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

(11) **EP 3 584 770 B1**

(12) **EUROPÄISCHE PATENTSCHRIFT**

(45) Veröffentlichungstag und Bekanntmachung des Hinweises auf die Patenterteilung:
17.07.2024 Patentblatt 2024/29

(21) Anmeldenummer: **19185512.1**

(22) Anmeldetag: **27.08.2014**

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

(52) Gemeinsame Patentklassifikation (CPC):
G07C 9/00571; G07C 9/0069; G07C 9/00857; G07C 9/00912; G07C 2009/00492; G07C 2009/00634; G07C 2009/00761; G07C 2009/0088; G07C 2009/00936

(54) **VERFAHREN ZUM BETREIBEN EINES SCHLIESSSYSTEMS, SCHLIESSSYSTEM UND ROHRTRESOR**

CLOSURE SYSTEM; METHOD FOR OPERATING A CLOSURE SYSTEM AND TUBE SAFE

PROCÉDÉ DE FONCTIONNEMENT D'UN SYSTÈME DE FERMETURE, SYSTÈME DE FERMETURE ET COFFRE-FORT TUBULAIRE

(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: **16.10.2013 DE 102013111429**

(43) Veröffentlichungstag der Anmeldung:
25.12.2019 Patentblatt 2019/52

(62) Dokumentnummer(n) der früheren Anmeldung(en) nach Art. 76 EPÜ:
14757911.4 / 3 058 553

(73) Patentinhaber: **Steinbach & Vollmann GmbH**
42579 Heiligenhaus (DE)

(72) Erfinder:
- **Engel-Dahan, Manuela**
  63619 Bad Orb (DE)
- **Knobling, Ralf**
  61137 Schöneck (DE)
- **Meisel, Thilo**
  64285 Darmstadt (DE)

(74) Vertreter: **Ostriga Sonnet Wirths & Vorwerk Patentanwälte**
Friedrich-Engels-Allee 432
42283 Wuppertal (DE)

(56) Entgegenhaltungen:
CH-A5- 655 351
FR-A1- 2 741 103
US-A- 4 609 780
US-A- 5 701 828
US-A- 6 082 153
US-A1- 2003 179 073
US-A1- 2007 290 797
US-A1- 2008 150 684
US-A1- 2013 043 973
US-B1- 6 331 812

- **"LOCK YOUR WORLD secure. easy. stable.", 5 December 2011 (2011-12-05), XP055069059, Retrieved from the Internet <URL:http://www.lockyourworld.com/uploads/media/system_overview.pdf> [retrieved on 20130702]**

EP 3 584 770 B1

Beschreibung

[0001] Die Erfindung betrifft ein Schließsystem.

[0002] US 2013/00439731 A1 offenbart ein elektronisches Schloss, System und Verfahren für einen dynamisch kontrollierten Zugang ohne, dass das Schloss mit einem Server kommuniziert oder verbunden ist.

[0003] US 2007/0290797 A1 offenbart eine Zugangsvorrichtung für ein System umfassend zumindest ein Schloss, das so konfiguriert ist, um Anweisungen zu erhalten und um einen Schließmechanismus zum Aufschließen des zumindest einen Schlosses Energie zu liefern und wobei ein Computer an einer von dem zumindest einen Schloss und der Zugangsvorrichtung entfernt gelegenen Stelle vorgesehen ist und die Vorgangsrichtung zumindest einen Schlüssel umfasst, welcher zur Kommunikation mit dem Computer konfiguriert ist.

[0004] US 2008/0150684 A1 offenbart ein Zugangssystem umfassend ein elektromechanisches Schloss und ein tragbares Zugangsgerät, mit welchem das elektromechanische Schloss zwischen einer geöffneten und einer geschlossenen Position betrieben werden kann, und wobei eine PIN oder ein Fingerabdruck oder eine Netzhaut als Sicherheitsmerkmal in dem tragbaren Öffnungsgerät überprüft wird und bei erfolgreicher Überprüfung das tragbare Öffnungsgerät ein Signal an einen Mikroprozessor in dem elektromechanischen Schloss sendet und wobei der Mikroprozessor dann überprüft, ob der Sicherheitscode mit einem in dem Mikroprozessor gespeicherten Code übereinstimmt.

[0005] US 5,701,828 B1 offenbart ein elektronisches Schließsystem für eine Zugangskontrolle zu einer Vielzahl von Gehäusen, welche einen jeweiligen Schließmechanismus mit einem spezifischen Zugangscode aufweisen, und wobei das System ferner ein Identifizierungssystem umfasst, mit welchem Personen sich für den Zugang zu einem oder mehreren der Gehäuse identifizieren können.

[0006] US 6,331,812 B1 offenbart ein programmierbares elektronisches Schließsystem, welches ein Schloss und einen Schlüssel umfasst, wobei Kodierungsdaten sowohl in dem Schlüssel als auch in dem Schloss mittels eines Eingabegerätes durch Programmieren modifiziert werden können.

[0007] US 6,082,153 B1 offenbart ein elektronisches Schließsystem umfassend einen elektronischen Schlüssel und beispielsweise mehrere elektronische Schlösser, wobei der elektronische Schlüssel und ein elektronisches Schloss wechselwirken und wobei in einem Speicher verschlüsselt spezifische Sicherheitscodes wie beispielsweise ein Startdatum, ab welchem der Schlüssel gültig ist und ein Zeitfenster, in welchem der Schlüssel benutzt werden kann, sowie eine Schlüsselkategorie des Schlüssels und eine Seriennummer des Schlüssels gespeichert werden.

[0008] US 2003/0179073 B1 offenbart ein elektronisches Schließsystem für eine Zugangskontrolle zu einer Vielzahl von Containern, wobei an den Containern ein elektronischer Schließmechanismus vorgesehen ist, welcher eine Kontrollvorrichtung zum Auslesen von Benutzersicherheitsmerkmalen umfasst.

[0009] In einer Präsentation (XP 055069059) wurde ein Verfahren zum Betreiben eines elektronischen Schließsystems sowie ein Schließsystem offenbart. Das Schließsystem umfasst einen elektronischen Schlüssel und ein elektronisches Schloss, welche zum Öffnen des elektronischen Schlosses zusammenwirken. Bei Schließsystemen besteht generell das Erfordernis, bei möglichst einfacher Bedienung eine möglichst hohe Sicherheit zu gewährleisten.

[0010] Diese Aufgabe wird erfindungsgemäß durch ein Schließsystem gemäß Anspruch 1 gelöst.

[0011] Vorteilhafte Weiterentwicklungen sind in den abhängigen Ansprüchen definiert.

[0012] Beispielsweise ist vorgesehen, dass bei einem Verfahren zum Betreiben eines Schließsystems umfassend einen elektronischen Schlüssel und ein elektronisches Schloss sowie eine im Schließbetrieb lokal getrennt vom elektronischen Schlüssel und vom elektronischen Schloss eingesetzte Zentraleinheit, von der Zentraleinheit mittels eines Berechtigungscodeermittlungsprogramms ein externer Berechtigungscode erzeugt wird, der externe Berechtigungscode dem elektronischen Schlüssel übermittelt wird, der externe Berechtigungscode vom elektronischen Schlüssel in einem Speicher abgelegt wird, wobei bei Zusammenwirken des elektronischen Schlüssels mit dem elektronischen Schloss vom elektronischen Schloss der externe Berechtigungscode aus dem Speicher ausgelesen und von einem Prozessor des elektronischen Schlosses dadurch überprüft wird, dass der Prozessor mit einem eigenen Berechtigungscodeermittlungsprogramm selbst einen eigenen Berechtigungscode ermittelt und mit dem vom elektronischen Schlüssel erhaltenen externen Berechtigungscode vergleicht und wobei der Prozessor bei Identität des ermittelten eigenen Berechtigungscodes mit dem übermittelten externen Berechtigungscode ein Öffnungsvorgang ermöglicht.

[0013] Ein Vorteil der erfindungsgemäßen Lösung ist darin zu sehen, dass aus einer Vielzahl von elektronischen Schlüsseln und einer Vielzahl von elektronischen Schlössern durch die Ausgabe des externen Berechtigungscodes nur ein bestimmter elektronischer Schlüssel in der Lage ist, bei Eingabe dieses externen Berechtigungscodes ein bestimmtes elektronisches Schloss zu öffnen.

[0014] Ein weiterer Vorteil der erfindungsgemäßen Lösung ist darin zu sehen, dass durch die Ermittlung eines externen Berechtigungscodes und Übermittlung desselben an den elektronischen Schlüssel die Möglichkeit besteht, bereits vor der Übermittlung des elektrischen Berechtigungscodes zu prüfen, ob die Umstände, unter denen eine Anforderung eines derartigen Berechtigungscodes durch eine Bedienungsperson gerechtfertigt ist und somit bereits lokal entfernt vom elektronischen Schlüssel und elektronischen Schloss die Voraussetzun-

gen für ein Öffnen des elektronischen Schlosses abgeklärt werden können.

[0015] Darüber hinaus ist bei der erfindungsgemäßen Lösung über die Ermittlung des externen Berechtigungscodes mittels der Zentraleinheit ein Missbrauch oder ein ungerechtfertigtes Öffnen durch einen Benutzer, der einen elektronischen Schlüssel zur Verfügung hat, nicht möglich.

[0016] Besonders günstig ist es für die Sicherheit, wenn ein Berechtigungscodeermittlungsprogramm der Zentraleinheit den externen Berechtigungscode so ermittelt, dass mit diesem nur eine einmalige Öffnung zugelassen wird.

[0017] Damit wird insbesondere verhindert, dass eine Bedienungsperson den Berechtigungscode speichert und erneut einzusetzen versucht.

[0018] In besonders einfacher Weise lässt sich mit dem Berechtigungscodeermittlungsprogramm der Zentraleinheit der Berechtigungscode als einmal gültiger Berechtigungscode dann ermitteln, wenn der Berechtigungscode unter anderem durch Berücksichtigung eines Zykluszählers in der Zentraleinheit ermittelt wird, wobei der Zykluszähler die Öffnungsvorgänge des zur Öffnung anstehenden elektronischen Schlosses ermittelt und festhält.

[0019] Um dem Berechtigungscodeermittlungsprogramm des elektronischen Schlosses ebenfalls die Möglichkeit zu geben, den richtigen eigenen Berechtigungscode zu ermitteln, ist vorgesehen, dass das Berechtigungscodeermittlungsprogramm des elektronischen Schlosses den eigenen Berechtigungscode ebenfalls unter Berücksichtigung eines Zykluszählers ermittelt.

[0020] Ferner ist vorzugsweise vorgesehen, dass die Berechtigungscodeermittlungsprogramme der Zentraleinheit und des elektronischen Schlosses den jeweiligen Berechtigungscode unter Berücksichtigung des Identifikationscodes des zum Einsatz kommenden elektronischen Schlüssels und des Identifikationscodes des zu öffnenden elektronischen Schlosses ermitteln.

[0021] Um eine möglichst hohes Sicherheitsniveau zu generieren, ist vorzugsweise vorgesehen, dass die Berechtigungscodeermittlungsprogramme die Berechtigungscodes mittels eines Hash-Algorithmus ermitteln.

[0022] Um sicherzustellen, dass das Berechtigungscodeermittlungsprogramm der Zentraleinheit und das Berechtigungscodeermittlungsprogramm des elektronischen Schlosses von denselben Parametern und Zuständen ausgehend den Berechtigungscode unabhängig voneinander ermitteln können, ist vorzugsweise vorgesehen, dass vor Montage des elektronischen Schlosses an den für diesen vorgesehenen Ort das elektronische Schloss durch die Zentraleinheit aktiviert wird, wobei die Zentraleinheit hierbei den Identifikationscode des elektronischen Schlosses, den Stand des Zykluszählers des elektronischen Schlosses mit dem in der Zentraleinheit abgespeicherten Identifikationscode des elektronischen Schlosses und den in der Zentraleinheit gespeicherten Stand des Zykluszählers abgleicht.

[0023] Unter dem Begriff abgleichen ist dabei zu verstehen, dass die entsprechenden Daten, das heißt beispielsweise der Identifikationscode und/oder der Stand des Zykluszählers, zwischen dem elektronischen Schloss und der Zentraleinheit ausgetauscht oder von einem derselben ausgelesen und im anderen derselben abgelegt werden.

[0024] Vorzugsweise ist dabei vorgesehen, dass der Identifikationscode des elektronischen Schlosses in einem gesicherten Speicher gespeichert wird.

[0025] Ferner vorzugsweise vorgesehen, dass die Zentraleinheit bei der Aktivierung des elektronischen Schlosses zu speichernde Passwörter, insbesondere Zuordnungspasswörter für den elektronischen Schlüssel und das elektronische Schloss, beispielsweise zu einer oder mehreren Zugangsgruppen, zwischen dem elektronischen Schloss und der Zentraleinheit abgleicht.

[0026] Zur Sicherheit ist es besonders vorteilhaft, wenn bei der Aktivierung des elektronischen Schlosses ein Zuordnungspasswort abgeglichen wird.

[0027] Das Zuordnungspasswort soll dabei die Zuordnung des elektronischen Schlosses zu einer bestimmten Gruppe von Schlössern und/oder einer bestimmten Gruppe von Schlüsseln festlegen.

[0028] Weiterhin sieht eine vorteilhafte Lösung vor, dass die Zentraleinheit bei der Aktivierung des elektronischen Schlüssels den Identifikationscode des elektronischen Schlüssels mit dem in der Zentraleinheit gespeicherten Identifikationscode des elektronischen Schüssels abgleicht.

[0029] Auch in diesem Fall ist der Begriff "abgleichen" derart zu verstehen, dass der elektronische Schlüssel zwischen beiden Einheiten ausgetauscht wird oder ein Auslesen in der einen Einheit und Abspeichern in der anderen Einheit oder ein gleichzeitiges Abspeichern in beiden Einheiten erfolgt.

[0030] Besonders sicher ist es für die Benutzung des elektronischen Schlüssels, wenn bei der Aktivierung des elektronischen Schlüssels ein Zuordnungspasswort in dem Speicher abgelegt wird.

[0031] Ferner ist vorzugsweise vorgesehen, dass der Identifikationscode des elektronischen Schlüssels in einem Speicher des elektronischen Schlüssels gespeichert wird.

[0032] Vorzugsweise ist der Speicher des elektronischen Schlüssels nur bei Verwendung eines Sicherheitshash-Codes beschreibbar und auslesbar.

[0033] Vorzugsweise ist dabei vorgesehen, dass von einem Prozessor im elektronischen Schlüssel zum Speichern des externen Berechtigungscodes der Sicherheitshash-Code ermittelt wird.

[0034] Ferner ist vorzugsweise ebenfalls vorgesehen, dass zum Auslesen des externen Berechtigungscodes aus dem gesicherten Speicher des elektronischen Schlüssels ein Prozessor im elektronischen Schloss einen Sicherheitshash-Code zum Zugriff auf den gesicherten Speicher erzeugt.

[0035] Hinsichtlich der Art des gesicherten Speichers

wurden bislang keinerlei näheren Angaben gemacht.

[0036] So sieht eine bevorzugte Lösung vor, als Speicher im elektronischen Schlüssel ein Speicher eines Sicherheitsprozessors verwendet wird, wobei der Sicherheitsprozessor insbesondere das Generieren des Sicherheitshash-Codes verlangt, um in dem Speicher des Sicherheitsprozessors Daten, beispielsweise den Berechtigungscode und/oder den Identifikationscode und/oder Passwörter ablegen zu können.

[0037] Um ferner zu verhindern, dass ein Angriff auf das elektronische Schloss per se erfolgt und dabei das elektronische Schloss zumindest anzeigt, ob irgendwelche relevanten Zustände durch ein Angriff mit einem nicht autorisierten elektronischen Schlüssel erreicht werden können, ist vorzugsweise vorgesehen, dass Zustandssignale des elektronischen Schlosses dem elektronischen Schlüssel zur Anzeige übermittelt werden und somit insbesondere das elektronische Schloss selber keine Möglichkeit zur Anzeige seiner Zustände aufweist.

[0038] Insbesondere ist dabei vorgesehen, dass der elektronische Schlüssel einen Prozessor aufweist, welcher Signalelemente zur Anzeige der vom elektronischen Schloss übermittelten Zustände des elektronischen Schlosses ansteuert.

[0039] Eine Ausführungsform eines Verfahrens für eine gesicherte Erlangung einer Zugangsberechtigung oder für eine gesicherte Schlüssel-Übergabe für wenigstens einen Benutzer mittels eines elektronischen Schloss und wenigstens eines vom Benutzer mitgeführten elektronischen Schlüssels, insbesondere gemäß den nachfolgend beschriebenen Merkmalen, umfasst folgende Verfahrensschritte:

Übersendung wenigstens einer für das elektronische Schloss und/oder den Benutzer charakteristische Information an eine entfernt vom elektronischen Schloss angeordnete zentrale Informationsverarbeitungsstelle oder Zentraleinheit mittels einer Kommunikationseinrichtung, Überprüfung der übersendeten Information durch die zentrale Informationsverarbeitungsstelle, Übersendung eines Berechtigungscodes an den Benutzer mittels der Kommunikationseinrichtung im Falle einer positiven Überprüfung der Information, Eingabe des Berechtigungscodes durch den Benutzer mittels der Eingabeeinheit in den mitgeführten elektronischen Schlüssel, Entriegelung des elektronischen Schlosses durch Zusammenwirken mit dem elektronischen Schüssel.

[0040] Beispielsweise ist hierzu vorgesehen, dass die für das Schloss charakteristische Information von einer Zahlenkombination oder von einem Barcode gebildet wird.

[0041] Alternativ oder ergänzend hierzu ist insbesondere vorgesehen, dass die für den Benutzer charakteristische Information von einer Buchstaben-/ Zahlenkombination und/oder von einem Passwort gebildet wird.

[0042] Besonders günstig ist es, wenn die Informationsverarbeitungsquelle oder die Zentraleinheit vor der Übersendung eines Berechtigungscodes an den Benutzer zusätzlich zu der für das Schloss und/oder für den Benutzer charakteristischen Information einen mit beiden Informationen verknüpften Zeit-Parameter für den Einsatzort und/oder die Einsatzzeit prüft.

[0043] Eine zweckmäßige Lösung sieht vor, dass das elektronische Schloss an einem Verschlussdeckel eines Rohrtresors angeordnet ist, dem nach Entriegelung des elektronischen Schlosses ein physikalischer Schlüssel für das Betreten wenigstens eines weiteren Raumes entnommen wird.

[0044] Ferner ist zweckmäßigerweise vorgesehen, dass das elektronische Schloss und/oder die von diesem freigegebene Einrichtung bei der Aktivierung und/oder der Deaktivierung eine Information an die zentrale Informationsverarbeitungsstelle oder die Zentraleinheit sendet.

[0045] Eine günstige Lösung sieht vor, dass für die Übersendung der wenigstens einen für das elektronische Schloss und/oder den Benutzer charakteristischen Information und/oder für den Empfang des Berechtigungscodes als Kommunikationseinrichtung ein Mobiltelefon verwendet wird.

[0046] Insbesondere ist es zweckmäßig, wenn die Kommunikationseinrichtung ein Anwendungsprogramm enthält, mittels dem die wenigstens eine für das elektronische Schloss und/oder den Benutzer charakteristische Information erfassbar ist und/oder mittels dem der Berechtigungscode empfangbar ist und/oder mittels dem der Berechtigungscode an den elektronischen Schlüssel übertragbar ist.

[0047] Eine besonders vorteilhafte Variante ist so ausgebildet, dass die Kommunikationseinrichtung und der elektronische Schlüssel eine Einheit bilden.

[0048] 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 die Zentraleinheit aufweisenden Informationsverarbeitungsstelle geprüft und erteilt.

[0049] Nach der Erteilung und Übersendung des Berechtigungscodes wird dieser an einen vom Benutzer mitgeführten elektronischen Schlüssel übermittelt, mittels dem dann die Entriegelung des elektronischen Schlosses erfolgt. Die Übermittlung des Berechtigungscodes an den elektronischen Schlüssel stellt eine weitere vorteilhafte Sicherheitsbarriere dar. Alternativ zu einer manuellen Eingabe des übermittelten Berechtigungscodes in den elektronischen Schlüssel mittels einer Eingabeeinrichtung kann die Übermittlung des Berechti-

gungscodes auch automatisch, beispielsweise durch eine Übertragung mittels Bluetooth, eines Infrarotsenders oder anderer Nahbereichsübertragungsverfahren von der Kommunikationseinrichtung an den elektronischen Schlüssel erfolgen.

[0050] 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 Öffnung 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.

[0051] Gemäß einer weiteren vorteilhaften Anwendung empfängt das elektronische Schloss nach erfolgter Prüfung der Berechtigungscodes eine von einer elektrischen Spannungsquelle des elektronischen Schlüssels übertragene

- optional 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.

[0052] 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.

[0053] Der Benutzer gibt diesen Berechtigungscode über die Eingabeeinheit an den von ihm mitgeführten elektronischen Schlüssel weiter und kann dann mit dem elektronischen Schlüssel das elektronische Schloss durch in Kontakt bringen oder durch eine berührungslose Signalübermittlung, beispielsweise über Funk, betätigen.

[0054] 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.

[0055] 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.

[0056] 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.

[0057] 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.

[0058] 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.

[0059] 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 - insbeson-

dere den Routenplan eines Wachmanns - für das vorgesehene Öffnen des Schlosses verifiziert.

[0060] 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.

[0061] 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.

[0062] Ein weiterer Vorteil der erfindungsgemäßen Lösung ist darin zu sehen, dass damit die Möglichkeit besteht, mit größtmöglicher Sicherheit den elektronischen Schlüssel und das elektronische Schloss einzusetzen, ohne dass allein mit dem elektronischen Schlüssel und dem elektronischen Schloss die Möglichkeit einer Öffnung besteht, sofern der extern erzeugte Berechtigungscode nicht vorhanden ist.

[0063] Um die Sicherheit des elektronischen Schlüssels zu erhöhen, ist vorzugsweise vorgesehen, dass der Speicher im elektronischen Schlüssel ein gesicherter Speicher ist und dass der Prozessor des elektronischen Schlüssels ein Sicherheitscode erzeugt, um den extern erzeugten Berechtigungscode in dem gesicherten Speicher abzulegen.

[0064] Um auch ferner beim Auslesen des Berechtigungscodes aus dem gesicherten Speicher ein hohes Sicherheitsniveau zu gewährleisten ist vorzugsweise vorgesehen, dass der Prozessor des elektronischen Schlosses einen Sicherheitscode erzeugt, um den in dem gesicherten Speicher abgelegten Berechtigungscode auszulesen.

[0065] Ferner ist vorzugsweise vorgesehen, dass der elektronische Schlüssel Anzeigeelemente aufweist, um von dem elektronischen Schloss dem elektronischen Schlüssel übermittelte Zustände des elektronischen Schlosses anzuzeigen.

[0066] In diesem Fall ist zweckmäßigerweise vorgesehen, dass der Prozessor des elektronischen Schlosses dem Prozessor des elektronischen Schlüssels Zustandssignale betreffend die vorliegenden Zustände des elektronischen Schlosses übermittelt und dass der Prozessor des elektronischen Schlosses entsprechend den übermittelten Zuständen die Anzeigeelemente des elektronischen Schlüssels ansteuert.

[0067] Hinsichtlich der Realisierung des gesicherten Speichers wurden bislang keine näheren Angaben gemacht.

[0068] So sieht eine vorteilhafte Lösung vor, dass der gesicherte Speicher der Speicher eines Sicherheitsprozessors ist.

[0069] Ein derartiger Sicherheitsprozessor ist vorzugsweise ein Prozessor, der lediglich bei Übermittlung eines Sicherheitscodes einen Zugriff auf den gesicherten Speicher zulässt.

[0070] Zweckmäßigerweise ist dabei der Sicherheitscode durch einen Hash-Algorithmus zu ermitteln.

[0071] Prinzipiell bestünde die Möglichkeit, das elektronische Schloss stets mit einer eigenen Spannungsversorgung zu betreiben.

[0072] Eine eigene Spannungsversorgung hat jedoch den Nachteil, dass in diesem Fall, insbesondere bei langer Nichtbenutzung des elektronischen Schlosses die Spannungsquelle keine ausreichende Spannung mehr liefert.

[0073] Aus diesem Grund ist zweckmäßigerweise vorgesehen, dass das elektronische Schloss durch eine Spannungsquelle des elektronischen Schlüssels betreibbar ist.

[0074] Dabei könnte das elektronische Schloss zusätzlich noch eine eigene Spannungsquelle aufweisen und nur bei Versagen derselben durch die Spannungsquelle des elektronischen Schlüssels betreibbar sein.

[0075] Besonders günstig ist es jedoch, wenn das elektronische Schloss stets nur die Spannungsquelle des elektronischen Schlüssels betreibbar ist, da dann das Anlegen der Spannung auch zum Starten der Funktionen des elektronischen Schlosses dienen kann.

[0076] Ferner sieht die erfindungsgemäße Lösung vor, dass das elektronische Schloss einen Schließantrieb zum Betätigen eines Schließriegels umfasst.

[0077] In diesem Fall ist somit das elektrische Schloss unmittelbar selbst in der Lage, einen Öffnungsvorgang durch Betätigen des Schließantriebs auszulösen oder ein Verschließen durch nicht Betätigen des Schließantriebs zuzulassen.

[0078] Für den Fall, dass das elektronische Schloss einen Schließantrieb aufweist, ist vorzugsweise ebenfalls vorgesehen, dass der Schließantrieb des elektronischen Schlosses durch die elektrische Spannungsquelle des elektronischen Schlüssels betreibbar ist.

[0079] In diesem Fall ist zweckmäßigerweise vorgesehen, dass das elektronische Schloss einen Spannungswandler aufweist, um den Schließantrieb zu betreiben, da ein derartiger Schließantrieb in der Regel höhere Spannungen erfordert, als sie zum Betreib der Prozessoren im elektronischen Schlüssel und im elektronischen Schloss erforderlich sind.

[0080] Eine weitere vorteilhafte Lösung sieht alternativ zum Vorsehen eines elektrischen Schließantriebs in dem elektronischen Schloss vor, dass das elektrische Schloss eine Schalteinheit aufweist, um ein externes Schließsystem zu aktivieren und zu blockieren.

[0081] In diesem Fall dient das elektronische Schloss

nicht selbst dazu, unmittelbar einen Schließvorgang oder ein Öffnungsvorgang auszulösen oder einzuleiten, vielmehr kann das elektronische Schloss dazu dienen, ein externes Schließsystem zu aktivieren oder zu blockieren.

[0082] Damit besteht beispielsweise die Möglichkeit durch Verwendung des elektronischen Schlüssels und des elektronischen Schlosses vorhandene Schließsysteme zu nutzen, die allerdings eine unzulängliche Sicherheitsstufe aufweisen.

[0083] Diese vorhandenen Schließsysteme können dadurch auf eine höhere Sicherheitsstufe gebracht werden, nämlich die Sicherheitsstufe des elektronischen Schlüssels oder des elektronischen Schlosses, wenn das elektronische Schloss das vorhandene Schließsystem aktiviert oder blockiert.

[0084] Eine weitere vorteilhafte Lösung sieht vor, dass der elektronische Schlüssel eine Schnittstelle zum Aktivieren des elektronischen Schlüssels mittels einer Zentraleinheit aufweist.

[0085] Die Zentraleinheit dient dazu, den externen Berechtigungscode zu erzeugen, so dass es erforderlich ist, dass die Zentraleinheit den elektronischen Schlüssel aktiviert und somit die für die Erzeugung des Berechtigungscodes erforderlichen Daten des elektronischen Schlüssels kennt.

[0086] Ferner ist vorgesehen, dass das elektronische Schloss eine Schnittstelle zum Aktivieren des elektronischen Schlosses durch eine Zentraleinheit aufweist.

[0087] In diesem Fall ist auch beim elektronischen Schloss eine Aktivierung erforderlich, um auch das elektronische Schloss in einen Zustand zu versetzen, der es diesem erlaubt, den externen Berechtigungscode zu erzeugen.

[0088] Insbesondere ist vorzugsweise vorgesehen, dass die Aktivierung des elektronischen Schlüssels beziehungsweise des elektronischen Schlosses durch die Zentraleinheit leitungsgebunden erfolgt, um bei der Aktivierung eine möglichst große Sicherheit gegen Übernahme der Daten durch Dritte zu erhalten.

[0089] Eine vorteilhafte Lösung eines elektronischen Schlüssels mit wenigstens zwei Kontakten zur Übermittlung von Daten und/oder Energie an ein elektronisches Schloss sieht wenigstens eine an einem Gehäuse des elektronischen Schlüssel vorgesehene Eingabeeinrichtung zur Eingabe eines Berechtigungscodes vor.

[0090] Dabei ist es von Vorteil, wenn die Eingabeeinrichtung und die Kontakte an unterschiedlichen Seiten des Gehäuses angeordnet sind.

[0091] Insbesondere ist es günstig, wenn die Eingabeeinrichtung an einer Vorderseite und die Kontakte an einer gegenüberliegenden Rückseite des Gehäuses angeordnet sind.

[0092] Zweckmäßigerweise ist der elektronische Schlüssel mit wenigstens einer elektrischen Spannung versehen.

[0093] Insbesondere ist der elektronische Schlüssel mit wenigstens einem Magneten zur Zentrierung im Zusammenwirken mit einem entsprechenden Gegenmagneten am elektronischen Schloss versehen.

[0094] Ferner sind die Kontakte des elektronischen Schlüssels federnd im Gehäuse gelagert.

[0095] Das elektronische Schließsystem umfasst ferner wenigstens ein elektronisches Schloss, das mit wenigstens zwei konzentrisch angeordneten Gegenkontakten und einer magnetischen Zentrierung versehen ist.

[0096] Insbesondere sind dabei die Gegenkontakte als konzentrische Kreise ausgebildet, die mit den Kontakten des elektronischen Schlüssels in beliebiger relativer Winkelposition des elektronischen Schlüssels in Kontakt treten.

[0097] Zweckmäßigerweise ist das elektronische Schloss an einem Verschlussdeckel eines Rohrtresors angeordnet, wobei der elektronische Schlüssel in Kontakt mit dem elektronischen Schloss als Handgriff für die Betätigung des Verschlussdeckels dient.

[0098] Beispielsweise ist das elektronische Schloss einem Motorschloss einer zu sichernden Einrichtung vorgeschaltet und aktiviert dessen Bestromung.

[0099] Es ist aber auch denkbar, dass zwischen dem elektronischen Schloss und dem Motorschloss ein Steuergerät angeordnet ist, dessen Bestromung durch den elektronischen Schlüssel bei Inkontaktbringen mit dem elektronischen Schloss und erfolgter Verifizierung des mittels der Eingabeeinheit eingegebenen Berechtigungscodes aktiviert wird.

[0100] Ferner ist vorzugsweise vorgesehen, dass die Ausführungsformen des elektronischen Schließsystems gemäß dem eingangs beschriebenen Verfahren zum Betreiben eines Schließsystems arbeiten.

[0101] Die Erfindung erlaubt es insbesondere einen elektronischen Schlüssel bereit zu stellen, der kurzfristig und wechselweise für das Öffnen verschiedenster Schlösser aktivierbar ist.

[0102] Dabei wirkt insbesondere ein erfindungsgemäßer elektronischer Schlüssel vorteilhaft mit wenigstens einem elektronischen Schloss zusammen.

[0103] Ein erfindungsgemäßer elektronischer Schlüssel zeichnet sich durch eine an einem Gehäuse des elektronischen Schlüssels vorgesehene Eingabeeinheit zur Eingabe eines Berechtigungscodes aus. Die Eingabeeinheit kann dabei in Form einer numerischen oder alphanumerischen Tastatur ausgebildet sein, wobei der Berechtigungscode für die gewünschte Freigabe in diesem Falle durch den Benutzer manuell eingegeben wird.

[0104] Gemäß einem weiteren Aspekt der Erfindung ist der elektronische Schlüssel mittels über die Eingabeeinheit eingebbarer Berechtigungscodes für das Öffnen verschiedener elektronischer Schlösser programmierbar.

[0105] Die Eingabeeinheit 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 Benut-

zer oder einer von diesem gehandhabten Kommunikationseinrichtung (beispielsweise einem Smartphone) übermittelten Berechtigungscode erfasst.

[0106] Der Berechtigungscode wird bevorzugt in einem Speicher des elektronischen Schlüssels zwischengespeichert und nach Inkontaktbringen mit einem elektronischen Schloss über wenigstens einen Kontakt an diesen übermittelt.

[0107] Der mittels der Eingabeeinheit separat ohne eine räumliche Nähe zu dem zu öffnenden elektronischen Schloss in den elektronischen Schlüssel eingebbare Berechtigungscode 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 Berechtigungscode an das elektronische Schloss angenähert wird.

[0108] 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 Berechtigungscode präpariert wurde.

[0109] Die Eingabeeinheit und die Kontakte sind bevorzugt an unterschiedlichen Seiten des Gehäuses angeordnet. Besonders bevorzugt 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 Gegenkontakten am elektronischen Schloss in Eingriff stehen.

[0110] Besonders bevorzugt ist der elektronische Schlüssel mit wenigstens einer elektrischen Spannungsquelle - vorzugsweise mit einem aufladbaren Akkumulator - versehen, der nicht nur der Eigenversorgung der elektronischen Komponenten des elektronische 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 nicht an eine eigene Spannungsversorgung angeschlossen werden kann.

[0111] 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.

[0112] 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 Motorschlosses oder eines sonstigen Aktors aktiviert wird.

[0113] Der elektronische Schlüssel ist bevorzugt 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.

[0114] Zur Unterstützung einer sicheren Kontaktbildung sind die Kontakte am elektronischen Schlüssel bevorzugt federnd in dessen Gehäuse gelagert.

[0115] Das elektronische Schließsystem umfasst außer dem elektronischen Schlüssel zumindest das elektronische Schloss, das mit wenigstens zwei konzentrisch angeordneten Gegenkontakten und einer magnetischen Zentrierung versehen ist.

[0116] 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.

[0117] 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.

[0118] Optional betätigt das elektronische Schloss dabei nach Bestätigung einer Authentifikation der Zugriffsberechtigung zunächst eine Steuerung, mittels dem dann eine fremde Betriebsspannungsquelle zur Betätigung eines Motorschlosses oder eines sonstigen Aktors aktiviert wird.

[0119] Die Gegenkontaktflächen 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.

[0120] Darüber hinaus betrifft die Erfindung noch einen Rohrtresor umfassend einen Rohrkörper und einen Rohrkörperdeckel und ein elektronisches Schließsystem.

[0121] Dabei wird in dem Rohrkörper vorzugsweise ein Schlüssel aufbewahrt, da diese in der Regel als Schlüsseltresor dient.

[0122] Um dabei in einfacher Weise einen Zugriff auf den Schlüssel zu erhalten und andererseits in einfacher Weise den Schlüssel in dem Rohrkörper deponieren zu können, ohne dass insbesondere ein Verklemmen mit dem Rohrkörperdeckel beim Überführen desselben in die Schließstellung erfolgt, ist gemäß einer Ausführungsform des erfindungsgemäßen Rohrtresors vorgesehen, dass an dem Rohrkörperdeckel ein Schlüsselcontainer gehalten ist, der mit dem Rohrkörperdeckel in den Rohrkörper einführbar oder aus diesem entnehmbar ist.

[0123] Vorzugsweise ist dabei der Schlüsselcontainer so ausgebildet, dass er einen Aufnahmeraum für einen Schlüssel aufweist, so dass der Schlüssel in einfacher Weise in dem Schlüsselcontainer deponierbar und aus diesem entnehmbar ist.

[0124] Ferner ist vorzugsweise vorgesehen, dass der Schlüssel an dem Schlüsselcontainer gegen ein vollständiges Entfernen von dem Schlüsselcontainer gesichert ist, dies stellt sicher, dass der Schlüssel nicht beim Einsatz desselben verloren geht oder unzulässigerweise vom Schlüsselcontainer entfernt wird.

[0125] Eine weitere vorteilhafte Lösung sieht vor, dass der Aufnahmeraum des Schlüsselcontainers durch eine Öffnung zugänglich ist, durch welche der Schlüssel herausnehmbar oder in diesen einlegbar ist.

[0126] Um sicher zu gehen, dass die Bedienungsperson den Schlüsselcontainer in dem Rohrkörper deponiert und zwar den Schlüsselcontainer beim Verschließen des Rohrkörpers so deponiert, dass ein Verschließen des Rohrkörpers durch den Rohrkörperdeckel erfolgt, ist vorzugsweise vorgesehen, dass die Position des Schlüsselcontainers in dem Rohrkörper durch einen Sensor erfassbar ist.

[0127] Der Sensor könnte durch jede Art von Sensor gebildet sein.

[0128] Besonders einfach und zuverlässig ist es, wenn der Sensor ein Magnetfeldsensor ist, welcher einen am Schlüsselcontainer gehaltenen Magnet erkennt.

[0129] Um das Sensorsignal in einfacher Weise auswerten zu können, ist vorzugsweise vorgesehen, dass der Sensor mit einer Übermittlungseinheit zusammenwirkt, welche eine Schließstellung des Rohrkörperdeckels einer Sicherheitszentrale, beispielsweise einer vorstehend genannten Zentraleinheit, übermittelt.

[0130] Um ganz sicher zu gehen, dass der Rohrkörper zutreffend durch den Rohrkörperdeckel verschlossen ist, sieht eine weitere vorteilhafte Lösung vor, dass am Rohrkörper ein Sensor angeordnet ist, welcher eine Schließstellung des Rohrkörperdeckels in dem Rohrkörper erfasst.

[0131] Auch in diesem Fall ist vorzugsweise vorgesehen, dass der Rohrkörperdeckel mit einem Magnet versehen ist, dessen Position der Sensor erfasst.

[0132] Auch dieser Sensor wirkt vorzugsweise mit der vorstehend bereits erläuterten Übermittlungseinheit zusammen, um einer Sicherheitszentrale oder der eingangs genannten Zentraleinheit das Verschließen des Rohrtresors zu übermitteln.

[0133] Weitere Merkmale und Vorteile der Erfindung sind Gegenstand der nachfolgenden Beschreibung sowie der zeichnerischen Darstellung einiger Ausführungsbeispiele.

[0134] In der Zeichnung zeigen:

Fig. 1 eine schematische Darstellung eines elektronischen Schlüssels und eines elektronischen Schlosses eines ersten Ausführungsbeispiels eines erfindungsgemäßen Schließsystems;

Fig. 2 eine schematische Darstellung einer Aktivierung des elektronischen Schlüssels und des elektronischen Schlosses mit einer Zentraleinheit des elektronischen Schließsystems;

Fig. 3 eine schematische Darstellung einer Möglichkeit einer Erzeugung und Übermittlung eines externen Berechtigungscodes;

Fig. 4 eine perspektivische Frontansicht eines ersten Ausführungsbeispiels eines Rohrtresors ohne aufgesetzten elektronischen Schlüssel;

Fig. 5 ein Schnitt durch den Rohrtresor längs Linie 5-5 in Fig. 4 mit aufgesetztem elektronischem Schlüssel;

Fig. 6 eine perspektivische Ansicht des Rohrtresors gemäß Fig. 4 beim Öffnen desselben;

Fig. 7 eine schematische Darstellung ähnlich Fig. 1 eines zweiten Ausführungsbeispiels eines erfindungsgemäßen Schließsystems;

Fig. 8 ein weiteres Ausführungsbeispiel eines Rohrtresors mit einem in einen Verschlussdeckel integrierten elektronischen Schloss und einem für das elektronische Schloss charakteristischen Code;

Fig. 9 ein Ablaufdiagramm, das die Übermittlung der Codes zwischen einem Benutzer und einer zentralen Informationsverarbeitungsstelle verdeutlicht;

Fig. 10 die Hand eines Benutzers bei der Eingabe des Berechtigungscodes in einen elektronischen Schlüssel;

Fig. 11 die Verwendung des elektronischen Schlüssels als Griff beim Öffnen des elektronischen Schlosses;

Fig. 12 die Anordnung eines physikalischen Schlüs-

sels an der Innenseite des Verschlussdeckels des Rohrtresors;

Fig. 13 ein Ablaufdiagramm, das die Kommunikation zwischen dem Benutzer, einem Client-Rechner, einem Server, einem Administrator und dem elektronischen Schloss verdeutlicht;

Fig. 14 ein Diagramm, das die Funktionen auf Seiten des Benutzers, des Clientrechners, des Servers und des Administrators verdeutlicht;

Fig. 15 einen schematischen Schaltplan für eine Anwendung eines elektronischen Schlosses im Zusammenwirken mit einem Steuergerät und einem Motorschloss;

Fig. 16 eine schematische Vorderansicht eines elektronischen Schlüssels, und

Fig. 17 eine schematische Ansicht der Rückseite eines elektronischen Schlüssels.

[0135] Ein in Fig. 1 dargestelltes erstes Ausführungsbeispiel eines erfindungsgemäßen, als Ganzes mit 10 bezeichneten elektronischen Schließsystems 10 umfasst einen elektronischen Schlüssel 12 sowie ein elektronisches Schloss 14.

[0136] Der elektronische Schlüssel 12 weist dabei einen insbesondere Federkontakte aufweisende Kontaktsatz 16 auf, welcher mit einem insbesondere konzentrische Kontaktringe aufweisende Gegenkontaktsatz 18 über eine galvanische Verbindung durch Ansetzen des Kontaktsatzes 16 an den Gegenkontaktsatz 18 in Wirkverbindung bringbar ist.

[0137] Aufgrund der elektrischen Wechselwirkung zwischen dem elektronischen Schlüssel 12 und dem elektronischen Schloss 14 ist es dann möglich, mittels des elektronischen Schlüssels 12 einen Schließriegel 22 zu betätigen, das heißt diesen beispielsweise von einer Verschließstellung in eine Offenstellung oder gegebenenfalls auch umgekehrt zu bewegen.

[0138] Der elektronische Schlüssel 12 umfasst hierzu eine Spannungsquelle 32, beispielsweise in Form einer Batterie, welche einen Prozessor 34 mit Strom und Spannung versorgt.

[0139] Der Prozessor 34 ist in der Lage mit einer Eingabeeinheit 36 in und mit einem Sicherheitsprozessor 38, der mit einem gesicherten Speicher 39 versehen ist, in Wechselwirkung zu treten.

[0140] In dem gesicherten Speicher 39 ist nicht nur ein Identifikationscode ICK und ein Zuordnungspasswort des Schlüssels 12 gespeichert, sondern es kann in diesem auch vom Prozessor 34 ein extern erzeugter Berechtigungscode BCZ abgespeichert werden.

[0141] Der Prozessor 34 ist noch mit einer Schnittstelle 42 versehen, welche zur Aktivierung und/oder Konfiguration des Prozessors 34 dient.

[0142] Ferner führt von dem Prozessor 34 eine Datenleitung 44 zu dem Speicher 39 und weiter zu einem Datenkontakt 46 des Kontaktsatzes 16.

[0143] Von der Spannungsquelle 32 führt direkt eine Masseleitung 48 einerseits zu dem Prozessor 34 und andererseits zu einem Massekontakt 52 des Kontaktsatzes 16.

[0144] Der Prozessor 34 ist in der Lage über eine Schalteinheit 54 eine von der Spannungsquelle 32 zu einem Versorgungskontakt 56 des Kontaktsatzes 16 führende Versorgungsleitung 58 zu aktivieren.

[0145] Bei einer Wechselwirkung des Kontaktsatzes 16 des elektronischen Schlüssels 12 mit dem Gegenkontaktsatz 18 des elektronischen Schlosses 14 berühren der Massekontakt 52 einen insbesondere als Kontaktring ausgebildeten Massegegenkontakt 62 und der Versorgungskontakt 56 einen insbesondere als Kontaktring ausgebildeten Versorgungsgegenkontakt 66. Damit ist ein im elektronischen Schloss 14 vorgesehener Prozessor 72 durch den elektronischen Schlüssel 12 aktivierbar und mit der Spannungsquelle 32 des elektronischen Schlüssels 12 betreibbar, ohne dass das elektronische Schloss 14 hierzu eine eigene Spannungsquelle benötigt.

[0146] Ferner berührt in diesem Fall auch der Datenkontakt 46 des Kontaktsatzes 16 einen insbesondere als Kontaktring ausgebildeten Gegendatenkontakt 68 des Gegenkontaktsatzes 18, der seinerseits über eine Datenleitung 74 mit dem Prozessor 72 verbunden ist.

[0147] Mit dem Prozessor 72 ist ferner noch einen Identifikationscode ICL des elektronischen Schlosses 14 sowie ein Zuordnungspasswort aufnehmender Speicher 76 in Form eines EEPROM, eine Uhr 78 und ein Schließantrieb 82 gekoppelt.

[0148] Ferner ist eine Aktivierung und/oder eine Konfiguration des Prozessors 72 über eine mit diesem gekoppelte Schnittstelle 84 möglich.

[0149] Der Prozessor 72 wird seinerseits mit der Spannung der Spannungsquelle 32 betrieben, im Fall eines über die Spannungsquelle 32 ebenfalls zu betreibenden Schließantriebs 82 ist vorzugsweise in dem elektronischen Schloss 14 ein Spannungswandler 86 vorgesehen, welcher die von der Spannungsquelle 32 zur Verfügung gestellte Spannung in eine höhere Spannung beispielsweise zum Betreiben des Schließantriebs umsetzt. Zusätzlich ist dem Prozessor 72 noch ein Protokollspeicher 88 zugeordnet, in welchem Aktivitäten des Prozessors 72 des elektronischen Schlosses 14 protokolliert und abgespeichert werden.

[0150] Das erfindungsgemäße Schließsystem 10 arbeitet nun wie folgt:
Dem elektronischen Schlüssel 12 wird über die Eingabeeinheit 36 der extern generierter Berechtigungscode BCZ übermittelt, welchen der Prozessor 34 in dem gesicherten Speicher 39 des Sicherheitsprozessors 38 ablegt.

[0151] Hierzu wird vom Prozessor 34 ein Sicherheitscode SC in Form eines Hash-Codes berechnet und dem

Sicherheitsprozessor 38 mit dem Berechtigungscode BCZ übermittelt.

[0152] Außerdem aktiviert der Prozessor 34 über die Schalteinheit 54 den Versorgungskontakt 56, so dass dieser auf der Versorgungsspannung der Spannungsquelle 32 liegt.

[0153] Ist eine Verbindung zwischen dem Kontaktsatz 16 des elektronischen Schlüssels 12 und dem Gegenkontaktsatz 18 des elektronischen Schlosses 14 hergestellt, so wird allein durch das Anliegen der Versorgungsspannung an dem Versorgungsgegenkontakt 66 und das Anliegen von Masse an dem Massengegenkontakt 62 der Prozessor 72 des elektronischen Schlosses 14 durch einen Reset hochgefahren und beginnt nun über die Verbindung der Datenleitung 74 mit der Datenleitung 44 mit dem Sicherheitsprozessor 38 zu kommunizieren.

[0154] Vor einem Auslesen des Inhalts des gesicherten Speichers 39 des Sicherheitsprozessors 38 erfolgt jedoch eine Überprüfung, ob der Sicherheitsprozessor 38 als solcher berechtigt ist, mit dem Prozessor 72 Daten auszutauschen, beispielsweise dadurch, dass überprüft wird, ob eine im Speicher 76 enthaltene Liste den Sicherheitsprozessor 38 gelistet hat.

[0155] Danach erfolgt die Berechnung eines Sicherheitscodes SC in Form eines Hash-Codes durch den Prozessor 72 und unter Anwendung des Sicherheitscodes SC ein Auslesen des gesicherten Speichers 39, der den Berechtigungscode BCZ umfasst.

[0156] Dieses Auslesen des Speichers 39 erfolgt dabei insbesondere ohne eine Aktivität des Prozessors 34 des elektronischen Schlüssels 12.

[0157] Nach Auslesen des Berechtigungscodes BCZ überprüft der Prozessor 72 aufgrund eines mit einem eigenen Berechtigungscodeermittlungsprogramm BCEPS ermittelten eigenen Berechtigungscodes BCS und eines den Berechtigungscode BCZ mit dem Berechtigungscode BCS in Hinblick auf Ihre Identität vergleichenden Berechtigungscodeüberprüfungsprogramms BCUP die Richtigkeit des Berechtigungscodes BCZ, und sieht im Falle einer der Berechtigungscodes BCZ und BCS ein Öffnen des elektronischen Schlosses 14 vor.

[0158] Bei Identität der Berechtigungscodes BCZ und BCS aktiviert der Prozessor 72 bei dem ersten Ausführungsbeispiel den Schließantrieb 82 und dieser bewegt den Schließriegel 22 beispielsweise von seiner Verriegelungsstellung in seine Offenstellung, so dass dann das elektronische Schloss 14 einen Zugang beispielsweise zu einer gesicherten Einheit freigibt.

[0159] Gleichzeitig erstellt der Prozessor 72 durch Auslesen der Uhr 78 ein Protokoll, das den Zugriff auf das Schloss 14, das Auslesen des Zugangsdatensatzes ZD aus dem Speicher 38 und das Aktivieren des Schließantriebs 82 festhält, wobei dieses Protokoll dann in dem Protokollspeicher 88 abgelegt wird.

[0160] Sämtliche Zustände des elektronischen Schlosses 14, die von dem Prozessor 72 ermittelt und dem Benutzer angezeigt werden sollen, werden vorzugsweise nicht von dem elektronischen Schloss 14 angezeigt, sondern über die Datenleitung 74 und die Datenleitung 44 dem Prozessor 34 des elektronischen Schlüssels 12 übertragen, der dann seinerseits einen oder mehrere optische Anzeigeeinheiten 92, 94, wie beispielsweise LED-Lampen oder Displayanzeigen oder akustische Signalgeber aktiviert, wie beispielsweise Summer, oder Tonfolgen, die durch einen Lautsprecher übertragen werden, generiert.

[0161] Um die vorgesehene Funktion des elektronischen Schlüssels 12 und des elektronischen Schlosses 14 zu erhalten, sind sowohl der elektronische Schlüssel 12 als auch das elektronische Schloss 14 durch eine Zentraleinheit 102 leitungsgebunden zu aktivieren, die ihrerseits über eine Schnittstelle 104 auf die Schnittstelle 42 des elektronischen Schlüssels 12 und über eine Schnittstelle 106 auf die Schnittstelle 84 des elektronischen Schlosses 14 zeitgleich oder auch nacheinander oder jeweils separat zugreifen kann, um sowohl den elektronischen Schlüssel 12 als auch das elektronische Schloss 14 zu aktivieren wobei insbesondere Zuordnungspasswörter und/oder der jeweilige Identifikationscode ICK sowie der jeweilige Identifikationscode ICL sowie Zykluszustände ZZ der Zykluszähler ZCZ und ZCS zwischen der Zentraleinheit 102 und dem elektronischen Schlüssel 12 sowie dem elektronischen Schloss 14 abgeglichen oder ausgetauscht werden, das heißt entweder übertragen oder ausgelesen werden.

[0162] Nach einer derartigen Aktivierung des elektronischen Schlüssels 12 und des elektronischen Schlosses 14 können die jeweiligen Verbindungen zwischen den Schnittstellen 42 und 104 sowie 84 und 106 getrennt werden und die Zentraleinheit 102 ist in der Lage, mittels eines in der Zentraleinheit 102 vorhandenen Berechtigungscodeermittlungsprogramms BCEPZ den jeweils einmaligen externen Berechtigungscode BCZ mittels eines Hash-Algorithmus zu ermitteln, welcher dann über die Eingabeeinheit 36 in den elektronischen Schlüssel 12, beispielsweise durch den Benutzer, eingegeben werden kann, worauf dann der Prozessor 34 des elektronischen Schlüssels 12 in der Lage ist, den Berechtigungscode BCZ in dem gesicherten Speicher 39 abzulegen.

[0163] Ferner ist das elektronische Schloss 14 dann in der Lage - wie beschrieben - nach Wechselwirkung mit dem elektronischen Schlüssel 12 den externen Berechtigungscode auszulesen und durch das Berechtigungscodeermittlungsprogramm BCEPS ebenfalls unter Heranziehung des Identifikationscodes ICK des Identifikationscodes ICS, des Zykluszustandes ZZ des eigenen Zykluszählers ZCS mittels desselben Hash-Algorithmus wie in der Zentraleinheit 102 den eigenen Berechtigungscode BCS zu ermitteln und zu überprüfen, ob dieser mit dem externen Berechtigungscode BCZ identisch ist und ein Öffnen des Schließriegels 22 erlaubt.

[0164] Wie in Fig. 3 dargestellt, lässt sich eine erfindungsgemäße Schließeinrichtung 10 beispielsweise im Feld dahingehend einsetzen, dass eine Bedienungsperson bei einem im Feld stationär angeordneten Schloss 14 mit einem elektronischen Schlüssel 12 ein Öffnen des

Schlosses 14 durch folgende Vorgehensweise einleiten kann.

[0165] Die Bedienungsperson, die ein im Feld stationär angeordnetes Schloss 14 öffnen möchte, fordert von der Zentraleinheit 102, beispielsweise über eine mobile Kommunikationseinheit 112, insbesondere ein tragbares Mobilfunkgerät oder ein anderes Kommunikationsgerät, die Übermittlung eines externen Berechtigungscodes BCZ an.

[0166] Hierzu kann seitens der Zentraleinheit 102 die Überprüfung einer Vielzahl von Angaben oder eine Abfrage einer Vielzahl von Angaben erfolgen, die vor Erhalt des Berechtigungscodes BCZ vorliegen müssen.

[0167] Derartige Daten sind beispielsweise ein lokaler Code LC des Schlosses 14 und/oder ein persönlicher Code PC der Bedienungsperson und/oder Zeitangaben ZA am Ort der Bedienungsperson und/oder Ortsangaben OA zu der Bedienungsperson.

[0168] Alle diese Informationen können von der Zentraleinheit 102 überprüft werden. In dem Fall, dass Überprüfung dieser gesamten Informationen und Angaben positiv ausfällt, generiert die Zentraleinheit 102 einen externen Berechtigungscode BCZ, da die Zentraleinheit 102 aus dem lokalen Code LC und/oder dem persönlichen Code PC und/oder den Zeitangaben und/oder den Ortsangaben OA auf die Identifikationscodes ICK und ICL schließen kann und daher unter Verwendung des dieser bekannten Identifikationscodes ICK des zum Öffnen zu verwendenden elektronischen Schlüssels 12 und des Identifikationscodes ICL des zu öffnenden elektronischen Schlosses 14 sowie des Zykluszustandes ZZ des Zykluszählers ZCZ mittels des Berechtigungscodeermittlungsprogramms BCEPZ den externen Berechtigungscode BCZ mittels eines Hash-Algorithmus, der der Bedienungsperson, beispielsweise akustisch oder als Nachricht oder als Datensatz, beispielsweise über die mobile Kommunikationseinheit 112, übermittelt wird.

[0169] Daraufhin erfolgt eine Übermittlung des Berechtigungscodes BCZ von der Bedienungsperson oder von der mobilen Kommunikationseinheit 112 über die Eingabeeinheit 36 zu dem elektronischen Schlüssel 12.

[0170] Der Berechtigungscode BCZ ist insbesondere nur ein Berechtigungscode BCZ, der zu einer einmaligen Öffnung des elektronischen Schlosses 14 berechtigt.

[0171] Diesen Berechtigungscode BCZ legt dann der elektronische Schlüssel 12 mittels eines Prozessors 34 in dem Speicher 39 ab.

[0172] Wird nun der Kontaktsatz 16 mit dem Gegenkontaktsatz 18 in Verbindung gebracht, so wird - wie bereits beschrieben - der Prozessor 72 des elektronischen Schlosses 14 aktiviert und liest - wie bereits beschrieben - den Berechtigungscode BCZ aus dem elektronischen Schlüssel 12 aus.

[0173] Durch eigene Berechnungen eines Berechtigungscodes BCS mittels seines Berechtigungscodeermittlungsprogramms BCEPS unter Verwendung des aus dem gesicherten Speicher 39 ausgelesenen Identifikationscodes ICK des elektronischen Schlüssels 12, des im Speicher 76 abgelegten Identifikationscodes ICK des elektronischen Schlosses 14 und des Zykluszustandes ZZ des Zykluszählers ZCS des elektronisches Schlosses 14 und durch Überprüfung der Identität des Berechtigungscodes BCZ mit dem Berechtigungscode BCS mittels seines Berechtigungscodeüberprüfungsprogramms BCUP ist der Prozessor 72 dabei in der Lage, zu ermitteln, ob der externe Berechtigungscode BCZ zu einer nachfolgenden Öffnung des Schließriegels 22 berechtigt und - wenn dies bei Identität der Berechtigungscodes der Fall ist - wird der Schließantrieb 82 zur Betätigung des Schließriegels 22 aktiviert.

[0174] Nach dem einmaligen Öffnen des elektronischen Schlosses 14 ist allerdings der Berechtigungscode BCZ zur einmaligen Öffnung des elektronischen Schlosses 14 verbraucht und kann nicht mehr zur Öffnung desselben eingesetzt werden.

[0175] Selbst wenn der Zugangsdatensatz ZD im elektronischen Schlüssel 12 gespeichert bleiben würde, würde somit ein erneutes Aktivieren des Prozessors 72 des elektronischen Schlosses 14 und eine Überprüfung des Berechtigungscodes BCZ ergeben, dass dieser nicht zu einem erneuten Öffnen des elektronischen Schlosses 14 berechtigt.

[0176] In der Zentraleinheit 102 kann die Überprüfung der über die mobile Kommunikationseinheit 12 übermittelten Informationen bezüglich des lokalen Codes und/oder des persönlichen Codes und/oder der Zeitangaben und/oder der Ortsangaben durch eine Person erfolgen, die beispielsweise die Aktivitäten der Bedienungsperson im Feld überwacht und in der Lage ist, zu beurteilen, ob diese Informationen konsistent sind.

[0177] Es ist aber auch möglich, diese Überprüfung durch die Zentraleinheit 102 programmgesteuert durchzuführen.

[0178] Die Ermittlung des Berechtigungscodes BCZ in der Zentraleinheit 102 erfolgt jedoch durch ein das Berechtigungscodeermittlungsprogramm BCEPZ, welches sämtliche oder nur einen Teil dieser Informationen zur Ermittlung des Berechtigungscodes BCZ heranzieht.

[0179] Dabei ist insbesondere der Vorteil des erfindungsgemäßen Schließsystems darin zu sehen, dass das elektronische Schloss 14 selbst keine Spannungsquelle benötigt, sondern beliebig lange unbenutzt sein kann, da die gesamte Stromversorgung zur Aktivierung des Prozessors 72 des elektronischen Schlosses und zum Betreiben des Prozessors 72 des elektronischen Schlosses über die Spannungsquelle 32 des elektronischen Schlüssels erfolgt, die von der Bedienungsperson mitgeführt wird und daher von der Bedienungsperson stets nachgeladen oder erneuert werden kann.

[0180] Ferner besteht durch die Aktivierung des elektronischen Schlüssels 12 und des dazugehörigen elektronischen Schlosses 14 durch die Zentraleinheit 102 eine eindeutige Korrelation zwischen dem elektronischen Schlüssel 12 und dem elektronischen Schloss 14 sowie der Zentraleinheit 102 und somit eine eindeutige Korrelation zwischen den für ein bestimmtes elektronisches

Schloss 14 zum Öffnen desselben vorgesehenen elektronischen Schlüssel 12 und der ebenfalls entsprechend korrelierten Zentraleinheit 102, die diese Korrelation von elektronischem Schlüssel 12, elektronischem Schloss 14 und Zentraleinheit 102 bei der Berechnung des Berechtigungscodes BCZ zugrunde legt. So lassen sich bei der Aktivierung von einem oder mehreren elektronischen Schlüsseln 12 und von einem oder mehreren für diesen elektrischen Schlüssel 12 vorgesehenen elektronischen Schlössern 14 durch Austausch von Passwörtern, Austausch oder Überprüfung der Identifikationscodes ICK und ICS sowie Abgleich der Zykluszähler Ausgangsbedingungen schaffen, mit denen die Berechtigungscodeermittlungsprogramme BCEPS und BCEPK unabhängig voneinander identische Berechtigungscodes BCZ und BCS ermitteln können.

[0181] Eine derartige elektronische Schließeinrichtung lässt sich beispielsweise bei einem als Ganzes mit 202 bezeichneten Rohrtresor einsetzen, der einen lokal fest installierten Rohrkörper 204 aufweist, in welchen ein das elektronische Schloss 14 umfassender Rohrkörperdeckel 206 einsetzbar und mit dem Rohrkörper 204 verriegelbar ist.

[0182] Dabei trägt der Rohrkörperdeckel 206 an seiner außenliegenden Frontseite 208 die Gegenkontakteinheit 18 des elektronischen Schlosses 14 mit den Kontaktringen 62, 66, 68.

[0183] Ferner ist der Rohrkörper 204 mit dem lokalen Code LC versehen, welcher es erlaubt, den bestimmten Rohrtresor 202 an dem jeweiligen bestimmten Ort zu identifizieren.

[0184] Wie in Fig. 5 dargestellt, dient der Rohrkörperdeckel als Gehäuse für die Aufnahme des elektronischen Schlosses 14, wobei in dem Rohrkörperdeckel 206 auch der Schließantrieb 82 und der Schließriegel 22 angeordnet sind, so dass der Schließriegel 22 beispielsweise in eine Schließriegelaufnahme 212 an einer Innenseite 214 des Rohrkörpers 204 eingreifen kann, um den Rohrkörperdeckel 206 in seiner in Fig. 5 dargestellten Schließstellung zu fixieren.

[0185] Da derartige Rohrtresore 202 häufig dazu dienen, Zugangsschlüssel sicher aufzubewahren, ist an dem Rohrkörperdeckel 206 noch ein Schlüsselcontainer 222 gehalten, beispielsweise fest montiert oder lösbar gehalten, welcher einen Aufnahmeraum 224 für einen Schlüssel 226 aufweist, wobei der Schlüssel 226 beispielsweise in dem Aufnahmeraum 224 auch noch durch ein Halteband 228 gesichert ist, so dass der Schlüssel 226 zwar aus dem Aufnahmeraum 224 entnommen werden kann, jedoch nicht vom Schlüsselcontainer 222 getrennt werden kann.

[0186] Ein derartiger Schlüsselcontainer 222 hat den großen Vorteil, dass dieser die Möglichkeit bietet, den Schlüssel 226 an dem Rohrkörperdeckel 206 derart anzuordnen, dass dieser mit dem Rohrkörperdeckel 206 in einfacher Weise und ohne dass sich der Schlüssel im Rohrkörper 204 verklemmen kann oder zwischen dem Rohrkörper 204 und dem Rohrkörperdeckel 206 verklemmen kann, in den Rohrkörper 204 eingeführt werden kann und durch Verriegeln des Rohrkörperdeckels 206 zuverlässig fixiert werden kann.

[0187] Darüber hinaus bietet ein Schlüsselcontainer 222 auch noch die Möglichkeit, beispielsweise bei Einbau des Rohrkörpers 206 in einer zur Feuchtigkeit liegenden Umgebung den Schlüssel 226 in dem Rohrkörper 204 trocken und/oder verschmutzungsfrei zu lagern, so dass beispielsweise in den Rohrkörper 204 eintretender Schmutz vom Schlüssel 226 während der Lagerung desselben ferngehalten werden kann.

[0188] Wie in Fig. 5 und Fig. 6 dargestellt, ist der erfindungsgemäße elektronische Schlüssel 12 in einem Gehäuse 232 angeordnet, das eine auf die Frontseite 208 des Rohrkörperdeckels 206 aufsetzbare Rückseite 234 aufweist, welche den Kontaktsatz 16 zur Kontaktierung des Gegenkontaktsatzes 18 an der Frontseite 208 des Rohrkörperdeckels 206 aufweist und andererseits an ihrer der Rückseite 234 gegenüberliegenden Frontseite 236 die Eingabeeinheit 36' trägt, die in diesem Fall als Tastenfeld oder Touchpanel ausgebildet ist und zur Eingabe des Berechtigungscodes BCZ dient.

[0189] Zur lösbaren Fixierung des Gehäuses 232 des elektronischen Schlüssels 12 am Rohrkörperdeckel 206 ist eine Magnetverbindung 238 vorgesehen, die entweder zwei Magnete M1, M2 oder einen Magnet M1 und ein durch diesen magnetisierbares Element umfasst.

[0190] Die Magnetverbindung dient dabei nicht nur zur lösbaren Fixierung des elektronischen Schlüssels 12 am elektronischen Schloss, sondern auch zur zentrierten Ausrichtung des Kontaktsatzes 16 relativ zum Gegenkontaktsatz 18.

[0191] Diese magnetische Kopplung zwischen dem Gehäuse 232 und dem Rohrkörperdeckel 206 ermöglicht es, bei entriegeltem elektronischem Schloss 14 mit dem Gehäuse 232 des elektronischen Schlüssels 12 den Rohrkörperdeckel 206, welcher das Gehäuse für das elektronische Schloss 14 darstellt, aus dem Rohrkörper 206 durch herausziehen des Rohrkörperdeckels 206 aus dem Rohrkörper 204 zu entnehmen.

[0192] Um ferner für eine lokale Anzeige dahingehend zu ermöglichen, dass der Rohrkörperdeckel 206 zuverlässig in dem Rohrkörper 204 sitzt, besteht die Möglichkeit, beispielsweise am Schlüsselcontainer 222 einen Magnet 242 vorzusehen, dessen Position innerhalb des Rohrkörpers durch einen Magnetfeldsensor 244 der am Rohrkörper angeordnet ist, hinsichtlich seiner Position im Rohrkörper 204 zu detektieren und dadurch festzustellen, ob der Schlüsselcontainer 222 und vorzugsweise dabei dann auch der Rohrkörperdeckel 206 in einer Position im Rohrkörper 204 angeordnet sind, in welcher der Rohrkörperdeckel 206 durch den beispielsweise durch einen elastischen Kraftspeicher 24 beaufschlagten Schließriegel 22 verriegelt ist.

[0193] Soll die Position des Rohrkörperdeckels 206 diesbezüglich ebenfalls erfasst werden, besteht auch die Möglichkeit, in dem Rohrkörperdeckel 206 einen Magnet 246 anzuordnen und dessen Position durch einen eben-

falls am Rohrkörper 204 angeordneten Magnetfeldsensor 248 zu erfassen, so dass die Möglichkeit besteht sowohl die richtige Position des Schlüsselcontainers 222 als auch die richtige Position des Rohrkörperdeckels 206 in seiner Schließstellung zu erfassen und beispielsweise Übermittlungseinheit 252 entweder drahtlos oder drahtgebunden einer Sicherheitszentrale oder auch der Zentraleinheit 102 zu übermitteln.

[0194] Bei einem zweiten Ausführungsbeispiel einer erfindungsgemäßen Schließeinrichtung 10, dargestellt in Fig. 7, sind all diejenigen Teile, die mit denen des ersten Ausführungsbeispiels identisch sind, mit denselben Bezugszeichen versehen, so dass hinsichtlich der Beschreibung derselben vollinhaltlich auf das erste Ausführungsbeispiel Bezug genommen werden kann.

[0195] Im Gegensatz zum ersten Ausführungsbeispiel ist allerdings das elektronische Schloss 14' nicht mit einem Schließantrieb 82 versehen, sondern mit einer Schalteinheit 262, die in der Lage ist, eine Verbindung zwischen externen Anschlüssen 264 und 266 des elektronischen Schlosses 14' herstellt oder unterbricht, so dass über die äußeren Anschlüsse 264 und 266 die Möglichkeit besteht, ein vorhandenes Schließsystem 268 zu aktivieren oder zu blockieren.

[0196] Beispielsweise können die äußeren Anschlüsse 266 und 264 dazu dienen, eine Stromzufuhr zu dem bereits vorhandenen Schließsystem 268 zu unterbrechen und somit dieses lahm zu legen oder die Stromzufuhr zu diesem herzustellen und somit das bereits vorhandene Schließsystem 268 zu aktivieren.

[0197] Das vorhandene Schließsystem 268 kann dabei ein beliebig aufgebautes Schließsystem, das beispielsweise bereits in einem Gebäude vorhanden und vollinstalliert ist, sein, so dass die erfindungsgemäße Schließeinrichtung 10' lediglich dazu dient, dieses Schließsystem 268 komplett lahm zu legen oder zu aktivieren.

[0198] Damit kann ein bereits vorhandenes Schließsystem 268, welches ein geringes Sicherheitsniveau hat, mit dem erfindungsgemäßen Schließsystem 10', welches ein sehr hohes Sicherheitsniveau aufweist, gesichert werden, ohne dass das vorhandene Schließsystem 268 komplett deinstalliert und ein neues Schließsystem installiert werden muss.

[0199] Eine in Fig. 8 dargestellte Verschlussvorrichtung 310 wird von einem Rohrtresor 312 gebildet, der diebstahls- und aufbruchssicher in einer Wand eines Gebäudes oder an einem stabilen Träger in der Nähe des Gebäudes angeordnet ist. Der Rohrtresor 312 ist mittels eines Verschlussdeckels 314 an seiner Vorderseite verschlossen. In den Verschlussdeckel 314 integriert ist ein elektronisches Schloss 316, wie es detailliert in der WO 2012/045474 A1 dargestellt und beschrieben ist, deren Offenbarungsgehalt hiermit zum Gegenstand der vorliegenden Anmeldung gemacht wird.

[0200] An der Innenseite des Verschlussdeckels 314 ist - wie in Figur 12 dargestellt - ein physikalischer Schlüssel 318 angeordnet, mittels dem wenigstens ein Zugang zu dem nicht dargestellten Gebäude und optional weitere Türen in diesem Gebäude geöffnet werden können.

[0201] An der mittels des elektronischen Schlosses 316, das beispielsweise dem des ersten Ausführungsbeispiels entspricht, versperrten Verschlussvorrichtung 310 ist ein für das elektronische Schloss 316 charakteristischer Code 320 angeordnet. Dieser ist im gezeigten Ausführungsbeispiel in Form eines Barcodes 320 ausgebildet, kann jedoch auch von einem Aztek-Code oder einem unsichtbaren magnetischen Code gebildet werden. Der Code 320 kann im einfachsten Falle von einem Benutzer 320 manuell ausgelesen werden. Gemäß einer vorteilhaften Ausgestaltung verfügt eine vom Benutzer 322 mitgeführte Kommunikationseinrichtung 324 über einen Sensor oder eine Leseeinrichtung zum automatischen Erfassen des Codes 320. Die Kommunikationseinrichtung 324 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 316 charakteristischer Code 320 verwendet werden. Wie schon erwähnt, können auch unsichtbare, magnetisch oder über ein Funksignal übermittelte Codes 320 durch das elektronische Schloss 316 oder eine in dessen Nähe angeordnete Einrichtung ausgesendet und von der Kommunikationseinrichtung 324 empfangen oder ausgelesen werden.

[0202] Das elektronische Schloss 316 ist mittels eines elektronischen Schlüssels 332 aufschließbar, sofern in diesen elektronischen Schlüssel 332 ein für das elektronische Schloss 316 passender Berechtigungscode 336 eingegeben wird. In Figur 10 ist dargestellt, wie der Berechtigungscode 336 vom Benutzer 322 über eine am elektronischen Schlüssel 332 angeordnete Tastatur eingegeben wird. Der elektronische Schlüssel 332 kann dann anschließend, wie in Figur 11 gezeigt, auf das elektronische Schloss 316 aufgesetzt und unmittelbar als Handgriff für das Öffnen des Verschlussdeckels 314 verwendet werden.

[0203] Diesem Vorgang voraus geht jedoch erfindungsgemäß die in den Figuren 9, 13 und 14 dargestellte Prozedur, bei der der Benutzer 322 die für das elektronische Schloss 316 charakteristische Information (den Code 320) und eine für seine Person charakteristische Information in Form eines Codes 326 -beispielsweise in Form eines persönlichen Passworts oder einer Buchstaben-/ Zahlenkombination - mittels der Kommunikationseinrichtung 324 an eine zentrale Informationsverarbeitungsstelle 330 - beispielsweise die Zentrale eines Sicherheitsdienstes - übermittelt. Die für das elektronische Schloss 316 charakteristische Information 320 und die für die Person des Benutzers 322 charakteristische Information 326 bilden gemeinsam einen Anfrage-Datensatz 334, der im einfachsten Fall manuell über ein Telefonat an die zentrale Informationsverarbeitungsstelle 330 übermittelt wird.

[0204] Gemäß einer vorteilhaften Ausgestaltung der

Erfindung erfolgt die Übermittlung des Anfrage-Datensatzes 334 automatisiert, beispielsweise als Zeichenkette in einer von der Kommunikationseinrichtung 324 versendeten Kurzmitteilung (SMS).

[0205] In der Informationsverarbeitungsstelle 330 wird der Anfrage-Datensatz 334 mit den darin enthaltenen Codes 320 und 326 vorzugsweise unter zusätzlichem Abgleich mit einem Zeit-Parameter 328 (beispielsweise dem Dienstplan oder Routenplan des Benutzers 322) geprüft. Sofern diese Überprüfung zu einem positiven Ergebnis führt, generiert die Informationsverarbeitungsstelle 330 einen Berechtigungscode 336, wie er beim ersten Ausführungsbeispiel des Schließsystems beschrieben wurde, und sendet diesen an die Kommunikationseinrichtung 324. Dies kann im einfachsten Fall wiederum durch ein Telefonat erfolgen.

[0206] Gemäß einer vorteilhaften Weiterbildung erfolgt die Übermittlung des Berechtigungscodes 336 an die Kommunikationseinrichtung 324 automatisiert, beispielsweise in Form einer in eine Kurzmitteilung (SMS) eingebetteten Zeichenkette.

[0207] Der Berechtigungscode 336 wird vom Benutzer 322, wie bereits in Verbindung mit Figur 10 erwähnt, entweder über eine Eingabeeinrichtung, insbesondere eine Tastatur manuell an den elektronischen Schlüssel 332 übertragen oder es erfolgt eine automatische Übertragung des Berechtigungscodes 336 von der Kommunikationseinrichtung 324 an den elektronischen Schlüssel 332. Diese Übertragung kann dadurch erfolgen, dass die Kommunikationseinrichtung 324 über einen Sender und der elektronische Schlüssel 332 über einen mit diesem Sender kommunizierenden Empfänger verfügt. Die Übertragung kann beispielsweise über ein Infrarot-Signal, über Bluetooth oder ein anderes geeignetes Nahübertragungs-Protokoll erfolgen.

[0208] Gemäß einer Weiterbildung der Erfindung können die Kommunikationseinrichtung 324 und der elektronische Schlüssel 332 auch eine bauliche Einheit bilden, die einen Sensor für das Erfassen des Codes 320, eine Eingabeeinrichtung für den Code 326, eine Sendeeinrichtung für die Übertragung des Anfrage-Datensatzes 334 an die zentrale Informationsverarbeitungsstelle 330, einen Empfänger für den Empfang des Berechtigungscodes 336 und einen Speicher zur Speicherung des Berechtigungscodes 336 im elektronischen Schlüssel 232 aufweist. Die Baueinheit enthält auch eine Software zur Erfassung der Codes 320 und 326, zur automatisierten Übertragung des Anfrage-Datensatzes 334, zum automatisierten Empfang und zur Speicherung des Berechtigungscodes 336.

[0209] Die zentrale Informationsverarbeitungsstelle 330 weist vorteilhaft wenigstens einen Client-Rechner 310 und wenigstens einen Server 3320 auf. Der Client-Rechner 3310 dient zum Empfang des Anfrage-Datensatzes 34 und zur Übermittlung dieses Datensatzes an den Server 3320. Der Daten-Verkehr zwischen dem Client-Rechner 3310 und dem Server 3320 ist in den Figuren mit 3315 bezeichnet.

[0210] Im Server 3320 werden zusätzlich Zeit-Parameter 328 gespeichert, die beispielsweise einen Routenplan des Benutzers 322 mit einer für das Öffnen des betreffenden elektronischen Schlosses 316 charakteristischen Zeit vorzugsweise mit einem entsprechenden Zeitpuffer (früheste Öffnungszeit, späteste Öffnungszeit, späteste Schließzeit) abbilden. Sämtliche Daten im Server 3320 werden von einem Administrator 3330 verwaltet. Der Datenverkehr zwischen dem Server 3320 und dem Administrator 3330 ist in den Figuren mit 3325 bezeichnet.

[0211] An den Server 3320 kann auch ein Signal übermittelt werden, das beim Öffnen und Schließen des elektronischen Schlosses 316 von einem am elektronischen Schloss 316 installierten Sender automatisch gesendet wird.

[0212] Das Verfahren und das Schließsystem können entgegen der Darstellung in den Figuren 9, 13 und 14 in einer fortgeschrittenen Ausführungsform auch vollautomatisch ohne menschliche Interaktion funktionieren. Der Empfang eines Anfrage-Datensatzes 334 durch den Client-Rechner 3310, die Übermittlung des Anfrage-Datensatzes 334 an den Server 3320, die Überprüfung der im Anfrage-Datensatz 334 enthaltenen charakteristischen Informationen (Codes 320 und 326), der Abgleich mit dem wenigstens einen Zeit-Parameter 328, die Generierung eines Berechtigungscodes 336 und die Übermittlung des Berechtigungscodes 336 an die Kommunikationseinrichtung 324, gegebenenfalls wiederum unter Zwischenschaltung eines Client-Rechners 3310 können vorzugsweise mittels einer Software gesteuert vollautomatisch erfolgen.

[0213] Dass das erfindungsgemäße Verfahren und System zur gesicherten Freigabe einer Zugangsberechtigung bzw. zur gesicherten Schlüsselübergabe auch auf Seiten des Benutzers 322 vollautomatisch erfolgen kann, wurde bereits im Zusammenhang mit den möglichen Ausführungsformen der Kommunikationseinrichtung 324 und des elektronischen Schlüssels 332 beschrieben.

[0214] Der elektronische Schlüssel 332 ist gemäß der Erfindung mit einer Eingabeeinrichtung 333 versehen, mittels der der Benutzer 322 den von der zentralen Informationsverarbeitungsstelle 330 an die Kommunikationseinrichtung 324 übermittelten Berechtigungscode 336 in den elektronischen Schlüssel eingeben kann. Ein derartiger, mit einer Eingabeeinrichtung 333 versehener elektronischer Schlüssel 332 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 332, der erst im Anschluss zur Öffnung eines elektronischen Schlosses verwendet wird, völlig unbeobachtet schon in einiger Entfernung vom elektronischen Schloss 316 erfolgen.

[0215] Als elektronischer Schlüssel 332 kann wie im

gezeigten Ausführungsbeispiel ein auf das elektronische Schloss 316 aufgesetzter, vorzugsweise durch Magnetkraft temporär mit dem elektronischen Schloss 316 verbundener Schlüssel 332 verwendet werden. Die Magnetkräfte werden durch einen Magneten 3329 im zentralen Bereich des elektronischen Schlüssels 332 und durch einen Gegenmagneten 3161 im zentralen Bereich des elektronischen Schlosses 316 bereitgestellt, die bevorzugt als Permanent-Ringmagnete ausgebildet sind und für eine automatische Zentrierung des elektronischen Schlüssels 332 mit dem elektronischen Schloss 316 sowie eine Ausrichtung der Kontakte 3324, 3325 und 3326 zu den konzentrisch angeordneten Gegenkontaktflächen 3164, 3165, 3166 am elektronischen Schloss 316 unabhängig vom relativen Winkel zueinander sorgen.

[0216] Es sind jedoch ebenso berührungslos über eine gewisse Distanz mit dem elektronischen Schloss 316 zusammenwirkende elektronische Schlüssel 332, beispielsweise in Form eines Transponders, verwendbar.

[0217] Der elektronische Schlüssel 332 weist ein Gehäuse 3321 auf, auf dessen Vorderseite gemäß Fig. 10 und 16 die Eingabeeinrichtung 333 angeordnet ist. Im gezeigten Ausführungsbeispiel ist dies eine numerische Tastatur mit 310 Zifferntasten 3331, einer Löschtaste 3332 ("C") und einer Eingabetaste 3333 ("OK"). Auf der Rückseite des Gehäuses 3321 treten drei federnd im Gehäuse gelagerte Kontakte 3324, 3325 und 3326 hervor, von denen der zentral angeordnete Kontakt 3325 beispielsweise die Plusspannung führt, der am weitesten außen liegende Kontakt 3324 die Masseverbindung darstellt und der Kontakt 3326 für eine serielle Datenübermittlung dient.

[0218] In der rückseitigen Ansicht des elektronischen Schlüssels 332 gemäß Fig. 17 ist auch der Deckel eines Akku-Fachs 3327 angedeutet, hinter dem ein Akkumulator 3332 angeordnet ist. Dieser ist beispielsweise als Lithium-Ionen-Akkumulator mit einer Ausgangsspannung ausgebildet.

[0219] Der elektronische Schlüssel 332 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 332 und optional auch zur Aufladung des Akkumulators 3322 dient.

[0220] Der elektronische Schlüssel 332 wirkt entweder mit dem in den Figuren 8 bis 13 gezeigten elektronischen Schloss 316 zum Beispiel an einem Rohrtresor 312 oder an einem geschützten Raum oder einer anderen, eine Zugangsberechtigung erfordernden Einrichtung zusammen. 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 316 geschützt werden.

[0221] Das Beispiel gemäß Fig. 15 zeigt, dass die geschützte Einrichtung durch das elektronische Schloss 316 auch nicht nur unmittelbar, sondern auch mittelbar freigegeben werden kann. In diesem Fall umfasst das elektronische Schloss 316 einen 220 V-Schutzmodul für eine nicht dargestellte geschützte Einrichtung, die letztendlich erst durch die Betätigung eines Motorschlosses 340 freigegeben wird.

[0222] Zwischen dem elektronischen Schloss 316, das beispielsweise dem des zweiten Ausführungsbeispiels gemäß Fig. 7 entspricht, und dem Motorschloss 340 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 316 aktiviert wird. Nach Übermittlung eines gültigen Berechtigungscodes 336 vom in Fig. 15 nicht dargestellten elektronischen Schlüssel 332 über den für die Datenübermittlung zuständigen Gegenkontakt 3166 wird die externe Spannungsversorgung am Steuergerät 350 aktiviert und das Motorschloss 350 betätigt. Eine detailliertere Beschreibung des Steuergeräts 50 folgt am Ende der Beschreibung.

[0223] 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 332 über das elektronische Schloss 316 bei Bedarf jederzeit initialisiert werden.

Patentansprüche

1. Elektronisches Schließsystem (10) umfassend einen elektronischen Schlüssel (12) und ein elektronisches Schloss (14), welche durch einen Kontaktsatz (16) und einen Gegenkontaktsatz (18) miteinander in Wechselwirkung bringbar sind, wobei der elektronische Schlüssel (12) einen Prozessor (34) und einen Speicher (39) aufweist und der Prozessor (34) mit dem Speicher (39) zusammenwirkt und einen Berechtigungscode (BCZ) in den Speicher (39) schreibt und wobei das elektronische Schloss (14) einen Prozessor (72) aufweist, welcher bei einer Wechselwirkung des elektronischen Schlüssels (12) mit dem elektronischen Schloss (14) über den Kontaktsatz (16) und den Gegenkontaktsatz (18) mit dem Speicher (39) im elektronischen Schlüssel (12) wechselwirkt, um den Berechtigungscode (BCZ) auszulesen,
   dadurch gekennzeichnet, dass der Berechtigungscode ein extern erzeugter Berechtigungscode (BCZ) ist und der Prozessor (34) des elektronischen Schlüssels (12) mit einer Eingabeeinheit (36) zusammenwirkt, durch welche der extern erzeugte Berechtigungscode (BCZ) dem Prozessor (34) übermittelbar ist, und dass mit dem extern erzeugten Berechtigungsode (BCZ) nur eine einmalige Öffnung zugelassen wird.

2. Elektronisches Schließsystem nach Anspruch 1, **dadurch gekennzeichnet, dass** der Speicher (39) ein gesicherter Speicher ist und dass der Prozessor (34)

des elektronischen Schlüssels (12) einen Sicherheitscode (SC) erzeugt, um den extern erzeugten Berechtigungscode (BCZ) in dem gesicherten Speicher (39) abzulegen, wobei insbesondere der gesicherte Speicher (39) der Speicher eines Sicherheitsprozessors (38) ist.

3. Elektronisches Schließsystem nach Anspruch 1 oder 2, **dadurch gekennzeichnet, dass** der Prozessor (72) des elektronischen Schlosses (14) einen Sicherheitscode (SC) erzeugt, um den in dem gesicherten Speicher (39) abgelegten Berechtigungscode (BCZ) auszulesen.

4. Elektronisches Schließsystem nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet, dass** der elektronische Schlüssel (12) Anzeigeelemente (92, 94) aufweist, um von dem elektronischen Schloss (14) dem elektronischen Schlüssel (12) übermittelte Zustände des elektronischen Schlosses (14) anzuzeigen, wobei insbesondere der Prozessor (72) des elektronischen Schlosses (14) dem Prozessor (34) des elektronisches Schlüssel (12) Zustandssignale betreffend Zustände des elektronischen Schlosses (14) übermittelt und dass der Prozessor (34) des elektronischen Schlüssel (12) entsprechend den übermittelten Zuständen die Anzeigeelemente (92, 94) des elektronischen Schlüssels (12) ansteuert.

5. Elektronisches Schließsystem nach einem der Ansprüche 1 bis 4, **dadurch gekennzeichnet, dass** das elektronische Schloss (14) durch eine elektrische Spannungsquelle (32) des elektronischen Schlüssels (12) betreibbar ist.

6. Elektronisches Schließsystem nach einem der Ansprüche 1 bis 5, **dadurch gekennzeichnet, dass** das elektronische Schloss (14) einen Schließantrieb (82) zum Betätigen eines Schließriegels (22) umfasst, wobei insbesondere der Schließantrieb (82) des elektronischen Schlosses (14) durch die elektrische Spannungsquelle (32) des elektronischen Schlüssels (12) betreibbar ist, wobei insbesondere das elektronische Schloss (14) einen Spannungswandler (86) aufweist, um den Schließantrieb (82) zu betreiben.

7. Elektronisches Schließsystem nach einem der Ansprüche 1 bis 5, **dadurch gekennzeichnet, dass** das elektronische Schloss (14') eine Schalteinheit (362) aufweist, um ein externes Schließsystem (268) zu aktivieren oder zu blockieren.

8. Elektronisches Schließsystem nach einem der Ansprüche 1 bis 7, **dadurch gekennzeichnet, dass** das der elektronische Schlüssel (12) eine Schnittstelle (42) zum Aktivieren des elektronischen Schlüssels (12) mittels einer Zentraleinheit (102) aufweist.

9. Elektronisches Schließsystem nach einem der Ansprüche 1 bis 8, **dadurch gekennzeichnet, dass** das elektronische Schloss (14) eine Schnittstelle (84) zum Aktivieren des elektronischen Schlosses (14) durch eine Zentraleinheit (12) aufweist.

10. Elektronisches Schließsystem nach Anspruch 8 oder 9, **dadurch gekennzeichnet, dass** die Aktivierung des elektronischen Schlüssels (12) beziehungsweise des elektronischen Schlosses (14) durch die Zentraleinheit (102) leitungsgebunden erfolgt.

11. Rohrtresor (202) umfassend einen Rohrkörper (204) und einen Rohrkörperdeckel (206) und ein elektronisches Schließsystem nach einem der voranstehenden Ansprüche, wobei das elektronische Schloss (14) in dem Rohrkörperdeckel (206) angeordnet ist, um den Rohrkörperdeckel (206) in seiner in den Rohrkörper (204) eingesetzten Schließstellung zu verriegeln oder zu entriegeln, **dadurch gekennzeichnet, dass** an dem Rohrkörperdeckel (206) ein Schlüsselcontainer (222) gehalten ist, der mit dem Rohrkörperdeckel (206) in den Rohrköper (204) einführbar oder aus diesem entnehmbar ist.

12. Rohrtresor nach Anspruch 11, **dadurch gekennzeichnet, dass** der Schlüsselcontainer (222) ein Aufnahmeraum (224) für einen Schlüssel (226) aufweist und/oder dass der Schlüssel (226) an dem Schlüsselcontainer (222) gegen ein vollständiges Entfernen vom Schlüsselcontainer (222) gesichert ist.

13. Rohrtresor nach Anspruch 11 oder 12, **dadurch gekennzeichnet, dass** die Position des Schlüsselcontainers (222) in dem Rohrkörper (204) durch einen Sensor (244) erfassbar ist, wobei insbesondere der Sensor ein Magnetfeldsensor (244) ist, welcher einen am Schlüsselcontainer (222) gehaltenen Magnet (342) erkennt und/oder der Sensor (244) mit einer Übermittlungseinheit (252) zusammenwirkt, welche eine Schließstellung des Rohrkörperdeckels (206) einer Sicherheitszentrale übermittelt.

14. Rohrtresor nach einem der Ansprüche 11 bis 13, **dadurch gekennzeichnet, dass** am Rohrkörper (204) ein Sensor (248) angeordnet ist, welcher eine Schließstellung des Rohrkörperdeckels (206) in dem Rohrkörper (204) erfasst, wobei insbesondere der Rohrkörperdeckel (206) mit einem Magnet (246) versehen ist, dessen Position der Sensor (248) erfasst.

Claims

1. Electronic locking system (10) comprising an electronic key (12) and an electronic lock (14), which can be brought into interaction with one another by a contact set (16) and a mating contact set (18), wherein the electronic key (12) has a processor (34) and a memory (39) and the processor (34) interacts with the memory (39) and writes an authorization code (BCZ) into the memory (39) and wherein the electronic lock (14) has a processor (72) which, when the electronic key (12) interacts with the electronic lock (14), interacts with the memory (39) in the electronic key (12) via the contact set (16) and the mating contact set (18) in order to read out the authorization code (BCZ),
characterized in that
the authorization code is an externally generated authorization code (BCZ) and the processor (34) of the electronic key (12) interacts with an input unit (36) by means of which the externally generated authorization code (BCZ) can be transmitted to the processor (34), and **in that** only a single opening is permitted with the externally generated authorization code (BCZ).

2. Electronic locking system according to claim 1, **characterized in that** the memory (39) is a secured memory and **in that** the processor (34) of the electronic key (12) generates a security code (SC) in order to store the externally generated authorization code (BCZ) in the secured memory (39), in particular the secured memory (39) being the memory of a security processor (38).

3. Electronic locking system according to claim 1 or 2, **characterized in that** the processor (72) of the electronic lock (14) generates a security code (SC) in order to read out the authorization code (BCZ) stored in the secured memory (39).

4. Electronic locking system according to one of claims 1 to 3, **characterized in that** the electronic key (12) has display elements (92, 94) for displaying states of the electronic lock (14) transmitted by the electronic lock (14) to the electronic key (12), wherein in particular the processor (72) of the electronic lock (14) transmits status signals to the processor (34) of the electronic key (12) concerning statuses of the electronic lock (14) and that the processor (34) of the electronic key (12) controls the display elements (92, 94) of the electronic key (12) in accordance with the transmitted statuses.

5. Electronic locking system according to one of claims 1 to 4, **characterized in that** the electronic lock (14) can be operated by an electrical voltage source (32) of the electronic key (12).

6. Electronic locking system according to one of claims 1 to 5, **characterized in that** the electronic lock (14) comprises a locking drive (82) for actuating a locking bolt (22), wherein in particular the locking drive (82) of the electronic lock (14) is operable by the electrical voltage source (32) of the electronic key (12), wherein in particular the electronic lock (14) comprises a voltage converter (86) to operate the locking drive (82).

7. Electronic locking system according to one of claims 1 to 5, **characterized in that** the electronic lock (14') has a switching unit (362) to activate or block an external locking system (268).

8. Electronic locking system according to one of claims 1 to 7, **characterized in that** the electronic key (12) comprises an interface (42) for activating the electronic key (12) by means of a central unit (102).

9. Electronic locking system according to any one of claims 1 to 8, **characterized in that** the electronic lock (14) has an interface (84) for activating the electronic lock (14) by means of a central unit (12).

10. Electronic locking system according to claim 8 or 9, **characterized in that** the electronic key (12) or the electronic lock (14) is activated by the central unit (102) in a wired manner.

11. Tubular safe (202) comprising a tubular body (204) and a tubular body cover (206) and an electronic locking system according to one of the preceding claims, wherein the electronic lock (14) is arranged in the tubular body cover (206), in order to lock or unlock the tubular body cover (206) in its closed position inserted into the tubular body (204), **characterized in that** a key container (222) is held on the tubular body cover (206), which key container can be inserted into or removed from the tubular body (204) with the tubular body cover (206).

12. Tubular safe according to claim 11, **characterized in that** the key container (222) has a receiving space (224) for a key (226) and/or **in that** the key (226) is secured on the key container (222) against complete removal from the key container (222).

13. Tubular safe according to claim 11 or 12, **characterized in that** the position of the key container (222) in the tubular body (204) can be detected by a sensor (244), in particular the sensor being a magnetic field sensor (244) which detects a magnet (342) held on the key container (222) and/or the sensor (244) interacts with a transmission unit (252) which transmits a closed position of the tubular body cover (206) to a security center.

14. Tube safe according to one of claims 11 to 13, **characterized in that** a sensor (248) is arranged on the tube body (204), which sensor detects a closed position of the tube body lid (206) in the tube body (204), in particular the tube body lid (206) being provided with a magnet (246), the position of which is detected by the sensor (248).

Revendications

1. Système de verrouillage électronique (10) comprenant une clé électronique (12) et une serrure électronique (14) qui peuvent être mises en interaction l'une avec l'autre par un jeu de contacts (16) et un jeu de contacts complémentaire (18), la clé électronique (12) présentant un processeur (34) et une mémoire (39) et le processeur (34) coopérant avec la mémoire (39) et écrivant un code d'autorisation (BCZ) dans la mémoire (39) et la serrure électronique (14) présente un processeur (72) qui, lors d'une interaction de la clé électronique (12) avec la serrure électronique (14), interagit avec la mémoire (39) dans la clé électronique (12) par l'intermédiaire du jeu de contacts (16) et du jeu de contacts complémentaire (18) afin de lire le code d'autorisation (BCZ), **caractérisé en ce que**
le code d'autorisation est un code d'autorisation (BCZ) généré de l'extérieur et le processeur (34) de la clé électronique (12) coopère avec une unité d'entrée (36) par laquelle le code d'autorisation (BCZ) généré de l'extérieur peut être transmis au processeur (34), et **en ce que** seule une ouverture unique est autorisée avec le code d'autorisation (BCZ) généré de l'extérieur.

2. Système de verrouillage électronique selon la revendication 1, **caractérisé en ce que** la mémoire (39) est une mémoire sécurisée et **en ce que** le processeur (34) de la clé électronique (12) génère un code de sécurité (SC) pour déposer le code d'autorisation (BCZ) généré de manière externe dans la mémoire sécurisée (39), la mémoire sécurisée (39) étant notamment la mémoire d'un processeur de sécurité (38).

3. Système de verrouillage électronique selon la revendication 1 ou 2, **caractérisé en ce que** le processeur (72) de la serrure électronique (14) génère un code de sécurité (SC) pour lire le code d'autorisation (BCZ) stocké dans la mémoire sécurisée (39).

4. Système de verrouillage électronique selon l'une des revendications 1 à 3, **caractérisé en ce que** la clé électronique (12) comporte des éléments d'affichage (92, 94) pour indiquer à la clé électronique (12) des états de la serrure électronique (14) transmis par la serrure électronique (14), le processeur (72) de la serrure électronique (14) transmettant notamment au processeur (34) de la clé électronique (12) des signaux d'état concernant des états de la serrure électronique (14), et **en ce que** le processeur (34) de la clé électronique (12) commande les éléments d'affichage (92, 94) de la clé électronique (12) en fonction des états transmis.

5. Système de verrouillage électronique selon l'une des revendications 1 à 4, **caractérisé en ce que** la serrure électronique (14) peut être actionnée par une source de tension électrique (32) de la clé électronique (12).

6. Système de verrouillage électronique selon l'une des revendications 1 à 5, **caractérisé en ce que** la serrure électronique (14) comprend un actionneur de verrouillage (82) pour actionner un pêne dormant (22), l'actionneur de verrouillage (82) de la serrure électronique (14) pouvant notamment être actionné par la source de tension électrique (32) de la clé électronique (12), la serrure électronique (14) comportant notamment un convertisseur de tension (86) pour actionner l'actionneur de verrouillage (82).

7. Système de verrouillage électronique selon l'une des revendications 1 à 5, **caractérisé en ce que** la serrure électronique (14') comporte une unité de commutation (362) pour activer ou bloquer un système de verrouillage externe (268).

8. Système de verrouillage électronique selon l'une des revendications 1 à 7, **caractérisé en ce que** la clé électronique (12) comporte une interface (42) pour activer la clé électronique (12) au moyen d'une unité centrale (102).

9. Système de verrouillage électronique selon l'une des revendications 1 à 8, **caractérisé en ce que** la serrure électronique (14) comporte une interface (84) d'activation de la serrure électronique (14) par une unité centrale (12).

10. Système de verrouillage électronique selon la revendication 8 ou 9, **caractérisé en ce que** l'activation de la clé électronique (12) ou de la serrure électronique (14) par l'unité centrale (102) est réalisée par câbles.

11. Coffre-fort tubulaire (202) comprenant un corps tubulaire (204) et un couvercle de corps tubulaire (206) et un système de verrouillage électronique selon l'une des revendications précédentes, la serrure électronique (14) étant disposée dans le couvercle de corps tubulaire (206), pour verrouiller ou déverrouiller le couvercle (206) du corps tubulaire dans sa position de fermeture insérée dans le corps tubulaire (204), **caractérisé en ce qu'**un conteneur de

clé (222) est maintenu sur le couvercle (206) du corps tubulaire, lequel peut être inséré dans le corps tubulaire (204) ou retiré de celuici avec le couvercle (206) du corps tubulaire.

12. Coffre-fort tubulaire selon la revendication 11, **caractérisé en ce que** le conteneur de clé (222) présente un espace de réception (224) pour une clé (226) et/ou **en ce que** la clé (226) est fixée au conteneur de clé (222) de manière à ne pas pouvoir être retirée complètement du conteneur de clé (222).

13. Coffre-fort tubulaire selon la revendication 11 ou 12, **caractérisé en ce que** la position du conteneur de clé (222) dans le corps tubulaire (204) peut être détectée par un capteur (244), le capteur étant notamment un capteur de champ magnétique (244) qui détecte un aimant (342) maintenu sur le conteneur de clé (222) et/ou le capteur (244) coopérant avec une unité de transmission (252) qui transmet une position de fermeture du couvercle du corps tubulaire (206) à une centrale de sécurité.

14. Coffre-fort tubulaire selon l'une des revendications 11 à 13, **caractérisé en ce qu'**un capteur (248) est disposé sur le corps tubulaire (204), lequel détecte une position de fermeture du couvercle du corps tubulaire (206) dans le corps tubulaire (204), le couvercle du corps tubulaire (206) étant notamment pourvu d'un aimant (246) dont le capteur (248) détecte la position.

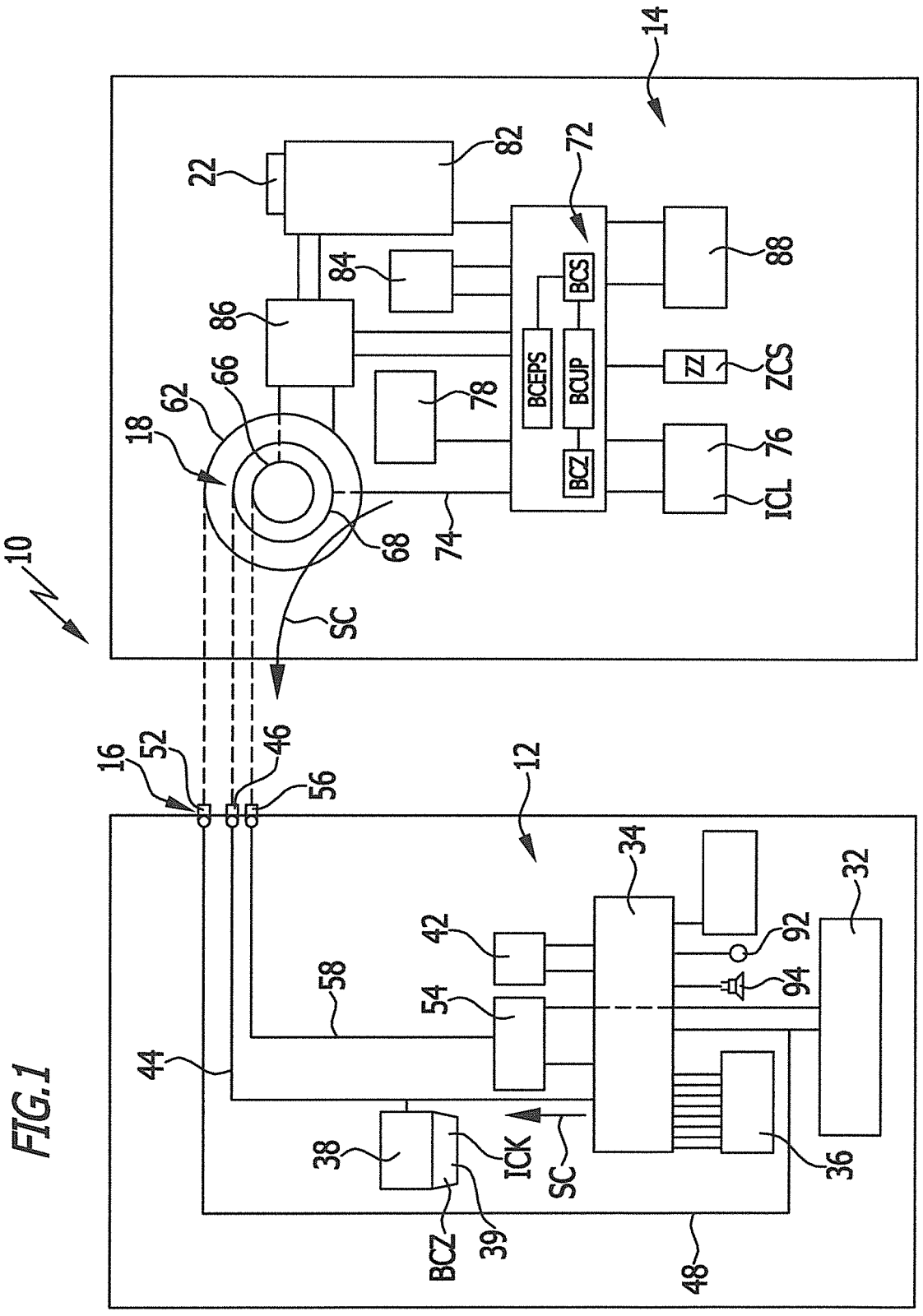
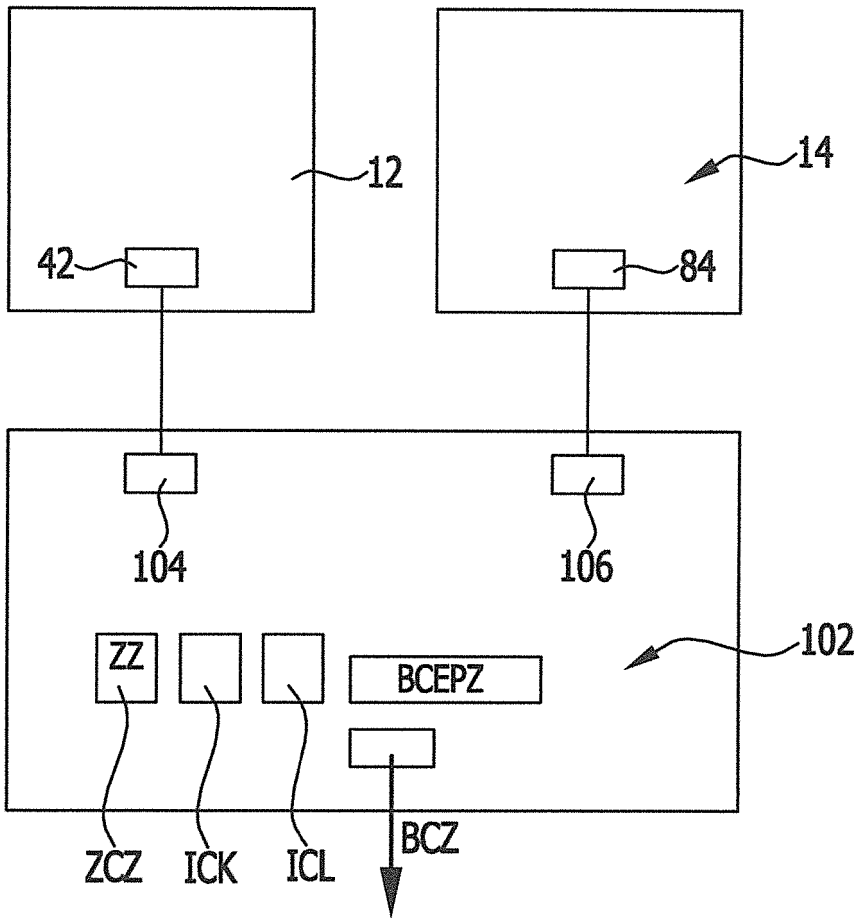

10
12
14
16
18
22
32
34
36
38
39
42
44
46
48
52
54
56
58
62
66
68
72
74
76
78
82
84
86
88
92
94
BCS
BCEPS
BCUP
BCZ
ZZ
ZCS
ICL
ICK
SC

FIG.1

FIG.2



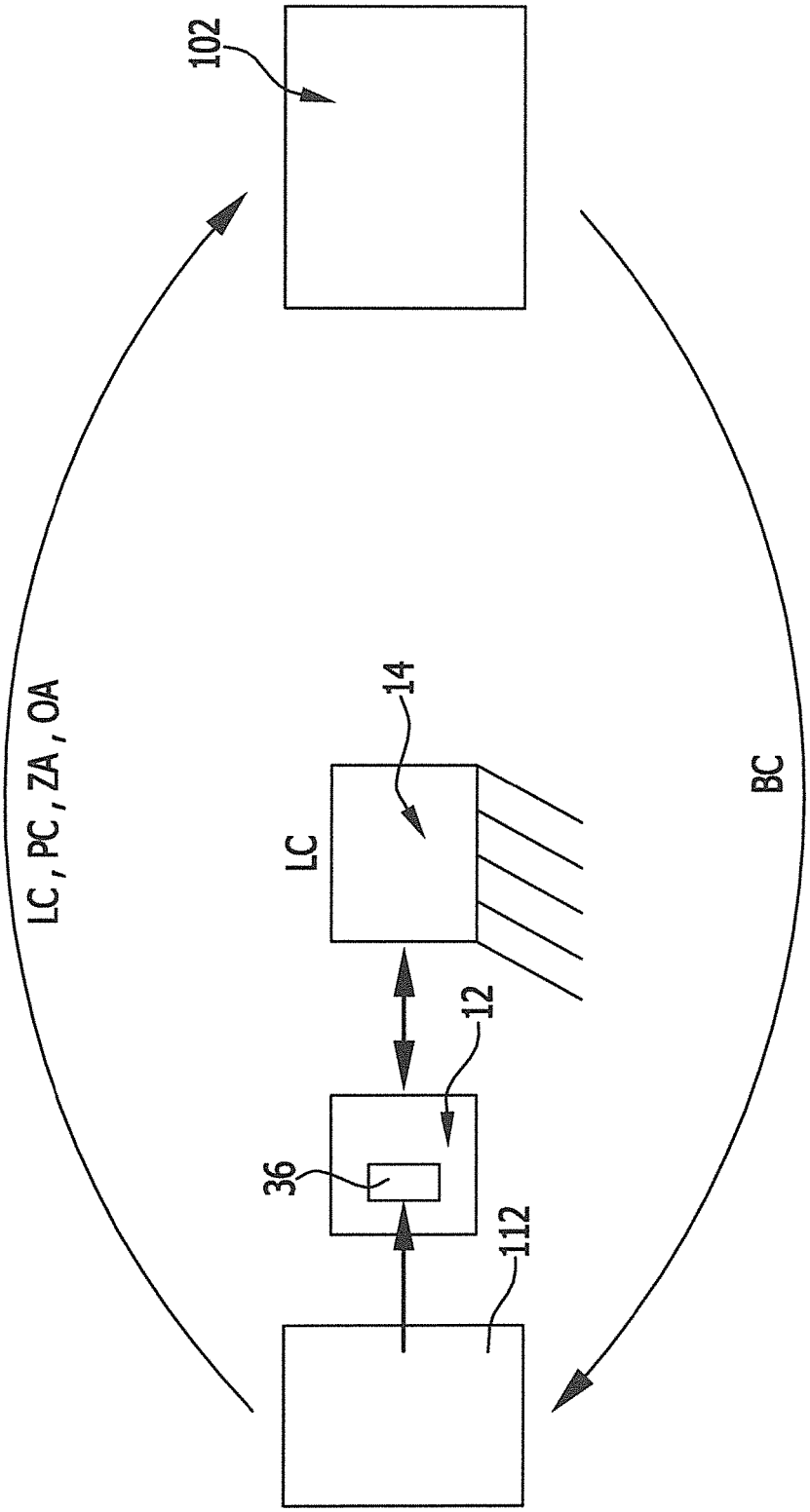


FIG.3

FIG.4

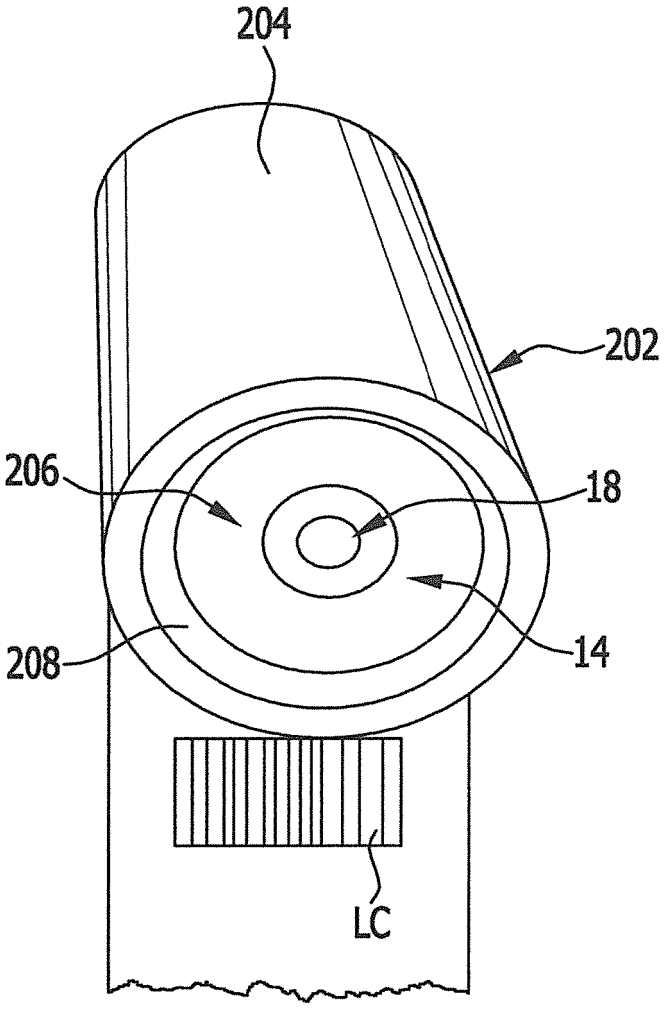


FIG.5

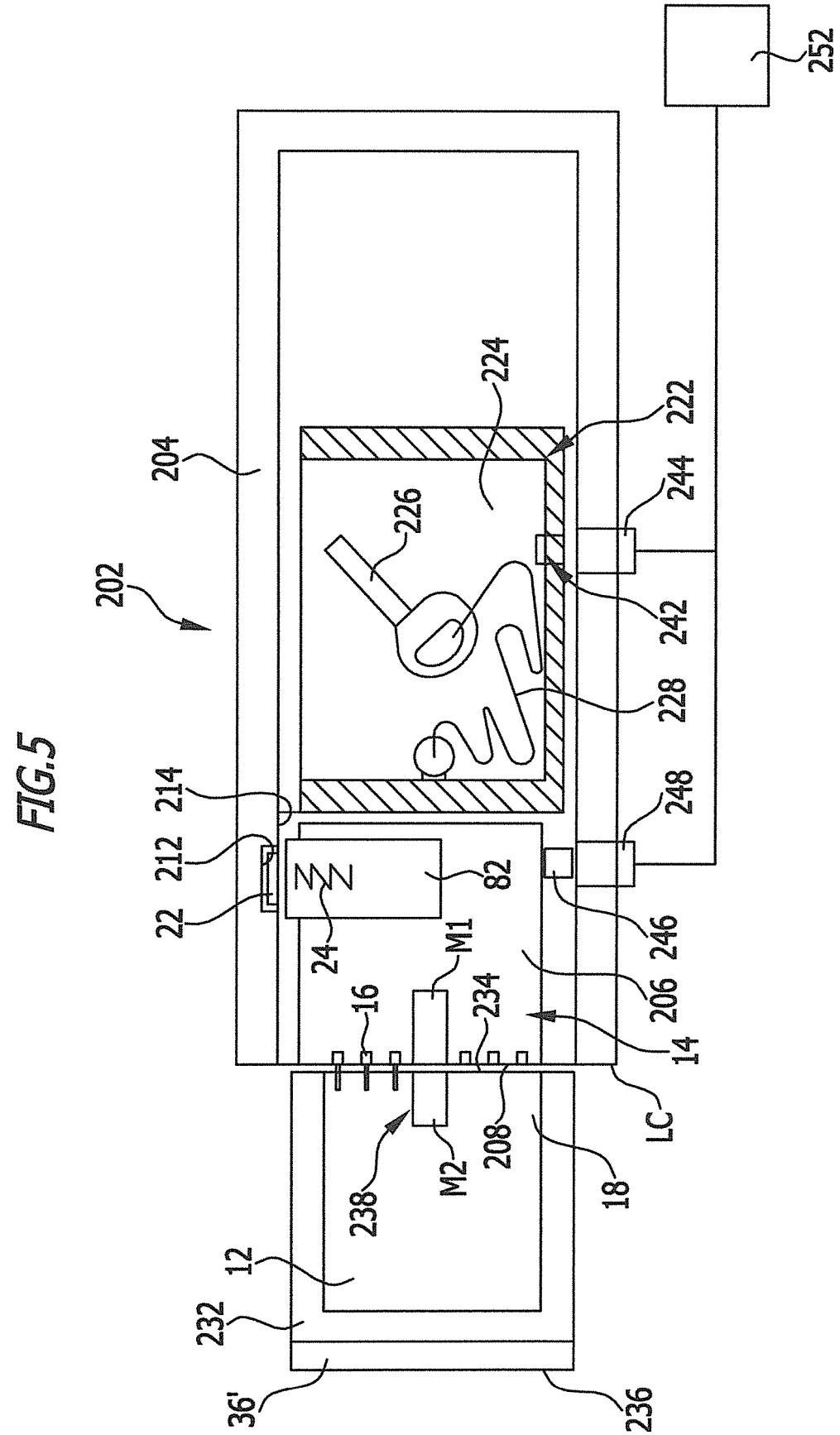
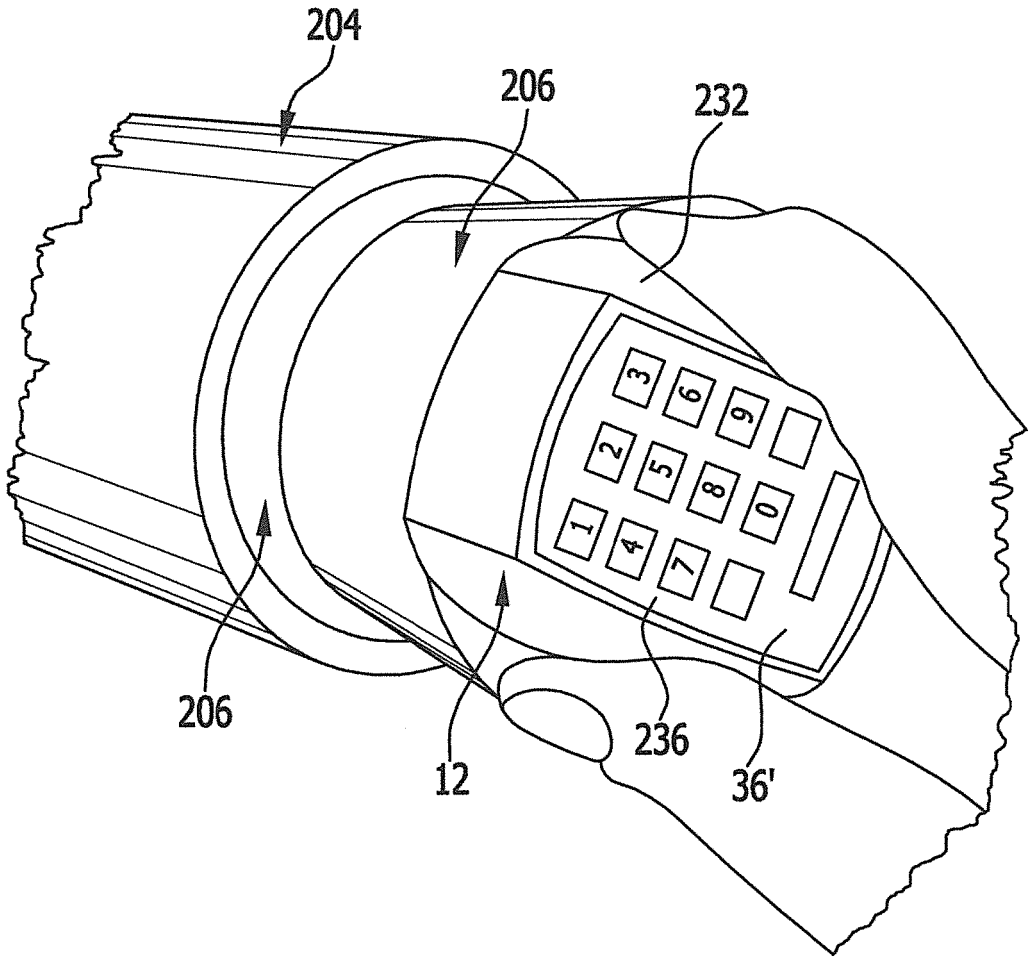

252
224
222
204
244
226
202
242
228
214
248
212
82
22
246
24
M1
206
16
234
14
LC
208
M2
18
238
12
232
36'
236

FIG.6



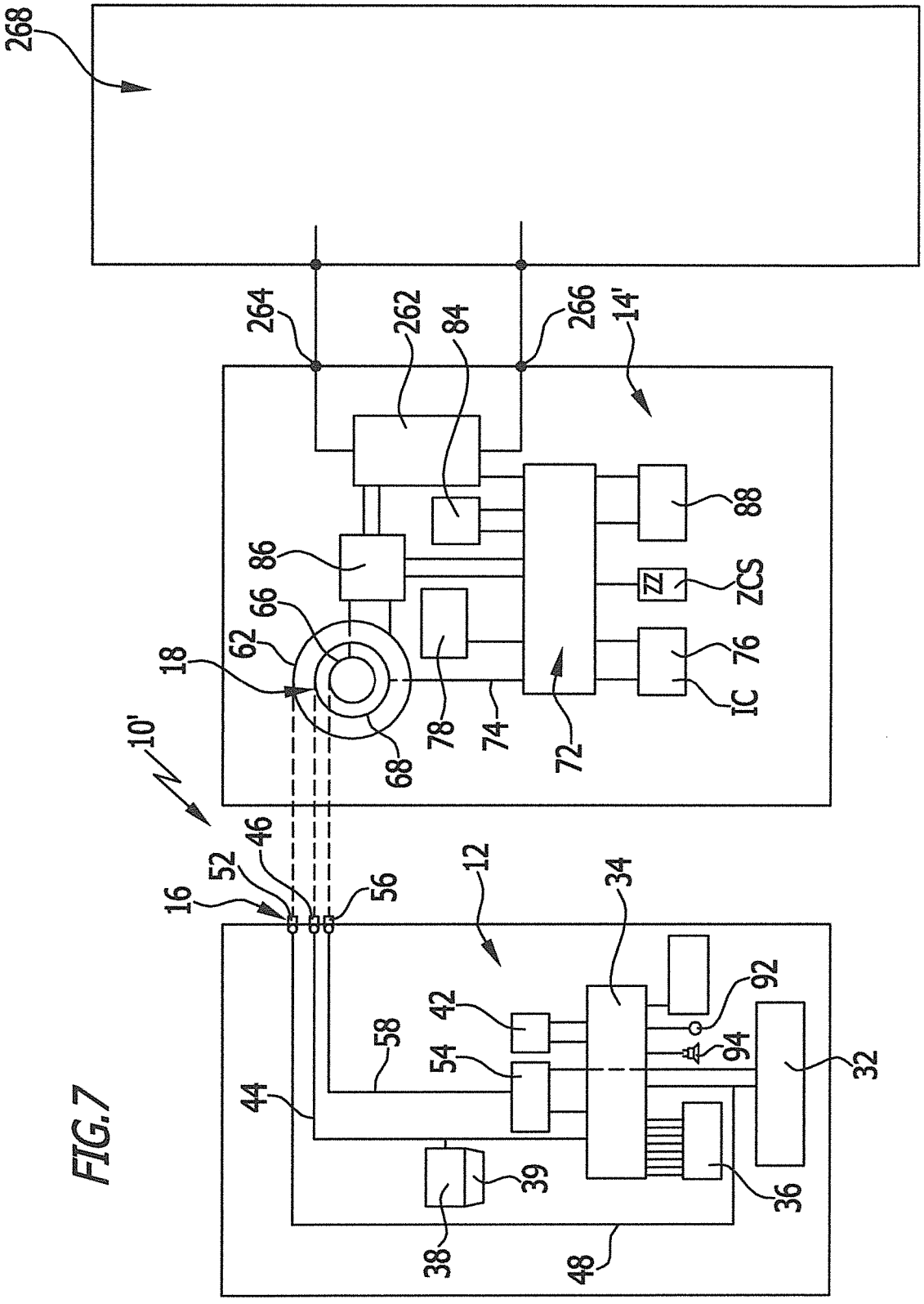

268
264
262
84
266
14'
88
86
ZCS
66
62
18
76
IC
10'
78
74
72
68
46
52
16
56
12
34
92
42
58
54
94
32
44
39
36
38
48

FIG.7

FIG.8

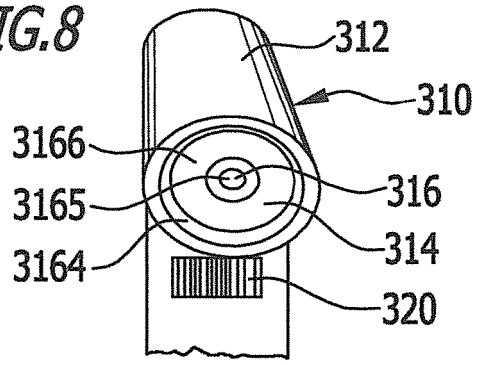


FIG.9

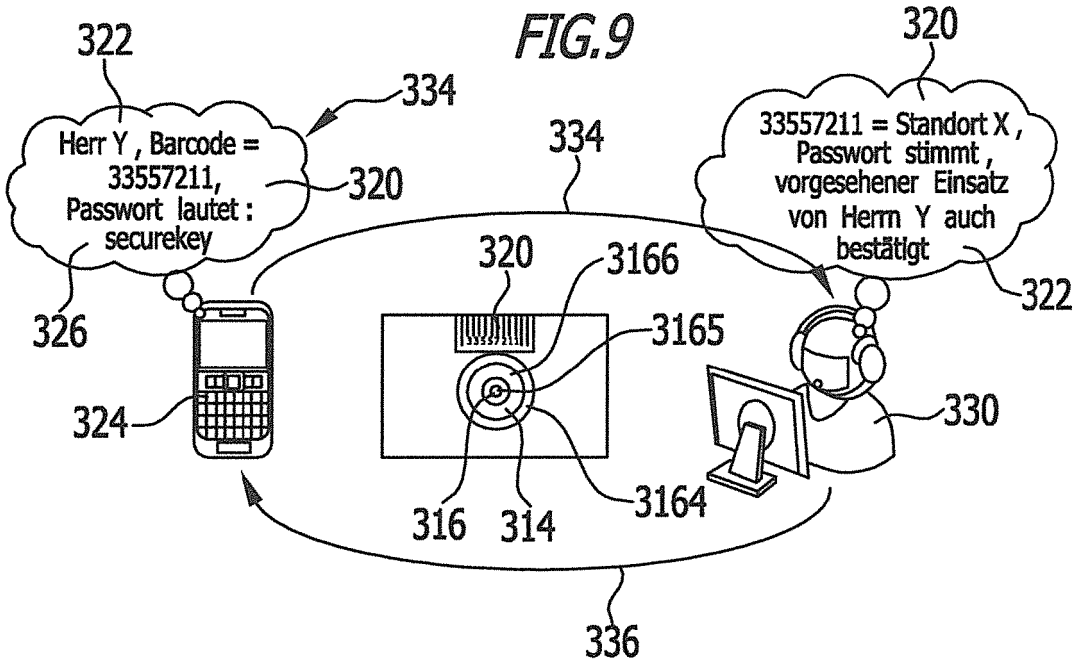


FIG.10

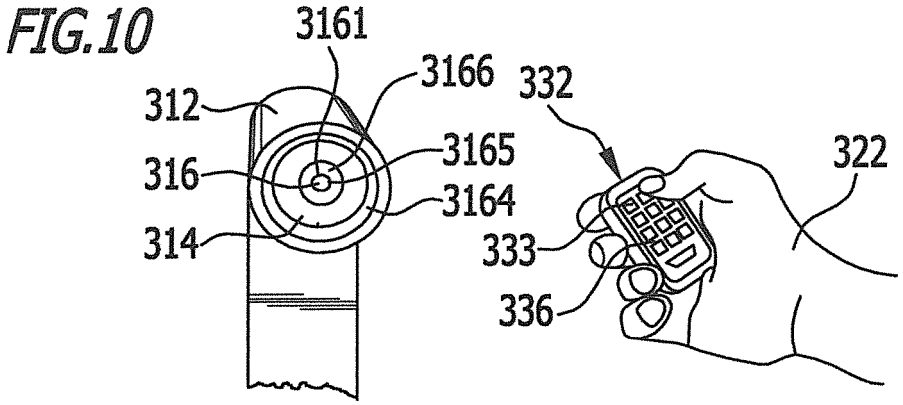


FIG.11

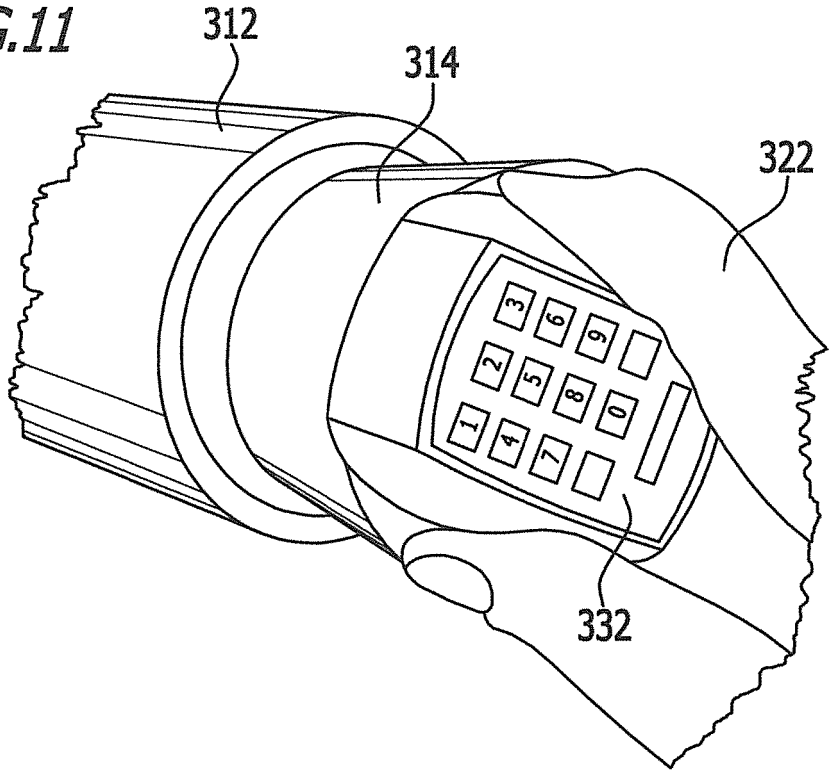


FIG.12

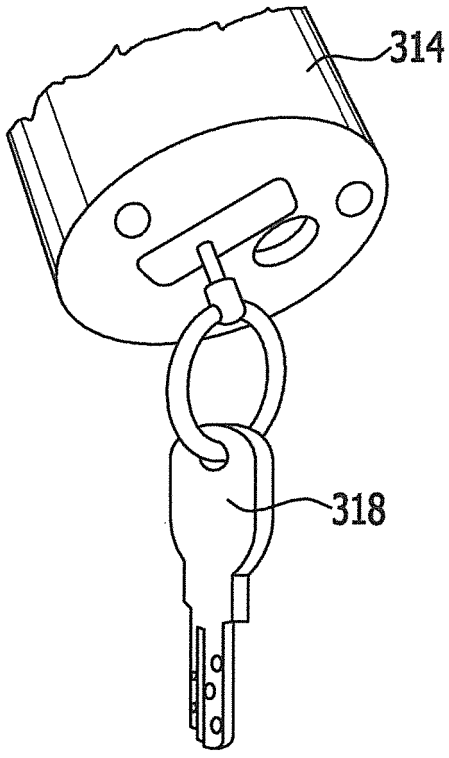
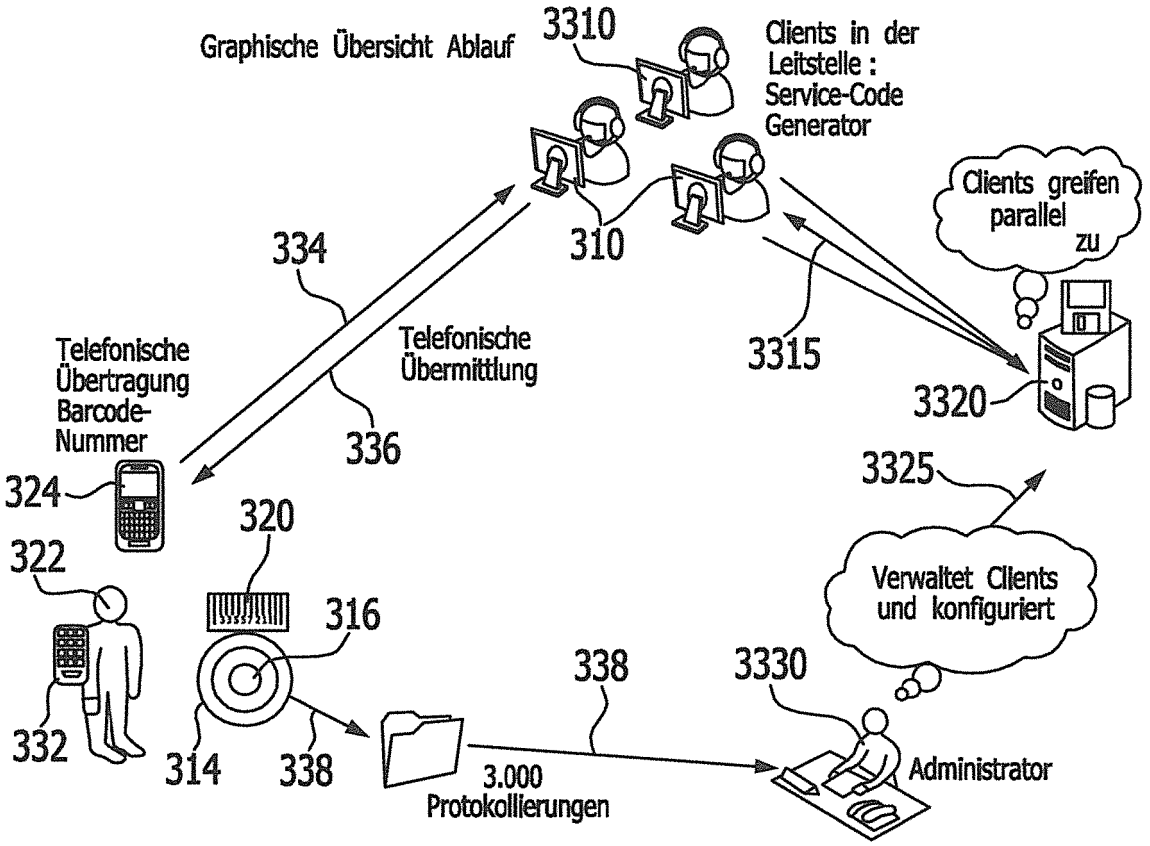


FIG.13


Graphische Übersicht Ablauf
3310
Clients in der Leitstelle : Service-Code Generator
Clients greifen parallel zu
334
310
Telefonische Übertragung Barcode-Nummer
Telefonische Übermittlung
3315
3320
336
324
3325
320
322
Verwaltet Clients und konfiguriert
316
338
3330
332
314
338
3.000 Protokollierungen
Administrator

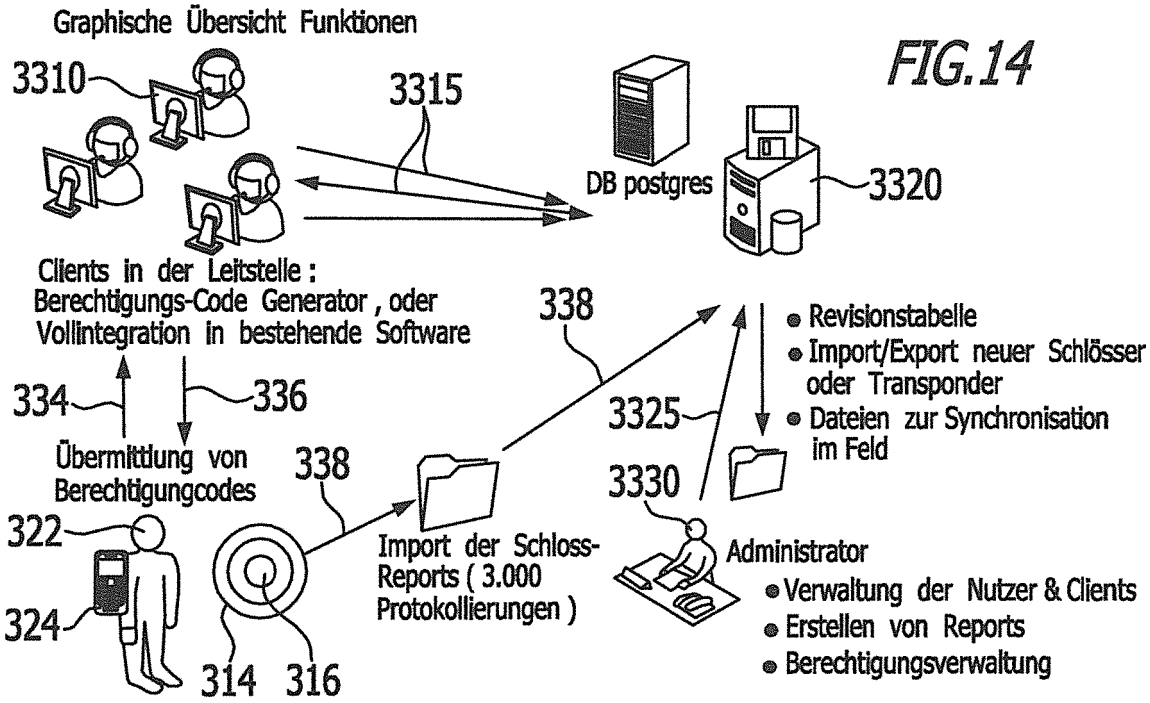

Graphische Übersicht Funktionen
3310
3315
DB postgres
3320
Clients in der Leitstelle : Berechtigungs-Code Generator , oder Vollintegration in bestehende Software
338
Revisionstabelle
Import/Export neuer Schlösser oder Transponder
Dateien zur Synchronisation im Feld
334
336
3325
Übermittlung von Berechtigungcodes
338
3330
322
Import der Schloss-Reports (3.000 Protokollierungen)
Administrator
Verwaltung der Nutzer & Clients
Erstellen von Reports
Berechtigungsverwaltung
324
314
316

FIG.14

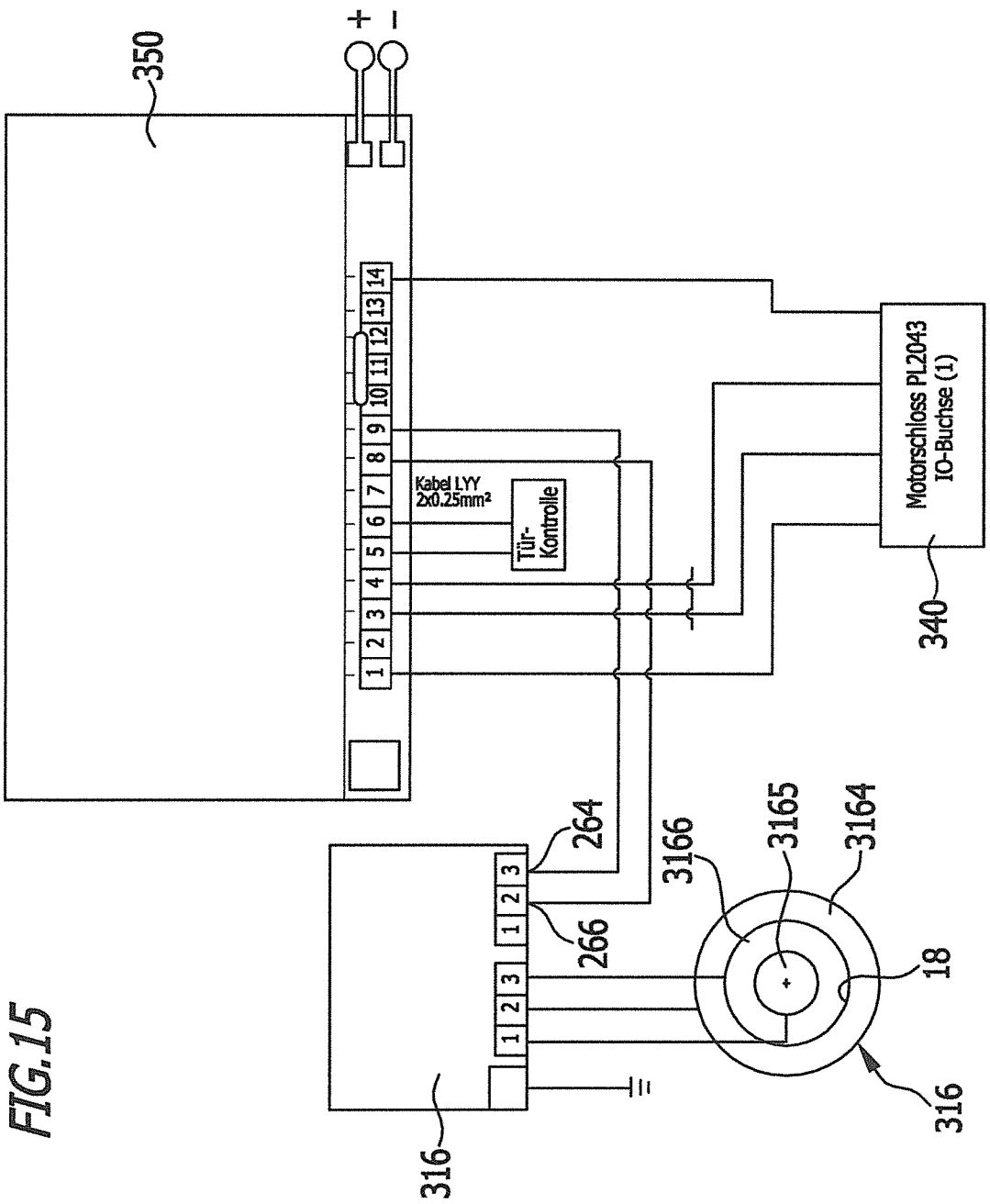

350
+
–
14
13
12
11
10
9
8
7
6
5
4
3
2
1
Kabel LYY
2x0.25mm²
Tür-
Kontrolle
Motorschloss PL2043
IO-Buchse (1)
340
264
266
3166
3165
3164
18
316
316

FIG.15

FIG.16

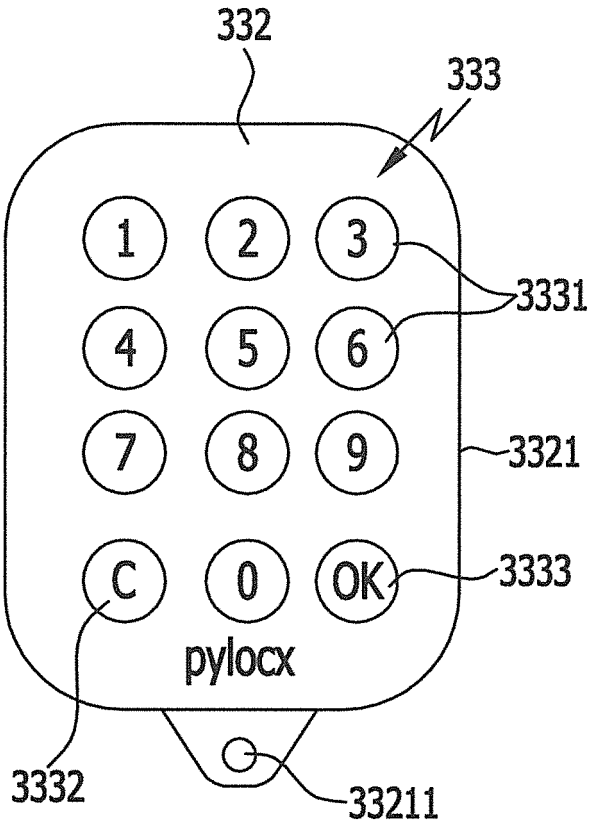
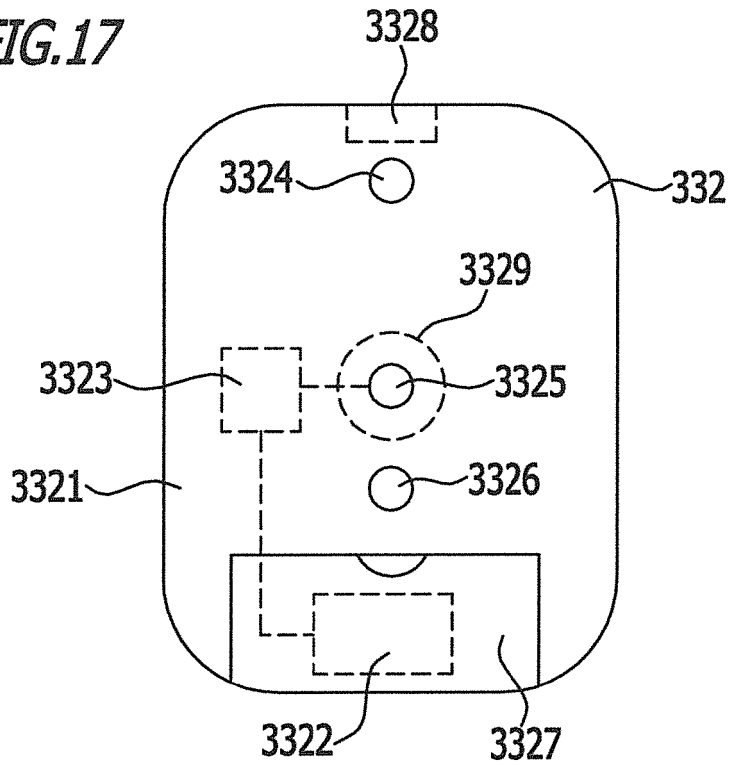

332
333
1
2
3
3331
4
5
6
7
8
9
3321
C
0
OK
3333
pylocx
3332
33211

FIG.17


3328
3324
332
3329
3323
3325
3321
3326
3322
3327

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

- US 201300439731 A1 **[0002]**
- US 20070290797 A1 **[0003]**
- US 20080150684 A1 **[0004]**
- US 5701828 B1 **[0005]**
- US 6331812 B1 **[0006]**
- US 6082153 B1 **[0007]**
- US 20030179073 B1 **[0008]**
- WO 2012045474 A1 **[0061] [0199]**