1.1 Formato general de los datos: Un mensaje (Packet) se compone de un encabezado ("Header”), una zona de datos opcional / variable ("Data”) y un código de autentificación 28, en particular en forma de una firma 50, preferiblemente una firma HMAC, más en particular una firma de 32 byte. Estos mensajes se envían de un teléfono inteligente 46 (ejemplo para terminal de usuario 14, 30) al equipo BLE 48 (ejemplo para el aparato de apertura y/o cierre de cerramiento de edificio o recinto 12, p. ej. control de puerta), a fin de intercambiar datos o transmitir comandos. La firma 50 tiene la finalidad de asegurar la comunicación en referencia a las modificaciones por terceros y autentificar el comando del teléfono inteligente 46 respecto al equipo BLE 48. La firma (Message Authentication Code) 50 se basa en un método HMAC. Las firmas HMAC son ejemplos especialmente preferidos para los códigos de autentificación usados para ello.

Las particularidades del método HMAC se pueden deducir en particular en Wikipedia, palabra clave “Keyed-Hash_Message_Authentification”, descargado el 19/10/2016, como literatura no de patentes de la solicitud.

1.2 Código de autentificación de mensaje (Message Authentication Code): La seguridad del control de cerramiento de edificio o recinto, como en particular control de puerta o control de portón, utiliza el “Message Authentication Code” para verificar el usuario respecto al portón 20. Para mantener cortas las designaciones, el “Message Authentication Code” 28 se designa a continuación como firma 50. El usuario envía para ello el encabezado que contiene el comando 54 a realizar y firma este por medio de HMAC (Keyed-Hash Message Authentication Code). El HMAC se especifica en RFC 2104, NIST Standard FIPS 198 y en RFC 4868. Se usa en IPSEC, TLS y SSH y actualmente es válido como seguro y no comprometido. La firma 50 se calcula por medio de

HMAC = HASH((ConnectionKey xor opad) || HASH((ConnectionKey xor ipad) || (Message||Challenge)))

donde “||” deben designar la operación de cadena y “HASH” la función hash sha256. Los rellenos opad e ipad se pueden deducir de los estándares.

El secreto común entre los participantes en la comunicación de teléfono inteligente y control de portón es la ConnectionKey (ejemplo para una clave de usuario individual 34), que se debe mantener de forma secreta. Si el teléfono inteligente 46 transmitiera la clave 34, entonces cualquier otra persona puede abrir con ello la puerta / el portón 20. La ConnectionKey digital se comporta por ello como una llave física formando una cerradura convencional.

1.3 ConnectionKey: La formación de la ConnectionKey (clave de usuario individual 34) se realiza por medio de combinación de calve específica al equipo DeviceKey (clave de equipo 40) y número de identificación de usuario UserID (ejemplo para la información de identificación de usuario 42). La concatenación de la información y la realización siguiente de una función hash proporcionan la ConnectionKey. El chip BLE genera en un instante definitivo (alternativamente durante el montaje) una clave de equipo aleatoria 40 específica al equipo “DeviceKey”, que solo está almacenada en el equipo 48 y nunca se entrega. Cada nuevo usuario obtiene una identificación unívoca, como p. ej. una identificación de 16 bit (UserID) en el registro. En este caso, el chip BLE determina una ConnectionKey por medio de sha256: ConnectionKey = SHA256(UserID || DeviceKey)

La ConnectionKey se almacena solo en el teléfono inteligente 46, pero no en el chip BLE. El teléfono inteligente 46 ofrece suficiente memoria para almacenar una pluralidad de claves, pero el chip BLE solo tiene un espacio de memoria limitado, de modo que es ventajosa la generación de una clave derivada de una clave principal.

Ventajas del método y objetivos:

- Expansión de clave de la UserID corta a “ConnectionKey” ® de 256 bits de longitud.
- No se intercambian claves globales.
- Cada participante tiene una clave de usuario individual 34 (p. ej. clave de 256 bit), que no se puede usar para calcular las claves de otros participantes. Un usuario conoce su “ConnectionKey” propia, entonces no puede calcular la “DeviceKey”, dado que debería invertir para ello la función sha256. Sin la “DeviceKey” no puede calcular la clave de los otros usuarios.
- Ahorro de memoria: El chip BLE no debe almacenar todas las claves, sino que puede calcularlas en cualquier momento a partir de la UserID.
- Borrado / bloqueo de las UserIDs por medio de listas de bloqueo con coste de memoria reducido
- Bloqueo de todas las claves mediante regeneración de la DeviceKey

1.4 Borrado o bloqueo de usuarios
El bloqueo de los usuarios se realiza a través de listas y la sustitución de claves.

2*.1. Proceso de registro*
a) “Usuario privilegiado” (usuarios registrados, propietarios de primeros terminales de usuario 14):

La lista de “RootUsers” contiene todos las UserID de usuarios privilegiados. En el orden ascendente se dan las UserIDs al RootUser. Tan pronto como estén agotados la capacidad de la lista o las posibles UserIDs o, por ejemplo, (con 16 bits la lista esté agotad cuando las UserID han alcanzado 65535 usuarios) no se pueden elaborar nuevos usuarios privilegiados en el sistema. Solo mediante la elaboración de una nueva “DeviceKey” se liberan de nuevo antiguas UserIDs. De este modo caducan todas las claves dadas hasta ahora y todos los usuarios se deben registrar nuevamente en el sistema. Un usuario privilegiado se bloquea mediante borrado de la lista de “RootUser”. El borrado de un usuario privilegiado bloquea automáticamente todas las claves limitadas temporalmente, que se generaron por medio de la clave bloqueada o se generan de forma abusiva en instantes posteriores. Para ello están autorizados todos los usuarios privilegiados.

b) “Usuarios no privilegiados”:
La lista de bloqueo “BlockedUsers” contiene combinaciones de la UserID y TemporalKey y caracteriza los usuarios a bloquear a través de la ID del usuario privilegiado que concede el acceso y del número de TemporalKey (de clave individual o grupo de claves).

Cada usuario anotado en la lista "BlockedUsers" es bloqueado automáticamente. Cada usuario privilegiado puede bloquear todo usuario privilegiado o levantar un bloqueo. Además, cada usuario privilegiado puede bloquear los usuarios no privilegiados firmados con su clave, por el contrario se pueden levantar también bloqueos de usuarios no privilegiados que no se han firmado por la clave propia.

2.2 DeviceKey
Cada equipo 48 genera de forma autónoma una clave de equipo aleatoria 40, como en particular una DeviceKey de 256 bits. Esta nunca abandonará el equipo 48 y es aleatoria “basada en hardware”. Los números aleatorios se deben recibir de una fuente a seleccionar de forma apropiada (p. ej. pila BLE, hardware externo). En una configuración ventajosa no está permitida la utilización de valores pseudo-aleatorios o valores calculados a partir de otra información (como p. ej. número de producto), dado que un debilitamiento de la “DeviceKey” debilitaría la seguridad de todo el sistema. De esta DeviceKey se derivan las ConnectionKey.

2.3 Challenge (ejemplo de clave parcial 45)
El chip BLE saca valores de forma aleatoria para una clave parcial 45, como p. ej. una Challenge de 32 bits y la pone a disposición públicamente a través de una notificación a cada equipo 14, 30. En este caso se pueden utilizar secuencias pseudo-aleatorias o mejor valores aleatorios generados por hardware. Cada comando debe contener en este ejemplo de realización la información de la challenge actual para el cálculo de la firma a fin de evitar los ataques de repetición de forma efectiva. En un ejemplo de realización, cada cambio de estado del sistema (p. ej. apertura, cierre) genera automáticamente una nueva challenge. Para ahorrar la cantidad de datos a transmitir, la challenge no es preferiblemente parte de un paquete.

2.4 RegisterKey (ejemplo de clave de registro 44)
La “RegisterKey” es el acceso al sistema del registro de usuarios privilegiados. El propietario (en el sentido del comprador de producto) debería evitar la transmisión de la “RegisterKey” y solo proporcionar esta información a un círculo de personas de mucha confianza. Una persona en el sentido de la “RegisterKey” puede generar usuarios privilegiados a voluntad y estos pueden crear de nuevo usuarios “no privilegiados”.

La utilización de la “RegisterKey” puede ocurrir como sigue:

1. “Propietario-centrado” El propietario tiene conocimiento exclusivo de la "RegisterKey". Genera todas las claves 34 para usuarios privilegiados y proporciona las claves 34 a través de una infraestructura de servidor

asegurada.

2. “Grupo” La "RegisterKey“ se le proporciona a un grupo de confianza y este puede utilizar a voluntad la clave de registro 44. En caso de mal uso, el equipo 48 se debe reiniciar y cambiar la “RegisterKey”.

En el caso de un secreto de clave comprometido, se puede utilizar un método de PIN / PUK para cambiar la “RegisterKey”. La información del PIN / PUK se debería conservar separada del equipo 48 y solo se debe usar para el cambio de la "RegisterKey".

3.1 Proceso de registro de usuarios privilegiados

El objetivo del proceso de registro es el registro de un usuario privilegiado (root) a través de una conexión opcionalmente cifrada y asegurada por MITM (MITM = Man-In-The-Middle). En este caso un cifrado AES de 128 bits se puede asumir en este caso por la pila de Bluetooth. La seguridad MITM se implementa por el protocolo. El registro sigue p. ej. el protocolo siguiente:

1. Teléfono inteligente 48 (como un primer equipo de usuario individual 14 escanea en busca del chip BLE
2. Teléfono inteligente 48 se conecta con el chip BLE 3. Chip BLE
3. El chip BLE posee RegisterKey secreta (anotado en las instrucciones de funcionamiento en la entrega en forma de texto o como código QR; alfanumérico; > 128 bits)
4. El teléfono inteligente 48 envía mensaje de registro (Register Message) 52:

• Datos: nombre de usuario (alfanumérico, p. ej. “hombre de muestra”, longitud 10 caracteres)
• Firma = HASH((RegisterKey xor opad) || HASH((RegisterKey xor ipad) || (Message||Challenge)))

5. El chip BLE-Chip examina la firma y almacena nuevo usuario, en caso satisfactorio (UserID++) UserID = número de usuario unívoco como número (16 bits) ConnectionKey = SHA256(UserID || DeviceKey)
6. El chip BLE cifra [ConnectionKey] por medio de hash de la RegisterKey: EncConnectionKey = ConnectionKey xor HASH(RegisterKey)
7. El chip BLE envía [UserID,EncConnectionKey] al teléfono inteligente a través de conexión cifrada.
8. El teléfono inteligente descifra la clave de conexión secreta [ConnectionKey] por medio de ConnectionKey = EncConnectionKey xor HASH(RegisterKey)

Nota: La conexión entre el chip BLE 48 y el teléfono inteligente 46 no se puede proteger la mayoría de las veces de manera fiable contra ataques MITM, no obstante, mediante el uso de la clave de registro se puede aumentar considerablemente el esfuerzo para la determinación de la clave de conexión. Es recomendable la utilización de una clave de al menos 256 bits de longitud.

4.1 Transmisión de clave por medio de cadena de firma

Cada usuario privilegiado puede conceder acceso a otras personas. A este respecto se debe predeterminar una limitación temporal. Si un usuario privilegiado pierde el acceso al sistema, entonces se vuelven inválidas automáticamente todas las claves derivadas.

El objetivo del protocolo descrito a continuación es la generación de una clave limitada temporalmente (clave de usuario temporal 36) o unión de claves y su intercambio entre un usuario privilegiado (“Root”) y un usuario no privilegiado (“User”).

1. El teléfono inteligente Root genera un mensaje que resume el mensaje de límite de tiempo, la ID del grupo y la UserID en un mensaje y calcula para ello la firma correspondiente. A continuación, la firma recibe el papel de una clave de usuario temporal 36 (“TemporalKey”) para el usuario no privilegiado. El usuario no privilegiado usa la TemporalKey como ConnectionKey para la firma de sus comandos propios para el control de puerta / portón. A partir de la TemporalKey no se puede calcular la ConnectionKey del usuario Root. Si se concede el acceso a un usuario durante períodos de tiempo recurrentes, entonces se calcula una clave separada para cada período de tiempo y todas las claves se reúnen en una unión de claves.

TemporalKey = HASH((ConnectionKey xor opad) || HASH((Connection-Key xor ipad) || (Message)))

2. El teléfono inteligente Root envía la unión de claves, que representa una cantidad de combinaciones [Message,Temporal Key], al usuario no privilegiado a través de un canal seguro. Cada clave de usuario temporal 36 es válida por un período de tiempo limitado [StartTime, EndTime], los períodos recurrentes se definen de forma individual.
3. Control de puerta / portón por usuarios privilegiados o no privilegiados: El teléfono inteligente del usuario temporal (ejemplo para el segundo terminal de usuario 30) escanea en busca de paquetes de anuncio del portón 20 que conoce. Tan pronto como se muestran los datos de una puerta 20 que conoce, el software de la aplicación extrae los datos relevantes respecto al estado del paquete de anuncio (por ejemplo, challenge actual). Si el usuario desea una interacción con el portón 20, presiona un botón / símbolo correspondiente. Acto seguido, el teléfono inteligente 30 se conecta con el equipo BLE 48, por lo que se detiene el anuncio. Los

paquetes se transmiten ahora desde el teléfono inteligente 30 al equipo BLE 48 a través de la conexión cifrada AES de 128 bits opcionalmente. El usuario usa la TemporalKey de la clave de usuario temporal 36 actualmente válida para la firma de sus mensajes, p. ej. apertura del portón. La integración de la challenge evita los ataques de repetición.

Firma = HASH((TemporalKey xor opad) || HASH((TemporalKey xor ipad) || Message||Challenge)))

4. El teléfono inteligente 30 del usuario sin privilegios envía un mensaje al dispositivo BLE 48
5. El dispositivo BLE 48 examina el período de tiempo y la challenge, si uno de los dos no se corresponde con las expectativas el sistema ignora la solicitud.
6. El dispositivo BLE 48 calcula independientemente la TemporalKey por medio de la ConnectionKey que conoce del usuario privilegiado que supuestamente ha concedido acceso al usuario no privilegiado. Entonces examina la firma y abre eventualmente el portón.

Lista de referencias:

10	Dispositivo de apertura y/o cierre de cerramiento de edificio o recinto
12	Aparato de apertura y/o cierre de cerramiento de edificio o recinto
14	Primer terminal de usuario (registrado, usuario privilegiado)
16	Cerramiento de edifico o recinto (p. ej. portón, puerta)
18	Accionamiento de puerta
20	Portón
21	Actuador
22	Aparato de comunicación de cerramiento de edifico o recinto
24	Aparato de autentificación
28	Código de autentificación (mensaje firmado)
30	Segundo terminal de usuario (usuario autorizado solo temporalmente)
32	Aparato de comunicación de terminal de usuario
34	Clave de usuario individual (ConnectionKey, usuario registrado)
36	Clave de usuario temporal (TemporalKey, usuario temporal)
38	Información sobre la limitación de tiempo (Time Span) del permiso de uso temporal
40	Clave de equipo (DeviceKey)
41	Generador aleatorio
42	Información de identificación de usuario (UserID)
44	Clave de registro
45	Clave parcial (Challenge)
46	Teléfono inteligente
48	Equipo BLE
50	Firma
52	Mensaje de registro
54	Comando (Command)
56	Estatus
58	Rutina de cálculo de código (cifrado o firma)

REIVINDICACIONES

1. Dispositivo de apertura y/o cierre de cerramiento de edificio o recinto (10) con un aparato de apertura y/o cierre de cerramiento de edificio o recinto (12), que comprende
un actuador (21), que se puede accionar mediante una señal de accionamiento, para permitir o bloquear un acceso a través de un cerramiento de edificio o recinto (16),
un aparato de comunicación de cerramiento de edificio o recinto (22) para la recepción y/o envío de mensajes cifrados y/o firmados (28) y
un aparato de autentificación individual (28) por aparato de apertura y/o cierre de cerramiento de edificio o recinto (12), que debido a la recepción de un código de autentificación válido (28) generado a partir de una o varias claves de código inicia la señal de accionamiento,
y
al menos un primer terminal de usuario móvil individual (14), que comprende un dispositivo de comunicación de terminal de usuario (32) para el envío y/o recepción de mensajes cifrados y/o firmados (28) y una memoria para el almacenamiento al menos de una clave de usuario individual (34), así como un dispositivo de cifrado para el cifrado y/o firma de mensajes por medio de la al menos una clave de usuario individual (34), donde
el aparato de autentificación individual (28) presenta una clave de equipo individual (40) y presenta una memoria y/o registro, en el que está almacenada y/o registrada una información de identificación de usuario (42) para cada usuario autorizado que utiliza un primer terminal de usuario móvil individual (14),
donde el aparato de autentificación (28) está configurado para calcular una clave de usuario individual (34) para cada primer terminal de usuario (14) por medio de un cálculo de código unívoco a partir de la clave de equipo (40) y la información de identificación de usuario (42), donde el al menos un primer terminal de usuario (14) está configurado para recibir y almacenar en la memoria su clave de usuario individual (34) para el respectivo aparato de autentificación individual (24) durante la fase de registro.

2. Dispositivo de apertura y/o cierre de cerramiento de edificio o recinto (10) según la reivindicación 1, **caracterizado por que** está previsto al menos un segundo terminal de usuario móvil individual (30), que comprende un aparato de comunicación de terminal de usuario (32) para el envío y/o recepción de mensajes cifrados y/o firmados (28) y una memoria para el almacenamiento al menos de una clave de usuario temporal (36), así como un aparato de cifrado para el cifrado y/o firma de mensajes por medio de la al menos una clave de usuario temporal (36), donde el primer terminal de usuario móvil individual (14) está configurado para recibir una información (38) sobre una limitación de tiempo para una autentificación temporal de un segundo usuario o para generarla a partir de especificaciones de usuario y para generar a partir de la información (38) sobre la limitación de tiempo y a partir de la clave de usuario temporal (34) una clave de usuario temporal (36) que contiene información sobre la clave de usuario individual (36) y la limitación de tiempo (38) y para transmitirla al al menos un segundo terminal de usuario móvil individual (30).

3. Dispositivo de apertura y/o cierre de cerramiento de edificio o recinto (10) según la reivindicación 2, **caracterizado por que** el al menos un segundo terminal de usuario (30) está configurado para cifrar los mensajes por medio de una clave de usuario temporal (36) y enviarlos de forma cifrada al aparato de comunicación de cerramiento de edificio o recinto (10) y/o por que el aparato de autentificación (24) genera de forma repetida una clave parcial temporal (45) válida solo para un intervalo de tiempo determinado o una acción determinada y en el caso de contacto con un terminal de usuario (14, 30) la envía a este, donde el terminal de usuario (14, 30) está configurado para firmar los mensajes con la clave de usuario (34, 36) y la clave parcial (45).

4. Dispositivo de apertura y/o cierre de cerramiento de edificio o recinto (10) según cualquiera de las reivindicaciones anteriores, **caracterizado por que** el aparato de autentificación (24) está configurado para generar la clave de usuario individual (34) durante la recepción de un mensaje firmado (28) a partir de la información de identificación de usuario (42) y la clave de equipo (40) y verificar por consiguiente el mensaje (28) firmado con la clave de usuario (34, 36) con vistas a la autenticidad y autorización del usuario.

5. Dispositivo de apertura y/o cierre de cerramiento de edificio o recinto (12) según cualquiera de las reivindicaciones anteriores, **caracterizado por que** está configurado para la firma por medio de HMAC y/o para la comunicación por medio de Bluetooth.

6. Dispositivo de apertura y/o cierre de cerramiento de edificio o recinto (10) según cualquiera de las reivindicaciones anteriores, **caracterizado por que** el dispositivo de apertura y/o cierre de cerramiento de edificio o recinto (10) está configurado de manera que el registro de usuarios se puede modificar o borrar o bloquear o desbloquear por medio de un primer terminal de usuario móvil (14).

7. Dispositivo de apertura y/o cierre de cerramiento de edificio o recinto (10) según cualquiera de las reivindicaciones anteriores, **caracterizado por que** está configurado de manera que se realiza un registro de usuarios autorizados por medio de mensajes, que están firmados por medio de una clave de registro (44), que se puede introducir o escanear en el primer terminal de usuario (14) a autorizar y está depositado en el aparato de autentificación (24).

8. Método para el funcionamiento de un aparato de apertura y/o cierre de cerramiento de edificio o recinto (12), que comprende

un actuador (21), que se puede accionar mediante una señal de accionamiento, para permitir o bloquear un acceso a través de un cerramiento de edificio o recinto (16),
un aparato de comunicación de cerramiento de edificio o recinto (32) para la recepción y/o envío de mensajes cifrados y/o firmados (28) y
un aparato de autentificación individual (24) por aparato de apertura y/o cierre de cerramiento de edificio o recinto (12), que debido a la recepción de un código de autentificación válido (28) generado a partir de una o varias claves de código (34, 36, 44, 45) inicia la señal de accionamiento,
usando al menos un primer terminal de usuario móvil individual (14), que comprende un aparato de comunicación de terminal de usuario (32) para el envío y/o recepción de mensajes cifrados y/o firmados (28) y una memoria para el almacenamiento al menos de una clave de usuario individual (34) así como un dispositivo de cifrado para el cifrado y/o firma de mensajes por medio de la al menos una clave de usuario individual (34), con las etapas siguientes b1) a b3):

b1) registro de una información de identificación de usuario (42) para cada usuario autorizado que utiliza un primer terminal de usuario individual (14) en un registro del aparato de autentificación (24),
b2) cálculo de una clave de usuario individual (34) por usuario autorizado por medio de una clave de equipo secreta (40) asociada al aparato de autentificación individual (24) y de la información de identificación de usuario asignada (42) mediante una rutina de cálculo de código unívoca (58) mediante el aparato de autentificación (24) y
b3) envío de la clave de usuario individual (34) en el curso de una fase de registro al primer terminal de usuario móvil individual asignado (14).

9. Método según la reivindicación 8, además **caracterizado por** las etapas siguientes a1) a a6):

a1) facilitación de al menos un segundo terminal de usuario móvil individual (30), que comprende un aparato de comunicación de terminal de usuario (32) para el envío y/o recepción de mensajes cifrados y/o firmados (28) y una memoria para el almacenamiento al menos de una clave de usuario temporal (36) así como un dispositivo de cifrado para el cifrado y/o firma de mensajes por medio de la al menos una clave de usuario temporal (36),
a2) recepción o generación de una información (38) sobre una limitación de tiempo para una autentificación temporal de un segundo usuario por medio del primer terminal de usuario móvil (14),
a3) generación de una clave de usuario temporal (36) a partir de la información de limitación de tiempo (38) y a partir de la clave de usuario individual (34), donde la clave de usuario temporal (36) contiene una información sobre la clave de usuario individual (34) y la limitación de tiempo (38),
a4) transmisión de la clave de usuario temporal (36) del primer terminal de usuario (14) al al menos un segundo terminal de usuario (30) y
a5) generación de un código de autentificación temporal individual (28) a partir de la clave de usuario individual (36) mediante el segundo terminal de usuario móvil (30), de modo que el código de autentificación temporal (28) contiene una información sobre la clave de usuario individual (34) y la limitación de tiempo (38) y
a6) inicio de la señal de accionamiento mediante el aparato de autentificación (24), cuando un código de autentificación temporal (28), que se corresponde con una clave de usuario individual (34), se recibe dentro de un intervalo de tiempo válido, determinado por la limitación de tiempo.

10. Método según la reivindicación 8 ó 9, **caracterizado por** la recepción de un mensaje (28) firmado con una clave de usuario (34, 36) mediante el aparato de comunicación de cerramiento de edificio o recinto (22), cálculo de la clave de usuario individual (34) a partir de la información de identificación de usuario (42) y la clave de equipo (40) y verificación del remitente y/o del contenido del mensaje (28) por medio de la clave de usuario individual calculada (34).

11. Método según una cualquiera de las reivindicaciones 8 a 10, **caracterizado por**

11.1 la generación de una clave parcial temporal (45), que es válida durante un intervalo de tiempo determinado o una acción determinada y
11.2 la notificación de la clave parcial temporal (45) durante o antes del contacto entre los aparatos de comunicación (22, 32), así como
11.3 la firma de mensajes por medio de claves de usuario (34, 36) y claves parciales (45) y
11.4 la repetición de estas etapas 11.1 a 11.3 o al menos de la etapa 11.1 con una nueva clave parcial temporal (45) tras la expiración del intervalo de tiempo o compleción de la acción.

12. Método según una cualquiera de las reivindicaciones 8 a 11, **caracterizado por** la firma por medio de HMAC y/o la comunicación por medio de Bluetooth.

13. Método según una cualquiera de las reivindicaciones 8 a 12, **caracterizado por** la modificación, el borrado, bloqueo o desbloqueo de un registro de usuarios por medio de un primer terminal de usuario móvil (14).

14. Método según una cualquiera de las reivindicaciones 8 a 13, **caracterizado por** el registro de usuarios autorizados por medio de mensajes que están firmados por medio de una clave de registro (44), que se puede introducir o escanear

en el primer terminal de usuario (14) a autorizar y está depositada en el aparato de autentificación (24).

15. Programa informático con medios de código de programa almacenados en particular en un soporte legible a máquina, concebido para la realización de las etapas del método del aparato de autentificación (24) según cualquiera de las reivindicaciones 8 a 14 cuando el programa informático se ejecuta en un procesador, y para la realización de las etapas del método del terminal (14, 30) según una cualquiera de las reivindicaciones 8 a 14 cuando el programa informático se ejecuta en un terminal (14, 30).

FIG 1

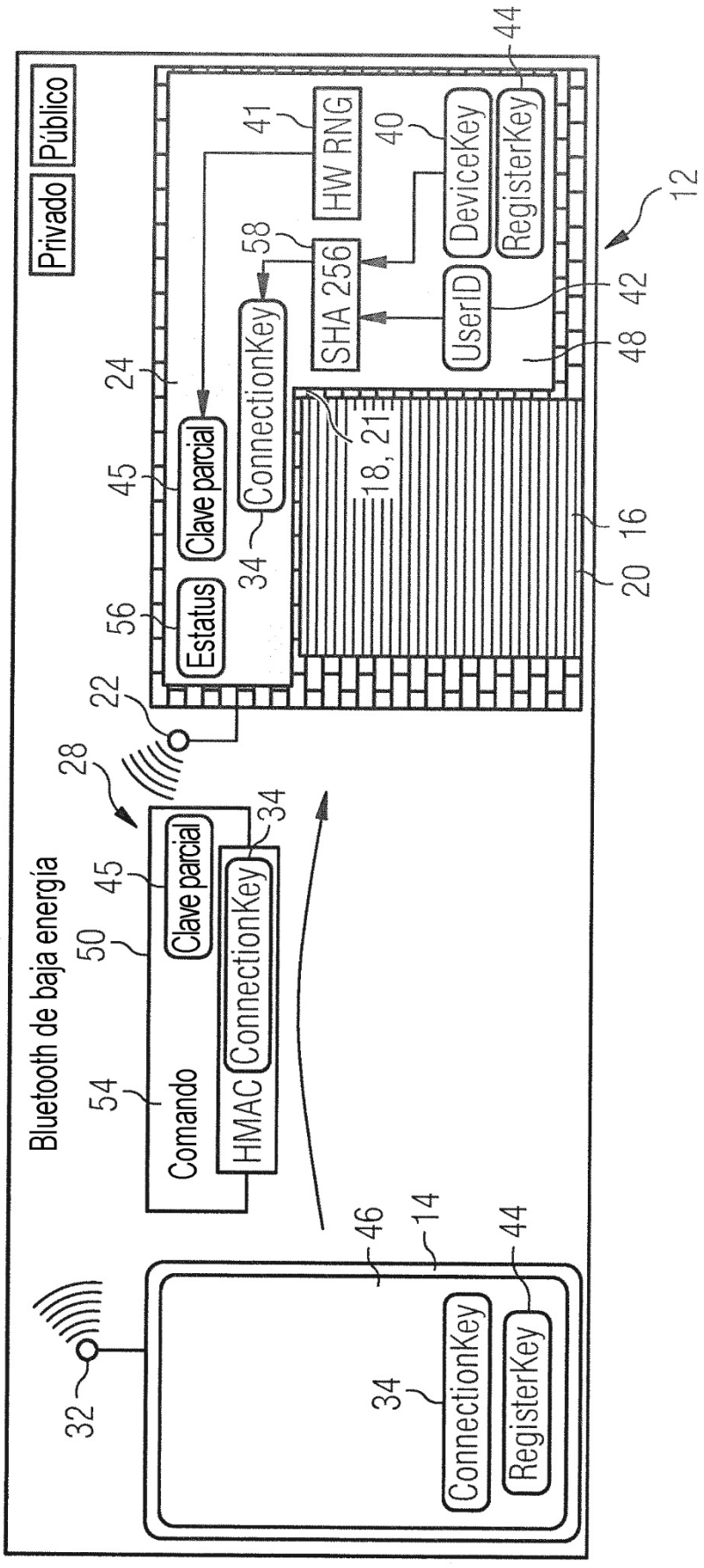

10
12
Privado
Público
Bluetooth de baja energía
Estatus
Clave parcial
ConnectionKey
HW RNG
SHA 256
DeviceKey
RegisterKey
UserID
18, 21
Comando
HMAC
ConnectionKey
Clave parcial
ConnectionKey
RegisterKey
22
24
28
32
34
40
41
42
44
45
46
48
50
54
56
58
16
20

FIG 2

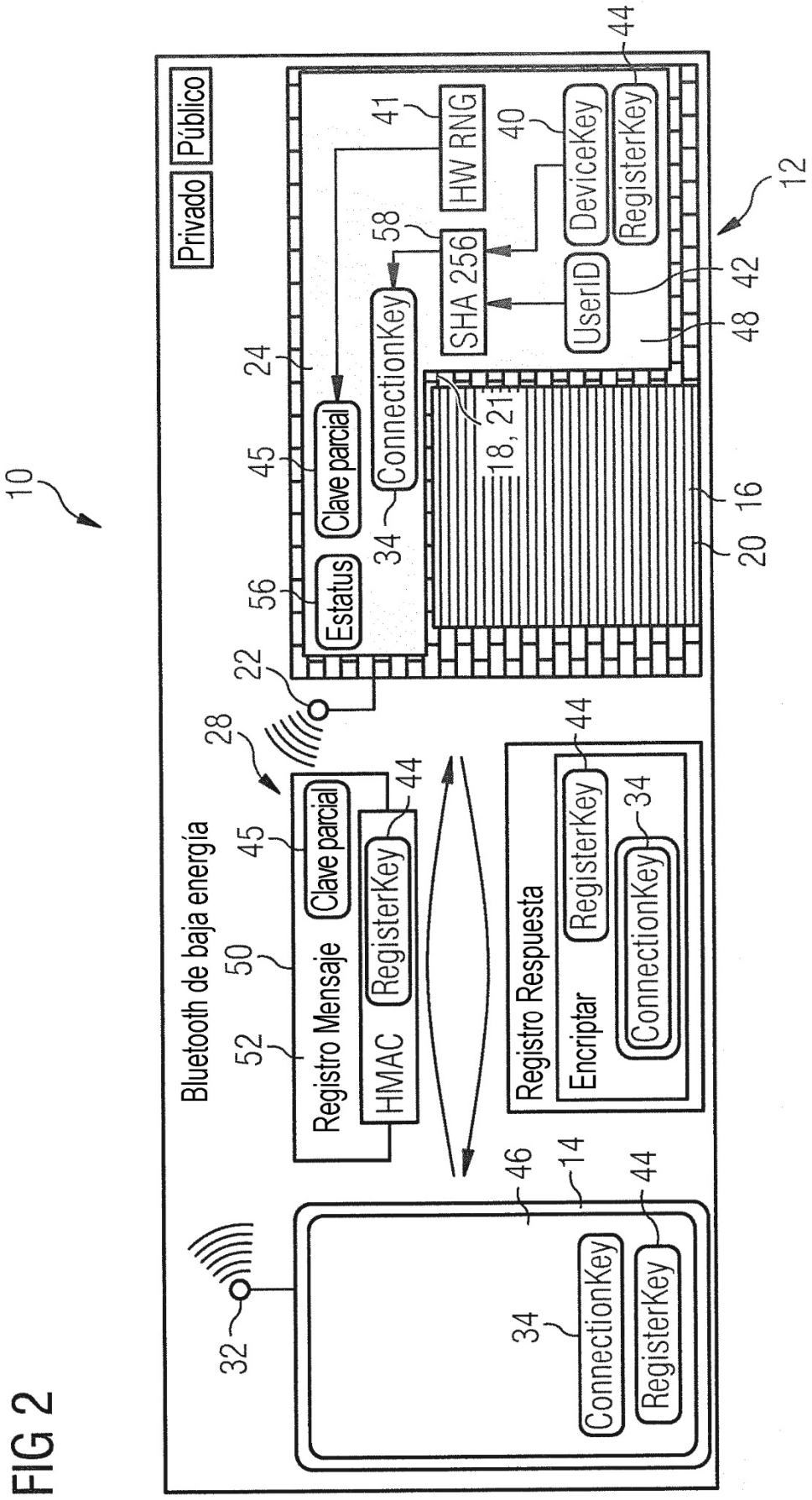
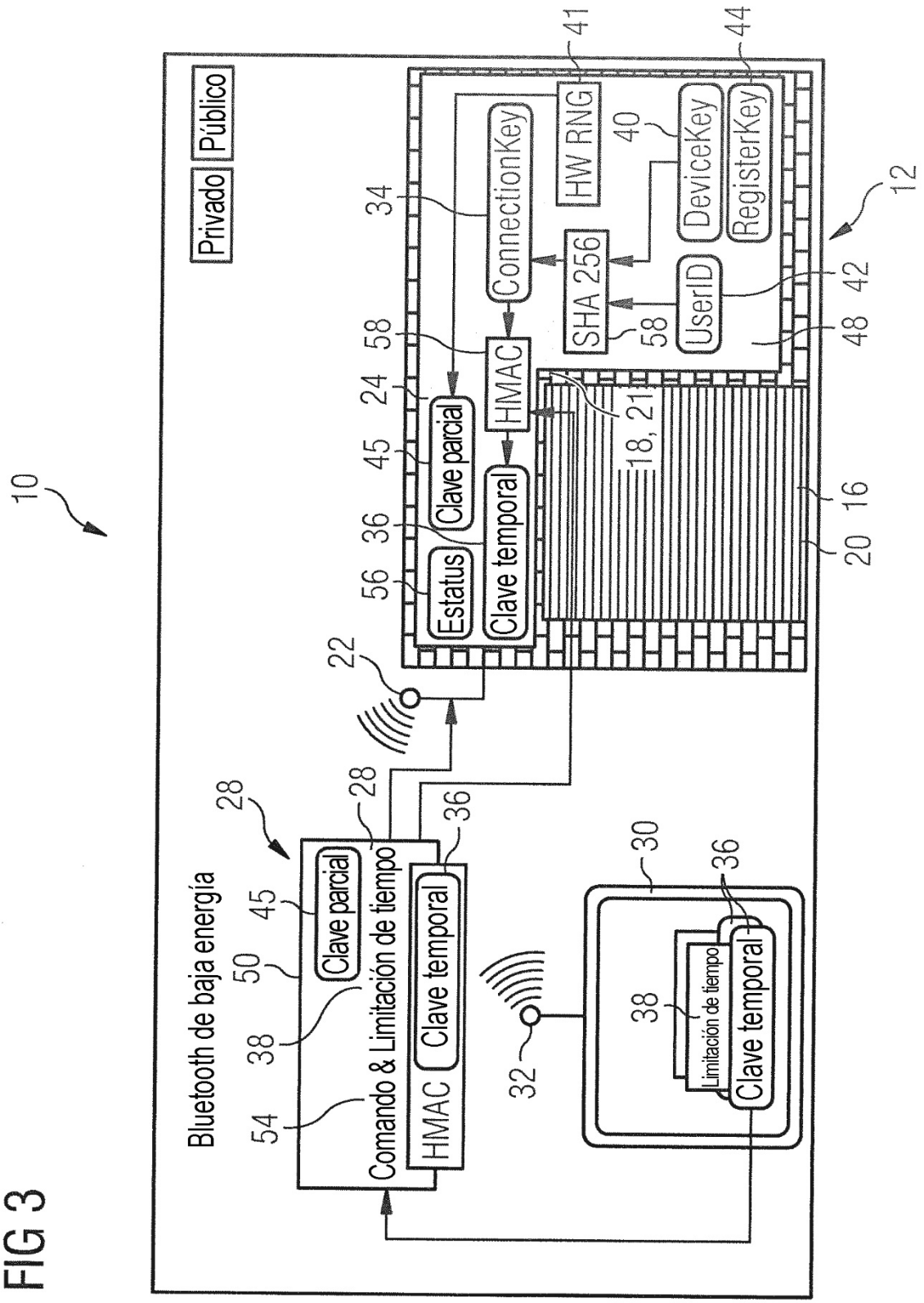

10
12
Privado
Público
Bluetooth de baja energía
HW RNG
41
DeviceKey
40
RegisterKey
44
SHA 256
58
UserID
42
48
ConnectionKey
34
Clave parcial
45
Estatus
56
24
18, 21
16
20
22
28
Registro Mensaje
50
Clave parcial
45
HMAC
52
RegisterKey
44
Registro Respuesta
Encriptar
RegisterKey
44
ConnectionKey
34
32
46
14
34
ConnectionKey
RegisterKey
44

FIG 3


10
Privado
Público
12
41
44
34
HW RNG
ConnectionKey
40
DeviceKey
RegisterKey
SHA 256
UserID
42
48
58
58
24
HMAC
18, 21
45
Clave parcial
36
Clave temporal
56
Estatus
16
20
22
28
28
36
30
36
Bluetooth de baja energía
Clave parcial
45
50
38
Comando & Limitación de tiempo
HMAC
Clave temporal
54
32
38
Limitación de tiempo
Clave temporal