(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 608 828**

(51) Int. CI.:

G07C 9/00 (2006.01)
G06K 7/10 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **17.10.2012 E 12188900 (0)**

(97) Fecha y número de publicación de la concesión europea: **28.09.2016 EP 2584539**

(54) Título: **Procedimiento para la configuración de una cerradura electromecánica**

(30) Prioridad:

20.10.2011 DE 102011054637

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
17.04.2017

(73) Titular/es:

ZACHER, MARC GASTON (100.0%)
Leistenstr. 12
97082 Würzburg, DE

(72) Inventor/es:

ZACHER, MARC GASTON

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Procedimiento para la configuración de una cerradura electromecánica

Campo técnico

La invención se refiere a un dispositivo para la configuración de una cerradura electromecánica.

Estado de la técnica

Las cerraduras electromecánicas intercambian datos con llaves correspondientes, siendo procesados o en la cerradura y/o en la llave los datos intercambiados, para comprobar una autorización de la llave. Según el resultado de la prueba, la cerradura habilita una autorización, por ejemplo el acceso al lugar asegurado por la cerradura o la posibilidad de cerrar una puerta.

Frecuentemente, las cerraduras electromecánicas están realizadas como llamadas cerraduras radioeléctricas. Estas cerraduras radioeléctricas comunican a través de un enlace radioeléctrico con llamadas llaves radioeléctricas y permiten de esta manera una comprobación de autorización sin contacto. La llave radioeléctrica puede ser por ejemplo un transpondedor pasivo que se pone delante de una cerradura radioeléctrica y después es leída por este. La distancia entre la llave radioeléctrica y la cerradura radioeléctrica generalmente es de sólo pocos cm (aprox. 0 a 50 cm). Alternativamente, la llave radioeléctrica puede tener un emisor activo que después del accionamiento de una tecla emite una señal que es recibida y evaluada por todas las cerraduras radioeléctricas en el alcance de emisión de habitualmente algunos metros (por ejemplo 0,5m a 50m). Este tipo se denomina como llave radioeléctrica activa. Este sistema ofrece la ventaja de que incluso con un acercamiento a la cerradura radioeléctrica puede accionarse la llave radioeléctrica y habilitarse la cerradura radioeléctrica.

Para la comprobación de la autorización de llaves eléctricas como por ejemplo llaves radioeléctricas, existe una multiplicidad de procedimientos, por ejemplo, las publicaciones para información de solicitud de patente DE4342641A1, DE19913931 y EP0671712A1 describen procedimientos de este tipo para la comprobación de la autorización de las llaves. Estos procedimientos consisten generalmente en si datos almacenados en la llave corresponden a datos almacenados en la cerradura. Al menos una parte de estos datos se transmite entre la cerradura y la llave a través de un protocolo de comunicación.

El documento DE10237715A1 describe una unidad de control de puerta para el acceso a un sistema de control de vehículo. La unidad de control de puerta puede recibir a través de un trayecto de datos datos de un servidor y está conectada a través de al menos un bus de vehículo a varios aparatos de control del vehículo para aplicar por la descarga de software o Remote Flashing nuevos códigos de programa en los aparatos de control. Para ello, el aparato de control de puerta se puede configurar libremente. Dicho de forma abreviada, la unidad de control de puerta se configura a través de un trayecto de datos de radio de tal forma que la unidad de control de puerta sirve a continuación de aparato de programación para un aparato de control.

El documento DE19701740A1 describe un sistema de cierre "Keyless Go" para un automóvil. El sistema de cierre tiene una llave en la que está almacenado un primer código relativamente largo que es consultado por el bloqueo de arranque y, dado el caso, lo habilita también. Además, esta llave tiene un segundo código más corto que ha de ser transmitido de forma correspondientemente rápida y se consulta para el desbloqueo de la puerta. Los códigos se transmiten de forma codificada de la manera habitual. La selección de un código correspondiente es realizada por la "cerradura" correspondiente, en concreto, o bien por un precomando o por la longitud de un número aleatorio transmitido por la cerradura que mediante el código correspondiente se codifica y después se vuelve a transmitir a la cerradura.

El documento DE10138217A1 propone indicar en una comunicación entre un transpondedor y una estación base información a la cabecera de los paquetes de datos acerca de los datos transmitidos en la sección central de los paquetes de datos, por ejemplo su identificador.

El documento WO2010/039598A2 parte de que las cerraduras electrónicas según el estado de la técnica comunican entre sí a través de una red común y entonces pueden ser configuradas a través de dicha red. Alternativamente, los dispositivos de control de acceso pueden ser configurados individualmente de forma directa. Estos dos modos de configurar cerraduras o bien se consideran demasiado complicados en cuanto al hardware o demasiado propensas a los errores. Por lo tanto, se propone localizar cada cerradura individualmente y ponerla en un modo de aprendizaje mediante una tarjeta Smart. En el modo de aprendizaje, la cerradura comunica con una PDA a través de un trayecto de datos de radio. Por medio de la PDA, la cerradura se integra en una posición de cierre y se somete al aprendizaje correspondiente.

El documento EP18035436A1 propone un lector de transpondedor que domina diferentes protocolos para poder comunicar de esta manera con diferentes transpondedores. Durante el aprendizaje de un transpondedor en un modo de programación, estos protocolos se prueban unos tras otros. Si un transpondedor reacciona a un protocolo determinado, a continuación, se consultan el tipo de transpondedor y un identificador de transpondedor. Esto se almacena entonces en el lector de transpondedor.

El documento WO0055796 describe de forma muy abstracta un procedimiento de comunicación entre un sistema de referencia y un lector. El sistema de referencia transmite al sistema de lectura informaciones para optimizar la velocidad de transmisión.

El documento US7,075,412B1 parte de la observación de que los protocolos para la comunicación de tags RFID con los lectores correspondientes se siguen perfeccionando constantemente. Esto requiere un reemplazo regular de los lectores. Para evitar esto, el software probablemente se adaptará como actualización de firmware al nuevo tag RFID.

El documento WO2008/144804 da a conocer un aparato de control de acceso que se configura con la ayuda de una tarjeta de chip de "Commisioning". En esta configuración se transmiten de la tarjeta de chip al aparato una ID de aparato y una clave de cifrado.

Exposición de la invención

La invención está basada en la observación de que existe una multitud de proveedores de sistemas de cierre electromecánicos, cuyos componentes no pueden intercambiarse o combinarse entre sí, aunque usen llaves radioeléctricas de la misma construcción que por ejemplo proceden de un proveedor común o están estandarizadas. Cuando uno se ha decidido por un sistema de cierre de un primer proveedor, se ha determinado el tipo de instalación de cierre y no se puede integrar posteriormente en la instalación de cierre existente una cerradura de otro proveedor, es decir que, generalmente, no es posible habilitarla y/o bloquearla con las llaves ya existentes del primer proveedor y/o añadirla a grupos de cierre existentes.

La invención tiene el objetivo de ofrecer un procedimiento con el que cerraduras electromecánicas de diferentes fabricantes puedan integrarse en un sistema de cierre.

Este objetivo se consigue mediante un procedimiento según la reivindicación 1. Formas de realización ventajosas de la invención se indican en las reivindicaciones subordinadas.

La invención está basada por una parte en el conocimiento de que una cerradura de un primer fabricante podría comunicar con llaves de un sistema de cierre de otro fabricante, pero que esto falla en la práctica porque los fabricantes usan diferentes protocolos de comunicación. Hasta ahora, estos protocolos de comunicación están codificados en el firmware correspondiente de las cerraduras y, por tanto, una vez suministrados ya no se pueden modificar o sólo con un gran esfuerzo. Por otra parte, la invención está basada en el conocimiento de que los protocolos de comunicación empleados entre una cerradura y una llave se pueden parametrizar. Por lo tanto, basta con transmitir a una cerradura la información sobre los parámetros del protocolo de comunicación empleado dentro de un determinado tipo de sistema de cierre, de tal forma que desde entonces pueda comunicar con estos parámetros y por tanto con otros componentes del tipo de sistema de cierre correspondiente. Por lo tanto, no es necesaria la complicada actualización de firmware si una cerradura debe "aprender" el protocolo de comunicación empleado en un tipo de instalación de cierre.

El procedimiento para la configuración de una cerradura electromecánica tiene al menos dos pasos; en concreto, como primer paso, la transmisión de al menos un parámetro de un primer soporte de datos a la cerradura según un primer protocolo de comunicación, y como paso posterior, la determinación de al menos un segundo protocolo de comunicación con la ayuda de los parámetros o del parámetro transmitidos según el primer protocolo de comunicación. Según el procedimiento, mediante la transmisión de informaciones necesarias para la comunicación entre componentes de un tipo de instalación de cierre determinado, una cerradura puede adaptarse a esta instalación de cierre determinada. Los componentes típicos de una instalación de cierre son generalmente llaves y cerraduras programables y generalmente también aparatos de programación. Por lo tanto, basta con prever un primer protocolo de comunicación, mediante el que los parámetros de al menos un tipo de instalación de cierre, es decir, los parámetros de un segundo protocolo de comunicación, pueden transmitirse a la cerradura y/o a al menos una llave. Después de la transmisión de los parámetros del segundo protocolo de comunicación, la cerradura se puede adaptar a un tipo de instalación de cierre determinado, lo que se puede activar por ejemplo mediante la transmisión. A continuación, la cerradura puede integrarse por ejemplo en una instalación de cierre existente de dicho tipo de instalación de cierre. Para la adaptación al tipo de instalación de cierre no es necesaria la instalación de un firmware dependiente del fabricante. Sólo mediante los parámetros transmitidos se garantiza que los datos transmitidos según el segundo protocolo de comunicación puedan ser interpretados correctamente por la cerradura. Dicho de otra manera, se transmiten informaciones a través del segundo protocolo de comunicación en un metalenguaje, a saber, el primer protocolo de comunicación, a la cerradura que entonces determina a partir de las informaciones transmitidas en el metalenguaje un lenguaje objeto, a saber, el segundo protocolo de comunicación. El lenguaje objeto puede contener patrones de comunicación, por ejemplo la longitud y la estructura de tramas que se intercambian según el segundo protocolo de comunicación, la velocidad de datos del segundo protocolo de comunicación así como informaciones sobre formatos de datos para informaciones que han de ser transmitidas según el segundo protocolo de comunicación, por ejemplo datos de fecha y/o de hora o algoritmos de codificación a usar. Un metalenguaje en el que se puede definir el segundo protocolo de comunicación puede ser por ejemplo XML o un lenguaje similar. A través del metalenguaje también se puede determinar una interfaz física, dicho de forma más general, un puerto del segundo protocolo de comunicación, por ejemplo, una frecuencia de emisión y/o de recepción determinada, una antena o una conexión.

Preferentemente, una comunicación según el primer protocolo de comunicación se tramita a través de la misma interfaz física o el mismo puerto que la comunicación según el segundo protocolo de comunicación. De esta manera, basta con prever una sola interfaz / puerto y se pueden reducir los costes de hardware. Por ejemplo, si la cerradura ha de integrarse en instalaciones de cierre en las que las llaves son exclusivamente transpondedores RFID pasivos, el primer protocolo de comunicación usa, al igual que los transpondedores RFID pasivos, la atenuación de un campo electromagnético emitido por la cerradura, para transmitir el al menos un parámetro según el primer protocolo de comunicación. Para ello, el al menos un parámetro puede estar almacenado por ejemplo en un transpondedor RFID y ser transmitido según el primer protocolo de comunicación. Alternativamente, los protocolos de comunicación evidentemente también pueden aprovechar diferentes canales de transmisión (= vías de transmisión). Por ejemplo, el segundo protocolo de comunicación puede prever una transmisión por la atenuación de un campo electromagnético emitido por la cerradura, previendo el primer protocolo de comunicación sin embargo la transmisión mediante una onda electromagnética de frecuencia modulada o mediante una conexión por cable.

El procedimiento se puede usar para todos los componentes de un sistema de cierre que comunican entre sí, es decir, no sólo para cerraduras. Por lo tanto, en realidad, es un procedimiento para la configuración de un componente de un sistema de cierre electromagnético. Sólo para mayor claridad, la invención se describe al ejemplo de una cerradura.

El componente, es decir, la cerradura, genera después de la transmisión de los parámetros el segundo protocolo de comunicación, es decir que tiene todas las informaciones para intercambiar con los demás componentes del tipo de instalación de cierre determinado por el segundo protocolo de comunicación. El intercambio de datos puede ser por ejemplo la realización de una consulta de autorización. El resultado puede ser por lo tanto también que una llave (como sinónimo de otro componente) no presente la autorización necesaria.

Preferentemente, las informaciones sobre la autorización de llaves de una instalación de cierre determinada se transmiten a la cerradura según el segundo protocolo de comunicación. Esto permite transmitir estas informaciones con las respectivas herramientas ("Tools") específicas del fabricante. En este caso, una cerradura se fabricaría con un firmware que contiene el primer protocolo de comunicación. La cerradura podría suministrarse entones a un intermediario comercial. El intermediario comercial puede entonces transmitir por medio del primer protocolo de comunicación los parámetros, con cuya ayuda la cerradura determina el segundo protocolo de comunicación. De esta manera, la cerradura se adapta a un tipo de instalación de cierre dado. En el siguiente paso, la cerradura se puede integrar en una instalación de cierre, por ejemplo, transmitiendo según el segundo protocolo de comunicación informaciones sobre llaves autorizadas.

En algunos tipos de sistema de cierre, la comprobación de autorización se realiza de tal forma que en primer lugar se establece un trayecto de datos seguro, es decir, codificado, entre las partes de comunicación. Para ello, se usan llamadas criptoclaves, que son valores que se deben mantener en secreto, con cuya ayuda de codifican y/o se descodifican los datos que han de ser transmitidos. Si las criptoclaves de dos partes de comunicación no corresponden una a otra, no se puede establecer un trayecto de datos seguro; no obstante, las partes de comunicación comunican entre sí, ya que por el segundo protocolo de comunicación son capaces de intercambiar los datos necesarios para establecer el trayecto de datos seguro. Este intercambio también se inicia correctamente, pero la comprobación de autorización se suspende porque la comprobación de las criptoclaves arroja que no corresponden una a otra. En la mayoría de las instalaciones de cierre, la criptoclave no forma parte de los parámetros del tipo de instalación de cierre, pero generalmente sí el algoritmo de codificación. Sin embargo, el algoritmo de codificación también puede estar predeterminado por un estándar y entonces preferentemente está depositado en el hardware o el firmware.

Si las criptoclaves se corresponden una a otra, esto generalmente se valora como "autorización fundamental". En algunos tipos de instalación de cierre, datos adicionales, depositados en la llave y/o la cerradura se comparan entre sí, por ejemplo, si la llave tiene una autorización para una puerta y/o un grupo de cierre determinados, si la autorización está limitada temporalmente, si hay excepciones dentro del grupo de cierre etc… Estas informaciones adicionales también se evalúan antes de la habilitación de la cerradura correspondiente.

Los parámetros del segundo protocolo de comunicación generalmente no son las informaciones pertenecientes a un objeto o edificio determinados (en lo sucesivo "información específica del objeto"), como el número de instalación de cierre o la pertenencia de un componente a un grupo de cierre determinado, sino las informaciones que son necesarias para poder leer y/o escribir informaciones específicas del objeto, si existe la autorización para ello. En una forma de realización de la invención, el término parámetro no designa necesariamente los comandos disponibles para la comunicación, preferentemente designa al menos las informaciones necesarias para la asignación de datos transmitidos a variables dadas. Esto es importante especialmente si según un protocolo de comunicación, los valores de varias variables se intercambian sucesivamente como secuencia de bits.

Como "parámetro" se designa cualquier información que se transmite del soporte de datos a la cerradura según el primer protocolo de comunicación para determinar el segundo protocolo de comunicación. Como "datos", en cambio, se designa todo aquello que se transmite según el segundo protocolo de comunicación. Cualquier tipo de memoria se puede usar como soporte de datos del que el al menos un parámetro del segundo protocolo de comunicación se transmite a la cerradura mediante el primer protocolo de comunicación. Las memorias típicas son memorias

magnéticas, memorias de semiconductores y memorias ópticas.

Preferentemente, la cerradura comunica por medio del segundo protocolo de comunicación con al menos una llave. Por lo tanto, con una parametrización correspondiente, la cerradura puede comunicar con llaves de cualquier tipo de instalación de cierre y, por lo tanto, se puede implementar en ese tipo de instalación de cierre.

Preferentemente, al menos el tamaño de los espacios vectoriales de las puertas y/o de las llaves y/o de los grupos de cierre se transmite como al menos un parámetro. Frecuentemente, estos tamaños son esenciales para la administración de memoria de la cerradura y/o de la llave así como para la longitud de bits de la variable y los campos correspondientes, porque en muchos sistemas de cierre durante la comprobación de autorización se intercambia la información en qué cerraduras y/o grupos de cierre está autorizada la llave correspondiente. Todas las puertas, grupos de cierre y llaves de una instalación de cierre forman la base para el espacio vectorial binario T, G o S correspondiente. Por tanto, las dimensiones de los espacios vectoriales T, G, S correspondientes limitan el número máximo de las cerraduras, grupos de cierre o llaves integrables en la instalación de cierre del tipo de instalación de cierre dado. La dimensión del espacio vectorial correspondiente es una información sobre el espacio de memoria necesario para la representación de los vectores, que es relevante para la extracción de estos vectores a partir de una secuencia de bits. Por ejemplo, el espacio vectorial G de los grupos se pueden representar como

$$\vec{\gamma} = \begin{pmatrix} \gamma_1 \\ \gamma_2 \\ \vdots \\ \gamma_m \end{pmatrix}; \ \gamma_i \in \{0,1\},$$

donde m es la dimensión del espacio vectorial y por tanto indica el número máximo de grupos de cierre administrables en el tipo de instalación de cierre dado. Un vector binario de la longitud m se almacena en algunos tipos de sistema de cierre tanto en la llave ($\vec{\gamma}$) como en la puerta (p). Una autorización de una llave determinada en una puerta determinada puede existir si el producto escalar $\vec{\gamma} \cdot \vec{\rho} = 1$. De manera correspondiente, en la comprobación de autorización se transmiten o bien $\vec{\gamma}$ o/o p y respectivamente el otro componente y m puede ser un parámetro relevante para evaluar una secuencia de bits que contiene un vector $\vec{\gamma}$. De manera correspondiente, también la representación de vectores binarios, como por ejemplo los vectores binarios de los espacios vectoriales T,G,S, puede ser parámetros del segundo protocolo de comunicación. Preferentemente, durante la transmisión de los parámetros se transmite una cabecera que caracteriza informaciones siguientes de la transmisión como parámetros del segundo protocolo de comunicación. De esta manera, con la ayuda de la cabecera, la cerradura puede distinguir si se produce una comunicación con una llave o si se adapta a un tipo de sistema de cierre.

Preferentemente, parámetros del segundo protocolo de comunicación se transmiten en bloques, identificando una sección de bloque determinada el parámetro y al menos una sección de bloque adicional el valor del parámetro. Preferentemente, el bloque contiene una indicación sobre su tamaño. Esto aumenta la flexibilidad del primer protocolo de comunicación y permite omitir parámetros no requeridos.

Un parámetro preferible de un segundo protocolo de comunicación es por ejemplo el tipo de codificación de la comunicación entre la cerradura y la llave, o el tipo de representación de limitaciones de tiempo de autorizaciones.

Otro parámetro preferible es el tipo de la consulta de datos de la cerradura o de la llave. Por ejemplo, el segundo protocolo de comunicación puede permitir una lectura y/o un acceso de escritura directos a determinadas áreas de memoria de la parte de comunicación correspondiente. Entonces, también las direcciones de salto (pointer) a las posiciones de memoria correspondientes son preferentemente parámetros del segundo protocolo de comunicación., Especialmente, durante la transmisión de los parámetros se puede transmitir la información acerca de cómo ha de ser interpretada una secuencia de bits transmitida según el segundo protocolo de comunicación. Algunos tipos de instalación de cierre leen durante la comprobación de una autorización de una llave datos de áreas de memoria estandarizadas de la llave, por ejemplo de un transpondedor RFID pasivo. Estos datos preferentemente se transmiten como secuencia de bits en la que están depositados los valores de dos o más variables. A continuación, los valores de las distintas variables se extraen para la comprobación de la autorización, como por ejemplo un número de grupo de cierre, un número de puerta etc., se extraen de la secuencia de bits. Las informaciones sobre las posiciones de los valores de las variables de la secuencia de bits preferentemente se transmiten según el primer protocolo de comunicación.

Preferentemente, al menos un parámetro en la cerradura tiene un valor estándar (valor por defecto) que durante la transmisión de las informaciones puede ser sustituido por otro valor. De esta manera, se puede reducir la cantidad de información que ha de ser transmitida y puede haber un "protocolo por defecto". Entonces basta con transmitir a la cerradura las diferencias del segundo protocolo de comunicación.

Preferentemente, se transmite al menos una información que representa el formato de datos de los datos almacenados o a almacenar en la llave y/o la cerradura. Por ejemplo, datos pueden ser almacenados y/ transmitidos de forma comprimida. Entonces, también la información de si y, si es el caso, qué procedimiento de compresión se aplica sería un parámetro transmitido preferentemente del segundo protocolo de comunicación.

Preferentemente, se transmite al menos una información que corresponde a al menos una dirección de memoria en al menos una llave de la que se leen datos para la comprobación de la autorización de la llave. Por ejemplo, se puede transmitir una dirección de entrada para la lectura de una criptoclave.

Preferentemente, se transmite al menos un parámetro, con cuya ayuda se selecciona un procedimiento de codificación para la protección de datos transmitidos según el segundo protocolo de comunicación. Entonces, la cerradura se puede emplear en sistemas de cierre con diferentes procedimientos de codificación.

Igualmente, la información sobre un determinado tipo de instalación de cierre se puede transmitir como parámetro a la cerradura. En este caso, en la cerradura está depositado para al menos un tipo de instalación de cierre un bloque de parámetros correspondiente. La transmisión de un solo tipo de instalación de cierre puede realizarse de forma sensiblemente más rápida que la transmisión de un bloque de parámetros entero. De esta manera, se puede reducir considerablemente el tiempo para el aprendizaje de la cerradura.

Preferentemente, las informaciones se transmiten del soporte de datos a través de la misma interfaz, a través de la que se realiza posteriormente también la comunicación con las llaves. De esta manera, se evitan interfaces adicionales y por tanto costes. Por ejemplo, puede ser suficiente poner delante de una cerradura un primer transpondedor RFID con los parámetros, de tal forma que puedan comunicar el primer transpondedor RFID y la cerradura para remitir de esta manera los parámetros para la comunicación posterior con las llaves que igualmente son transpondedores RFID. Después se produce la comunicación con el primer transpondedor RFI a través del primer protocolo de comunicación y la comunicación con los transpondedores RFI adicionales según el segundo protocolo de comunicación.

Preferentemente, durante la transmisión se remiten informaciones a al menos dos protocolos de comunicación. Entonces, una cerradura puede estar integrada al mismo tiempo en dos o más instalaciones de cierre de distintos tipos. Entonces, por ejemplo, puede intentar en primer lugar una comunicación con una llave según un primer segundo protocolo de comunicación y, si esta falla, una comunicación según al menos un segundo protocolo de comunicación adicional.

La invención se ha descrito con la ayuda de una cerradura que se ha de ajustar a una instalación de cierre. Sin embargo, las cerraduras y las llaves electrónicas básicamente se pueden intercambiar entre sí - exceptuando sus componentes mecánicos. Por ello, de la misma manera, también se puede adaptar una llave a un tipo de instalación de cierre dado. Lo mismo es válido para cualquier otro componente de una instalación de cierre que comunique con una llave o una cerradura.

Según la invención no se graba firmware nuevo en la cerradura. Al código de programa del firmware tan sólo se transmiten, por medio del al menos un parámetro transmitido según el primer protocolo de comunicación, las informaciones para la determinación del segundo protocolo de comunicación que se ha de usar a continuación. Habitualmente, el firmware se encuentra en una memoria de programas. El al menos un parámetro preferentemente no se descarga a la memoria de programas, sino a una memoria de datos.

Después de haberse determinado el segundo protocolo de comunicación, se pone un indicador preferentemente duradero que evita un cambio del segundo protocolo de comunicación. De esta manera, se incrementa la seguridad de manipulación de la cerradura.

Descripción de los dibujos

A continuación, la invención se describe con la ayuda de ejemplos de realización haciendo referencia al único dibujo como ejemplo.

En el procedimiento en la figura 1, un componente de un sistema de cierre electromecánico, por ejemplo una cerradura 10 electromecánica comunica con un soporte de datos 20 según un primer protocolo de comunicación dado, es decir, conocido por la cerradura 10 y el soporte de datos 20. El soporte de datos 20 puede ser por ejemplo la tarjeta de transpondedor RFID representada. La cerradura 10 está representada aquí por ejemplo como cilindro con pomo. Para la comunicación, entre la cerradura 10 y el soporte de datos 20 en primer lugar se establece un trayecto de datos 30 codificado y, a continuación, se transmite del soporte de datos 10 una cabecera 31 a la cerradura 20. Con la ayuda de la cabecera 31, la cerradura reconoce si a continuación se transmiten o no parámetros 33 de un segundo protocolo de comunicación que pertenece a un tipo de instalación de cierre determinado. Si como se indica se han de transmitir parámetros 33, se pasa a un "modo de aprendizaje" indicado por una flecha 32. En el modo de aprendizaje se parametriza un segundo protocolo de comunicación con la ayuda de los parámetros 33 transmitidos. Ahora, la cerradura puede integrarse en una instalación de cierre concreta, por ejemplo comunicándola una ID de cerradura 34, y/o una ID de grupo 35 y/o parámetros de codificación 36 de la instalación de cierre concreta. Esto se puede realizar entonces con la ayuda del segundo protocolo de

comunicación, por ejemplo, por medio de un soporte de datos 22 separado, una unidad de configuración (no representada) o una central de la instalación de cierre (no representada). La cerradura 10 tiene ahora todas las informaciones que necesita para comprobar la autorización 37 de una llave 24 de las instalaciones de cierre.

También son posibles otras posibilidades de iniciar el modo de aprendizaje. Por ejemplo, en un soporte de datos puede estar depositado un archivo con un nombre de archivo predeterminado, que contiene al menos un parámetro. La cerradura consulta al soporte de datos si presenta un archivo con un nombre determinado. Si es el caso, se pasa al modo de aprendizaje, es decir que lee el al menos un parámetro del soporte de datos, por ejemplo de un archivo, y con la ayuda del al menos un parámetro determina el segundo protocolo de comunicación. A continuación, preferentemente se pone un indicador, por ejemplo un bit, que impide una nueva llamada del modo de aprendizaje. Para ello, la cerradura preferentemente consulta el indicador y sólo si no está puesto el indicador comprueba si debe pasar al modo de aprendizaje o no. El indicador puede comprobarse en cualquier momento antes de la configuración del segundo protocolo de comunicación. El sentido de la consulta del indicador es impedir que un segundo protocolo de comunicación una vez determinado sea sustituido por un nuevo segundo protocolo de comunicación para evitar manipulaciones.

Lista de signos de referencias

10 Cerradura
20 Soporte de datos / tarjeta RFID
24 Llave
30 Trayecto de datos codificado
31 Cabecera (encabezamiento de datos)
32 Modo de aprendizaje
33 Parámetros
34 ID de cerradura
35 ID de grupos
36 Parámetros de codificación
37 Autorización

REIVINDICACIONES

1. Procedimiento para configurar un componente de un sistema de cierre electromecánico, que presenta al menos los pasos:

- la transmisión de al menos un parámetro de un primer soporte de datos al componente según un primer protocolo de comunicación,
- la generación de al menos un segundo protocolo de comunicación después de la transmisión con la ayuda de los parámetros o del parámetro transmitidos según el primer protocolo de comunicación por medio del componente mediante la parametrización del segundo protocolo de comunicación con la ayuda de los parámetros transmitidos,
- la puesta de un indicador en el componente después de la generación, impidiendo el componente una nueva modificación del segundo protocolo de comunicación cuando está puesto el indicador,
- la inserción del componente en el sistema de cierre electromecánico después de la generación mediante la comunicación de una ID de cerradura (34) y/o de una ID de grupo (35) y/o de parámetros de codificación (36) al componente por medio del segundo protocolo de comunicación y
- el intercambio de datos con otros componentes del sistema de cierre por medio del segundo protocolo de comunicación.

2. Procedimiento según la reivindicación 1, **caracterizado porque** el componente es una cerradura y porque la cerradura se integra en una instalación de cierre, de tal forma que a la cerradura se transmiten según el segundo protocolo de comunicación informaciones sobre llaves autorizadas.

3. Procedimiento según la reivindicación 1 o 2, **caracterizado porque** como parámetros (33) se transmite al menos la posición de al menos un valor de al menos una variable en una secuencia de bits que se intercambia según el segundo protocolo de comunicación.

4. Procedimiento según cualquiera de las reivindicaciones anteriores, **caracterizado porque** el componente (10) comunica por medio del segundo protocolo de comunicación con al menos una llave (24).

5. Procedimiento según cualquiera de las reivindicaciones anteriores, **caracterizado porque** informaciones sobre la autorización de llaves (24) de una instalación de cierre determinada se transmiten a una cerradura (10) según el segundo protocolo de comunicación.

6. Procedimiento según cualquiera de las reivindicaciones anteriores, **caracterizado porque** como parámetros (33) se transmite al menos el tamaño de los espacios vectoriales de las puertas y/o de las llaves (24) y/o de los grupos de cierre.

7. Procedimiento según cualquiera de las reivindicaciones anteriores, **caracterizado porque** durante la transmisión por medio del primer protocolo de comunicación, antes del parámetro se transmite una cabecera (31) que caracteriza informaciones siguientes como parámetros (33) del segundo protocolo de comunicación.

8. Procedimiento según cualquiera de las reivindicaciones anteriores, **caracterizado porque** los parámetros (33) se transmiten en bloques, identificando una sección de bloque determinada el parámetro (33) y al menos una sección de bloque adicional el valor del parámetro (33).

9. Procedimiento según cualquiera de las reivindicaciones anteriores, **caracterizado porque** se transmite al menos un parámetro (33) que corresponde al formato de datos de los datos almacenados o a almacenar en la llave (24) y/o la cerradura (10).

10. Procedimiento según cualquiera de las reivindicaciones anteriores, **caracterizado porque** se transmite al menos un parámetro (33) que corresponde a al menos una dirección de memoria en al menos una llave (24), de la que se leen datos para la comprobación de la autorización de la llave (24).

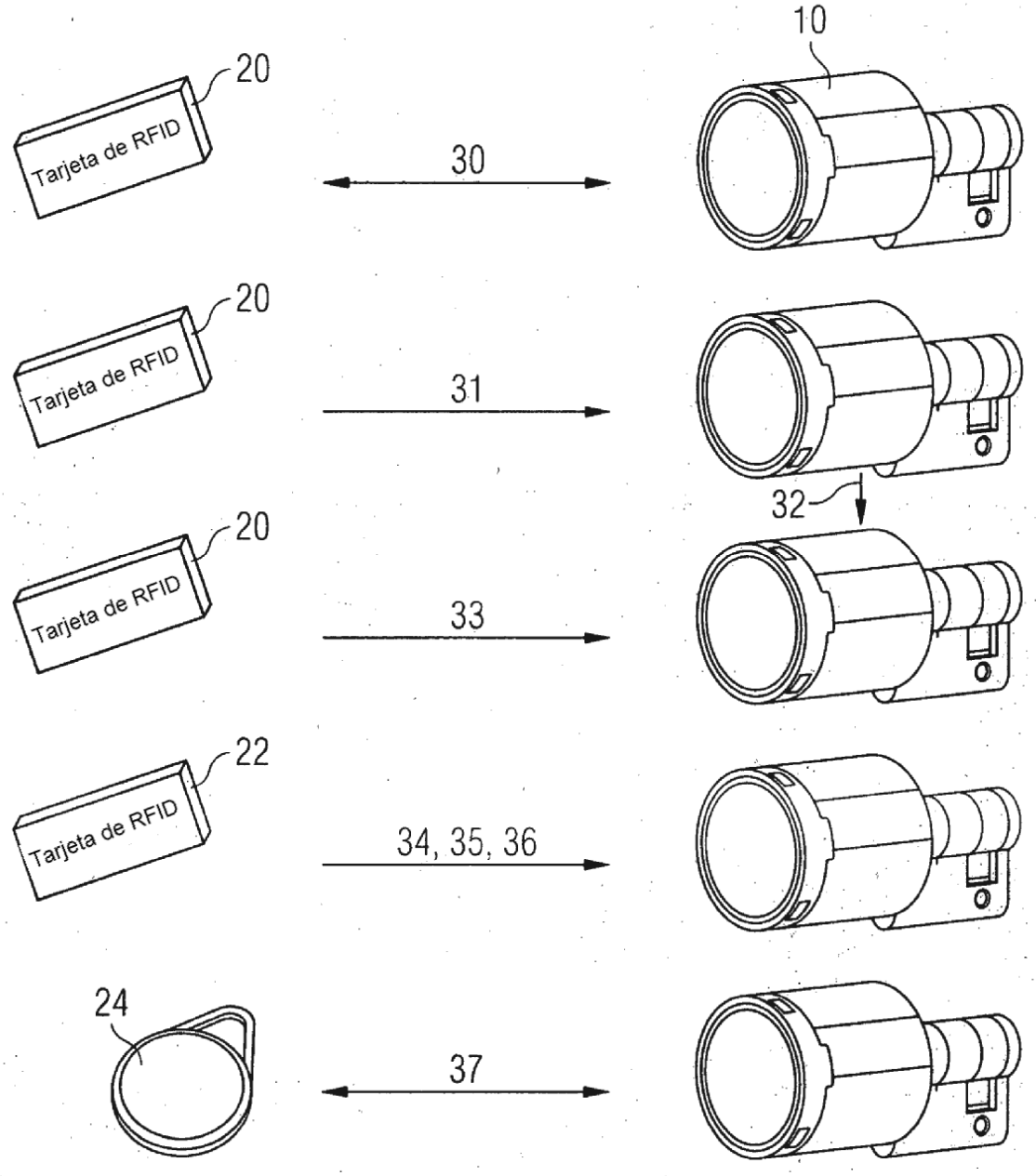
11. Procedimiento según cualquiera de las reivindicaciones anteriores, **caracterizado porque** se transmite al menos un parámetro (33), con cuya ayuda se selecciona un procedimiento de codificación para la protección de datos transmitidos según el segundo protocolo de comunicación.

12. Procedimiento según cualquiera de las reivindicaciones anteriores, **caracterizado porque** se transmite la información sobre la pertenencia de la cerradura (10) a una instalación de cierre determinada.

13. Procedimiento según cualquiera de las reivindicaciones anteriores, **caracterizado porque** se transmite al menos un parámetro, con cuya ayuda se determina un formato de datos para el almacenamiento y/o la transmisión de una indicación de fecha y/o de una indicación de hora y/o de un período de tiempo de autorización.

14. Procedimiento según cualquiera de las reivindicaciones anteriores, **caracterizado porque** la transmisión del al menos un parámetro se realiza a través de una primera interfaz física y porque la transmisión de datos según el segundo protocolo de comunicación se realiza a través de la misma interfaz física.

Fig. 1


10
20
Tarjeta de RFID
30
20
Tarjeta de RFID
31
32
20
Tarjeta de RFID
33
22
Tarjeta de RFID
34, 35, 36
24
37