(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 2 584 539 B1

(12) **EUROPÄISCHE PATENTSCHRIFT**

(45) Veröffentlichungstag und Bekanntmachung des Hinweises auf die Patenterteilung:
28.09.2016 Patentblatt 2016/39

(51) Int Cl.:
G07C 9/00 *(2006.01)* ***G06K 7/10*** *(2006.01)*

(21) Anmeldenummer: **12188900.0**

(22) Anmeldetag: **17.10.2012**

(54) **Verfahren zum Konfigurieren eines elektromechanischen Schlosses**

Method for configuring an electromechanical lock

Procédé de configuration d'une serrure électromécanique

(84) Benannte Vertragsstaaten:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

(30) Priorität: **20.10.2011 DE 102011054637**

(43) Veröffentlichungstag der Anmeldung:
24.04.2013 Patentblatt 2013/17

(73) Patentinhaber: **Zacher, Marc Gaston**
97082 Würzburg (DE)

(72) Erfinder: **Zacher, Marc Gaston**
97082 Würzburg (DE)

(74) Vertreter: **Jöstingmeier, Martin**
Lohr, Jöstingmeier & Partner
Junkersstraße 3
82178 Puchheim (DE)

(56) Entgegenhaltungen:
EP-A2- 1 835 436
WO-A1-00/55796
WO-A1-2008/144804
WO-A2-2010/039598
US-A- 4 924 210
US-A1- 2008 290 995
US-B1- 7 075 412

Anmerkung: Innerhalb von neun Monaten nach Bekanntmachung des Hinweises auf die Erteilung des europäischen Patents im Europäischen Patentblatt kann jedermann nach Maßgabe der Ausführungsordnung beim Europäischen Patentamt gegen dieses Patent Einspruch einlegen. Der Einspruch gilt erst als eingelegt, wenn die Einspruchsgebühr entrichtet worden ist. (Art. 99(1) Europäisches Patentübereinkommen).

EP 2 584 539 B1

Printed by Jouve, 75001 PARIS (FR)

Beschreibung

Technisches Gebiet

[0001] Die Erfindung betrifft ein Verfahren zum Einrichten eines elektromechanischen Schlosses.

Stand der Technik

[0002] Elektromechanische Schlösser tauschen Daten mit entsprechenden Schlüsseln aus, wobei entweder im Schloss und/oder im Schlüssel die ausgetauschten Daten verarbeitet werden, um eine Berechtigung des Schlüssels zu überprüfen. Je nach Ergebnis der Prüfung gibt das Schloss eine Berechtigung frei, z.B. den Zugang zu einem durch das Schloss gesicherten Ort, oder die Möglichkeit eine Tür zu verriegeln.

[0003] Elektromechanische Schlösser sind oft als sogenannte Funkschlösser realisiert. Diese Funkschlösser kommunizieren über eine Funkverbindung mit sogenannten Funkschlüsseln und ermöglichen so eine berührungslose Berechtigungsprüfung. Der Funkschlüssel kann z.B. ein passiver Transponder sein, der vor ein Funkschloss gehalten und dann von diesem ausgelesen wird. Dabei beträgt der Abstand zwischen dem Funkschlüssel und dem Funkschloss in der Regel nur wenige cm (ca. 0 - 50cm). Alternativ kann der Funkschlüssel einen aktiven Sender haben, der nach Betätigung eines Tasters ein Signal sendet, welches von allen Funkschlössern im Sendebereich von üblicherweise einigen Metern (etwa 0,5m - 50m) empfangen und ausgewertet wird. Dieser Typ wird als aktiver Funkschlüssel bezeichnet. Dieses System hat den Vorteil, dass schon bei einer Annäherung an das Funkschloss der Funkschlüssel betätigt und das Funkschloss freigegeben werden kann.

[0004] Zur Überprüfung der Berechtigung von elektrischen Schlüsseln, wie z.B. Funkschlüsseln gibt es eine Vielzahl von Verfahren, beispielsweise beschreiben die Offenlegungsschriften DE 43 42 641 A1, DE 199 13 931 und EP 0 671 712 A1 solche Verfahren zum Überprüfen der Berechtigung von Schlüsseln. Solche Verfahren beruhen in der Regel darauf, ob im Schlüssel gespeicherte Daten zu im Schloss gespeicherten Daten passen. Zumindest ein Teil dieser Daten wird über ein Kommunikationsprotokoll zwischen Schloss und Schlüssel übertragen.

[0005] DE 102 37 715 A1 beschreibt eine Gateway-Steuereinheit zum Zugriff auf ein Fahrzeugsteuersystem. Die Gateway-Steuereinheit kann über eine Funkdatenstrecke Daten von einem Server empfangen und ist über wenigstens einen Fahrzeugbus an mehrere Steuergeräte des Fahrzeugs angebunden, um per Software Download bzw. Remote Flashing neue Programmcodes auf die Steuergeräte aufzubringen. Das Gateway-Steuergerät kann dafür frei konfiguriert werden. Verkürzt formuliert wird die Gateway-Steuereinheit über eine Funkdatenstrecke so konfiguriert, dass die Gateway-Steuereinheit anschließend als Programmiergerät für ein Steuergerät dient.

[0006] DE 197 01 740 A1 beschreibt ein "Keyless Go" Schließsystem für ein Kraftfahrzeug. Das Schließsystem hat einen Schlüssel, in dem ein erster vergleichsweise langer Code gespeichert ist, der von der Wegfahrsperre abgefragt wird und diese gegebenenfalls frei schaltet. Zudem hat dieser Schlüssel einen zweiten kürzeren Code, der entsprechend schnell zu übertragen ist und zur Entriegelung der Tür abgefragt wird. Die Codes werden, wie üblich, verschlüsselt übertragen. Das Auswählen eines entsprechenden Codes erfolgt durch das jeweilige "Schloss" und zwar entweder durch ein Precommand oder durch die Länge einer vom Schloss übertragenen Zufallszahl, die mittels des entsprechenden Codes verschlüsselt und dann zum Schloss zurück übertragen wird.

[0007] DE 101 38 217 A1 schlägt vor, bei einer Kommunikation zwischen einem Transponder und einer Basisstation dem Header der Datenpakete Informationen über die im Mittelabschnitt der Datenpakete übertragenen Daten, z.B. deren Kennung, anzugeben.

[0008] WO 2010/039598 A2 geht davon aus, dass elektronische Schlösser nach dem Stand der Technik über ein gemeinsames Netzwerk miteinander kommunizieren und dann über dieses Netzwerk konfiguriert werden. Alternativ können die Zugangskontrolleinrichtungen individuell unmittelbar konfiguriert werden. Diese beiden Arten, Schlösser zu konfigurieren, werden als entweder hardwaremäßig zu aufwändig oder fehleranfällig angesehen. Daher wird vorgeschlagen jedes Schloss einzeln aufzusuchen und durch eine Smart-Card in einen Lernmodus zu bringen. In dem Lernmodus kommuniziert das Schloss über eine Funkdatenstrecke mit einem PDA. Mittels des PDA wird das Schloss in eine Schließlage integriert und entsprechend angelernt.

[0009] EP 1 8035 436 A1 schlägt ein Transponder-Lesegerät vor, das unterschiedliche Protokolle beherrscht, um dadurch mit verschiedenen Transpondern kommunizieren zu können. Beim Anlernen eines Transponders in einem Programmiermodus werden diese Protokolle der Reihe nach ausprobiert. Reagiert ein Transponder auf ein bestimmtes Protokoll, werden anschließend der Transpondertyp und eine Transponderkennung abgefragt. Dies wird dann in dem Transponder-Lesegerät gespeichert.

[0010] WO 00 55 796 beschreibt sehr abstrakt ein Kommunikationsverfahren zwischen einem Referenzsystem und einem Lesegerät. Das Referenzsystem überträgt auf das Lesesystem Informationen um die Übertragungsgeschwindigkeit zu optmieren.

[0011] US 7,075,412 B1 geht von der Beobachtung aus, dass sich die Protokolle zur Kommunikation von RFID-Tags mit den entsprechenden Lesegeräten ständig weiter entwickeln. Das bedinge einen regelmäßigen Austausch der Lesegeräte. Um dies zu vermeiden wird die Software vermutlich als Firmwareupdate an das die neuen RFID-Tags angepasst.

[0012] WO 2008/144804 offenbart ein Zugangskont-

rollgerät, das mit Hilfe von einer "Commisioning"-Chipkarte konfiguriert wird. Bei dieser Konfiguration werden eine Geräte-ID und Chiffrierschlüssel von der Chipkarte an das Gerät Übertragen.

Darstellung der Erfindung

[0013] Der Erfindung liegt die Beobachtung zugrunde, dass es eine Vielzahl von Anbietern elektromechanischer Schließsysteme gibt, deren Komponenten nicht gegeneinander austauschbar oder miteinander kombinierbar sind, obgleich sie baugleiche Funkschlüssel einsetzen, die z.B. von einem gemeinsamen Lieferanten stammen oder standardisiert sind. Hat man sich für ein Schließsystem eines ersten Anbieters entschieden, ist der Schließanlagentyp festgelegt und kann man später ein Schloss eines anderen Anbieters nicht in die dann bestehende Schließanlage integrieren, d.h. in der Regel nicht mit den schon vorhandenen Schlüsseln des ersten Anbieters freigeben und/oder sperren und/oder sie zu bestehenden Schließgruppen hinzufügen.

[0014] Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren anzubieten, mit dem elektromechanische Schlösser verschiedener Hersteller in ein Schließsystem integriert werden können.

[0015] Diese Aufgabe wird durch ein Verfahren nach Anspruch 1 gelöst. Vorteilhafte Ausgestaltungen der Erfindung sind in den Unteransprüchen angegeben.

[0016] Die Erfindung beruht zum einen auf der Erkenntnis, dass ein Schloss eines ersten Herstellers theoretisch zwar mit Schlüsseln eines Schließsystems eines anderen Herstellers kommunizieren könnte, dass dies jedoch in der Praxis fehlschlägt, weil die Hersteller unterschiedliche Kommunikationsprotokolle verwenden. Diese Kommunikationsprotokolle sind bisher in der jeweiligen Firmware der Schlösser kodiert und somit nach der Auslieferung nicht mehr oder nur mit großem Aufwand veränderbar. Zum anderen beruht die Erfindung auf der Erkenntnis, dass die verwendeten Kommunikationsprotokolle zwischen einem Schloss und einen Schlüssel parametrisierbar sind. Deshalb genügt, es einem Schloss die Informationen über die Parameter des innerhalb eines bestimmten Schließsystemtyps verwendeten Kommunikationsprotokolls zu übertragen, so dass es fortan mit diesen Parametern und somit mit anderen Komponenten des entsprechenden Schließsystemtyps kommunizieren kann. Ein kompliziertes Firmwareupdate kann daher entfallen, wenn ein Schloss das in einem Schließanlagentyp verwendete Kommunikationsprotokoll "erlernen" soll.

[0017] Das Verfahren zum Einrichten eines elektromechanischen Schlosses, hat zumindest zwei Schritte; nämlich als ersten Schritt das Übertragen von wenigsten einem Parameter von einem ersten Datenträger an das Schloss nach einem ersten Kommunikationsprotokoll, und als späteren Schritt das Bestimmen von mindestens einem zweiten Kommunikationsprotokoll anhand der bzw. des nach dem ersten Kommunikationsprotokoll übertragenen Parameter bzw. Parameters. Nach dem Verfahren kann ein Schloss durch Übermittlung von zur Kommunikation zwischen Komponenten eines bestimmten Schließanlagentyps notwendigen Informationen an diese bestimmte Schließanlage angepasst, sozusagen angelernt, werden. Typische Komponenten einer Schließanlage sind meist programmierbare Schlüssel und Schlösser und meist auch Programmiergeräte. Es genügt also ein erstes Kommunikationsprotokoll vorzusehen, mittels dessen die Parameter zumindest eines Schließanlagentyps, also die Parameter eines zweiten Kommunikationsprotokolls auf das Schloss und/oder wenigstens einen Schlüssel übertragbar sind. Nach der Übertragung der Parameter des zweiten Kommunikationsprotokolls kann das Schlöss an einen bestimmten Schließanlagentyp zangepasst werden, dies kann beispielsweise durch die Übertragung ausgelöst werden. Anschließend kann das Schloss z.B. in eine bestehende Schließanlage dieses Schließanlagentyps integriert werden. Das Aufspielen einer herstellerabhängigen Firmware ist zur Anpassung an den Schließanlagentyp nicht notwendig. Erst durch die übertragenen Parameter wird sichergestellt, dass die nach dem zweiten Kommunikationsprotokoll übermittelten Daten von dem Schloss richtig interpretiert werden können. Anders formuliert werden Informationen über das zweite Kommunikationsprotokoll in einer Metasprache, nämlich dem ersten Kommunikationsprotokoll an das Schloss übertragen, das dann aus den in der Metasprache übermittelten Informationen eine Objektsprache, nämlich das zweite Kommunikationsprotokoll ermittelt. Die Objektsprache kann Kommunikationsmuster enthalten, z.B. die Länge und der Aufbau von Frames die nach dem zweiten Kommunikationsprotokoll ausgetauscht werden, die Datenrate des zweiten Kommunikationsprotokoll als auch Informationen über Datenformate für nach dem zweiten Kommunikationsprotokoll zu übertragende Informationen, z.B. Datums und/oder Zeitangaben oder zu verwendende Verschlüsselungsalgorithmen. Eine Metasprache in der sich das zweite Kommunikationsprotokoll definieren lässt, kann z.B. XML oder eine ähnliche Sprache sein. Über die Metasprache kann auch eine physikalische Schnittstelle, allgemeiner ein Port des zweiten Kommunikationsprotokolls bestimmt werden, z.B. eine bestimmte Sende- und/oder Empfangsfrequenz, eine Antenne oder ein Anschluss.

[0018] Bevorzugt wird eine Kommunikation nach dem ersten Kommunikationsprotokoll über die gleiche physikalische Schnittstelle bzw. den gleichen Port abgewickelt, wie die Kommunikation nach dem zweiten Kommunikationsprotokoll. Dadurch genügt es eine einzige Schnittstelle/Port vorzusehen und die Hardwarekosten können reduziert werden. Wenn beispielsweise das Schloss in Schließanlagen integriert werden soll, bei der die Schlüssel ausschließlich passive RFID-Transponder sind, dann nutzt das erste Kommunikationsprotokoll bevorzugt ebenso wie passive RFID-Transponder die Dämpfung eines vom Schloss emittierten elektromagne-

tischen Felds, um den wenigstens einen Parameter nach dem ersten Kommunikationsprotokoll zu übertragen. Dazu kann der wenigstens eine Parameter z.B. in einem RFID-Transponder gespeichert sein und nach dem ersten Kommunikationsprotokoll übertragen werden. Alternativ können die Kommunikationsprotokolle natürlich auch unterschiedliche Übertragungskanäle (= Übertragungswege) nutzen. Beispielsweise kann das zweite Kommunikationsprotokoll eine Übertragung durch Dämpfung eines vom Schloss emittierten elektromagnetischen Felds vorsehen, das erste Kommunikationsprotokoll aber die Übertragung mittels einer frequenzmodulieren elektromagnetischen Welle oder mittels einer Kabelverbindung.

[0019] Das Verfahren kann für alle miteinander kommunizierenden Komponenten eines Schließsystems, d.h. nicht nur für Schlösser verwendet werden. Es ist also genau genommen ein Verfahren zum Einrichten einer Komponente eines elektromechanischen Schließsystems. Lediglich der Anschaulichkeit halber wird die Erfindung am Beispiel eines Schlosses erläutert.

[0020] Die Komponente, also das Schloss, generiert nach der Übertragung der Parameter das zweite Kommunikationsprotokoll, d.h. es hat alle Informationen, um mit anderen Komponenten des durch das zweite Kommunikationsprotokoll bestimmten Schließanlagentyps Daten auszutauschen. Das Austauschen von Daten kann beispielsweise das Durchführen einer Berechtigungsabfrage sein. Das Ergebnis kann also auch sein, dass ein Schlüssel (als Synonym für eine andere Komponente) nicht die notwendige Berechtigung aufweist.

[0021] Bevorzugt werden Informationen über die Berechtigung von Schlüsseln einer bestimmten Schließanlage nach dem zweiten Kommunikationsprotokoll auf das Schloss übertragen. Das ermöglicht es diese Informationen mit den jeweils herstellerspezifischen Werkzeugen ("Tools") zu übertragen. In diesem Fall würde ein Schloss mit einer Firmware gefertigt, die das erste Kommunikationsprotokoll enthält. Das Schloss könnte dann an einen Zwischenhändler ausgeliefert werden. Der Zwischenhänaler Kann dann mittels des ersten Kommunikationsprotokolls die Parameter übermitteln anhand der das Schloss das zweite Kommunikationsprotokolls bestimmt. Dadurch wird das Schloss an einen gegeben Schließanlagentyp angepasst. Im folgenden Schritt kann das Schloss in eine Schließanlage integriert werden, z.B. indem man Informationen über berechtigte Schlüssel nach dem zweiten Kommunikationsprotokoll übermittelt.

[0022] Bei einigen Schließsystemtypen erfolgt die Berechtigungsprüfung derart, dass zunächst eine sichere, d.h. verschlüsselte Datenstrecke zwischen den Kommunikationspartnern aufgebaut wird. Dabei werden sogenannte Kryptokeys verwendet, das sind geheim zuhaltende Werte, anhand der zu übertragende Daten verschlüsselt und/oder entschlüsselt werden. Passen die Kryptokeys zweier Kommunikationspartner nicht zueinander, kann keine sichere Datenstrecke aufgebaut werden; gleichwohl kommunizieren die Kommunikationspartner miteinander, denn sie sind durch das zweite Kommunikationsprotokoll in der Lage den zum Aufbau der sicheren Datenstrecke nötigen Daten auszutauschen. Dieser Austausch wird auch korrekt initiiert, jedoch wird die Berechtigungsprüfung abgebrochen, weil die Prüfung der Kryptokeys ergibt, dass sie nicht zueinander passen. Der Kryptokey gehört bei den meisten Schließanlagen nicht zu den Parametern des Schließanlagentyps, wohl aber meist der Verschlüsselungsalgorithmus. Der Verschlüsselungsalgorithmus jedoch kann auch durch einen Standard vorgegeben sein kann und ist dann bevorzugt in der Hardware oder Firmware hinterlegt.

[0023] Passen die Kryptokeys zueinander, wird dies meist als "grundsätzliche Berechtigung" bewertet. Bei manchen Schließanlagentypen werden zusätzliche im Schlüssel und/oder Schloss abgelegte Daten miteinander verglichen, z.B. ob der Schlüssel eine Berechtigung für eine bestimmte Tür und/oder Schließgruppe hat, ob die Berechtigung zeitlich beschränkt ist, ob es innerhalb einer Schließgruppe Ausnahmen gibt etc.. Diese zusätzlichen Informationen werden vor der Freigabe des entsprechenden Schlosses meist mit ausgewertet.

[0024] Die Parameter des zweiten Kommunikationsprotokolls sind in der Regel nicht die zu einem bestimmten Objekt oder Gebäude gehörenden Informationen (nachfolgend "objektspezifische Informationen"), wie die Schließanlagennummer oder die Zugehörigkeit einer Komponente zu einer bestimmten Schließgruppe, sondern die Informationen, die notwendig sind, um objektspezifische Informationen lesen und/oder schreiben zu können, sofern die Berechtigung dafür vorliegt. Der Begriff Parameter bezeichnet in einer Ausführungsform der Erfindung nicht notwendigerweise die für die Kommunikation zur Verfügung stehenden Befehle, bevorzugt bezeichnet er zumindest die für die Zuordnung von übertragenen Daten zu gegebenen Variablen notwendigen Informationen. Das ist insbesondere dann wichtig, wenn nach einem Kommunikationsprotokoll die Werte mehrerer Variablen nachaneinander als Bitfolge ausgetauscht werden.

[0025] Als "Parameter" wird jede Information bezeichnet, die von dem Datenträger auf das Schloss nach dem ersten Kommunikationsprotokoll übertragen wird, um das zweite Kommunikationsprotokoll zu bestimmen. Als "Daten" wird hingegen all das bezeichnet, was nach dem zweiten Kommunikationsprotokoll übertragen wird. Jede Art von Speicher kann als Datenträger genutzt werden, aus dem der wenigstens eine Parameter des zweiten Kommunikationsprotokolls mittels dem ersten Kommunikationsprotokoll an das Schloss übertragen wird. Typische Speicher sind Magnetspeicher, Halbleiterspeicher und optische Speicher.

[0026] Vorzugsweise kommuniziert das Schloss mittels des zweiten Kommunikationsprotokolls mit mindestens einem Schlüssel. Das Schloss kann also bei entsprechender Parametrierung mit Schlüsseln eines beliebigen Schließanlagentyps kommunizieren und somit in

diesen Schließanlagentyp eingebunden werden.

[0027] Bevorzugt wird zumindest die Größe der Vektorräume der Türen und/oder der Schlüssel und/oder der Schließgruppen als wenigsten ein Parameter übertragen. Diese Größen sind oft wesentlich für die Speicherverwaltung des Schlosses und/oder des Schlüssels sowie für die Bitlänge der entsprechenden Variablen und Felder, weil bei vielen Schließsystemen bei der Berechtigungsprüfung die Information ausgetauscht wird, in welchen Schlössern und/oder Schließgruppen der jeweilige Schlüssel berechtigt ist. Alle Türen, Schließgruppen und Schlüssel einer Schließanlage bilden die Basis für den jeweiligen binären Vektorraum T, G bzw. S. Somit begrenzen die Dimensionen der jeweiligen Vektorräume T, G, S die maximale Anzahl der in einer Schließanlage des gegeben Schließanlagentyps integrierbaren Schlösser, Schließgruppen bzw. Schlüssel. Die Dimension des entsprechenden Vektorraums ist eine Information über den zur Darstellung der Vektoren benötigten Speicherplatzes, die beim extrahieren solcher Vektoren aus einer Bitfolge relevant ist. Beispielsweise lässt sich der Vektorraum G der Gruppen darstellen als

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

wobei m die Dimension des Vektorraums ist und somit die beim gegebenen Schließanlagentyp maximale Anzahl der verwaltbaren Schließgruppen angibt. Ein binärer Vektor der Länge m wird manchen Schließsystemtypen sowohl auf dem Schlüssel ($\vec{\gamma}$) als auch in der Tür (p) gespeichert. Eine Berechtigung eines bestimmten Schlüssels an einer bestimmten Tür kann vorliegen wenn das Skalarprodukt $\vec{\gamma} \cdot \vec{\rho} = 1.$ Entsprechend wird bei der Berechtigungsprüfung entweder $\vec{\gamma}$ oder/oder p und die jeweils andere Komponente übertragen und m kann ein relevanter Parameter sein, um eine einen Vektor $\vec{\gamma}$ enthaltende Bitfolge auszuwerten. Entsprechend kann auch die Darstellung von binären Vektoren, wie z.B. der binären Vektoren der Vektorräume T,G,S Parameter des zweiten Kommunikationsprotokolls sein. Bevorzugt wird bei der Übertragung der Parameter ein Header übertragen, der nachfolgende Informationen der Übertragung als Parameter des zweiten Kommunikationsprotokolls kennzeichnet. Dadurch kann das Schloss anhand des Headers unterscheiden, ob eine Kommunikation mit einem Schlüssel erfolgt oder ob es an einen Schließsystemtyp angepasst wird.

[0028] Bevorzugt werden Parameter des zweiten Kommunikationsprotokolls in Blöcken übertragen, wobei ein bestimmter Blockabschnitt den Parameter identifiziert und wenigstens ein weiterer Blockabschnitt den Wert des Parameters. Bevorzugt enthält der Block eine Angabe über seine Größe. Dies erhöht die Flexibilität des ersten Kommunikationsprotokolls, und ermöglicht es nicht benötigte Parameter wegzulassen.

[0029] Ein bevorzugter Parameter eines zweiten Kommunikationsprotokolls ist, z.B. die Art der Verschlüsselung der Kommunikation zwischen Schloss und Schlüssel, oder die Art der Darstellung zeitlicher Begrenzungen von Berechtigungen.

[0030] Ein anderer bevorzugter Parameter ist die Art der Abfrage von Daten aus dem Schloss oder Schlüssel. Beispielsweise kann das zweite Kommunikationsprotokoll einen unmittelbaren Lese und/oder Schreibzugriff auf bestimmte Speicherbereiche des jeweiligen Kommunikationspartners ermöglichen. Dann sind auch die Sprungadressen (Pointer) zu den entsprechenden Speicherstellen vorzugsweise Parameter des zweiten Kommunikationsprotokolls. Insbesondere kann bei der Übertragung der Parameter die Information darüber übertragen werden, wie eine nach dem zweiten Kommunikationsprotokoll übertragene Bitfolge zu interpretieren ist. Einige Schließanlagentypen lesen bei der Überprüfung einer Berechtigung eines Schlüssels Daten aus standardisierten Speicherbereichen des Schlüssels, z.B. eines passiven RFID-Transponders, aus. Diese Daten werden bevorzugt als Bitfolge übertragen, in die Werte von zwei oder mehr Variablen abgelegt sind. Anschließend werden die Werte der einzelnen Variablen zur Prüfung der Berechtigung, wie z.B. eine Schließgruppennummer, eine Türnummer etc., aus der Bitfolge extrahiert. Die Informationen über die Positionen der Werte der Variablen in der Bitfolge, werden bevorzugt nach dem ersten Kommunikationsprotokoll übertragen.

[0031] Bevorzugt hat wenigstens ein Parameter in dem Schloss einen Standard-Wert (Default-Wert), der bei der Übertragung der Informationen durch einen anderen Wert ersetzt werden kann. Dadurch kann die zu übertragende Informationsmenge reduziert werden und es kann ein "Default-Protokoll" geben. Es genügt dann die Abweichungen des zweiten Kommunikationsprotokolls an das Schloss zu übertragen.

[0032] Bevorzugt wird mindestens eine Information übertragen, die für das Datenformat der auf dem Schlüssel und/oder dem Schloss gespeicherten oder zu speichernden Daten steht. Beispielsweise können Daten komprimiert gespeichert und oder übertragen werden. Dann wäre auch die Information ob und wenn ja welches Kompressionsverfahren Anwendung findet ein vorzugsweise übertragener Parameter des zweiten Kommunikationsprotokolls.

[0033] Bevorzugt wird mindestens eine Information übertragen, die für mindestens eine Speicheradresse in mindestens einem Schlüssel steht, aus der zur Prüfung der Berechtigung des Schlüssels Daten gelesen werden. Beispielsweise kann eine Einstiegsadresse zum Auslesen eines Kryptokeys übertragen werden.

[0034] Bevorzugt wird mindestens ein Parameter übertragen, anhand dessen ein Verschlüsselungsver-

fahren zum Schutz von nach dem zweiten Kommunikationsprotokoll übertragenen Daten ausgewählt wird. Dann kann das Schloss in Schließsystemen mit verschiedenen Verschlüsselungsverfahren eingesetzt werden.

[0035] Ebenso kann die Information über einen bestimmen Schließanlagentyp an das Schloss als Parameter übertragen werden. In diesem Fall ist auf dem Schloss für wenigstens einen Schließanlagentyp ein entsprechender Parametersatz hinterlegt. Die Übertragung nur eines Schließanlagentyps kann wesentlich schneller erfolgen als die Übertragung eines ganzen Parametersatzes. Dadurch kann die Zeit zum Anlernen des Schlosses erheblich verkürzt werden.

[0036] Bevorzugt werden die Informationen über die gleiche Schnittstelle von dem Datenträger übertragen, über den später auch die Kommunikation mit den Schlüsseln erfolgt. Dadurch werden zusätzliche Schnittstellen und somit Kosten vermieden. Beispielsweise kann es genügen einen ersten RFID-Transponder mit den Parametern vor ein Schloss zu halten, so dass der erste RFID-Transponder und dass Schloss kommunizieren können, um so die Parameter für die spätere Kommunikation mit den Schlüsseln, die ebenfalls RFID-Transponder sind zu übergeben. Dann erfolgt die Kommunikation mit dem ersten RFID-Transponder über das erste Kommunikationsprotokoll und die Kommunikation mit den weiteren RFID-Transpondern nach dem zweiten Kommunikationsprotokoll.

[0037] Bevorzugt werden bei der Übertragung Informationen zu mindestens zwei Kommunikationsprotokollen übergeben. Dann kann ein Schloss gleichzeitig in zwei oder mehr Schließanlagen unterschiedlichen Typs eingebunden sein. Es kann dann beispielsweise zunächst eine Kommunikation nach einem ersten zweiten Kommunikationsprotokoll mit einem Schlüssel versuchen und wenn diese fehlschlägt eine Kommunikation nach mindestens einem weiteren zweiten Kommunikationsprotokoll beginnen.

[0038] Die Erfindung wurde anhand eines in eine Schließanlage einzupassenden Schlosses beschrieben. Jedoch sind elektronische Schlösser und Schlüssel - abgesehen von ihren mechanischen Komponenten-grundsätzlich gegeneinander austauschbar. Deshalb kann auf die gleiche Weise auch ein Schlüssel an einen gegebenen Schließanlagentyp angepasst werden. Gleiches gilt für jede andere Komponente einer Schließanlage, die mit einem Schlüssel oder einem Schloss kommuniziert.

[0039] Nach der Erfindung wird keine neue Firmware auf das Schloss aufgespielt. Dem Programmcode der Firmware werden lediglich mittels dem nach dem ersten Kommunikationsprotokoll wenigstens einen übertragenen Parameter die Informationen zur Bestimmung des anschließend zu verwendenden zweiten Kommunikationsprotokolls übermittelt. Die Firmware befindet sich üblicherweise in einem Programmspeicher. Der wenigstens eine Parameter wird vorzugsweise nicht in den Programmspeicher, sondern in einen Datenspeicher geladen.

[0040] Nachdem das zweite Kommunikationsprotokoll bestimmt wurde wird ein bevorzugt dauerhaftes Flag gesetzt, das eine Änderung des zweiten Kommunikationsprotokolls verhindert. Dadurch wird die Manipulationssicherheit des Schlosses erhöht.

Beschreibung der Zeichnungen

[0041] Die Erfindung wird nachstehend anhand von Ausführungsbeispielen unter Bezugnahme auf die einzige Zeichnung exemplarisch beschrieben.

[0042] Bei dem Verfahren in Figur 1 kommuniziert ein eine Komponente eines elektromechanischen Schließsystems, beispielsweise ein elektromechanisches Schloss 10 mit einem Datenträger 20 nach einem gegebenen, d.h. dem Schloss 10 und dem Datenträger 20 bekannten ersten Kommunikationsprotokoll. Der Datenträger 20 kann beispielsweise die gezeigte RFID-Transponderkarte sein. Das Schloss 10 ist hier beispielhaft als Knaufzylinder dargestellt. Zur Kommunikation wird zwischen dem Schloss 10 und dem Datenträger 20 zunächst eine verschlüsselte Datenstrecke 30 aufgebaut, und anschließend von dem Datenträger 10 an das Schloss 20 ein Header 31 übertragen. Anhand des Headers 31 erkennt das Schloss, ob nachfolgend Parameter 33 eines zweiten Kommunikationsprotokolls, das zu einem bestimmten Schließanlagentyp gehört, übertragen werden oder nicht. Sofern wie angedeutet Parameter 33 übertragen werden sollen geht es in einen "Lernmodus", der durch einen Pfeil 32 angedeutet ist. Im Lernmodus wird ein zweites Kommunikationsprotokoll anhand der Übertragenen Parameter 33 parametriert. Nun ist kann das Schloss in eine konkrete Schließanlage eingefügt werden, z.B. in dem man ihm eine Schloss-ID 34, und/oder eine Gruppen-ID 35 und/oder Verschlüsselungsparameter 36 der konkreten Schließanlage mitteilt. Dies kann dann anhand des zweiten Kommunikationsprotokolls erfolgen, beispielsweise mittels mit einem separaten Datenträger 22, einer Konfigurationseinheit (nicht dargestellt) oder einer Zentrale der Schließanlage (nicht dargestellt). Das Schloss 10 hat nun alle Informationen, die es benötigt um die Berechtigung 37 eines Schlüssels 24 der Schließanlagen zu überprüfen.

[0043] Auch andere Möglichkeiten den Lernmodus zu initiieren sind möglich. Beispielsweise kann auf einem Datenträger eine Datei mit einem vorbestimmen Dateinamen abgelegt sein, der den wenigstens einen Parameter enthält. Das Schloss fragt den Datenträger ab, ob er eine Datei mit dem bestimmten Namen aufweist. Sofern ja, geht es in den Lernmodus, d.h.es liest den wenigstens einen Parameter aus dem Datenträger aus, beispielsweise aus der Datei, und bestimmt anhand des wenigstens einen Parameters das zweite Kommunikationsprotokoll. Bevorzugt wird anschließend ein Flag, z.B. ein Bit, gesetzt, dass ein erneutes Aufrufen des Lernmodus verhindert. Dazu fragt das Schloss vorzugsweise den Flag ab, und prüft nur dann, ob es in den Lernmodus gehen soll oder nicht, wenn das Flag nicht gesetzt ist.

Das Flag kann zu jedem Zeitpunkt vor der Konfiguration des zweiten Kommunikationsprotokolls geprüft werden. Sinn der Abfrage des Flags ist es zu verhindern, dass ein einmal bestimmtes zweites Kommunikationsprotokoll durch ein neues zweites Kommunikationsprotokoll ersetzt wird um dadurch Manipulationen zu verhindern.

Bezugszeichenliste

[0044]

10	Schloss
20	Datenträger/RFID-Karte
24	Schlüssel
30	verschlüsselte Datenstrecke
31	Header (Datenkopf)
32	Lernmodus
33	Parameter
34	Schloss-ID
35	Gruppen-ID
36	Verschlüsselungsparameter
37	Berechtigung

Patentansprüche

1. Verfahren zum Einrichten einer Komponente eines elektromechanischen Schließsystems, aufweisend zumindest die Schritte:

- Übertragen von wenigstens einem Parameter von einem ersten Datenträger an die Komponente nach einem ersten Kommunikationsprotokoll,
- Generieren von mindestens einem zweiten Kommunikationsprotokoll nach der Übertragung anhand der bzw. des nach dem ersten Kommunikationsprotokoll übertragenen Parameter bzw. Parameters mittels der Komponente durch Parametrieren des zweiten Kommunikationsprotokolls anhand der übertragenen Parameter,
- Setzen eines Flags in der Komponente nach dem Generieren, wobei die Komponente eine erneute Änderung des zweiten Kommunikationsprotokolls verhindert, wenn das Flag gesetzt ist,
- Einfügen der Komponente in das elektromechanisches Schließsystem nach dem Generieren indem der Komponente eine Schloss-ID (34) und/oder eine Gruppen-ID (35) und/oder Verschlüsselungsparameter (36) mittels des zweiten Kommunikationsprotokolls mitgeteilt wird, und
- Austauschen von Daten mit anderen Komponenten des Schließsystems mittels des zweiten Kommunikationsprotokolls.

2. Verfahren nach Anspruch 1,
dadurch gekennzeichnet, dass
die Komponente ein Schloss ist, und dass das Schloss in eine Schließanlage integriert wird, indem dem Schloss Informationen über berechtigte Schlüssel nach dem zweiten Kommunikationsprotokoll übermittelt werden.

3. Verfahren nach Anspruch 1 oder 2,
dadurch gekennzeichnet, dass
als Parameter (33) zumindest die Position wenigstens eines Wertes wenigstens einer Variablen in einer Bitfolge, die nach dem zweiten Kommunikationsprotokoll ausgetauscht wird, übertragen wird.

4. Verfahren nach einem der vorstehenden Ansprüche
dadurch gekennzeichnet, dass
die Komponente (10) mittels des zweiten Kommunikationsprotokolls mit mindestens einem Schlüssel (24) kommuniziert.

5. Verfahren nach einem der vorstehenden Ansprüche
dadurch gekennzeichnet, dass
Informationen über die Berechtigung von Schlüsseln (24) einer bestimmten Schließanlage nach dem zweiten Kommunikationsprotokoll auf ein Schloss (10) übertragen werden.

6. Verfahren nach einem der vorstehenden Ansprüche
dadurch gekennzeichnet, dass
als Parameter (33) zumindest die Größe der Vektorräume der Türen und/oder der Schlüssel (24) und/oder der Schließgruppen übertragen wird.

7. Verfahren nach einem der vorstehenden Ansprüche,
dadurch gekennzeichnet, dass
beim Übertragen mittels des ersten Kommunikationsprotokolls vor dem Parameter ein Header (31) übertragen wird, der nachfolgende Informationen als Parameter (33) des zweiten Kommunikationsprotokolls kennzeichnet.

8. Verfahren nach einem der vorstehenden Ansprüche,
dadurch gekennzeichnet, dass
die Parameter (33) in Blöcken übertragen werden, wobei eine bestimmter Blockabschnitt den Parameter (33) identifiziert und wenigstens ein weiterer Blockabschnitt den Wert des Parameters (33).

9. Verfahren nach einem der vorstehenden Ansprüche,
dadurch gekennzeichnet, dass
mindestens ein Parameter (33) übertragen wird, der für das Datenformat der auf dem Schlüssel (24) und/oder dem Schloss (10) gespeicherten oder zu speichernden Daten steht.

10. Verfahren nach einem der vorstehenden Ansprüche,
dadurch gekennzeichnet, dass

mindestens ein Parameter (33) übertragen wird, der für mindestens eine Speicheradresse in mindestens einem Schlüssel (24) steht, aus der bei zur Prüfung der Berechtigung des Schlüssels (24) Daten ausgelesen werden.

11. Verfahren nach einem der vorstehenden Ansprüche, **dadurch gekennzeichnet, dass**
mindestens ein Parameter (33) übertragen wird, anhand der ein Verschlüsselungsverfahren zum Schutz von nach dem zweiten Kommunikationsprotokoll übertragenen Daten ausgewählt wird.

12. Verfahren nach einem der vorstehenden Ansprüche, **dadurch gekennzeichnet, dass**
die Information über die Zugehörigkeit des Schlosses (10) zu einer bestimmten Schließanlage übertragen wird.

13. Verfahren nach einem der vorstehenden Ansprüche **dadurch gekennzeichnet, dass**
wenigstens ein Parameter übertragen wird, anhand dessen ein Datenformat zur Speicherung und/oder Übertragung einer Datumsangabe und/oder Zeitangabe und/oder eines Berechtigungszeitraumes bestimmt wird.

14. Verfahren nach einem der vorstehenden Ansprüche, **dadurch gekennzeichnet, dass**
die Übertragung des wenigstens einen Parameters über eine erste physikalische Schnittstelle erfolgt und dass die Übertragung von Daten nach dem zweiten Kommunikationsprotokoll über die gleiche physikalische Schnittstelle erfolgt.

Claims

1. Method for commissioning a component of an electromechanical locking system, comprising at least the steps of:

- transmitting at least one parameter from a first data carrier to the component according to a first communication protocol,
- after transmission, based on the parameter/s transmitted according to the first communication protocol, generating at least one second communication protocol by means of the component, by parameterizing the second communication protocol based on the transmitted parameters,
- after generating, setting a flag in the component, wherein the component prevents a repeated change of the second communication protocol when the flag is set,
- after generating, inserting the component into the electromechanical locking system, in that a lock-ID (34) and/or a group-ID (35) and/or encryption parameter (36) are/is communicated to the component by means of the second communication protocol, and
- exchanging data with other components of the locking system by means of the second communication protocol.

2. Method according to claim 1, **characterized in that**
the component is a lock, and that the lock is integrated into a locking system by transmitting information to the lock about authorized keys according to the second communication protocol.

3. Method according to claim 1 or 2, **characterized in that**
at least the position of at least one value of at least one variable in a bit sequence is transmitted as parameter (33), wherein the bit sequence is exchanged according to the second communication protocol.

4. Method according to one of the preceding claims, **characterized in that**
the component (10) communicates with at least one key (24) by means of the second communication protocol.

5. Method according to one of the preceding claims, **characterized in that**
information about the authorization of keys (24) of a specific locking system is transmitted to a lock (10) according to the second communication protocol.

6. Method according to one of the preceding claims, **characterized in that**
at least the size of the vector spaces of the doors and/or of the keys (24) and/or of the locking groups are transmitted as parameter (33).

7. Method according to one of the preceding claims, **characterized in that**
when transmitting by means of the first communication protocol, a header (31) is transmitted before the parameter, which header designates the subsequent information as parameter (33) of the second communication protocol.

8. Method according to one of the preceding claims, **characterized in that**
the parameter (33) are transmitted in blocks, wherein a specific block section identifies the parameter (33), and at least another block section identifies the value of the parameter (33).

9. Method according to one of the preceding claims, **characterized in that**
at least one parameter (33) is transmitted that stands

for the data format of the data stored or data to be stored on the key (24) and/or the lock (10).

10. Method according to one of the preceding claims, **characterized in that** at least one parameter (33) is transmitted that stands for at least one memory address in at least one key (24) from which memory adress data is read for checking authorization of the key (24).

11. Method according to one of the preceding claims, **characterized in that** at least one parameter (33) is transmitted, on the basis of which an encryption method is selected for protecting data transmitted according to the second communication protocol data.

12. Method according to one of the preceding claims, **characterized in that** the information about the assignmet of the lock (10) to a specific locking system is transmitted.

13. Method according to one of the preceding claims, **characterized in that** at least one parameter is transmitted, by which a data format for storage and/or transmission of a date designation and/or time designation and/or an authorization period is determined.

14. Method according to one of the preceding claims, **characterized in that** the transmission of the at least one parameter is conducted via a first physical interface, and that the transmission of data according to the second communication protocol is conducted via the same physical interface.

Revendications

1. Procédé pour le paramétrage d'un composant d'un système de fermeture électromécanique, comprenant au moins les étapes suivantes :

- transmission d'au moins un paramètre d'un premier support de données au composant suivant un premier protocole de communication,
- génération d'au moins un deuxième protocole de communication après la transmission à l'aide du ou des paramètres transmis suivant le premier protocole de communication au moyen du composant par paramétrage du deuxième protocole de communication à l'aide des paramètres transmis,
- activation d'un indicateur dans le composant après la génération, le composant empêchant une nouvelle modification du deuxième protocole de communication quand l'indicateur est activé,
- introduction du composant dans le système de fermeture électromécanique après la génération par la transmission au composant d'un identifiant de serrure (34) et/ou d'un identifiant de groupe (35) et/ou de paramètres de codage (36) au moyen du deuxième protocole de communication, et
- échange de données avec d'autres composants du système de fermeture au moyen du deuxième protocole de communication.

2. Procédé selon la revendication 1, **caractérisé en ce que** le composant est une serrure et **en ce que** la serrure est intégrée dans une installation de fermeture par le fait que des informations sur les clés autorisées sont transmises à la serrure suivant le deuxième protocole de communication.

3. Procédé selon la revendication 1 ou 2, **caractérisé en ce que** le paramètre (33) transmis est la position d'au moins une valeur d'au moins une des variables dans une séquence de bits échangée suivant le deuxième protocole de communication.

4. Procédé selon l'une des revendications précédentes, **caractérisé en ce que** le composant (10) communique avec au moins une clé (24) au moyen du deuxième protocole de communication.

5. Procédé selon l'une des revendications précédentes, **caractérisé en ce que** des informations sur l'autorisation de clés (24) d'une certaine installation de fermeture sont transmises à une serrure (10) suivant le deuxième protocole de communication.

6. Procédé selon l'une des revendications précédentes, **caractérisé en ce que** le paramètre (33) transmis est au moins la taille des espaces vectoriels des clés (24) et/ou des groupes de fermeture.

7. Procédé selon l'une des revendications précédentes, **caractérisé en ce que** lors de la transmission au moyen du premier protocole de communication, un en-tête (31) caractérisant les informations suivantes comme un paramètre (33) du deuxième protocole de communication est transmis avant le paramètre.

8. Procédé selon l'une des revendications précédentes, **caractérisé en ce que** les paramètres (33) sont transmis sous forme de bloc, dans lesquels une certaine section de bloc identifie le paramètre (33) et au moins une autre section de bloc la valeur du paramètre (33).

9. Procédé selon l'une des revendications précédentes, **caractérisé en ce qu'**au moins un paramètre

(33) représentant le format de données des données enregistrées ou à enregistrer sur la clé (24) et/ou la serrure (10) est transmis.

10. Procédé selon l'une des revendications précédentes, **caractérisé en ce qu'**au moins un paramètre (33) représentant au moins une adresse en mémoire dans au moins une clé (24) à partir de laquelle des données sont lues pour vérifier l'autorisation de la clé (24) est transmis.

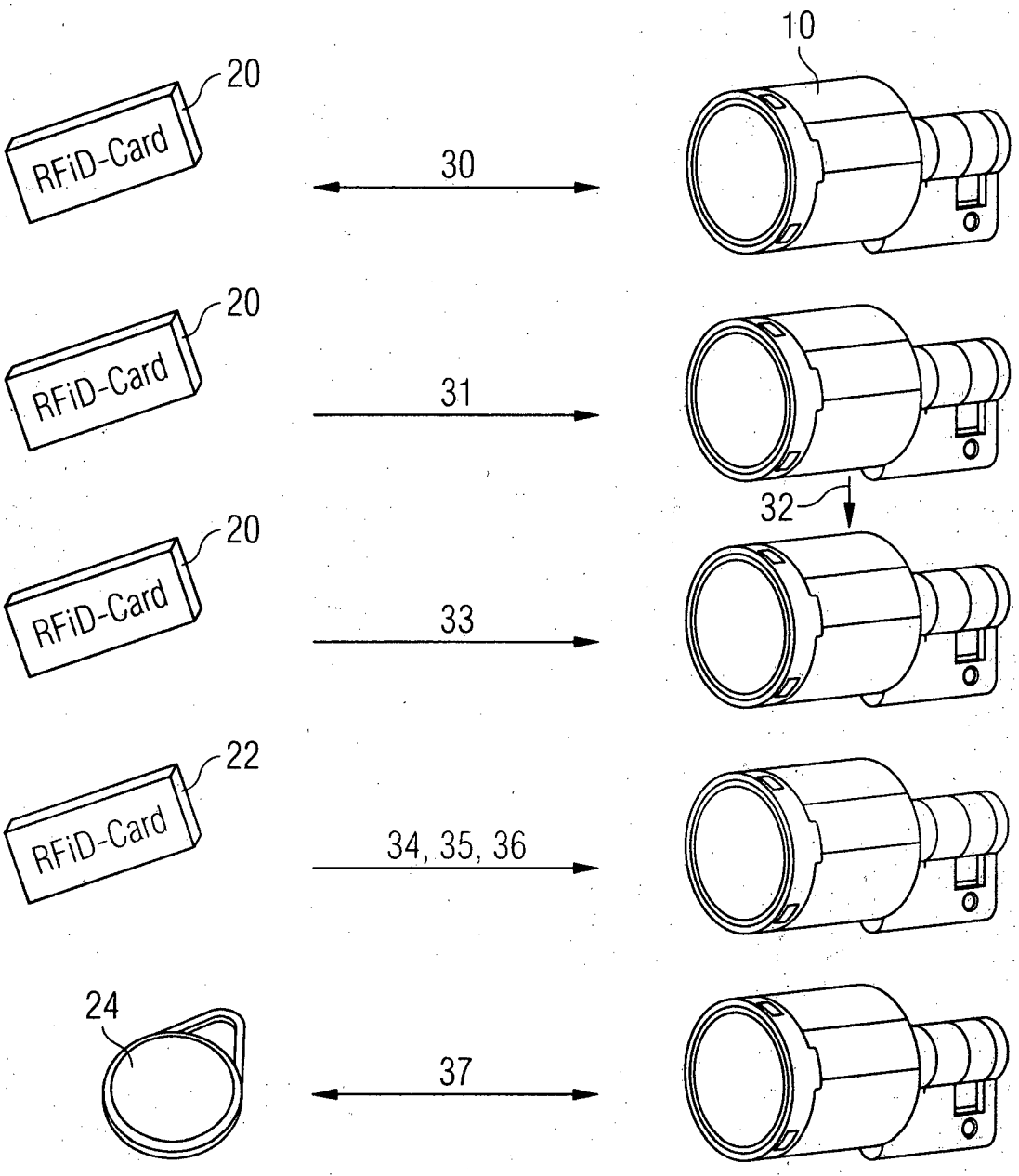
11. Procédé selon l'une des revendications précédentes, **caractérisé en ce qu'**au moins un paramètre (33) à l'aide duquel un procédé de codage est choisi pour la protection des données transmises suivant le deuxième protocole de communication est transmis.

12. Procédé selon l'une des revendications précédentes, **caractérisé en ce que** l'information concernant l'appartenance de la clé (10) à une certaine installation de fermeture est transmise.

13. Procédé selon l'une des revendications précédentes, **caractérisé en ce qu'**au moins un paramètre à l'aide duquel un format de données est déterminé pour l'enregistrement et/ou la transmission d'une indication de date et/ou d'une indication d'heure et/ou d'une période d'autorisation est transmis.

14. Procédé selon l'une des revendications précédentes, **caractérisé en ce que** la transmission de l'au moins un paramètre passe par une première interface physique et **en ce que** la transmission de données suivant le deuxième protocole de communication passe par la même interface physique.

Fig. 1


10
20
RFiD-Card
30
20
RFiD-Card
31
32
20
RFiD-Card
33
22
RFiD-Card
34, 35, 36
24
37

IN DER BESCHREIBUNG AUFGEFÜHRTE DOKUMENTE

Diese Liste der vom Anmelder aufgeführten Dokumente wurde ausschließlich zur Information des Lesers aufgenommen und ist nicht Bestandteil des europäischen Patentdokumentes. Sie wurde mit größter Sorgfalt zusammengestellt; das EPA übernimmt jedoch keinerlei Haftung für etwaige Fehler oder Auslassungen.

In der Beschreibung aufgeführte Patentdokumente

- DE 4342641 A1 **[0004]**
- DE 19913931 **[0004]**
- EP 0671712 A1 **[0004]**
- DE 10237715 A1 **[0005]**
- DE 19701740 A1 **[0006]**
- DE 10138217 A1 **[0007]**
- WO 2010039598 A2 **[0008]**
- EP 18035436 A1 **[0009]**
- WO 0055796 A **[0010]**
- US 7075412 B1 **[0011]**
- WO 2008144804 A **[0012]**