



(11) **EP 2 842 110 B9**

(12) **KORRIGIERTE EUROPÄISCHE PATENTSCHRIFT**

(15) Korrekturinformation:
Korrigierte Fassung Nr. 1 (W1 B1)
Korrekturen, siehe
Ansprüche DE 1

(48) Corrigendum ausgegeben am:
30.03.2022 Patentblatt 2022/13

(45) Veröffentlichungstag und Bekanntmachung des
Hinweises auf die Patenterteilung:
15.12.2021 Patentblatt 2021/50

(21) Anmeldenummer: **13718851.2**

(22) Anmeldetag: **27.04.2013**

(51) Internationale Patentklassifikation (IPC):
G07C 9/00 (2020.01)

(52) Gemeinsame Patentklassifikation (CPC):
G07C 9/00571; G07C 9/00182; G07C 9/0069;
G07C 9/00912; G07C 2009/00634;
G07C 2009/00761; G07C 2009/00936

(86) Internationale Anmeldenummer:
PCT/EP2013/058827

(87) Internationale Veröffentlichungsnummer:
WO 2013/160481 (31.10.2013 Gazette 2013/44)

(54) **ELEKTRONISCHES SCHLIEßSYSTEM UND VERFAHREN ZUR FREIGABE EINER
ZUGANGSBERECHTIGUNG**

ELECTRONIC CLOSURE SYSTEM AND A METHOD FOR ALLOWING AN ACCESS
AUTHORISATION

SYSTÈME DE VERROUILLAGE ÉLECTRONIQUE ET PROCÉDÉ DE VALIDATION D'UNE
AUTORISATION D'ACCÈS

(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: **27.04.2012 DE 102012008395**

(43) Veröffentlichungstag der Anmeldung:
04.03.2015 Patentblatt 2015/10

(73) Patentinhaber: **Lock Your World GmbH & Co. KG
63619 Bad Orb (DE)**

(72) Erfinder:
• **ENGEL-DAHAN, Manuela**
D-63619 Bad Orb (DE)
• **KNOBLING, Ralf**
61137 Schöneck (DE)
• **MEISEL, Thilo**
64285 Darmstadt (DE)

(74) Vertreter: **Hoeger, Stellrecht & Partner**
Patentanwälte mbB
Uhlandstrasse 14c
70182 Stuttgart (DE)

(56) Entgegenhaltungen:
WO-A1-2009/128854 WO-A2-2004/077848
DE-A1-102009 013 650 DE-U1-202011 003 043
US-A1- 2006 170 533

- **Lockyourworld: "Pylocx Rohrtresor von Lock Your World", , 19. Oktober 2011 (2011-10-19), Seite 1, XP054975180, Gefunden im Internet: URL: <http://www.youtube.com/watch?v=yfGQjyqO0jY> [gefunden am 2013-07-02]**
- **"LOCK YOUR WORLD secure. easy. stable.", , 5. Dezember 2011 (2011-12-05), XP055069059, Gefunden im Internet: URL: http://www.lockyourworld.com/uploads/media/system_overview.pdf [gefunden am 2013-07-02]**

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 2 842 110 B9

Beschreibung

[0001] Die Erfindung betrifft ein elektronisches Schließsystem umfassendes elektronisches Schließsystem sowie ein Verfahren für eine gesicherte Erlangung einer Zugangsberechtigung oder für eine gesicherte Schlüssel-Übergabe.

[0002] Insbesondere für externe Sicherheitsdienste aber auch für eigenes Personal einer Firma besteht die Problematik, dass das Mitführen eines Schlüssels, insbesondere Generalschlüssels, der einen Zugang zu sämtlichen Räumen eines Gebäudes ermöglicht, ein erhebliches Sicherheitsrisiko darstellt, wenn dieser Schlüssel durch Missbrauch oder durch kriminelle Handlungen (Diebstahl, Raub oder Kidnapping, illegale Herstellung eines Nachschlüssels) in falsche Hände gerät.

[0003] Aus der DE 10 2005 033 898 A1 ist ein Verfahren und eine Einrichtung zur Erteilung einer Zugangsberechtigung zu einer Wohnung bekannt. Dort wird ausgelöst durch eine fernmündliche Anfrage eines Benutzers per Funk, bei der der Benutzer einen Code übermittelt, von einer Servicestelle ein Signal an ein Telemetriemodul einer Gegensprechanlage gesendet, die dem berechtigten Benutzer den Zugang zur Haustür und anschließend auch zur Wohnungstür erteilt.

[0004] Aus der DE 20 2011 003 043 U1 ist eine elektronische Kontaktstelle mit drei Kontakten, einem dazu passender Stecker oder Schlüssel und einer magnetischen Zentrierung des Steckers an der Kontaktstelle bekannt.

[0005] In der WO 2009/128854 A1 werden Verfahren und Einrichtungen für eine Zugangskontrolle offenbart.

[0006] Die DE 10 2009 013 650 A1 betrifft eine Anordnung zur Entriegelung eines elektrisch betriebenen Schlosses eines Fahrzeugs mit eigener Energieversorgung.

[0007] XP055069059 entspricht einer Präsentation von "Pylocx", die vor dem Prioritätstag auf der Webseite "www.LockYourWorld.com" abrufbar war. Sie beschreibt eine Zugangskontrolle mit einem elektronischen Schloss und einem elektronischen Schlüssel, welcher magnetische Kontakte zur Übermittlung von Daten und Energie an das Schloss und eine Eingabeeinrichtung zur Eingabe eines Berechtigungscodes umfasst.

[0008] Der Erfindung liegt die Aufgabe zugrunde, einen elektronischen Schlüssel bereit zu stellen, der kurzfristig und wechselweise für das Öffnen verschiedenster Schlösser aktivierbar ist. Die Aufgabe umfasst ferner die Bereitstellung eines elektronischen Schließsystems, in dem ein erfindungsgemäßer elektronischer Schlüssel vorteilhaft mit wenigstens einem elektronischen Schloss zusammenwirkt. Schließlich besteht die Aufgabe auch darin, unter Verwendung eines erfindungsgemäßen elektronischen Schlüssels und/oder eines erfindungsgemäßen Schließsystems ein Verfahren für eine gesicherte Erlangung einer Zugangsberechtigung oder für eine gesicherte Schlüssel-Übergabe anzugeben.

[0009] Diese Aufgabe wird hinsichtlich des elektroni-

schen Schließsystems durch die im Patentanspruch 1 angegebenen Merkmale und hinsichtlich des Verfahrens durch die Merkmale des Anspruchs 5 gelöst. Vorteilhafte Ausgestaltungen der Erfindung sind in den jeweils darauf bezogenen Unteransprüchen enthalten.

[0010] Ein erfindungsgemäßer elektronischer Schlüssel zeichnet sich durch eine an einem Gehäuse des elektronischen Schlüssels vorgesehene Eingabeeinrichtung zur Eingabe eines Berechtigungscodes aus. Die Eingabeeinrichtung kann dabei in Form einer numerischen oder alphanumerischen Tastatur ausgebildet sein, wobei der Berechtigungscodes für die gewünschte Freigabe in diesem Falle durch den Benutzer manuell eingegeben wird. Gemäß der Erfindung ist der elektronische Schlüssel mittels über die Eingabeeinheit eingebbarer Berechtigungscodes für das Öffnen verschiedener elektronischer Schlösser programmierbar.

[0011] Die Eingabeeinrichtung kann alternativ oder ergänzend auch von einer elektronischen Erfassungseinrichtung gebildet werden. Diese kann beispielsweise von einem Lese- oder Empfangsgerät gebildet werden, das einen per Funk-, Bluetooth-, RFID- oder NFC-Kommunikation oder per optischer Übermittlung, beispielsweise eines Barcodes, QR-Codes oder ähnlichem, vom Benutzer oder einer von diesem gehandhabten Kommunikationseinrichtung (beispielsweise einem Smartphone) übermittelten Berechtigungscodes erfasst.

[0012] Der Berechtigungscodes wird bevorzugt in einem Speicher des elektronischen Schlüssels zwischengespeichert und nach Inkontaktbringen mit einem elektronischen Schloss über wenigstens einen Kontakt an diesen übermittelt.

[0013] Als elektronisches Schloss im Sinne dieser Erfindung wird jede elektronische Kontaktstelle bezeichnet, die für eine folgende Betätigung oder eine Freigabe einer Zugangsberechtigung geeignet ist.

[0014] Der mittels der Eingabeeinrichtung separat ohne eine räumliche Nähe zu dem zu öffnenden elektronischen Schloss in den elektronischen Schlüssel eingebaare Berechtigungscodes erhöht wesentlich die Sicherheit bei der Authentifikation der Zugriffsberechtigung, da die entsprechenden Zugangsdaten von nicht legitimierten Dritten kaum abgefangen werden können und der elektronische Schlüssel erst mit fertig eingegebenem Berechtigungscodes an das elektronische Schloss angenähert wird.

[0015] Ein eventuell entwendeter oder verloren gegangener elektronischer Schlüssel ist für den Dieb oder den Finder wertlos, da dieser nicht erkennen kann, für welches elektronische Schloss der betreffende Schlüssel durch den Berechtigungscodes präpariert wurde.

[0016] Die Eingabeeinrichtung und die Kontakte sind an unterschiedlichen Seiten des Gehäuses angeordnet. Dabei ist die Eingabeeinrichtung an einer Vorderseite des Gehäuses und sind die Kontakte an einer Rückseite des Gehäuses angeordnet. Dadurch lässt sich die Eingabeeinrichtung auch sehr einfach in einer Position betätigen, in der die Kontakte mit den jeweiligen Gegen-

kontakten am elektronischen Schloss in Eingriff stehen.

[0017] Außerdem ist der elektronische Schlüssel mit wenigstens einer elektrischen Spannungsquelle" die ein aufladbarer Akkumulator ist, versehen, der nicht nur der Eigenversorgung der elektronischen Komponenten des elektronischen Schlüssels dient, sondern darüber hinaus auch zur Speisung des elektronischen Schlosses zumindest während des Öffnungsvorgangs oder eines Initialisierungs- oder Aktivierungsvorgangs, während dessen das elektronische Schloss an eine eigene Spannungsversorgung angeschlossen werden kann. Außerdem ist der elektronische Schlüssel mit einem elektrischen Spannungswandler versehen, durch den eine geringere Ausgangsspannung des Akkumulators im elektronischen Schlüssel in eine vom elektronischen Schloss benötigte höhere Betriebsspannung umgewandelt wird. Beispielsweise ist der elektrische Spannungswandler als DC/DC-Wandler ausgebildet, der eine Eingangsspannung von beispielsweise 3,7 V einer als Akkumulator dienenden wieder aufladbaren Lithium-Ionen-Batterie in eine Ausgangsspannung von 12 V umwandelt, die zur Ansteuerung der meisten gängigen Motorschlösser oder elektrischer Aktoren ausreicht.

[0018] Der Vorteil besteht darin, dass die mit dem elektronischen Schloss versehene Einrichtung nicht ständig mit einer Betriebsspannung versorgt werden muss, da der erforderliche Strom zur Öffnung nur bei Bedarf vom elektronischen Schlüssel geliefert wird. So können beispielsweise entfernt von einem Stromnetz aufgestellte Rohrtresore, in denen physikalische Schlüssel deponiert sind, ganz ohne feste Stromversorgung aber auch ohne auszutauschende Batterien betrieben werden. Dadurch reduzieren sich Wartungsaufwand und Verschleiß dieser Systeme.

[0019] Schließfächer, Wertsachenfächer oder Tresore können ebenfalls ohne ständige Spannungsversorgung betrieben werden, da der Strom für eine Initialisierung eines Zugangs vom elektronischen Schlüssel geliefert wird. Optional betätigt das elektronische Schloss dabei nach Bestätigung einer Authentifikation der Zugriffsberechtigung zunächst ein Steuergerät, mittels dem dann eine fremde Betriebsspannungsquelle zur Betätigung eines Motorschlösses oder eines sonstigen Aktors aktiviert wird.

[0020] Der elektronische Schlüssel ist mit wenigstens einem Magneten -insbesondere einem Ringmagneten - zur Zentrierung im Zusammenwirken mit einem entsprechenden Gegenmagneten am elektronischen Schloss versehen. Durch die sich anziehenden Magnetkräfte bringt der elektronische Schlüssel sich bei einer Annäherung an das elektronische Schloss selbsttätig in die Kontaktposition.

[0021] Zur Unterstützung einer sicheren Kontaktbildung sind die Kontakte am elektronischen Schlüssel bevorzugt federnd in dessen Gehäuse gelagert.

[0022] Das elektronische Schließsystem umfasst außer dem elektronischen Schlüssel zumindest ein elektronisches Schloss, das mit wenigstens zwei konzent-

risch angeordneten Gegenkontakten und einer magnetischen Zentrierung versehen ist.

[0023] Gemäß einer vorteilhaften Anwendung eines elektronischen Schließsystems ist das elektronische Schloss an einem Verschlussdeckel eines Rohrtresors angeordnet ist, wobei der elektronische Schlüssel in seiner Kontaktposition mit dem elektronischen Schloss gleichzeitig bevorzugt als Handgriff für die Betätigung des Verschlussdeckels dient.

[0024] Gemäß einer alternativen Anwendung eines elektronischen Schließsystems ist das elektronische Schloss einem Motorschloss oder einem Aktor einer zu sichernden Einrichtung vorgeschaltet und aktiviert dessen Bestromung. Wie bereits erwähnt können dadurch Schließfächer, Wertsachenfächer oder Tresore ohne ständige Spannungsversorgung betrieben werden, da der Strom für eine Initialisierung eines Zugangs vom elektronischen Schlüssel geliefert wird. Optional betätigt das elektronische Schloss dabei nach Bestätigung einer Authentifikation der Zugriffsberechtigung zunächst ein Steuergerät, mittels dem dann eine fremde Betriebsspannungsquelle zur Betätigung eines Motorschlösses oder eines sonstigen Aktors aktiviert wird.

[0025] Die Gegenkontaktf Flächen am elektronischen Schloss sind bevorzugt als konzentrische Kreise ausgebildet sind, die mit den Kontakten des elektronischen Schlüssels in beliebiger relativer Winkelposition des elektronischen Schlüssels in Kontakt treten. Da keinerlei rotatorische Ausrichtung des elektronischen Schlüssels in Bezug auf das elektronische Schloss erforderlich ist, ist das Andocken des elektronischen Schlüssels am elektronischen Schloss vom Benutzer auch bei schlechten Sichtverhältnissen extrem einfach durchzuführen.

[0026] Ein erfindungsgemäßes Verfahren für eine gesicherte Erlangung einer Zugangsberechtigung oder für eine gesicherte Schlüssel-Übergabe für wenigstens einen Benutzer mittels eines erfindungsgemäßen Schließsystems zeichnet sich durch folgende Verfahrensschritte aus:

- Übersendung wenigstens einer für das elektronische Schloss (16) und/oder den Benutzer (22) charakteristischen Information (20; 22; 34) an eine entfernt vom elektronischen Schloss (16) angeordnete zentrale Informationsverarbeitungsstelle (30) mittels einer Kommunikationseinrichtung (24),
- Überprüfung der übersendeten Information (20; 22; 34) durch die zentrale Informationsverarbeitungsstelle (30),
- Übersendung eines Berechtigungscodes (36) an den Benutzer (22) mittels der Kommunikationseinrichtung (24) im Falle einer positiven Überprüfung der Information (20; 22; 34),
- Eingabe des Berechtigungscodes (36) durch den Benutzer (22) mittels der Eingabeeinrichtung (33) in den mitgeführten elektronischen Schlüssel (32),
- Entriegelung des elektronischen Schlosses (16) durch Zusammenwirken mit dem elektronischen

Schlüssel (32).

[0027] Durch die Überprüfung einer für das elektronische Schloss charakteristischen Information, beispielsweise einen im Bereich des Schlosses angeordneten, maschinell mittels einer Kommunikationseinrichtung oder manuell durch den Benutzer auslesbaren Codes und einer für den Benutzer charakteristischen Information, beispielsweise einem Passwort oder einer in die Kommunikationseinrichtung eingegebenen Buchstaben-/Zahlenkombination, die mittels einer Kommunikationseinrichtung an eine vom Schloss entfernt angeordnete zentrale Informationsverarbeitungsstelle gesendet und dort geprüft werden, ist ein hohes Maß an Sicherheit gegeben. Die Zugangsberechtigung wird nicht vor Ort im Bereich des zu öffnenden elektronischen Schlosses sondern entfernt davon in der Informationsverarbeitungsstelle geprüft und erteilt.

[0028] Nach der Erteilung und Übersendung des Berechtigungs_codes wird dieser an einen vom Benutzer mitgeführten elektronischen Schlüssel übermittelt, mittels dem dann die Entriegelung des elektronischen Schlosses erfolgt. Die Übermittlung des Berechtigungs_codes an den elektronischen Schlüssel stellt eine weitere vorteilhafte Sicherheitsbarriere dar. Alternativ zu einer manuellen Eingabe des übermittelten Berechtigungs_codes in den elektronischen Schlüssel mittels einer Eingabeeinrichtung kann die Übermittlung des Berechtigungs_codes auch automatisch, beispielsweise durch eine Übertragung mittels Bluetooth, eines Infrarotsenders oder anderer Nahbereichsübertragungsverfahren von der Kommunikationseinrichtung an den elektronischen Schlüssel erfolgen.

[0029] Das elektronische Schloss kann dabei selbst bereits eine Zugangsberechtigung zu einem geschützten Bereich oder einer geschützten Einrichtung ermöglichen. In einer alternativen Ausführungsform wird der geschützte Bereich jedoch von einem relativ kleinen, außen an einem Gebäude oder in der Nähe des Gebäudes angeordneten einbruchssicheren Behälter, beispielsweise einem Rohrtresor, gebildet. In diesem Rohrtresor gibt das elektronische Schloss nach Entriegelung durch den elektronischen Schlüssel den Zugang zu einem physikalischen Schlüssel frei, mittels dem dann das Gebäude betreten werden kann. Dabei ist der physikalische Schlüssel besonders vorteilhaft mit der Innenseite eines das elektronische Schloss beinhaltenden Verschlussdeckels des Rohrtresors verbunden, so dass dessen Rückgabe an den Rohrtresor nach Verlassen des Gebäudes und dem Wiederverschließen des Rohrtresors mittels des Verschlussdeckels zwangsweise erfolgt.

[0030] Gemäß einer weiteren vorteilhaften Anwendung empfängt das elektronische Schloss nach erfolgter Authentifikationsprüfung eine von einer elektrischen Spannungsquelle des elektronischen Schlüssels übertragene durch einen Spannungswandler veränderte Spannung und leitet diese zur Aktivierung eines elektrischen Motorschlosses oder eines elektrischen Aktors

-optional unter Zwischenschaltung eines Steuergeräts - an diese weiter.

[0031] In einer besonders einfachen Form wird die Kommunikationseinrichtung von einem Mobiltelefon gebildet, mittels dem der Benutzer - beispielsweise ein Wachmann eines Sicherheitsdienstes - die Informationsverarbeitungsstelle - beispielsweise die Servicezentrale des Sicherheitsdienstes - anruft und seinen Namen, eine für das Schloss spezifische Information und ein Passwort übermittelt, woraufhin die Informationsverarbeitungsstelle diese Informationen prüft, gegebenenfalls zusätzlich mit einem dort hinterlegten Einsatzplan abgleicht und bei einer positiven Bewertung aller Informationen einen Berechtigungscode an den Benutzer oder die Kommunikationseinrichtung übermittelt. Der Berechtigungscode kann dem Benutzer telefonisch mitgeteilt werden oder auch über eine von einem Rechner in der Informationsverarbeitungsstelle generierte Kurzmitteilung (SMS).

[0032] Der Benutzer gibt diesen Berechtigungscode über die Eingabevorrichtung an den von ihm mitgeführten elektronischen Schlüssel weiter und kann dann mit dem elektronischen Schlüssel das elektronische Schloss durch in Kontakt bringen betätigen.

[0033] Ausgehend von dieser besonders einfachen Form können einer oder mehrerer dieser Schritte automatisiert erfolgen. So kann beispielsweise mittels einer in der Kommunikationseinrichtung gespeicherten Software ("App") und entsprechenden Sensoren - beispielsweise einer Kamera eines als Kommunikationseinrichtung dienenden Smartphones - der Code des elektronischen Schlosses automatisch ausgelesen werden. Dies kann beispielsweise mittels eines in dem Smartphone gespeicherten Barcode-Leseprogramms oder Aztec-Code-Leseprogramms erfolgen, wozu in diesen Fällen ein entsprechender grafischer Code im Bereich des elektronischen Schlosses angeordnet ist. Es sind jedoch ebenso auch andere im Bereich des elektronischen Schlosses angeordnete elektronische Signalgeber und entsprechend darauf ausgerichtete Sensoren in der Kommunikationseinrichtung möglich, beispielsweise ein unsichtbares, magnetisch codiertes Signal.

[0034] Der Berechtigungscode kann auch als Barcode, QR-Code oder in ähnlicher Form an das Smartphone des Benutzers übermittelt werden. Der übermittelte Code wird dann in dem Falle, dass er in maschinenlesbarer Form übermittelt wird, von der Kommunikationseinrichtung (dem Smartphone) an eine elektronische Eingabevorrichtung am elektronischen Schlüssel übertragen.

[0035] Die für den Benutzer charakteristische Information kann auch durch die in der Kommunikationseinrichtung gespeicherte Software automatisiert beispielsweise nach Einlesen der für das elektronische Schloss spezifischen Information abgefragt und vom Benutzer beispielsweise als Buchstaben-/Zahlenkombination eingegeben und an die Informationsverarbeitungsstelle übermittelt werden.

[0036] Als weiterer vorteilhafter Verfahrensschritt ist

vorgesehen, dass die Informationsverarbeitungsstelle vor der Übersendung eines Berechtigungscodes an den Benutzer zusätzlich zu der für das elektronische Schloss und/oder für den Benutzer charakteristischen Information eine mit beiden Informationen durch einen Einsatzplan verknüpfte Information für den Einsatzort und/oder die Einsatzzeit prüft. Hierdurch wird eine zusätzliche Sicherheit geschaffen, da ausgeschlossen wird, dass ein Zugangscode auch völlig außerhalb einer normalen vorgesehenen Route eines Sicherheitspersonals übermittelt wird.

[0037] Eine weitere vorteilhafte Ausgestaltung der Erfindung sieht vor, dass das elektronische Schloss und/oder die von diesem geschützte Einrichtung beim Freigeben und beim Schließen des elektronischen Schlosses eine Information an die zentrale Informationsverarbeitungsstelle sendet.

[0038] Eine vorteilhafte Weiterbildung des Systems sieht vor, dass die Prüfung in der zentralen Informationsverarbeitungsstelle weiterhin die Auswertung wenigstens eines Zeit-Parameters umfasst, der die für das Schloss und/oder den Benutzer charakteristischen Information anhand eines hinterlegten Zeitplans - insbesondere den Routenplan eines Wachmanns - für das vorgesehene Öffnen des Schlosses verifiziert.

[0039] In einer besonderen Ausgestaltung kann vorgesehen sein, dass die Kommunikationseinrichtung und der elektronische Schlüssel eine Einheit bilden. Diese Einheit vereint alle Funktionen eines Senders und Empfängers zur Erfassung und Übersendung der für das Schloss und/oder den Benutzer charakteristischen Informationen an eine zentrale Informationsverarbeitungsstelle und zum Empfang eines Berechtigungscodes mit der Funktion des elektronischen Schlüssels. Mittels des eingegangenen Berechtigungscodes wird der elektronische Schlüssel, beispielsweise ein magnetischer Transponder, so programmiert, dass dieser zum Öffnen des elektronischen Schlosses verwendbar ist.

[0040] Die vorliegende Erfindung ist beispielsweise in Verbindung mit einem Rohrtresor anwendbar, wie er beispielsweise in der WO 2012/045474 A1 offenbart ist. Dabei dient der Transponder als elektronischer Schlüssel nach dem Aufsetzen auf das elektronische Schloss unmittelbar als Handgriff für das Entnehmen des Verschlussdeckels.

[0041] Nachfolgend wird ein Ausführungsbeispiel der Erfindung anhand der Zeichnung erläutert. Es zeigt:

- Fig. 1 einen Rohrtresor mit einem in einen Verschlussdeckel integrierten elektronischen Schloss und einem für das elektronische Schloss charakteristischen Code,
 Fig. 2 ein Ablaufdiagramm, das die Übermittlung der Codes zwischen einem Benutzer und einer zentralen Informationsverarbeitungsstelle verdeutlicht,
 Fig. 3 die Hand eines Benutzers bei der Eingabe des Berechtigungscodes in einen elektronischen

- Schlüssel,
 Fig. 4 die Verwendung des elektronischen Schlüssels als Griff beim Öffnen des elektronischen Schlosses,
 5 Fig. 5 die Anordnung eines physikalischen Schlüssels an der Innenseite des Verschlussdeckels des Rohrtresors,
 Fig. 6 ein Ablaufdiagramm, das die Kommunikation zwischen dem Benutzer, einem Client-Rechner, einem Server, einem Administrator und dem elektronischen Schloss verdeutlicht,
 10 Fig. 7 ein Diagramm, das die Funktionen auf Seiten des Benutzers, des Clientrechners, des Servers und des Administrators verdeutlicht
 Fig. 8 einen schematischen Schaltplan für eine Anwendung eines elektronischen Schlosses im Zusammenwirken mit einem Steuergerät und einem Motorschloss,
 15 Fig. 9 eine schematische Vorderansicht eines elektronischen Schlüssels, und
 20 Fig. 10 eine schematische Ansicht der Rückseite eines elektronischen Schlüssels.

[0042] Die in Fig. 1 dargestellte Verschlussvorrichtung 10 wird von einem Rohrtresor 12 gebildet, der diebstahls- und aufbruchssicher in einer Wand eines Gebäudes oder an einem stabilen Träger in der Nähe des Gebäudes angeordnet ist. Der Rohrtresor 12 ist mittels eines Verschlussdeckels 14 an seiner Vorderseite verschlossen. In den Verschlussdeckel 14 integriert ist ein elektronisches Schloss 16, wie es detailliert in der WO 2012/045474 A1 dargestellt und beschrieben ist, deren Offenbarungsgehalt hiermit zum Gegenstand der vorliegenden Anmeldung gemacht wird.

[0043] An der Innenseite des Verschlussdeckels 14 ist - wie in Figur 5 dargestellt - ein physikalischer Schlüssel 18 angeordnet, mittels dem wenigstens ein Zugang zu dem nicht dargestellten Gebäude und optional weitere Türen in diesem Gebäude geöffnet werden können.

[0044] An der mittels des elektronischen Schlosses 16 versperrten Verschlussvorrichtung 10 ist ein für das elektronische Schloss 16 charakteristischer Code 20 angeordnet. Dieser ist im gezeigten Ausführungsbeispiel in Form eines Barcodes 20 ausgebildet, kann jedoch auch von einem Aztek-Code oder einem unsichtbaren magnetischen Code gebildet werden. Der Code 20 kann im einfachsten Falle von einem Benutzer 20 manuell ausgelesen werden. Gemäß einer vorteilhaften Ausgestaltung verfügt eine vom Benutzer 22 mitgeführte Kommunikationseinrichtung 24 über einen Sensor oder eine Leseeinrichtung zum automatischen Erfassen des Codes 20. Die Kommunikationseinrichtung 24 kann beispielsweise von einem Smartphone gebildet werden, dessen Kamera in Verbindung mit einem gespeicherten Anwendungsprogramm ("App") zum Einlesen eines Barcodes oder alternativ eines Aztek-Codes dient, die im Ausführungsbeispiel als für das elektronische Schloss 16 charakteristischer Code 20 verwendet werden. Wie schon

erwähnt, können auch unsichtbare, magnetisch oder über ein Funksignal übermittelte Codes 20 durch das elektronische Schloss 16 oder eine in dessen Nähe angeordnete Einrichtung ausgesendet und von der Kommunikationseinrichtung 24 empfangen oder ausgelesen werden.

[0045] Das elektronische Schloss 16 ist mittels eines elektronischen Schlüssels 32 aufschließbar, sofern in diesen elektronischen Schlüssel 32 ein für das elektronische Schloss 16 passender Berechtigungscode 36 eingegeben wird. In Figur 3 ist dargestellt, wie der Berechtigungscode 36 vom Benutzer 22 über eine am elektronischen Schlüssel 32 angeordnete Tastatur eingegeben wird. Der elektronische Schlüssel 32 kann dann anschließend, wie in Figur 4 gezeigt, auf das elektronische Schloss 16 aufgesetzt und unmittelbar als Handgriff für das Öffnen des Verschlussdeckels 14 verwendet werden.

[0046] Diesem Vorgang voraus geht jedoch erfindungsgemäß die in den Figuren 2, 6 und 7 dargestellte Prozedur, bei der der Benutzer 22 die für das elektronische Schloss 16 charakteristische Information (den Code 20) und eine für seine Person charakteristische Information in Form eines Codes 26 - beispielsweise in Form eines persönlichen Passworts oder einer Buchstaben-/Zahlenkombination - mittels der Kommunikationseinrichtung 24 an eine zentrale Informationsverarbeitungsstelle 30 - beispielsweise die Zentrale eines Sicherheitsdienstes - übermittelt. Die für das elektronische Schloss 16 charakteristische Information 20 und die für die Person des Benutzers 22 charakteristische Information 26 bilden gemeinsam einen Anfrage-Datensatz 34, der im einfachsten Fall manuell über ein Telefonat an die zentrale Informationsverarbeitungsstelle 30 übermittelt wird. Gemäß einer vorteilhaften Ausgestaltung der Erfindung erfolgt die Übermittlung des Anfrage-Datensatzes 34 automatisiert, beispielsweise als Zeichenkette in einer von der Kommunikationseinrichtung 24 versendeten Kurzmitteilung (SMS).

[0047] In der Informationsverarbeitungsstelle 30 wird der Anfrage-Datensatz 34 mit den darin enthaltenen Codes 20 und 26 vorzugsweise unter zusätzlichem Abgleich mit einem Zeit-Parameter 28 (beispielsweise dem Dienstplan oder Routenplan des Benutzers 22) geprüft. Sofern diese Überprüfung zu einem positiven Ergebnis führt, sendet die Informationsverarbeitungsstelle 30 einen Berechtigungscode 36 an die Kommunikationseinrichtung 24. Dies kann im einfachsten Fall wiederum durch ein Telefonat erfolgen. Gemäß einer vorteilhaften Weiterbildung erfolgt die Übermittlung des Berechtigungscode 36 an die Kommunikationseinrichtung 24 automatisiert, beispielsweise in Form einer in eine Kurzmitteilung (SMS) eingebetteten Zeichenkette.

[0048] Der Berechtigungscode 36 wird vom Benutzer 22, wie bereits in Verbindung mit Figur 3 erwähnt, über eine Eingabeeinrichtung, insbesondere eine Tastatur manuell an den elektronischen Schlüssel 32 übertragen.

[0049] Die zentrale Informationsverarbeitungsstelle

30 weist vorteilhaft wenigstens einen Client-Rechner 310 und wenigstens einen Server 320 auf. Der Client-Rechner 310 dient zum Empfang des Anfrage-Datensatzes 34 und zur Übermittlung dieses Datensatzes an den Server 320. Der Daten-Verkehr zwischen dem Client-Rechner 310 und dem Server 320 ist in den Figuren mit 315 bezeichnet.

[0050] Im Server 320 werden zusätzlich Zeit-Parameter 28 gespeichert, die beispielsweise einen Routenplan des Benutzers 22 mit einer für das Öffnen des betreffenden elektronischen Schlosses 16 charakteristischen Zeit vorzugsweise mit einem entsprechenden Zeitpuffer (früheste Öffnungszeit, späteste Öffnungszeit, späteste Schließzeit) abbilden. Sämtliche Daten im Server 320 werden von einem Administrator 330 verwaltet. Der Datenverkehr zwischen dem Server 320 und dem Administrator 330 ist in den Figuren mit 325 bezeichnet.

[0051] An den Server 320 wird vorzugsweise auch ein Signal übermittelt, das beim Öffnen und Schließen des elektronischen Schlosses 16 von einem am elektronischen Schloss 16 installierten Sender automatisch gesendet wird. Das erfindungsgemäße Verfahren und das erfindungsgemäße System können entgegen der Darstellung in den Figuren 2, 6 und 7 in einer fortgeschrittenen Ausführungsform auch vollautomatisch ohne menschliche Interaktion funktionieren. Der Empfang eines Anfrage-Datensatzes 34 durch den Client-Rechner 310, die Übermittlung des Anfrage-Datensatzes 34 an den Server 320, die Überprüfung der im Anfrage-Datensatz 34 enthaltenen charakteristischen Informationen (Codes 20 und 26), der Abgleich mit dem wenigstens einen Zeit-Parameter 28, die Generierung eines Berechtigungscode 36 und die Übermittlung des Berechtigungscode 36 an die Kommunikationseinrichtung 24, gegebenenfalls wiederum unter Zwischenschaltung eines Client-Rechners 310 können vorzugsweise mittels einer Software gesteuert vollautomatisch erfolgen.

[0052] Dass das erfindungsgemäße Verfahren und System zur gesicherten Freigabe einer Zugangsberechtigung bzw. zur gesicherten Schlüssel-Übergabe auch auf Seiten des Benutzers 22 vollautomatisch erfolgen kann, wurde bereits im Zusammenhang mit den möglichen Ausführungsformen der Kommunikationseinrichtung 24 und des elektronischen Schlüssels 32 beschrieben.

[0053] Der elektronische Schlüssel 32 ist gemäß der Erfindung mit einer Eingabeeinrichtung 33 versehen, mittels der der Benutzer 22 den von der zentralen Informationsverarbeitungsstelle 30 an die Kommunikationseinrichtung 24 übermittelten Berechtigungscode 36 in den elektronischen Schlüssel eingeben kann. Ein derartiger, mit einer Eingabeeinrichtung 33 versehener elektronischer Schlüssel 32 ist generell auch an Stelle der heute schon weit verbreiteten stationären Eingabeeinrichtungen verwendbar, bei denen die Eingabe eines Codes durch einen berechtigten Benutzer von einem unberechtigten Beobachter relativ leicht beobachtet werden kann und dadurch ein erhebliches Sicherheitsrisiko darstellt.

Dagegen kann die Eingabe eines Codes in einen mobilen elektronischen Schlüssel 32, der erst im Anschluss zur Öffnung eines elektronischen Schlosses verwendet wird, völlig unbeobachtet schon in einiger Entfernung vom elektronischen Schloss 16 erfolgen.

[0054] Als elektronischer Schlüssel 32 kann wie im gezeigten Ausführungsbeispiel ein auf das elektronische Schloss 16 aufgesetzter, durch Magnetkraft temporär mit dem elektronischen Schloss 16 verbundener Schlüssel 32 verwendet werden. Die Magnetkräfte werden durch einen Magneten 329 im zentralen Bereich des elektronischen Schlüssels 32 und durch einen Gegenmagneten 161 im zentralen Bereich des elektronischen Schlosses 16 bereitgestellt, die bevorzugt als Permanent-Ringmagnete ausgebildet sind und für eine automatische Zentrierung des elektronischen Schlüssels 32 mit dem elektronischen Schloss 16 sowie eine Ausrichtung der Kontakte 324, 325 und 326 zu den konzentrisch angeordneten Gegenkontakflächen 164, 165, 166 am elektronischen Schloss 16 unabhängig vom relativen Winkel zueinander sorgen.

[0055] Es sind jedoch ebenso berührungslos über eine gewisse Distanz mit dem elektronischen Schloss 16 zusammenwirkende elektronische Schlüssel 32, beispielsweise in Form eines Transponders, verwendbar.

[0056] Der elektronische Schlüssel 32 weist ein Gehäuse 321 auf, auf dessen Vorderseite gemäß Fig. 3 und 9 die Eingabeeinrichtung 33 angeordnet ist. Im gezeigten Ausführungsbeispiel ist dies eine numerische Tastatur mit 10 Zifferntasten 331, einer Lösch Taste 332 ("C") und einer Eingabetaste 333 ("OK"). Auf der Rückseite des Gehäuses 321 treten drei federnd im Gehäuse gelagerte Kontakte 324, 325 und 326 hervor, von denen der zentral angeordnete Kontakt 325 beispielsweise die Plusspannung führt, der am weitesten außen liegende Kontakt 324 die Masseverbindung darstellt und der Kontakt 326 für eine serielle Datenübermittlung dient.

[0057] In der rückseitigen Ansicht des elektronischen Schlüssels 32 gemäß Fig. 10 ist auch der Deckel eines Akku-Fachs 327 angedeutet, hinter dem ein Akkumulator 332 angeordnet ist. Dieser ist beispielsweise als Lithium-Ionen-Akkumulator mit einer Ausgangsspannung von 3,7 V ausgebildet.

[0058] Zur Erhöhung der Ausgangsspannung auf beispielsweise 12 V ist ein Spannungswandler in Form eines DC/DC-Wandlers 323 im elektronischen Schlüssel 32 angeordnet.

[0059] Der elektronische Schlüssel 32 ist weiterhin mit wenigstens einer Schnittstelle 328 versehen, die im vorliegenden Fall beispielsweise von einer Micro-USB-Schnittstelle gebildet wird und zur Programmierung des elektronischen Schlüssels 32 und optional auch zur Aufladung des Akkumulators 322 dient.

[0060] Der elektronische Schlüssel 32 wirkt entweder mit dem in den Figuren 1 bis 5 gezeigten elektronischen Schloss 16 zum Beispiel an einem Rohrtresor 12 oder an einem geschützten Raum oder einer anderen, eine Zugangsberechtigung erfordernden Einrichtung zusam-

men. Der Begriff der "Einrichtung" ist hierbei sehr weit zu sehen. Es können Maschinen, Fahrzeuge oder ähnliches, aber auch Schließfächer, Wertfächer, Tresore oder Türen zu Sicherheitsbereichen durch ein elektronisches Schloss 16 geschützt werden.

[0061] Das Beispiel gemäß Fig. 8 zeigt, dass die geschützte Einrichtung durch das elektronische Schloss 16 auch nicht nur unmittelbar, sondern auch mittelbar freigegeben werden kann. In diesem Fall wirkt das elektronische Schloss 16 als 220 V-Schutzmodul für eine nicht dargestellte geschützte Einrichtung, die letztendlich erst durch die Betätigung eines Motorschlusses 40 freigegeben wird.

[0062] Zwischen dem elektronischen Schloss 16 und dem Motorschloss 40 ist in diesem Fall noch ein Steuergerät 50 angeordnet, das mittels einer eigenen Spannungsversorgung versorgbar ist, die jedoch erst durch die Betätigung des elektronischen Schlosses 16 aktiviert wird. Nach Übermittlung eines gültigen Berechtigungscodes 36 vom in Fig. 8 nicht dargestellten elektronischen Schlüssel 32 über den für die Datenübermittlung zuständigen Gegenkontakt 166 wird die externe Spannungsversorgung am Steuergerät 50 aktiviert und das Motorschloss 50 betätigt. Für die Phase der Überprüfung des Berechtigungscodes 36 wird dagegen die erforderliche Betriebsspannung am Steuergerät 50 vom elektronischen Schlüssel 32 über das elektronische Schloss 16 bereitgestellt. Eine detailliertere Beschreibung des Steuergeräts 50 folgt am Ende der Beschreibung.

[0063] Der Vorteil einer mittelbaren Betätigung liegt darin, dass bei einer Nichtbenutzung der geschützten Einrichtung an dieser auch keine Betriebsspannung anliegen muss. Diese kann durch den elektronischen Schlüssel 32 über das elektronische Schloss 16 bei Bedarf jederzeit initialisiert werden.

[0064] An Stelle der gezeigten drei Kontakte 324, 325 und 326 des elektronischen Schlüssels 32 mit den drei Gegenkontakten 164, 165 und 166 des elektronischen Schlosses, genügen bei einer Abwandlung auch zwei dieser Kontakte, wenn die Datenübertragung beispielsweise gleichzeitig mit über den Massekontakt erfolgt.

[0065] Ein Lithium-Ionen-Akkumulator 322 kann mit einer Eingangsspannung von 3,7 V mittels eines DC/DC-Wandlers mit hohem Wirkungsgrad bei einer Ausgangsspannung von 12 V kurzzeitig eine Leistung von 7 Watt bereitstellen. Die Kapazität des Akkumulators 322 reicht dann ohne Nachladung für ca. 700 Öffnungsvorgänge. Ein Unterspannungsschutz signalisiert bevorzugt am elektronischen Schlüssel 32 mittels einer Diode und/oder eines Summers einen Abfall der Akku-Spannung beispielsweise auf 2,7 V, so dass vor einem weiteren Einsatz eine Nachladung des Akkumulators 322 erfolgen muss.

[0066] Vorteilhaft ist auch das Vorsehen eines nicht dargestellten Kondensators im Steuergerät 50 zur Pufferung der vom elektronischen Schlüssel 32 übermittelten Energie. Der Kondensator wird während oder unmittelbar nach Prüfung der Zugangsberechtigung geladen und führt dann mit seiner gespeicherten Ladungs-Kapa-

azität allein den anschließenden Öffnungs- bzw. Freigabevorgang aus. Der Kondensator gewährleistet, dass das elektronische Schloss 16 bei einer mangelhaften Restkapazität des Akkumulators 322 nicht während eines Öffnungsvorgangs in einer Zwischenstellung hängen bleibt.

[0067] Durch Verwendung von Teilen aus dem Mobilfunkbereich sind der elektronische Schlüssel, das elektronische Schließsystem und das erfindungsgemäße Verfahren kostengünstig realisierbar.

Beschreibung des Steuergeräts 50:

Funktionsbaugruppen

[0068] Die Steuerelektronik kann in 5 Unterfunktionsbaugruppen aufgeteilt werden:

- Microcontroller mit Speicher und Resetcontroller
- Identifikationsbaustein mit Timer und Signalisierung
- Schaltstufe und Festspannungsausgängen
- Stromversorgung
- DC/DC Wandler (Wird dieses Modul eingesetzt, entfällt die externe Stromversorgung!)

Microcontroller mit Speicher und Reset-Controller:

[0069] Zur zentralen Steuerung und Auswertung des gesamten Informationsaustauschs zwischen Pylocx-Systemschlüssel (elektronischer Schlüssel 32) und Steuergerät 50 inklusive der Ansteuerung des Motorschlösses 40 wird ein PIC Microcontroller der Firma Microchip verwendet. Hierbei spielen Energiebedarf, hohe Integrationsdichte,

[0070] Wirtschaftlichkeit aber auch die große Erfahrung mit dem PC-Assembler die entscheidende Rolle. Um Daten nichtflüchtig zu speichern, kommuniziert der Microcontroller über einen I²C Bus mit einem EEPROM mit 256Kb.

[0071] Um beim Einschalten der Stromversorgung bzw. bei kurzfristigen Spannungseinbrüchen den Microcontroller definiert ein- und auszuschalten, wird ein Resetcontroller eingesetzt. Dieser Resetcontroller schaltet den Microcontroller bei einer Betriebsspannung <2,4V in den Reset und gibt den Reset bei einer Betriebsspannung >2,7V wieder frei.

Identifikationsbaustein mit Timer und Signalisierung:

[0072] Jedes Steuermodul (Steuergerät 50) muss eine eindeutige, einmalige und unveränderbare Identifikation besitzen. Der gewählte Baustein aus der DS Familie der Fa. Dallas besitzt eine solchen ROM Code und eignet sich somit hervorragend. Zusätzlich ist in diesem Baustein eine Echtzeituhr integriert, die zum Protokollieren von Ereignissen notwendig ist. Die Echtzeituhr benötigt natürlich eine kontinuierliche Stromversorgung, weshalb hier eine Lithium-Knopfzelle eingesetzt wird. Die Lithi-

umzelle stellt mindestens für 10 Jahre die Stromversorgung der Echtzeituhr sicher. Der Identifikationsbaustein kommuniziert über ein MicroLAN Protokoll mit dem Microcontroller.

[0073] Um den Bediener über Zustände des Steuergerätes 50 zu informieren, ist ein akustischer Signalgeber (Piezo-Piepser) integriert, der auch durch das Gehäuse gut zu hören ist. Sollte eine abgesetzte Signalisierung gewünscht werden, ist über den entsprechenden Ausgang eine akustische und/oder optische Signalquelle anschließbar. Diese externe Signalisierung läuft synchron zur Internen.

Schaltstufe und Festspannungsausgänge:

[0074] Das Steuermodul (Steuergerät 50) soll hinsichtlich der anzuschließenden Motorschlösser 40 und elektrischer Riegel sehr universell einsetzbar sein. Aus diesem Grund wurde ein Relais als potentialfreier Umschalter zur Ansteuerung der Motorschlösser 40 bzw. der elektrischen Riegel ausgewählt. Wird zur Ansteuerung von Schaltelementen eine Gleichspannung benötigt, kann über den entsprechenden Ausgang eine Festspannung über den potentialfreien Umschalter geschaltet werden. Der Festspannungsausgang kann über einen Jumper (im Inneren des Steuergerätes) konfiguriert werden. Es stehen 3 Spannungen zur Auswahl: 6V, 9V oder 12V jeweils max. 500mA. Die Festspannungen sind stabilisiert und entstört (Restwelligkeit < 20mV).

Stromversorgung:

[0075] Das Steuermodul (Steuergerät 50) wird über Netzspannung versorgt. Als Netzteil kommt ein gekapseltes Schaltnetzteil zur Anwendung. Zum Schutz vor Überlast befindet sich eine Feinsicherung (200mA träge) im Primärkreis des Netzteils. Die Feinsicherung befindet sich im Inneren des Steuergeräts 50. Durch entsprechende Schaltungstechnik des Schaltnetzteils, sind Eingangsspannungen von 110 bis 250 VAC 50/60 Hz anschließbar. Das Schaltnetzteil liefert 12VDC Ausgangsspannung, die 6 VDC und 9 VDC werden aus den 12 VDC über Festspannungsregler (auf Kühlblech) generiert.

[0076] Bei Stromausfall kann das Steuergerät 50 von außen mit Spannung versorgt werden (Notbestromung). Hierzu wird ein Pylocx-Notbestromungsgerät mit der Pylocx-Kontaktstelle (elektronisches Schloss 16) verbunden. Dabei wird die Spannung der internen Batterie (9V) des Pylocx-Notbestromungsgeräts über den Mittelkontakt 165 der Pylocx-Kontaktstelle (elektronisches Schloss 16) direkt dem Steuermodul (Steuergerät 50) zur Verfügung gestellt. Sodann wird der entsprechende Pylocx-Transponder mit dem Notbestromungsgerät verbunden. Die weitere Bedienung ist wie im Normalbetrieb. Es ist zu beachten, dass durch den 9V-Notbetrieb 12V-Schlösser nur eingeschränkt versorgt werden können. Ebenfalls ist der Strom durch den Batteriebetrieb auf

300mA beschränkt.

DC/DC Wandler:

[0077] Der DC/DC Wandler wird über den Notstromeingang (innerster Kontakt der Kontaktstelle) des Steuergerätes angesteuert. Die hier eingespeiste Spannung (3,7 VDC) des Akkus 322 aus dem elektronischen Schlüssel 32 wird vom DC/DC Wandler auf 12 VDC hochtransformiert. Diese 12 VDC werden dem Stromversorgungsteil des Steuergerätes zugeführt. Anstelle der 12 VDC die das Schaltnetzteil aus den 230 VAC generiert, stehen nun für die interne Elektronik des Steuergerätes sowie zur Ansteuerung eines externen Motorschlusses direkt diese 12 VDC zu Verfügung. Somit ist keine externe Stromversorgung zum Betrieb notwendig.

Weitere Hardwarekomponenten auf der Steuerelektronik:

[0078] Um die Firmware des Microcontrollers im Fertigungsprozess zu laden, ist eine 5-polige Kontaktleiste vorhanden. Über diese Kontaktleiste kann auch ein Software-Update der Firmware durchgeführt werden. Die Kontaktleiste befindet sich direkt auf der Leiterplatte des Steuergerätes 50 und ist für den Nutzer nicht zugänglich. Des weiteren wurden EMV Schutzkomponenten an den Schnittstellen nach außen vorgesehen. Der MicroLAN, die Steuereingänge und der Universaleingang sind über Suppressor-Dioden geschützt, der externe Signalausgang ist über ein VDR-Überspannung geschützt. Um die Schutzfunktion zu erhöhen, befinden sich weitere Bauelemente zum Schutz der MicroLAN Leitung und der Betriebsspannungsleitung auf der Leiterplatte. Die MicroLAN Leitung wird über einen weiteren Varistor geschützt. Die Notbestromungsleitung wird ebenfalls mit einem Varistor geschützt. Zusätzlich ist zum Schutz von DC Spannung eine Zenerdiode mit PPTC eingefügt. Mit diesen Maßnahmen werden Gleichspannungen (ohne Strombegrenzung) bis 30V und statische Hochspannung bis 6kV sicher abgeblockt. Um 220 V Wechselspannung, die über die Kontaktstelle eingespeist werden kann, abzublocken, können zwei Gasableiter in einem separaten Gehäuse zwischen Steuergerät 50 und Kontaktstelle (elektronisches Schloss 16) geschaltet werden. Die obligatorischen Blockkondensatoren wurden berücksichtigt.

Bezugszeichenliste

[0079]

10	Verschlussvorrichtung
12	Rohrtresor
14	Verschlussdeckel
16	elektronisches Schloss
161	Gegenmagnet
164	Gegenkontaktfläche

165	Gegenkontaktfläche
166	Gegenkontaktfläche
18	Schlüssel
20	Code (für 16)
22	Benutzer
24	Kommunikationseinrichtung (von 22)
26	Code (von 22)
28	Zeit-Parameter
30	Informationsverarbeitungsstelle
310	Client-Rechner
315	Datenverkehr (zwischen 310 und 320)
320	Server
325	Daten-Verkehr (zwischen 320 und 330)
330	Administrator
32	elektronischer Schlüssel
321	Gehäuse
3211	Befestigungsöse
322	Akkumulator
323	Spannungswandler (DC/DC)
324	Kontakt
325	Kontakt
326	Kontakt
327	Akku-Fach
328	Schnittstelle (z.B. Micro-USB)
329	Magnet
33	Eingabeeinrichtung (Tastatur)
331	Tasten (alphanumerisch)
332	Löschtaste (Clear)
333	Eingabetaste (OK)
34	Anfrage-Datensatz
36	Berechtigungscodes
38	Öffnungs-/Schließsignal (von 16)
40	Motorschloss
50	Steuergerät

Patentansprüche

- Elektronisches Schließsystem mit einem elektronischen Schlüssel (32), wenigstens einem elektronischen Schloss (16), einer entfernt vom elektronischen Schloss (16) angeordneten zentralen Informationsverarbeitungsstelle und einer Kommunikationseinrichtung (24) zur Übersendung wenigstens einer für das elektronische Schloss (16) und/oder den Benutzer (22) charakteristischen Information (20; 22; 34) an die zentrale Informationsverarbeitungsstelle (30), wobei der elektronische Schlüssel (32) wenigstens zwei Kontakte (324, 325, 326) zur Übermittlung von Daten und Energie an das elektronische Schloss (16) und wenigstens eine an einem Gehäuse (321) des elektronischen Schlüssel (32) vorgesehene Eingabeeinrichtung (33) zur Eingabe eines Berechtigungscodes (36) umfasst, wobei der elektronische Schlüssel (32) mittels über die Eingabeeinrichtung (33) eingetragener Berechtigungscodes für das Öffnen verschiedener elektronischer Schlösser programmierbar ist, wobei die Eingabe-

- einrichtung (33) und die Kontakte (324, 325, 326) an unterschiedlichen Seiten des Gehäuses (321) angeordnet sind, wobei die Eingabeeinrichtung (33) an einer Vorderseite und die Kontakte (324, 325, 326) an einer gegenüberliegenden Rückseite des Gehäuses (321) angeordnet sind und wobei der elektronische Schlüssel mit wenigstens einem aufladbaren Akkumulator als elektrische Spannungsquelle (322) und einem elektrischen Spannungswandler, durch den eine geringere Ausgangsspannung des Akkumulators im elektronischen Schlüssel in eine vom elektronischen Schloss benötigte höhere Betriebsspannung umgewandelt wird, versehen ist und wobei der elektronische Schlüssel (32) mit wenigstens einem Magneten (329) zur Zentrierung im Zusammenwirken mit einem entsprechenden Gegenmagneten (161) am elektronischen Schloss (16) versehen ist, wobei ferner das wenigstens eine elektronische Schloss (16) mit wenigstens zwei konzentrisch angeordneten Gegenkontakten (164, 165, 166) und einer magnetischen Zentrierung versehen ist, wobei das elektronische Schloss nichtständig mit einer Betriebsspannung versorgt wird, wobei die zentrale Informationsverarbeitungsstelle (30) zur Überprüfung der übersendeten Information (20; 22; 34) und zu einer Übersendung eines Berechtigungscodes (36) an den Benutzer (22) mittels der Kommunikationseinrichtung (24) im Falle einer positiven Überprüfung der Information (20; 22; 34) ausgebildet ist, und wobei nach einer Eingabe des Berechtigungscodes (36) durch den Benutzer (22) mittels der Eingabeeinrichtung (33) in den mitgeführten elektronischen Schlüssel (32) durch in Kontakt bringen des elektronischen Schlüssels (32) mit dem elektronischen Schloss (16) eine Übermittlung von Daten und Energie vom elektronischen Schlüssel (32) an das elektronische Schloss (16) eine Entriegelung des elektronischen Schlosses (16) bewirken kann.
2. Elektronisches Schließsystem nach Anspruch 1, **dadurch gekennzeichnet, dass** die Gegenkontakte (164, 165, 166) als konzentrische Kreise ausgebildet sind, die mit den Kontakten (324, 325, 326) des elektronischen Schlüssels (32) in beliebiger relativer Winkelposition des elektronischen Schlüssels (32) in Kontakt treten.
3. Elektronisches Schließsystem nach Anspruch 1 oder 2, **dadurch gekennzeichnet, dass** das elektronische Schloss (16) an einem Verschlussdeckel (14) eines Rohrtresors (12) angeordnet ist, wobei der elektronische Schlüssel (32) in Kontakt mit dem elektronischen Schloss (16) als Handgriff für die Betätigung des Verschlussdeckels (14) dient.
4. Elektronisches Schließsystem nach Anspruch 1 oder 2, **dadurch gekennzeichnet, dass** das elektronische Schloss (16) einem Motorschloss (40) ein-
ner zu sichernden Einrichtung vorgeschaltet ist und dessen Bestromung aktiviert und dass insbesondere zwischen dem elektronischen Schloss (16) und dem Motorschloss (40) ein Steuergerät (50) angeordnet ist, dessen Bestromung durch den elektronischen Schlüssel (32) bei Inkontaktbringen mit dem elektronischen Schloss (16) und erfolgter Verifizierung des mittels der Eingabeeinrichtung (33) eingegebenen Berechtigungscodes (36) aktiviert wird.
5. Verfahren für eine gesicherte Erlangung einer Zugangsberechtigung oder für eine gesicherte Schlüssel-Übergabe mittels eines elektronischen Schließsystems nach einem der Ansprüche 1 bis 4, wobei das Verfahren folgende Verfahrensschritte umfasst:
- Übersendung wenigstens einer für das elektronische Schloss (16) und/oder den Benutzer (22) charakteristischen Information (20; 22; 34) an eine entfernt vom elektronischen Schloss (16) angeordnete zentrale Informationsverarbeitungsstelle (30) mittels einer Kommunikationseinrichtung (24),
 - Überprüfung der übersendeten Information (20; 22; 34) durch die zentrale Informationsverarbeitungsstelle (30),
 - Übersendung eines Berechtigungscodes (36) an den Benutzer (22) mittels der Kommunikationseinrichtung (24) im Falle einer positiven Überprüfung der Information (20; 22; 34),
 - Eingabe des Berechtigungscodes (36) durch den Benutzer (22) mittels der Eingabeeinrichtung (33) in den mitgeführten elektronischen Schlüssel (32),
 - Entriegelung des elektronischen Schlosses (16) durch Zusammenwirken mit dem elektronischen Schlüssel (32).
6. Verfahren nach Anspruch 5, **dadurch gekennzeichnet, dass** die für das Schloss (16) charakteristische Information (20) von einer Zahlenkombination oder von einem Barcode gebildet wird.
7. Verfahren nach Anspruch 5 oder 6, **dadurch gekennzeichnet, dass** die für den Benutzer (22) charakteristische Information (26) von einer Buchstabe-/Zahlenkombination und/oder von einem Passwort gebildet wird.
8. Verfahren nach einem der Ansprüche 5 bis 7, **dadurch gekennzeichnet, dass** die Informationsverarbeitungsstelle (30) vor der Übersendung eines Berechtigungscodes (36) an den Benutzer (22) zusätzlich zu der für das Schloss (16) und/oder für den Benutzer (22) charakteristischen Information (20; 26) einen mit beiden Informationen verknüpften Zeitparameter (28) für den Einsatzort und/oder die Ein-

satzzeit prüft.

9. Verfahren nach einem der Ansprüche 5 bis 8, **dadurch gekennzeichnet, dass** das elektronische Schloss (16) an einem Verschlussdeckel (14) eines Rohrtresors (12) angeordnet ist, dem nach Entriegelung des elektronischen Schlosses (16) ein physikalischer Schlüssel (18) für das Betreten wenigstens eines weiteren Raumes entnehmbar ist. 5
10. Verfahren nach einem der Ansprüche 5 bis 8, **dadurch gekennzeichnet, dass** das elektronische Schloss (16) einen von einer elektrischen Spannungsquelle (322) des elektronischen Schlüssels (32) empfangenen Strom zur Aktivierung eines Motorschlosses (40) an dieses weiterleitet. 10
11. Verfahren nach einem der Ansprüche 5 bis 8, **dadurch gekennzeichnet, dass** das elektronische Schloss (16) einen von einer elektrischen Spannungsquelle (322) des elektronischen Schlüssels (32) empfangenen Strom zur Aktivierung eines Steuergeräts (50) an dieses weiterleitet. 15
12. Verfahren nach einem der Ansprüche 5 bis 11, **dadurch gekennzeichnet, dass** das elektronische Schloss (16) und/oder die von diesem freigegebene Einrichtung (14; 40; 50) bei der Aktivierung und/oder der Deaktivierung eine Information (38) an die zentrale Informationsverarbeitungsstelle (30) sendet. 20
13. Verfahren nach einem der Ansprüche 5 bis 12, **dadurch gekennzeichnet, dass** für die Übersendung der wenigstens einen für das elektronische Schloss (16) und/oder den Benutzer (22) charakteristischen Information (20; 22; 34) und für den Empfang des Berechtigungscode (36) als Kommunikationseinrichtung (24) ein Mobiltelefon verwendet wird. 25
14. Verfahren nach einem der Ansprüche 5 bis 13, **dadurch gekennzeichnet, dass** die Kommunikationseinrichtung (24) ein Anwendungsprogramm enthält, mittels dem die wenigstens eine für das elektronische Schloss (16) und/oder den Benutzer (22) charakteristische Information (20; 22; 34) erfassbar ist und/oder mittels dem der Berechtigungscode (36) empfangbar ist. 30

Claims

1. An electronic closure system with an electronic key (32), at least one electronic lock (16), a central data processing centre arranged remotely from the electronic lock (16) and a communication device (24) for transmitting to the central data processing centre (30) at least one item of information (20; 22; 34) characteristic of the electronic lock (16) and/or the user 35

(22), wherein the electronic key (32) comprises at least two contacts (324, 325, 326) for the transmittal of data and energy to the electronic lock (16) and at least one input device (33) provided at a housing (321) of the electronic key (32) and for entering an authorisation code (36), wherein the electronic key (32) is programmable, by means of authorisation codes which can be entered by the input device (33), for the opening of different electronic locks, wherein the input device (33) and the contacts (324, 325, 326) are arranged on different sides of the housing (321), wherein the input device (33) is arranged at a front side of the housing (321) and the contacts (324, 325, 326) are arranged on an opposite rear side of the housing (321) and wherein the electronic key is provided with at least one rechargeable battery as a source (322) of electrical voltage and with an electric voltage converter, by means of which a lower output voltage of the battery in the electronic key is converted into a higher operating voltage required by the electronic lock, and wherein the electronic key (32) is provided with at least one magnet (329) for the purposes of centring in cooperation with a corresponding counter-magnet (161) at the electronic lock (16), wherein further the at least one electronic lock (16) is provided with at least two concentrically-arranged mating contacts (164, 165, 166) and a magnetic centring arrangement, wherein the electronic lock is not constantly supplied with an operating voltage, wherein the central data processing centre (30) is configured to check the transmitted information (20; 22; 34) and for a transmittal of an authorisation code (36) to the user (22) by means of the communication device (24) in the case of a positive check of the information (20; 22; 34), and wherein, after an input of the authorisation code (36) by the user (22) by means of the input device (33) in the accompanying electronic key (32) by bringing into contact the electronic key (32) and the electronic lock (16), a transmittal of data and energy from the electronic key (32) to the electronic lock (16) can effect an unlocking of the electronic lock (16). 40

2. An electronic closure system in accordance with Claim 1 **characterised in that** the mating contacts (164, 165, 166) are in the form of concentric circles which come into contact with the contacts (324, 325, 326) of the electronic key (32) at any relative angular position of the electronic key (32). 45
3. An electronic closure system in accordance with Claim 1 or 2, **characterised in that** the electronic lock (16) is arranged on a closure cap (14) of a tubular key safe (12), wherein the electronic key (32) serves as a handle for actuating the closure cap (14) when the key is in contact with the electronic lock (16). 50
4. An electronic closure system in accordance with

Claim 1 or 2, **characterised in that** the electronic lock (16) is connected upstream of a motor lock (40) of a device that is to be secured and activates the power supply thereto and **in that** in particular a control device (50) is arranged between the electronic lock (16) and the motor lock (40), and the power supply thereto is activated by the electronic key (32) when the key is brought into contact with the electronic lock (16) and the authorisation code (36) entered by means of the input device (33) has been verified.

5. A method for secure acquisition of an access authorisation or for secure delivery of a key by means of an electronic closure system according to any of Claims 1 to 4, wherein the method comprises the following method steps:

- transmittal of at least one item of information (20; 22; 34) characteristic of the electronic lock (16) and/or the user (22) to a central data processing centre (30) that is remote from the electronic lock by means of a communication device (24),
- checking of the sent information (20; 22; 34) by the central data processing centre (30),
- transmittal of an authorisation code (36) to the user (22) by means of the communication device (24) in the case of a positive check of the information (20; 22; 34),
- entry, by the user (22) by means of the input device (33), of the authorisation code (36) into the accompanying electronic key (32),
- unlocking of the electronic lock (16) by cooperation with the electronic key (32).

6. A method in accordance with Claim 5, **characterised in that** the item of information (20) characteristic of the lock (16) is formed of a number combination or by a bar code.

7. A method in accordance with Claim 5 or 6, **characterised in that** the item of information (26) characteristic of the user (22) is formed by a letter/number combination and/or a password.

8. A method in accordance with any of Claims 5 to 7, **characterised in that**, before the transmittal of an authorisation code (36) to the user (22), the data processing centre (30) examines, in addition to the information (20; 26) characteristic of the lock (16) and/or the user (22), a time parameter (28) for the place of use and/or the time of use that is linked to both items of information.

9. A method in accordance with any of Claims 5 to 8, **characterised in that** the electronic lock (16) is arranged on a closure cap (14) of a tubular key safe

(16) from which, after unlocking of the electronic lock (16), there is removable a physical key (18) for entering at least one further area.

10. A method in accordance with any of Claims 5 to 8, **characterised in that** the electronic lock (16) passes on a current for activating a motor lock (40) that it received from an electrical voltage source (322) of the electronic key (32) to said motor lock.

11. A method in accordance with any of Claims 5 to 8, **characterised in that** the electronic lock (16) passes on a current for activating a control device (50) that it received from an electrical voltage source (322) of the electronic key (32) to said control device.

12. A method in accordance with any of Claims 5 to 11, **characterised in that** the electronic lock (16) and/or the device (14; 40; 50) released thereby sends an item of information (38) to the central data processing centre (30) upon the activation and/or the deactivation thereof.

13. A method in accordance with any of Claims 5 to 12, **characterised in that** a mobile telephone is used as a communication device (24) for the transmittal of the at least one item of information (20; 22; 34) characteristic of the electronic lock (16) and/or the user (22) and for the reception of the authorisation code (36).

14. A method in accordance with any of Claims 5 to 13, **characterised in that** the communication device (24) contains an application program by means of which the at least one item of information (20; 22; 34) characteristic of the electronic lock (16) and/or the user (22) is detectable and/or by means of which the authorisation code (36) is receivable.

Revendications

1. Système de verrouillage électronique avec une clé électronique (32), au moins une serrure électronique (16), un poste de traitement d'information central agencé de façon éloignée de la serrure électronique (16) et un équipement de communication (24) pour envoyer au moins une information (20 ; 22 ; 34) caractéristique de la serrure électronique (16) et/ou de l'utilisateur (22) au poste de traitement d'information (30) central, dans lequel la clé électronique (32) comprend au moins deux contacts (324, 325, 326) pour transmettre des données et une énergie à la serrure électronique (16), au moins un équipement de saisie (33) prévu contre un logement (321) de la clé électronique (32) pour la saisie d'un code d'autorisation (36), dans lequel la clé électronique (32) peut être programmée au moyen d'un code d'autorisation

- pouvant être saisi via l'équipement de saisie (33) pour l'ouverture de serrures électroniques différentes, dans lequel l'équipement de saisie (33) et les contacts (324, 325, 326) sont agencés sur des côtés différents du logement (321), dans lequel l'équipement de saisie (33) est agencé sur un côté avant et les contacts (324, 325, 326) sont agencés sur un côté arrière opposé du logement (321), et dans lequel la clé électronique est dotée d'au moins un accumulateur chargeable en tant que source de tension électrique et d'un transformateur de tension électrique, via lequel une tension de sortie plus basse de l'accumulateur dans la clé électronique est transformée en une tension de fonctionnement plus élevée requise par la serrure électronique, et dans lequel la clé électronique (32) est dotée d'au moins un aimant (329) pour le centrage au niveau de la serrure électronique (16) en coopération avec un contre-aimant (161) correspondant, dans lequel en outre l'au moins une serrure électronique (16) est dotée d'au moins deux contre-contacts (164, 165, 166) concentrique et un centrage magnétique, dans lequel la serrure électronique n'est pas constamment alimentée avec une tension de fonctionnement, dans lequel le poste de traitement d'information (30) central est conçu pour la vérification de l'information (20 ; 22 ; 34) envoyée transmise et un envoi d'un code d'autorisation (36) à l'utilisateur (22) au moyen de l'équipement de communication (24) dans le cas d'une vérification positive de l'information (20 ; 22 ; 34), et dans lequel après une saisie du code d'autorisation (36) par l'utilisateur (22) dans la clé électronique (32) amenée avec au moyen de l'équipement de saisie (33), via la mise en contact de la clé électronique (32) avec la serrure électronique (16), une transmission de donnée et d'énergie de la clé électronique (32) vers la serrure électronique (16) peut provoquer un déverrouillage de la serrure électronique (16).
2. Système de verrouillage électronique selon la revendication 1, **caractérisé en ce que** les contre-contacts (164, 165, 166) sont conçus en tant que cercles concentriques qui entrent en contact avec les contacts (324, 325, 326) de la clé électronique (32) dans une position angulaire relative au choix de la clé électronique (32).
 3. Système de verrouillage électronique selon la revendication 1 ou 2, **caractérisé en ce que** la serrure électronique (16) est agencée contre un bouchon de fermeture (14) d'un coffre-fort cylindrique (12), dans lequel la clé électronique (32), en contact avec la serrure électronique (16), sert de poignée pour l'actionnement du bouchon de fermeture (14).
 4. Système de verrouillage électronique selon la revendication 1 ou 2, **caractérisé en ce que** la serrure électronique (16) est montée en amont d'une serrure motorisée (40) d'un équipement à sécuriser et active l'alimentation en courant de celle-ci, et **en ce qu'**entre la serrure électronique (16) et la serrure motorisée (40) est en particulier agencé un appareil de commande (50) dont l'alimentation en courant est activée par la clé électronique (32) lors de la mise en contact avec la serrure électronique (16) et la vérification réussie du code d'autorisation (36) saisi au moyen de l'équipement de saisie (33).
 5. Procédé pour une obtention sécurisée d'une autorisation d'accès ou pour une remise sécurisée de clé au moyen d'un système de verrouillage électronique selon l'une des revendications 1 à 4, dans lequel le procédé comprend les étapes de procédé suivantes :
 - envoi d'au moins une information (20 ; 22 ; 34) caractéristique de la serrure électronique (16) et/ou de l'utilisateur (22) à un poste de traitement d'information (30) central agencé de façon éloignée de la serrure électronique (16) au moyen d'un équipement de communication (24),
 - vérification de l'information (20 ; 22 ; 34) envoyée par le poste de traitement d'information (30) central,
 - envoi d'un code d'autorisation (36) à l'utilisateur (22) au moyen de l'équipement de communication (24) dans le cas d'une vérification positive de l'information (20 ; 22 ; 34),
 - saisie du code d'autorisation (36) par l'utilisateur (22) dans la clé électronique (32) amenée avec au moyen de l'équipement de saisie (33),
 - déverrouillage de la serrure électronique (16) par coopération avec la clé électronique (32).
 6. Procédé selon la revendication 5, **caractérisé en ce que** l'information (20) caractéristique de la serrure (16) est formée d'une combinaison de chiffres ou d'un code à barres.
 7. Procédé selon la revendication 5 ou 6, **caractérisé en ce que** l'information (26) caractéristique de l'utilisateur (22) est formée d'une combinaison de lettres/chiffres et/ou d'un mot de passe.
 8. Procédé selon l'une des revendications 5 à 7, **caractérisé en ce que** le poste de traitement d'information (30), avant l'envoi d'un code d'autorisation (36) à l'utilisateur (22), vérifie également, outre l'information (20 ; 26) caractéristique de la serrure (16) et/ou de l'utilisateur (22), un paramètre de temps (28) associé aux deux informations pour le lieu d'exploitation et/ou le temps d'exploitation.
 9. Procédé selon l'une des revendications 5 à 8, **caractérisé en ce que** la serrure électronique (16) est

agencée contre un bouchon de fermeture (14) d'un coffre-fort cylindrique (12) dont, après déverrouillage de la serrure électronique (16), une clé physique (18) peut être retirée pour pouvoir pénétrer dans au moins une autre pièce.

5

10. Procédé selon l'une des revendications 5 à 8, **caractérisé en ce que** la serrure électronique (16) transfère un courant reçu d'une source de tension (322) électrique de la clé électronique (32) à une serrure motorisée (40) pour l'activation de celle-ci. 10
11. Procédé selon l'une des revendications 5 à 8, **caractérisé en ce que** la serrure électronique (16) transfère un courant reçu d'une source de tension (322) électrique de la clé électronique (32) à un appareil de commande (50) pour l'activation de celui-ci. 15
12. Procédé selon l'une des revendications 5 à 11, **caractérisé en ce que** la serrure électronique (16) et/ou l'équipement (14 ; 40 ; 50) libéré par celle-ci émet une information (38) vers le poste de traitement d'information (30) central lors de l'activation et /ou de la désactivation. 20
25
13. Procédé selon l'une des revendications 5 à 12, **caractérisé en ce qu'un** téléphone portable est utilisé en tant qu'équipement de communication (24) pour l'envoi de l'au moins une information (20 ; 22 ; 34) caractéristique de la serrure électronique (16) et/ou de l'utilisateur (22) et pour la réception du code d'autorisation (36). 30
14. Procédé selon l'une des revendications 5 à 13, **caractérisé en ce que** l'équipement de communication (24) contient un programme d'application au moyen duquel la au moins une information (20 ; 22 ; 34) caractéristique de la serrure électronique (16) et/ou de l'utilisateur (22) peut être détectée et/ou au moyen duquel le code d'autorisation (36) peut être reçu. 35
40
45
50
55

FIG. 1

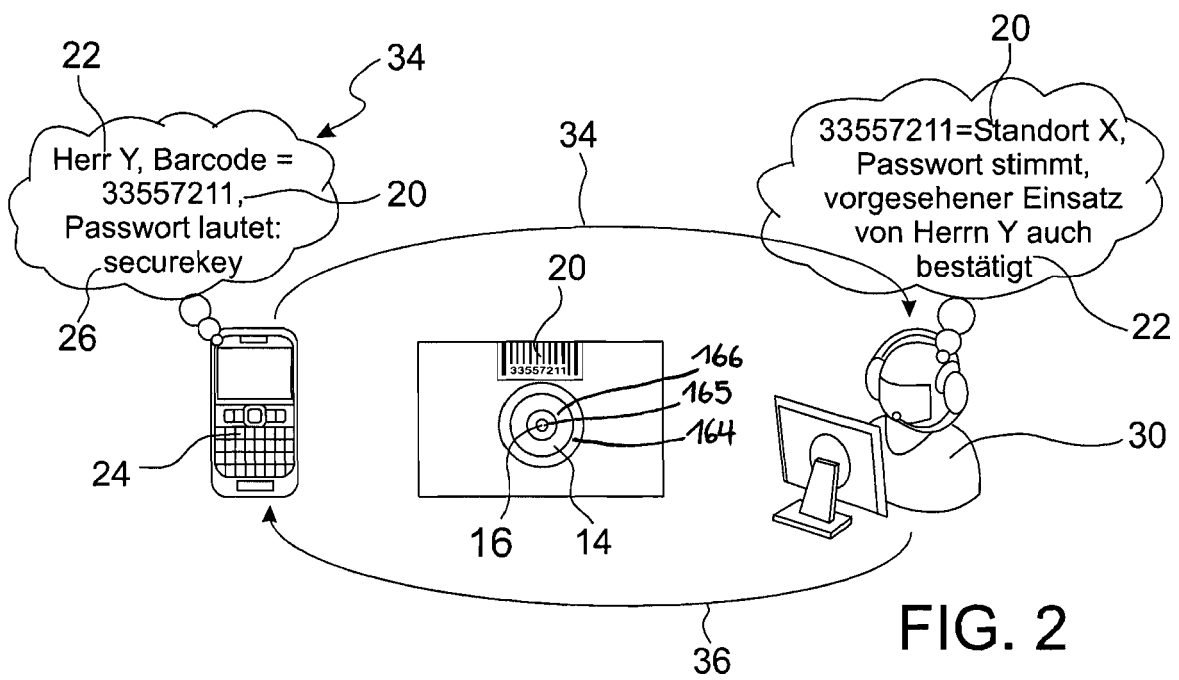
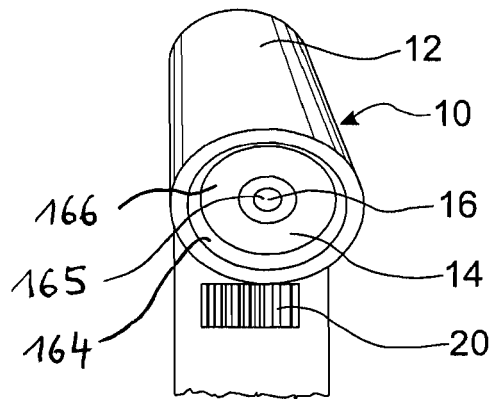


FIG. 2

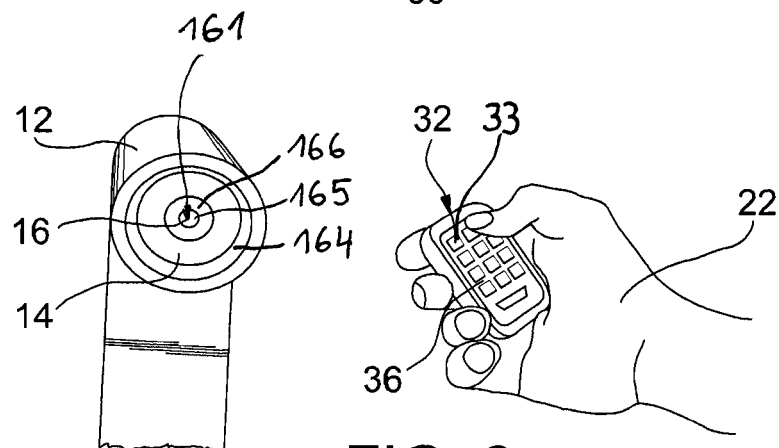


FIG. 3

FIG. 4

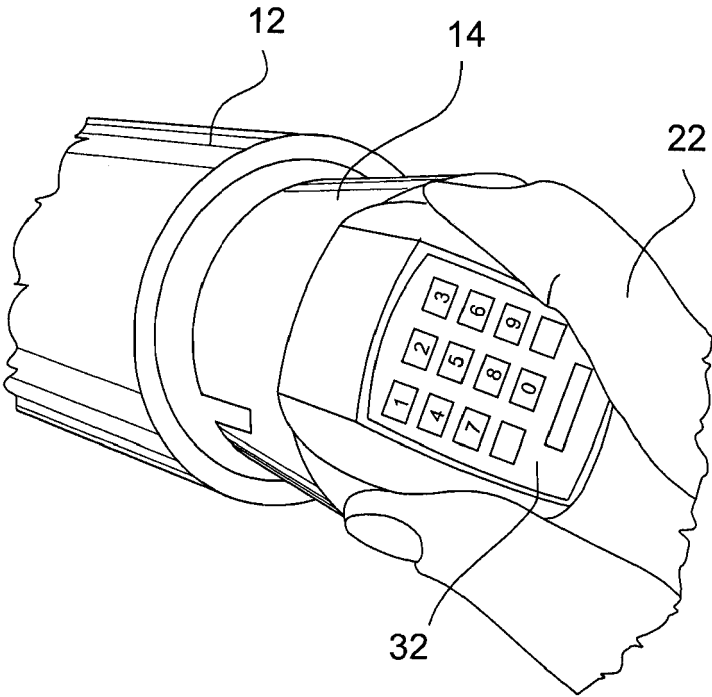
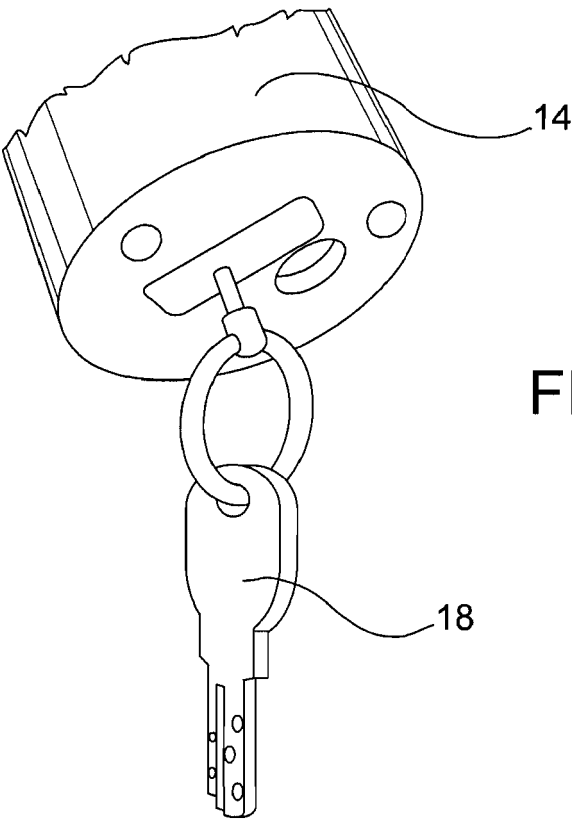
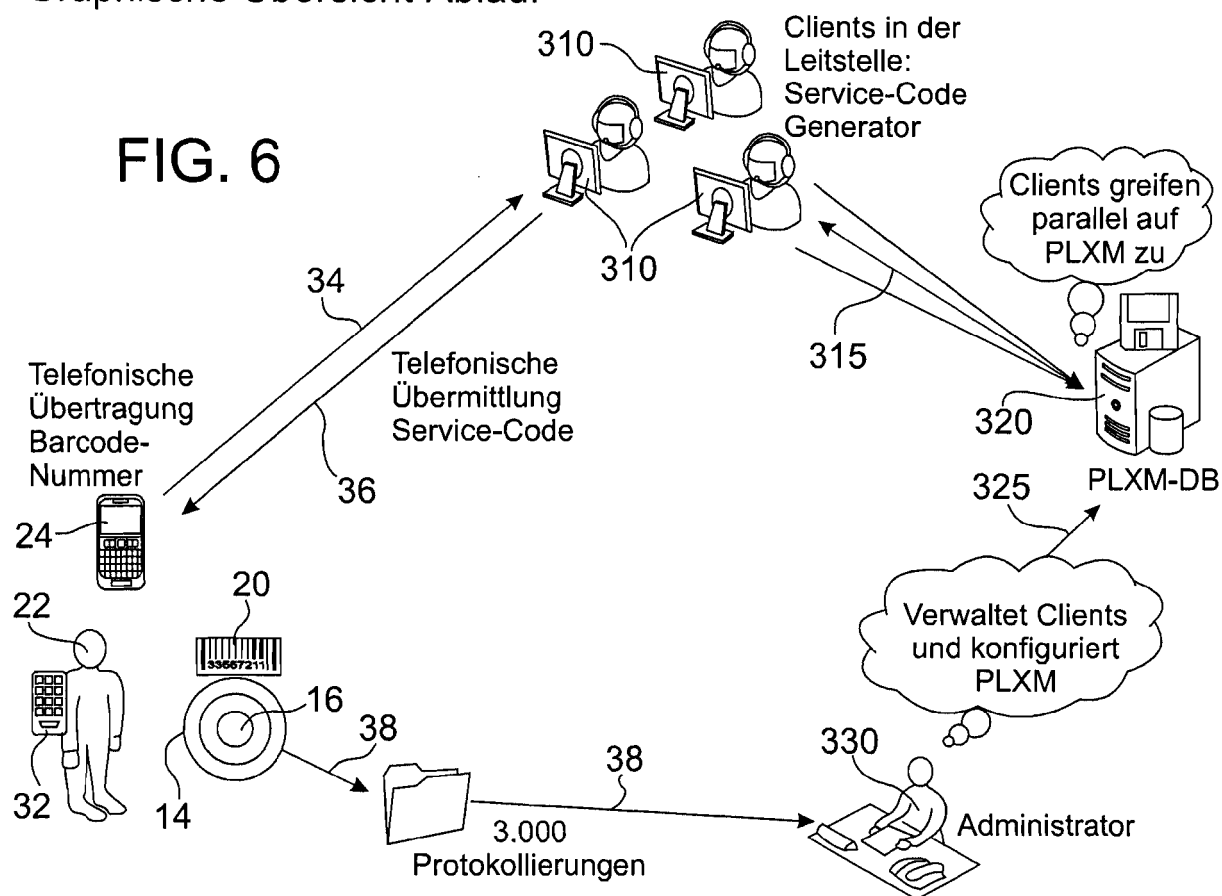


FIG. 5



Graphische Übersicht Ablauf



Graphische Übersicht Funktionen

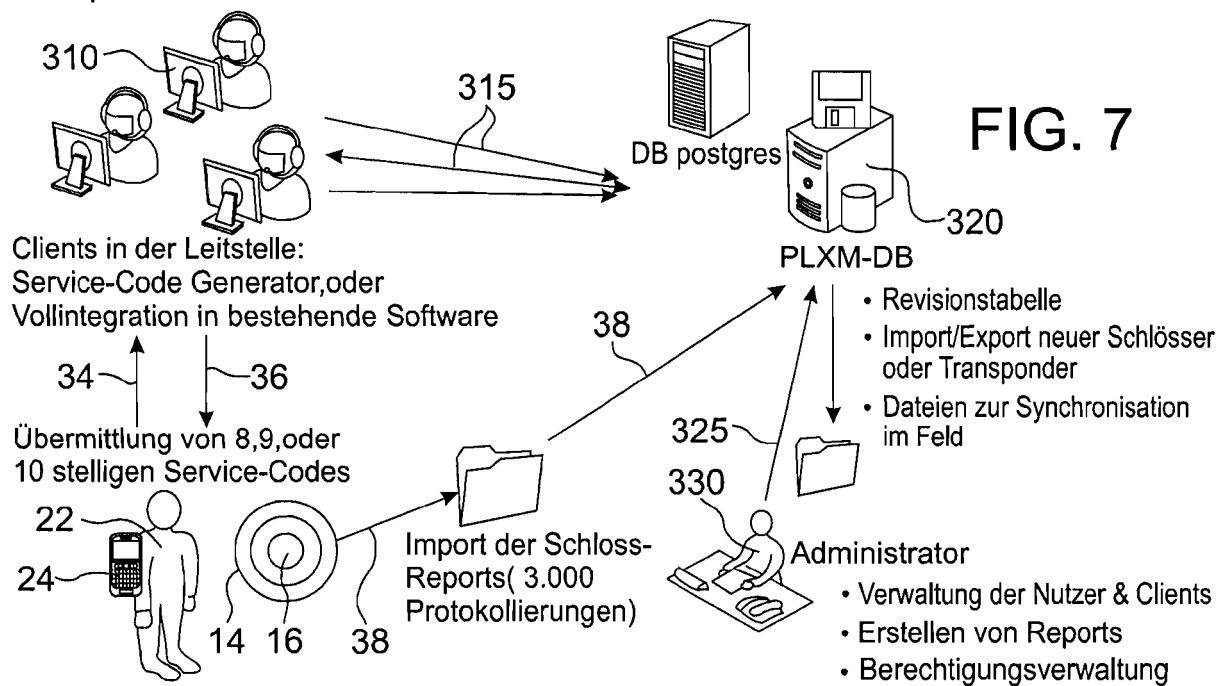
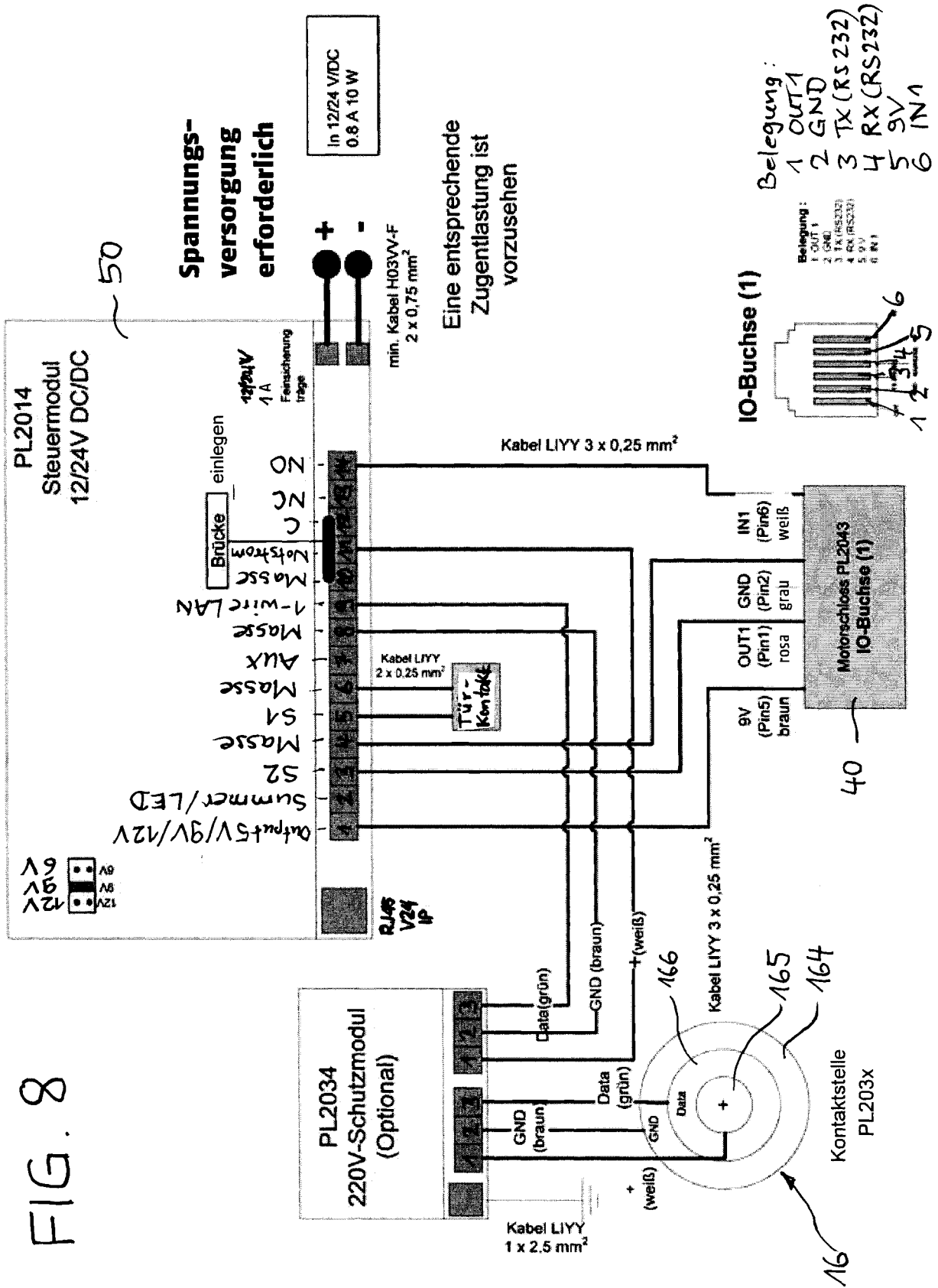


FIG. 8



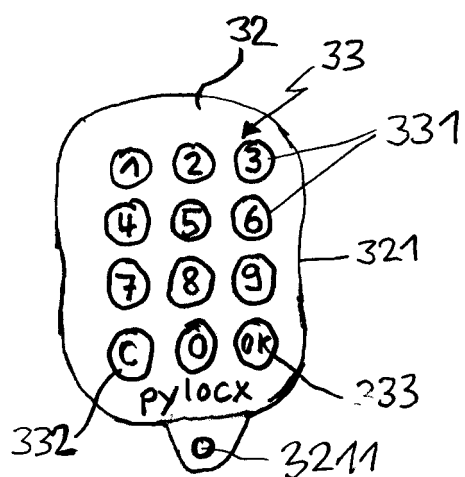


FIG. 9

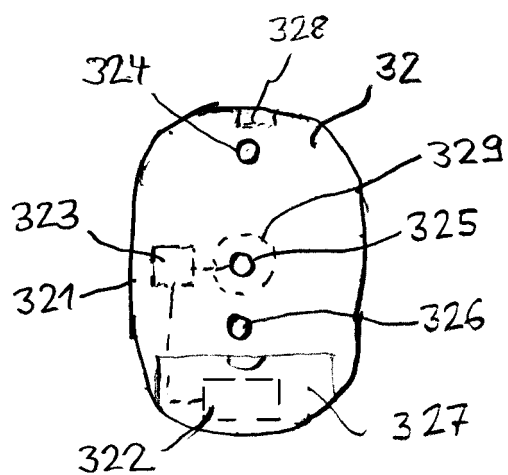


FIG. 10

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 102005033898 A1 [0003]
- DE 202011003043 U1 [0004]
- WO 2009128854 A1 [0005]
- DE 102009013650 A1 [0006]
- WO 2012045474 A1 [0040] [0042]

In der Beschreibung aufgeführte Nicht-Patentliteratur

- Pylocx, www.LockYourWorld.com [0007]