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

(11) **EP 3 327 686 B1**

(12) **EUROPÄISCHE PATENTSCHRIFT**

(45) Veröffentlichungstag und Bekanntmachung des Hinweises auf die Patenterteilung:
02.11.2022 Patentblatt 2022/44

(21) Anmeldenummer: **17202089.3**

(22) Anmeldetag: **16.11.2017**

(51) Internationale Patentklassifikation (IPC):
G07F 19/00 *(2006.01)* ***E05B 47/00*** *(2006.01)*

(52) Gemeinsame Patentklassifikation (CPC):
G07F 19/00; G07F 19/205

(54) VERFAHREN ZUR VERWALTUNG EINES ÖFFNUNGSZUSTANDES EINES WERTBEHÄLTNISSES SOWIE SYSTEM HIERFÜR

METHOD FOR MANAGING AN OPENING STATE OF A VALUE CONTAINER AND SYSTEM THEREFOR

PROCÉDÉ DE GESTION D'UN ÉTAT D'OUVERTURE D'UN COFFRE-FORT AINSI QUE SYSTÈME ASSOCIÉ

(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: **23.11.2016 DE 102016122606**
16.05.2017 DE 102017110587

(43) Veröffentlichungstag der Anmeldung:
30.05.2018 Patentblatt 2018/22

(73) Patentinhaber: **Insys Microelectronics GmbH**
93049 Regensburg (DE)

(72) Erfinder:
- **Lücke, Detlef**
  93077 Bad Abbach (DE)
- **Bauer, Mario**
  93107 Thalmassing (DE)

(74) Vertreter: **Hannke, Christian**
Hannke Bittner & Partner
Patent- und Rechtsanwälte mbB
Prüfeninger Straße 1
93049 Regensburg (DE)

(56) Entgegenhaltungen:
DE-A1-102012 008 395
US-A1- 2012 229 251
US-A1- 2013 187 756
US-A1- 2014 375 422
US-A1- 2015 102 906
US-A1- 2016 145 904

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

EP 3 327 686 B1

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zur Verwaltung eines Öffnungszustandes eines Wertbehältnisses sowie System hierfür.

[0002] Wertbehältnisse sind aus dem Bereich des Cash-Handling (deutsch: "Bargeldabwicklung, Bargeldlogistik") bekannt und werden beispielsweise im Einzelhandel als Safe oder bei Kreditinstituten als Geldautomat bzw. Geldautomatenschrank zur Sicherung von Geldbeträgen eingesetzt.

[0003] Die folgende Beschreibung bezieht sich zwar der Einfachheit halber nur auf Geldautomaten, gilt aber analog auch für die erwähnten Safes oder für andere hinsichtlich ihrer Sicherungsart vergleichbare Wertbehältnisse. Ein Wertbehältnis kann im Sinne der Erfindung außerdem auch allgemein ein gesicherter Bereich sein, zu dessen Zugang mindestens eine Sicherheitsmaßnahme zu überwinden ist (Beispiele hierfür sind Räume von Forschungslaboratorien, Eigenheime, Schließfachbereiche einer Bank etc.).

[0004] Zur Sicherung dieser Wertbehältnisse werden zumeist Hochsicherheitsschlösser eingesetzt. Diese sichern beispielsweise den Zugang zu den Geldfächern der Geldautomaten und können nur durch spezielle Sicherheitsmechanismen wie etwa der Eingabe eines Codes geöffnet werden, welcher beispielsweise einem Mitarbeiter des Geldinstituts bzw. einem Wertdienstleister (im Folgenden als "Benutzer" oder als "autorisierter Benutzer" bezeichnet) bekannt ist. Ferner wird jedem einzelnen Benutzer meistens eine eigene Personalnummer und/ oder PIN zugeteilt, mittels derer er im System eindeutig identifizierbar ist. Bevorzugt ist dabei zumindest die PIN nur dem Benutzer selbst bekannt.

[0005] Generell weist ein derartiges Hochsicherheitsschloss also zwei Funktionen auf: zum einen eine Schnittstellenfunktion zur Kommunikation mit dem autorisierten Benutzer in Bezug auf Durchführung der erforderlichen Sicherheitsmaßnahmen, und zum anderen eine Sicherungsfunktion bezüglich der Wertinhalte des Geldautomaten. Der Zugang zu den Wertbehältnissen ist also mittels Sicherheitsmaßnahmen in Bezug auf Hardware und auch Software geschützt.

[0006] Eines oder mehrere dieser Schlösser befinden sich beispielsweise an der Hinterseite des Geldautomaten und sind somit für den (Standard-)Bankkunden nicht sichtbar. Schlösser an der Vorderseite sind beispielsweise durch ein zusätzliches Blech abgedeckt. Nach erfolgreichem Passieren der Sicherheitsmaßnahmen, welche beispielsweise anhand von einigen Schritten des nachfolgend erläuterten Verfahrens abgebildet sind, kann der autorisierte Benutzer das Schloss bzw. die Schlösser öffnen und Geld nachfüllen bzw. entnehmen.

[0007] Die Schnittstellenfunktion wird zum Beispiel durch ein Bedienterminal (auch Bedieneinheit oder Bedienteil genannt) bzw. einer Eingabeeinheit oder Bedienmodul abgebildet.

[0008] Ferner wird die Sicherungsfunktion beispielsweise durch mindestens ein mechanisches und/oder elektronisches Sicherungselement des Zugangs zum Geldfach als erstem Modul oder Schlossmodul abgebildet. Oft sind zwei Sicherungselemente angeordnet. Die Sicherungselemente liegen hierbei vorteilhaft als mechanische Schließeinrichtungen oder auch als mechanische und/oder elektronische bzw. intelligente Schlossriegel vor.

[0009] Zum heutigen Zeitpunkt ist es beispielsweise erforderlich, dass der Benutzer zum Öffnen des Wertbehältnisses seine eigene PIN sowie einen Schlüssel für das Schloss mit sich führt, was ein hohes Risiko darstellt, da beispielsweise Schlüssel oder PIN unrechtmäßig entwendet werden können. Ferner kann es vorkommen, dass der Benutzer durch Unachtsamkeit vor dem falschen Wertbehältnis steht. In manchen Fällen muss sich der Benutzer über einen Anruf beim Kundendienst des Automatenbetreibers erst einen Code zur Eingabe am Wertbehältnis ansagen lassen, was zeitintensiv und umständlich ist. Ferner müssen sich die Benutzer häufig umständlich mittels am Wertbehältnis angeordneter Detektionseinrichtungen identifizieren; beispielsweise über ein RFID-System mit einem durch den Benutzer mitgeführten Transponder, welcher einen kennzeichnenden Code enthält, sowie einem Lesegerät zum Auslesen dieses Kenn-Codes, welches am Wertebehältnis oder in dessen Umgebung angeordnet ist. Dieser Prozess ist aus heutiger Sicht nicht zu einem hohen Grad automatisierbar, was die Fehleranfälligkeit und Prozesszeit erhöht.

[0010] Die Druckschrift US 2012/229251 A1 offenbart ein Öffnungsverfahren für ein elektronisches Schloss, bei dem ein Smartphone einen auf dem Schloss aufgedruckten QR Code, welcher eine schlossspezifische Kennung codiert, erfasst, um basierend auf der Kennung einen dynamischen Öffnungscode von einem Server anzufordern.

[0011] Die Druckschrift US 2015/102906 A1 offenbart eine Kopplung eines elektronischen Schlosses mit einem mobilen Endgerät und eine Autorisierung der Schlossöffnung basierend auf einer Kennung des Schlosses, Kennung des mobilen Endgerätes und vordefinierten Zeitbeschränkungen, wobei die die Öffnung durch einen von einem Web Service an das elektronische Schloss versandten Befehl ausgelöst wird.

[0012] Die Druckschrift US 2014/375422 A1 offenbart ein Auslesen eines durch ein elektronisches Schloss dynamisch generierten QR Codes, welche eine eindeutige Schlosskennung sowie Protokolldaten bezüglich der Benutzer-Schloss-Interaktionen codiert, durch ein mobiles Endgerät. Der ausgelesene QR Code wird vom mobilen Endgerät an einen Server gesendet, welcher den Öffnungscode für das Schloss an das mobile Endgerät retourniert.

[0013] Die Druckschrift DE 102012008395 A1 offenbart eine Übermittlung eines an einem elektronischen Schloss angebrachten Barcode und benutzerspezifischer Information durch ein mobiles Endgerät an eine zentrale Informationsverarbeitungsstelle, welche basie-

rend auf den erhaltenen Daten sowie eines Zeit-Parameters feststellt, ob eine Berechtigung für das Übermitteln eines Öffnungscodes für das Schloss an das mobile Endgerät vorliegt.

[0014] Die Druckschrift US 2016/145904 A1 offenbart ein elektronisches Schloss, welches die Verriegelungs- bzw. Entriegelungsoperationen mittels eines Sensor detektiert, um diese Operationen zu protokollieren und Manipulationen am Schloss zu erkennen.

[0015] Die Druckschrift US 2013/187756 A1 offenbart eine elektronisches Schloss, dessen Entriegelung mittels Betätigen einer vorbestimmten Tastenkombination an einer Eingabevorrichtung des Wertbehältnisses gestartet (PIN Code) wird. Der erhaltene PIN-Code wird an einen elektronischen Schlüssel weitergeleitet. Falls dieser einen übereinstimmenden PIN-Code enthält, wird ein Öffnungsbefehl an das elektronische Schloss übermittelt.

[0016] Die Erfindung hat daher die Aufgabe, das Verfahren zum Öffnen und/ oder Schließen eines Wertbehältnisses anhand eines erfindungsgemäßen Verfahrens und eines erfindungsgemäßen Systems einfacher und prozesssicherer zu gestalten.

[0017] Das erfindungsgemäße Verfahren (100) zur Verwaltung eines Öffnungszustandes eines Wertbehältnisses, welches eine Bedieneinheit und mindestens ein mechanisches und/ oder elektrisches Schloss umfasst, ist durch die folgenden Schritte gekennzeichnet:

(101) Starten des Verfahrens über eine Eingabevorrichtung der Bedieneinheit,
(103) Anzeigen eines ersten Anzeigecodes, bevorzugt in Form eines QR-Codes, mittels einer Anzeigeeinrichtung der Bedieneinheit,
(104) Erfassen des ersten Anzeigecodes mittels eines Endgeräts,
(105) Übermitteln des ersten Anzeigecodes an einen Server durch das Endgerät,
(107) Übermitteln eines Öffnungscodes an das Endgerät durch den Server,
(108) Empfangen des Öffnungscodes auf dem Endgerät,
(109) Eingabe des Öffnungscodes an das Wertbehältnis über die Eingabevorrichtung der Bedieneinheit,
(110) Entriegeln des mindestens einen mechanischen und/ oder elektrischen Schlosses des Wertbehältnisses.

[0018] Es wird demnach vorgeschlagen, Einmal-Codes automatisiert zu generieren und dem Benutzer zur Öffnung des Wertbehältnisses zur Verfügung zu stellen. Der Benutzer muss also demnach keine Daten mit sich führen, die eventuell entwendet werden könnten.

[0019] Der Zusatz "QR" beim QR-Code leitet sich vom englischen Ausdruck "quick response" ("schnelle Antwort") ab und weist bereits darauf hin, dass mittels dieser Codes eine schnelle Erfassung der dadurch codierten Daten möglich ist.

[0020] Ein QR-Code besteht generell aus einer quadratischen Matrix aus schwarzen und weißen Quadraten, die die kodierten Daten binär darstellen; beispielsweise stehen ein weißes Quadrat in der Matrix für "0" und ein schwarzes Quadrat in der Matrix für "1" des Binärcodes. Eine spezielle Markierung in drei der vier Ecken des Quadrats gibt die Orientierung (Leserichtung) vor. Die Daten im QR-Code sind durch einen fehlerkorrigierenden Code geschützt, wodurch es selbst bei einem partiellen Verlust des Codes noch möglich ist, diesen zu dekodieren.

[0021] Im Code enthalten sind die Versionsinformation des Codes und das benutzte Datenformat. Der Datenteil enthält die kodierten Daten in redundanter Form. Zur Feldbegrenzung enthält der QR-Code in nur drei seiner Ecken ein bestimmtes Muster. Über das fehlende Muster in der vierten Ecke erkennt das Lesegerät die Orientierung. Mit zunehmender Größe des Codes werden weitere Muster hinzugefügt, um die Ausrichtung des Codes besser erkennbar zu machen. Zwischen den drei Hauptpositionsmarkierungen befindet sich eine Linie aus einer Folge streng abwechselnder Bits, worüber sich die Matrix definiert.

[0022] Es lassen sich also nahezu beliebig viele Daten mittels eines QR-Codes codieren und abbilden. Unter anderem können beispielsweise Sätze oder Kennnummern codiert werden. Bevorzugt umfasst die zweite Bedieneinheit eine Anzeigeeinrichtung in Form eines Touchpads. Alternativ dazu kann die zweite Bedieneinheit eine nicht-berührungssensitive Anzeigeeinrichtung und mindestens einen Tastenblock aufweisen.

[0023] Gemäß einer Verfahrensvariante ist es vorteilhaft, wenn der Benutzer nach dem Schritt (108) oder nach dem Schritt (109) seine Personalnummer und/ oder seine persönliche, nur ihm bekannte PIN eingeben muss, um Schritt (110) durchführen zu können. Somit ist gewährleistet, dass selbst dann, wenn der Öffnungscode beim Schritt (107) durch Dritte abgefangen wird, das Wertbehältnis ohne Kenntnis der genannten Daten nicht geöffnet werden kann.

[0024] Das Verfahren wird fortgeführt durch die weiteren Schritte:

(111) Verriegeln des mindestens einen mechanischen und/ oder elektrischen Schlosses des Wertbehältnisses,
(112) Anzeigen eines zweiten Anzeigecodes, bevorzugt in Form eines QR-Codes, mittels der Anzeigeeinrichtung der Bedieneinheit,
(113) Erfassen des zweiten Anzeigecodes mittels des Endgeräts,
(114) Übermitteln des zweiten Anzeigecodes an den Server durch das Endgerät,
(115) Ende des Verfahrens.

[0025] Das Wertbehältnis wird also zum einen hinsichtlich der beteiligten Hardware geschlossen. Damit ist

auch das Verfahren hinsichtlich der beteiligten Hardware abgeschlossen. Zum anderen wird das Verfahren auch hinsichtlich der beteiligten Software als abgeschlossen gekennzeichnet werden, indem die obigen Schritte 112 bis 114 bzw. 112 bis 115 durchgeführt werden. Es wird auf dem Server nach dem Schritt 114 eine Bestätigung darüber gespeichert werden, dass das Verfahren abgeschlossen ist.

[0026] Gemäß einer bevorzugten Ausführungsform erfolgen alle Schritte außer die Schritte 101, 102, 104, 109, 110, 111 und 113 automatisch und/ oder werden durch eine Durchführung oder ein Beenden eines vorhergehenden Schrittes ausgelöst/gestartet. Dies beschleunigt das Verfahren enorm, da durch das automatische Starten oder Auslösen nur sehr kurze Verzögerungszeiten zwischen den einzelnen Schritten zu erwarten sind. Außerdem reduziert sich die Fehlerwahrscheinlichkeit, da die Beteiligung eines menschlichen Benutzers an dem Verfahren weitestgehend reduziert ist.

[0027] Sensoren am Wertbehältnis, welche erkennen, dass das elektronische und/ oder mechanische Schloss geöffnet oder verriegelt wurde, senden Signale an eine Steuereinheit des Wertbehältnisses. Die Steuereinheit gibt dann Ausgabesignale weiter, beispielsweise an die zweite Anzeigeeinrichtung, die dann den zweiten Anzeigecode anzeigt.

[0028] Erfindungsgemäß wird der erste und der zweite Anzeigecode auf Basis von mindestens drei verschiedenen generiert, wobei die mindestens drei Datensätze ausgewählt sind aus Datensätzen, welche ein aktuelles Datum, eine aktuelle Uhrzeit, eine Seriennummer des Wertbehältnisses oder einen Standort des Wertbehältnisses codieren.

[0029] Die Anzeigecodes werden also anhand spezifischer Datensätze generiert und können somit einem Vorgang, einem Wertbehältnis und/ oder einem Benutzer eindeutig zugeordnet werden. Damit ist die Möglichkeit gegeben, die Kompatibilität zwischen dem Wertbehältnis, dem Endgerät, welches einem bestimmten Nutzer zuordenbar oder zugeordnet ist, und/ oder dem Server nach jedem erfolgten Schritt, insbesondere nach den Schritten 104, 105, 107, 109 und/ oder 113, 114 des Verfahrens zu überprüfen.

[0030] In der Software (App) auf dem Endgerät ist das Verfahren nur für einen vorbestimmten, begrenzten Zeitraum und/ oder zumindest temporär begrenzt nur für ein bestimmtes Wertbehältnis freigeschalten. Wird dennoch versucht, das Verfahren bei einem anderen Wertbehältnis und/ oder zu einem anderen Zeitpunkt zu starten, so wird nach dem Scan des Öffnungscodes (Schritt 104) eine Fehlermeldung auf dem mobilen Endgerät angezeigt und/ oder an den Server gesendet werden. In einer nicht erfindungsgemäßen Ausführungsform kann nach dem Schritt 105 seitens des Servers eine Fehlermeldung an das Endgerät gesendet werden.

[0031] Erfindungsgemäß wird der Offnungscode auf Basis von mindestens drei anhand des ersten Anzeigecodes codierten Datensätzen generiert, wobei die mindestens drei Datensätze die Seriennummer des Wertbehältnisses, das aktuelle Datum und die aktuelle Uhrzeit ist. Wird nicht nur einer, sondern mehrere Datensätze für die Generierung verwendet, werden diese aus den genannten Datensätzen (Seriennummer, Datum, Uhrzeit) ausgewählt. Gemäß einer weiteren Variante ist es bevorzugt, wenn zur Generierung des Öffnungscodes Datensätze wie die PIN und/ oder die Personalnummer des Benutzers verwendet werden. So ist sichergestellt, dass mit dem spezifisch generierten Öffnungscode nur das bestimmte Wertbehältnis mit passender Seriennummer geöffnet werden kann. Ferner ist sichergestellt, dass der Öffnungscode hinsichtlich seiner Aktualität überprüft wird und/ oder dass beispielsweise nur in einem vorbestimmbaren Zeitfenster nach Übermitteln des Öffnungscodes an das Endgerät der Öffnungscode an das Endgerät übertragen und das Wertbehältnis tatsächlich geöffnet werden kann.

[0032] Es ist weiterhin vorteilhaft, wenn der Öffnungscode ein Einmalcode ist und anhand eines auf dem Server abgespeicherten Algorithmus generiert wird. Im Sinne der Erfindung wird unter dem Begriff "Einmalcode" verstanden, dass die Informationen, welche der Einmalcode enthält, sich von vorhergehenden und/ oder nachfolgenden Einmalcodes zumindest bezüglich eines Parameters unterscheiden. So ist zum Beispiel gewährleistet, dass bei einem Öffnungscode, welcher als numerischer Code anhand einer Reihenfolge von beispielsweise sechs Ziffern ausgebildet ist, die Reihenfolge eines ersten Einmalcodes sich zumindest bezüglich einer Ziffer von der Reihenfolge eines zweiten Einmalcodes unterscheidet.

[0033] Das bedeutet, dass die Datensätze, welche zur Generierung des Öffnungscodes verwendet werden, bevorzugt nicht identische Öffnungscodes generieren dürfen. Insofern ist ein spezieller Algorithmus vorteilhaft, mittels welcher der Öffnungscode generiert wird.

[0034] Aus dem Stand der Technik sind hier die Begriffe "deterministisch" und "nichtdeterministisch" bekannt. Bei einem deterministischen Algorithmus ist zu jedem Zeitpunkt seiner Ausführung der Folgeschritt eindeutig bestimmt; der Algorithmus liefert also bei der gleichen Eingabe immer die gleiche Ausgabe. Dahingegen weist ein nicht-deterministischer Algorithmus an mindestens einer Stelle zwei oder mehr Möglichkeiten der Fortsetzung auf, zwischen welchen gewählt werden kann; der Algorithmus wird also durch einen Zufallsmechanismus beeinflusst. Werden also zur Generierung des Öffnungscodes in zwei Fällen nur einer oder mehrere Datensätze verwendet, die sich in beiden Fällen nicht unterscheiden (beispielsweise die Seriennummer des Wertbehältnisses und/ oder die Uhrzeit, welche für zwei unterschiedliche Tage gilt, aber zufällig gleich ist), so muss zur Generierung eines Einmalcodes ein nicht-deterministischer Algorithmus verwendet werden. Werden dagegen einer oder mehrere Datensätze verwendet, die sich in beiden Fällen unterscheiden (beispielsweise das aktuelle Datum), so kann zur Generierung eines Einmal-

codes ein deterministischer oder ein nicht-deterministischer Algorithmus verwendet werden.

[0035] Gemäß einer weiter bevorzugten Ausführungsform des Verfahrens umfasst der Server eine Auswerteeinheit, einen Codegenerator, eine Datenbank, eine Managementsoftware und/ oder ein Zugriffsmanagement, wobei mittels der Auswerteeinheit die Anzeigecodes ausgewertet und/ oder verglichen werden, wobei mittels des Codegenerator der Öffnungscode generiert wird, wobei mittels der Datenbank Datensätze wie Angaben zu Benutzern und/ oder Angaben zum Wertbehältnis gespeichert werden und aus der Datenbank abgerufen werden, wobei mittels der Managementsoftware Eingangssignale und Ausgangssignale verarbeitet werden, und wobei mittels des Zugriffsmanagements Zugriffsberechtigungen auf das System und/ oder auf das Verfahren gesteuert werden.

[0036] Mittels der Auswerteeinheit sind zudem Datensätze verarbeitbar und Signale bzw. Datensätze an eine andere Einheit sendbar. Die Art der Verarbeitung bzw. des Sendens von Datensätzen durch die Auswerteeinheit kann zum Beispiel mittels eines Programms oder Software vorbestimmt werden. Die Auswerteeinrichtung kann beispielsweise in Form eines Prozessors (Central Processing Unit, CPU) vorliegen.

[0037] Bevorzugt umfasst der Codegenerator mindestens einen der oben beschriebenen Algorithmen. Weiterhin bevorzugt kann zwischen verschiedenen Algorithmen gewählt werden, um die Sicherheit des Verfahrens zusätzlich zu erhöhen.

[0038] Ferner ist es bevorzugt, wenn das Verfahren mittels einer Log-Datei protokolliert wird, welche mindestens einen der folgenden Datensätze umfasst: eine Identifikation des dem Verfahren zugrundeliegenden Vorgangs und/ oder eine weitere Beschreibung des Vorgangs, eine Identifikation des Wertbehältnisses, bevorzugt in Form einer Seriennummer, eine Nummer der Schlossriegel oder Schlösser des Wertbehältnisses, eine Identifikation von beteiligten Benutzern, eine Identifikation von verwendeten Öffnungscodes und/ oder Zeitangaben. Bevorzugt ist diese Log-Datei auf einer jeweiligen Speichereinheit des Endgeräts, des Wertbehältnisses und/ oder des Servers speicherbar bzw. wird dort gespeichert.

[0039] Ferner ist es bevorzugt, wenn das Verfahren mittels eines einem einzelnen Wertbehältnis zugeordneten Vorgangsprotokolls protokolliert wird, welches mindestens einen der folgenden Datensätze umfasst: eine oder mehrere Zeitangaben, am jeweiligen Wertbehältnis durchgeführte Vorgänge, welche bevorzugt einer der Zeitangaben zugeordnet sind, die Identifikation von an den Vorgängen beteiligten Benutzern, die Identifikation von verwendeten Öffnungscodes, Angaben über eine Dauer des Verfahrens und/ oder Angaben darüber, ob der Schritt durchgeführt wurde. Bevorzugt ist dieses Vorgangsprotokoll auf einer jeweiligen Speichereinheit des Endgeräts, des Wertbehältnisses und/ oder des Servers speicherbar bzw. wird dort gespeichert.

[0040] Die Aufgabe der Erfindung wird ebenfalls gelöst durch ein System zur Verwaltung eines Öffnungszustandes eines Wertbehältnisses mittels eines Verfahrens nach einem der Ansprüche 1-6, umfassend ein Wertbehältnis mit einer Bedieneinheit und mindestens einem mechanischen und/ oder elektrischen und entriegelbaren Schloss, wobei mittels einer Anzeigeeinrichtung der Bedieneinheit Anzeigecodes anzeigbar sind, und wobei mittels einer Eingabevorrichtung der Bedieneinheit Öffnungscodes eingebbar sind, ein Endgerät, mittels welchem die Anzeigecodes erfassbar und die Öffnungscodes empfangbar sind, einen Server, an welchen die Anzeigecodes übermittelbar sind und mittels welchem die Öffnungscodes an das Endgerät übermittelbar sind, eine Funkverbindung zwischen Endgerät und Server und/ oder eine Netzwerkumgebung für den Server.

[0041] Bevorzugt umfasst der Server des Systems ferner: eine Auswerteeinheit, mittels welcher die Anzeigecodes auswertbar und/ oder vergleichbar sind, und/ oder einen Codegenerator, mittels welchem der Öffnungscode generierbar ist, eine Datenbank, mittels welcher Datensätze wie Angaben zu Benutzern und/ oder Angaben zum Wertbehältnis speicherbar und aus der Datenbank abrufbar sind, und/ oder eine Managementsoftware, mittels welcher Eingangssignale und Ausgangssignale verarbeitbar sind, und/ oder ein als ausführbares Programm abgespeichertes Zugriffsmanagement, mittels welchem Zugriffsberechtigungen auf das System und/ oder auf das Verfahren steuerbar sind.

[0042] Vorteile und Zweckmäßigkeiten sind der nachfolgenden Beschreibung in Verbindung mit der Zeichnung zu entnehmen.

[0043] Es zeigen:

Fig. 1 einen Überblick über an einem Beispiel eines erfindungsgemäßen Verfahrens beteiligte Komponenten in einer schematischen Darstellung;

Fig. 2 einen Wertdienstleister;

Fig. 3-6 Schritte des Verfahrensbeispiels und daran beteiligte Komponenten;

Fig. 7 Beispiele für eine Log-Datei und ein Vorgangsprotokoll;

Fig. 8 ein Beispiel eines erfindungsgemäßen Systems.

[0044] Es sei vorab erwähnt, dass das gezeigte Verfahren 100 und das gezeigte System 300 beispielsweise auch bei einem oben erwähnten Safe, wie er im Einzelhandel verwendet wird, angewendet werden können, auch wenn sich die Beschreibung der Figuren auf einen Geldautomaten einer Bank bezieht.

[0045] In Fig. 1 ist demnach ein Wertbehältnis 1 in Form eines Geldautomaten eines Geldinstituts wie bei-

spielsweise einer Bank gezeigt, welches eine erste Anzeigeeinrichtung 2 sowie eine erste Bedieneinheit 3 umfasst. Die erste Bedieneinheit 3 umfasst beispielsweise noch ein Kartensteckfach für die Geldkarte des Kunden, ein Nummernfeld zur Eingabe der zur Geldkarte gehörenden PIN sowie ein Ausgabefach/Einlegefach für Banknoten. Diese Elemente 2, 3 stehen dem Kunden der Bank zur Verfügung, wenn er Geld am Wertbehältnis 1 abheben oder einzahlen will, und werden im Folgenden nicht näher erläutert.

[0046] Mittels der Fig. 1 ist noch eine zweite Bedieneinheit 4 des Wertbehältnisses 1 abgebildet, welche dem autorisierten Benutzer 6 zur Verfügung steht (siehe auch Fig. 3). Diese umfasst vorliegend eine Eingabevorrichtung, welche zumindest zum Teil in Form eines Tastenblocks 4a zur Eingabe von Ziffern, Zeichen und/ oder Buchstaben ausgestaltet ist, ein Display als zweite Anzeigeeinrichtung 4b sowie weitere Tasten 4c, welche ebenfalls Teil der Eingabevorrichtung sein können. Diese zweite Bedieneinheit 4 ist beispielsweise an der gemäß Fig. 1 abgebildeten Vorderseite des Wertbehältnisses 1 unterhalb des Geldausgabefachs angeordnet. Vorteilhaft ist die zweite Bedieneinheit 4 hinter einer Abdecktür angeordnet, zu deren Öffnung beispielsweise das Betätigen eines mechanischen und/ oder elektrischen Schlüssels notwendig ist. Alternativ kann die zweite Bedieneinheit 4 an der Hinterseite des Wertbehältnisses 1, also auf der der gezeigten Vorderseite abgewandten Seite, angeordnet sein.

[0047] Generell ist es auch möglich, dass der Benutzer 6 über die erste Bedieneinheit 3 das im Folgenden beschriebene Verfahren 100 startet, und hierzu beispielsweise an der Bedieneinheit 3 (beispielsweise durch Eingabe einer speziellen Tastenkombination) zunächst ein separates Bedienmenü öffnet. Bevorzugt ist im Rahmen der Erfindung jedoch, dass die dem Benutzer 6 zugeordnete Bedieneinheit 4 nicht auch dem Kunden der Bank zur Verfügung steht und somit als eigenständige Einheit ausgebildet ist. Die zweite Bedieneinheit 4 ist somit bevorzugt nicht Teil der ersten Bedieneinheit 3, wird mithin auch nicht durch diese ausgebildet, und umgekehrt. Dies erhöht die Sicherheit des Verfahrens.

[0048] Ferner umfasst das Wertbehältnis 1 noch mindestens eine Steuerungseinheit CU (schematisch anhand der Fig. 1 gezeigt), welche Signale verarbeitet. Beispielsweise empfängt diese Steuerungseinheit CU Eingabesignale, welche durch das Betätigen der Tasten auf dem Tastenblock 4a oder 4c gesendet werden. Bestimmt durch diese Eingabesignale und einer entsprechenden auf dem Wertbehältnis 1 installierten Betriebssoftware kann die Steuerungseinheit CU dann Ausgabesignale senden. Beispielsweise ergeht so an die zweite Anzeigeeinrichtung 4b der Befehl, das der jeweils betätigten Taste zuordenbare Symbol anzuzeigen.

[0049] Vorteilhaft sind die einzelnen Betätigungselemente (Tastenblock 4a, Tasten 4c) der zweiten Bedieneinheit 4 mindestens doppelt belegbar, so dass eine einzelne Taste beispielsweise sowohl einen Buchstaben als auch eine Zahl oder ein anderes Symbol codieren kann. Ebenfalls gezeigt ist ein sogenannter QR-Code 5'.

[0050] Gemäß Fig. 2 ist ein Mitarbeiter einer CIT-Firma (CIT = Cash-In-Transit, Geldtransport) als Benutzer 6 gezeigt, welcher über seine Firma beispielsweise durch die Bank damit beauftragt ist, Wertbehältnisse 1 zu leeren und/ oder zu füllen.

[0051] Gemäß der Fig. 3 ist schematisch veranschaulicht, dass die zweite Bedieneinheit 4 beispielsweise unterhalb der ersten Bedieneinheit 3 und an der Vorderseite des Wertbehältnisses angeordnet ist.

[0052] Beispielsweise betätigt der Benutzer 6 zum Starten des Verfahrens 100 zur Öffnung des Wertbehältnisses 1 zunächst eine Taste oder eine Tastenkombination auf dem Tastenfeld 4a der zweiten Bedieneinheit 4 gemäß einem ersten Schritt 101. Vorteilhaft ist im Rahmen der Erfindung diese Taste oder Tastenkombination beispielsweise durch eine entsprechende Programmierung der Software der zweiten Bedieneinheit 4 vorbestimmbar, so dass dem Benutzer 6 zum Start des Verfahrens 100 diese spezifische Taste oder Tastenkombination bekannt sein muss.

[0053] Der Benutzer 6 führt ein Endgerät 7 (beispielsweise ein mobiles Endgerät wie ein Handy, einen Laptop, ein Tablet oder einen mobilen Handscanner) mit sich, auf welchem eine vorinstallierte Anwendung (Applikation) in einem weiteren Schritt 102 gestartet wird. Beispielsweise wird hierfür die Anwendung mit dem Handelsnamen "INSYS locks App" verwendet. Vorteilhaft ist diese Anwendung nicht über gängige Plattformen im Internet frei verfügbar, sondern muss separat beim Hersteller des Wertbehältnisses 1 oder beim Programmierer der dazugehörigen Betriebssoftware des Wertbehältnisses 1 angefragt werden. Alternativ ist es möglich, dass eine kundenspezifische Anwendung verwendet wird, welche die zur Ausführung des Verfahrens notwendigen Funktionen aufweist. Beispielsweise werden Funktionen dieser Anwendung vom Benutzer 6 bereits für andere Verfahren benutzt (wie beispielsweise das Scannen der Codes).

[0054] Das Betätigen der Taste/Tastenkombination aus Schritt 101 führt dazu, dass in einem weiteren Schritt 103 mittels der zweiten Anzeigeeinrichtung 4b der zweiten Bedieneinrichtung 4 ein erster Code, welcher bevorzugt als QR-Code 5a ausgestaltet ist, angezeigt wird. Denkbar wäre aber auch, dass ein anderer Code (Barcode, Touchcode) für das Verfahren 100 verwendet wird.

[0055] Dieser QR-Code 5a wird in einem weiteren Schritt 104 mittels des Endgeräts 7 gescannt, also erfasst.

[0056] Im Schritt 105 übermittelt das Endgerät 7 diesen gescannten QR-Code 5a oder die mittels ihm codierten Daten an einen Server 8 (siehe hierzu auch Darstellung gemäß Fig. 4). Bevorzugt werden dieser Code 5a oder die codierten Daten verschlüsselt an den Server 8 übertragen.

[0057] Mittels des Servers 8 bzw. Einrichtungen auf dem Server 8 wird der QR-Code 5a bevorzugt zunächst

entschlüsselt, bevor er in einem weiteren Schritt 106 verifiziert wird.

[0058] Im Schritt 107 sendet der Server 8 einen Öffnungscode 9 zurück an das Endgerät 7 des Benutzers 6. Im Schritt 108 wird dieser Öffnungscode 9 auf dem Endgerät 7 empfangen und/ oder angezeigt. Wie gemäß der Fig. 5 dargestellt ist, kann dieser Öffnungscode 9 beispielsweise als sechsstelliger Nummerncode (in diesem Beispiel als Reihenfolge der Ziffern "651249") ausgestaltet sein.

[0059] Der Öffnungscode 9 wird vom Benutzer 6 - vorteilhaft über den Tastenblock 4a oder ein Touchpad der zweiten Bedieneinheit 4 - im Schritt 109 eingegeben. Nach Eingabe des Codes 9 kann beispielsweise in einem Schritt 109a noch eine separate Taste oder Tastenkombination der weiteren Tasten 4c betätigt werden (beispielsweise die Bestätigungs-Taste, welche ein Hakensymbol anzeigt), um das Beenden der Eingabe zu bestätigen. Weiter optional ist die Eingabe der dem jeweiligen Benutzer 6 eineindeutig zugeordneten PIN und/ oder der Personalnummer vor oder nach der Eingabe des Öffnungscodes.

[0060] Anschließend kann das Wertbehältnis (Safe) in einem Schritt 110 geöffnet werden, wobei dieser Schritt 110 das Entriegeln mindestens eines elektronischen und/ oder mechanischen Schlosses (nicht gezeigt) umfasst, welches am Wertbehältnis 1 angeordnet ist und im verriegelten Zustand beispielsweise dessen Geldfächer verriegelt.

[0061] Gemäß der Fig. 6 ist gezeigt, wie in weiteren optionalen Verfahrensschritten das Wertbehältnis 1 wieder geschlossen werden kann.

[0062] Zunächst wird der Schritt 110 rückgängig gemacht, das heißt, dass in einem weiteren

[0063] Schritt 111 das Wertbehältnis 1 geschlossen wird. Hierzu wird das mindestens eine elektronische und/ oder mechanische Schloss wieder verriegelt. Damit wird das Verfahren 100 zunächst hinsichtlich der beteiligten Hardware abgeschlossen.

[0064] Anschließend wird in einem weiteren Schritt 112 über die zweite Anzeigeeinrichtung 4b ein zweiter QR-Code 5b angezeigt. Die Anzeige dieses zweiten QR-Codes 5b automatisch und wird beispielsweise durch das Durchführen des Schritts 111 ausgelöst.

[0065] Analog zum Schritt 104 scannt nun der Benutzer 6 den QR-Code 5b in einem weiteren Schritt 113.

[0066] Analog zum Schritt 105 wird anschließend der zweite QR-Code 5b oder die mittels ihm codierten Daten in einem weiteren Schritt 114 an einen Server 8 übermittelt werden. Damit wird das Verfahren 100 in der beteiligten Software als abgeschlossen gekennzeichnet.

[0067] Es gilt also, dass vorteilhaft beispielsweise lediglich an den Schritten 101, 102, 104, 109, 110, 111 und 113 die Beteiligung oder das Eingreifen einer menschlichen Person notwendig ist. Alle anderen Schritte erfolgen automatisch und/ oder werden durch die Durchführung oder das Beenden des vorhergehenden Schritts ausgelöst/gestartet.

[0068] Gemäß der Fig. 7 ist gezeigt, inwiefern das Verfahren 100 vorteilhaft protokolliert werden kann. Dabei ist eine Log-Datei 30 abgebildet, welche Informationen über die Identifikation 31 des dem Verfahren 100 zugrundeliegenden Vorgangs, der weiteren Beschreibung 32 des Vorgangs, die Identifikation 33 des Wertbehältnisses 1 (beispielsweise anhand dessen Seriennummer), die Nummer der Schlossriegel oder Schlösser des Wertbehältnisses 1 (Bezugszeichen 34, 37, 40), einer Identifikation der beteiligten Benutzer 6 (Bezugszeichen 35, 38) und der verwendeten Einmalcodes/Öffnungscodes 9 (Bezugszeichen 36, 39, 41, hier beispielhaft verdeckt angezeigt), weitere Infos 44, für welches Schloss (Schlossriegel 1 oder 2) beispielsweise ein Rückcode (im Sinne eines zweiten QR-Codes 5b) erforderlich ist, sowie Zeitangaben 42, 43 über Zeitpunkt und Dauer umfasst.

[0069] Die Tatsache, dass der Schlossriegel 1 in der Log-Datei 30 zweimal auftaucht, ist beispielsweise darauf zurückzuführen, dass zum Öffnen dieses Schlossriegels 1 die Eingabe zweier Einmalcodes 9 erforderlich ist. Beispielsweise wird dieses Erfordernis durch die Anzahl der beteiligten Benutzer 6 bestimmt, welche in der weiteren Beschreibung 32 hinterlegt ist.

[0070] Aus der Log-Datei 30 ist ebenfalls ersichtlich, dass zum Schließen des Wertbehältnisses 1 vorliegend nicht für alle Schlossriegel 1, 2 die Eingabe eines zweiten QR-Codes 5b erforderlich ist, sondern beispielsweise nur für den Schlossriegel 1. Dies spart Zeit und gewährleistet dennoch eine protokollierbare Aussage darüber, ob das Wertbehältnis 1 zumindest teilweise wieder geschlossen wurde.

[0071] Ebenfalls abgebildet ist ein einem speziellen Wertbehältnis 1 zugeordnetes Vorgangsprotokoll 50 mit Vorgängen 51 bis 56. Zu sehen sind einem ersten Datum 58 zuordenbare Vorgänge 54, 55 und 56 und einem zweiten, späteren Datum 57 zuordenbare Vorgänge 51, 52 und 53. Die Vorgänge an einem speziellen Wertbehältnis 1 sind also zählbar.

[0072] Ebenfalls ersichtlich ist, welcher 35, 38 der Benutzer 6 an welchem der Vorgänge 51-56 beteiligt war oder ist. Anhand der gezeigten Öffnungscodes 9, welche sichtbar oder verdeckt dargestellt werden, lässt sich außerdem deren Verwendung für den jeweiligen Vorgang 51-56 feststellen.

[0073] Die Angaben in der Spalte 60 erlauben einen Aufschluss darüber, wie lange der Öffnungsvorgang gedauert hat, welcher der Schlossriegel (1 oder 2) geöffnet wurde und ob ein Rückcode (im Sinne eines zweiten QR-Codes 5b) erforderlich war oder nicht.

[0074] Anhand der Spalte 59 lässt sich feststellen, ob das Wertbehältnis 1 geöffnet wurde oder nicht. Der Schritt 110 des Verfahrens 100 ist also detektierbar und protokollierbar.

[0075] Die Tatsache, dass bei den Vorgängen 51-53 eine Öffnung des Wertbehältnisses 1 verneint wird, lässt darauf schließen, dass der Öffnungsvorgang (Verfahren 100) noch nicht abgeschlossen ist; beispielsweise ist denkbar, dass im Verfahren 100 gerade der Schritt 109

durchgeführt wird. Bei den Vorgängen 54-56 handelt es sich dagegen offensichtlich um bereits abgeschlossene Vorgänge, bei denen die Öffnung des Wertbehältnisses 1 bestätigt wird.

[0076] Denkbar ist, dass der Benutzer 6 bei einem unerwarteten Fehler beim Verfahren 100 eine Hotline seiner CIT-Firma anruft, wobei die Mitarbeiter dann nach Einloggen Einblick in das Vorgangsprotokoll 50 erhalten und Daten und Angaben hieraus an den Benutzer 6 weitergeben.

[0077] Die Fig. 8 zeigt nochmals einen Überblick eines zugrundeliegenden Systems 300 für die Verwaltung eines Öffnungszustandes eines Wertbehältnisses 1 mittels eines Verfahrens nach einem der Ansprüche 1-9.

[0078] Die QR-Codes 5a,5b kodieren Angaben über das aktuelle Datum sowie über die Seriennummer des beteiligten Wertbehältnisses und/ oder dessen Standort. Ferner kann beispielsweise aus einer Datenbank 21 oder dem Server 8 abgerufen werden, welcher Benutzer 6 an dem aktuellen Vorgang bzw. dem Verfahren 100 beteiligt sein müsste. Vorteilhaft ist die Zuordnung eines Benutzers 6 zu einer bestimmten Dienstfahrt von vorneherein im System 300 festlegbar, um Missbrauch zu vermeiden.

[0079] Mindestens drei Datensätze des QR-Codes 5a bestimmen den Offnungscode 9.

[0080] Diese drei Datensätze sind die Seriennummer 33 des Wertbehältnisses 1, die Datumsangaben und die Uhrzeitangaben 42. Daraus kann insbesondere der Server 8 den legitimierten Benutzer 6 ermitteln. Auf Grundlage dieser Datensätze wird ein Öffnungscode 9 generiert.

[0081] Weiterhin ist es möglich, dass auch die Identität des beteiligten Endgeräts 7 (beispielsweise in Form von dessen IP-Adresse oder Handynummer) an den Server 8 gesendet und/ oder als Grundlage für die Generierung des Öffnungscodes 9 dienen kann. Ferner ist es möglich, dass erst nach Verifizierung dieser Identität durch den Server 8 das Verfahren 100 fortgesetzt werden kann.

[0082] Bevorzugt werden für separate Vorgänge (siehe Vorgangsprotokoll 50) am gleichen Wertbehältnis 1 stets unterschiedliche Öffnungscodes 9 generiert. Weiter bevorzugt kann ein einzelner Öffnungscode 9 nicht zweimal hintereinander oder nicht zweimal hintereinander innerhalb einer vorbestimmbaren Zeitspanne und/ oder einer Anzahl von Vorgängen am gleichen Wertbehältnis 1 eingegeben werden.

[0083] Beispielsweise wird die Verbindung von Endgerät 7 zu Server 8 über eine Funkverbindung 23 aufgebaut. Der Server 8 ist dabei vorteilhaft in einem Netzwerk integriert bzw. mit dem Internet 20 verbunden.

[0084] Auf dem Server 8 ist vorteilhaft eine Auswerteeinheit 81 gespeichert, welche den ankommenden QR-Code 5a (bzw. dessen zugrundeliegenden Daten) auswertet und/ oder vergleicht. Die Auswerteeinheit 81 kann beispielsweise in Form eines Prozessors (Central Processing Unit, CPU) vorliegen.

[0085] Ebenfalls ist ein Codegenerator 82 vorgesehen, welcher wie oben beschrieben die Daten aus dem QR-Code 5a dazu verwendet, einen Öffnungscode 9 zu generieren.

[0086] In einer Datenbank 83 lassen sich Fahrerangaben (Name, Geburtsdatum etc.) sowie Angaben zum Wertbehältnis 1 (Seriennummer, Standort, Anzahl der Schlossriegel etc.) speichern und daraus abrufen.

[0087] Eine Managementsoftware 84 ist installiert, um Eingangssignale und Ausgangssignale adäquat zu verarbeiten. Bevorzugt ist diese Software 84 mit der auf dem Wertbehältnis 1 ausführbaren Software synchronisiert.

[0088] Mittels des Zugriffsmanagements 85, was beispielsweise als ausführbares Programm auf dem Server 8 gespeichert werden kann und mittels welchem Zugriffsberechtigungen auf das System 300 und/ oder auf das Verfahren 100 steuerbar sind, kann beispielsweise einem bestimmten Benutzer 6 - auch unmittelbar - die Berechtigung zur Durchführung des Verfahrens 100 gegeben oder entzogen werden. Über ein Terminal zur Administration 22 ist die Verwaltung des Systems 300 möglich.

[0089] Das beschriebene System und das beschriebene Verfahren bieten also eine enorm hohe Sicherheit und Prozesssicherheit sowie eine schnelle Durchführbarkeit. Außerdem lassen sich alle Schritte wie beschrieben protokollieren und nachvollziehen.

Bezugszeichenliste

[0090]

1	Wertbehältnis
2	erste Anzeigeeinrichtung
3	erste Bedieneinheit
4	zweite Bedieneinheit
5', 5a, 5b	QR-Code
6	Benutzer
7	Endgerät
8	Server
9	Öffnungscode
20	Netzwerk/ Internet
21	Datenbank
22	Terminal
23	Funkverbindung
30	Logdatei
31	Identifikation eines dem Verfahren zugrundeliegenden Vorgangs
32	weitere Beschreibung des Vorgangs
33	Identifikation des Wertbehältnisses
34, 37, 40	Nummer der Schlossriegel oder Schlösser des Wertbehältnisses
35, 38	Identifikation von beteiligten Benutzern
36, 39, 41	Identifikation von verwendeten Öffnungscodes
42,43	Zeitangaben
44	weitere Informationen
50	Vorgangsprotokoll
51-56	Vorgang
57,58	Zeitangaben

59, 60	weitere Angaben im Vorgangsprotokoll
81	Auswerteeinheit
82	Codegenerator
83	Datenbank
84	Managementsoftware
85	Zugriffsmanagement
100	Verfahren
101-114	Schritte
300	System

Patentansprüche

1. Verfahren (100) zur Verwaltung eines Öffnungszustandes eines Wertbehältnisses (1), wobei das Wertbehältnis (1) eine Bedieneinheit (4) und mindestens ein mechanisches und/ oder elektrisches Schloss umfasst,
gekennzeichnet durch die folgenden Schritte:

(101) Starten des Verfahrens über eine Eingabevorrichtung (4a, 4c) der Bedieneinheit (4),
(102) Starten einer vorinstallierten Anwendung auf einem Endgerät (7),
(103) Anzeigen eines ersten Anzeigecodes, bevorzugt in Form eines QR-Codes (5a), mittels einer Anzeigeeinrichtung (4b) der Bedieneinheit (4), wobei der erste Anzeigecode auf Basis von mindestens drei verschiedenen Datensätzen generiert wird, wobei die mindestens drei Datensätze ausgewählt sind aus Datensätzen, welche ein aktuelles Datum, eine aktuelle Uhrzeit (42), eine Seriennummer (33) des Wertbehältnisses (1) oder einen Standort des Wertbehältnisses (1) codieren,
(104) Erfassen des ersten Anzeigecodes mittels des Endgeräts (7),
(105) Übermitteln des ersten Anzeigecodes an einen Server (8) durch das Endgerät (7),
(107) Übermitteln eines Öffnungscodes (9) an das Endgerät (7) durch den Server (8), wobei der Öffnungscode (9) auf Basis von den mindestens drei anhand des ersten Anzeigecodes codierten Datensätzen generiert wird, wobei die mindestens drei Datensätze die Seriennummer (33) des Wertbehältnisses (1), das aktuelle Datum und die aktuelle Uhrzeit (42) sind,
(108) Empfangen des Öffnungscodes (9) auf dem Endgerät (7),
(109) Eingabe des Öffnungscodes (9) an das Wertbehältnis (1) über die Eingabevorrichtung (4a, 4c) der Bedieneinheit (4),
(110) Entriegeln des mindestens einen mechanischen und/ oder elektrischen Schlosses des Wertbehältnisses (1),
(111) Verriegeln des mindestens einen mechanischen und/ oder elektrischen Schlosses des Wertbehältnisses (1),
(111a) Erkennen des Verriegelns des mindestens einen mechanischen und/ oder elektrischen Schlosses des Wertbehältnisses (1) durch einen Sensor am Wertbehältnis (1) und Senden eines entsprechenden Sensorsignals an eine Steuereinheit des Wertbehältnisses (1),
(111b) Senden eines Ausgabesignals an die Anzeigeeinrichtung (4b) der Bedieneinheit (4) durch die Steuereinheit,
(112) Anzeigen eines zweiten Anzeigecodes in Reaktion auf das empfangene Ausgabesignal von der Steuereinheit, bevorzugt in Form eines QR-Codes (5b), mittels der Anzeigeeinrichtung (4b) der Bedieneinheit (4), wobei der zweite Anzeigecode auf Basis mindestens eines dritten Datensatzes generiert wird, wobei der mindestens eine dritte Datensatz ausgewählt ist aus Datensätzen, welche ein aktuelles Datum, eine aktuelle Uhrzeit (42), eine Seriennummer (33) des Wertbehältnisses (1) oder einen Standort des Wertbehältnisses (1) codieren,
(113) Erfassen des zweiten Anzeigecodes mittels des Endgeräts (7),
(114) Übermitteln des zweiten Anzeigecodes an den Server (8) durch das Endgerät (7), (114a) Speichern einer Bestätigung auf dem Server (8) zum software-seitigen Abschluss des Verfahrens,
(115) Ende des Verfahrens,
wobei eine Kompatibilität zwischen dem Wertbehältnis (1), dem Endgerät (7), welches einem bestimmten Benutzer zuordenbar oder zugeordnet ist, und dem Server nach den Schritten Erfassen des ersten Anzeigecodes mittels des Endgeräts (7), Übermitteln des ersten Anzeigecodes an einen Server (8) durch das Endgerät (7) und/oder Übermitteln eines Öffnungscodes (9) an das Endgerät (7) durch den Server (8), Eingabe des Öffnungscodes (9) an das Wertbehältnis (1) über die Eingabevorrichtung (4a, 4c) der Bedieneinheit (4), und/oder Erfassen des zweiten Anzeigecodes mittels des Endgeräts (7), Übermitteln des zweiten Anzeigecodes an den Server (8) durch das Endgerät (7) anhand der Datensätze, auf deren Basis der erste und/oder der zweite Anzeigecode generiert werden, überprüft wird,
wobei ein Start des Verfahrens (100) durch die vorinstallierte Anwendung auf dem Endgerät (7) nur für einen vorbestimmten, begrenzten Zeitraum und/oder temporär begrenzt nur für ein bestimmtes Wertbehältnis (1) freigeschaltet wird und wobei nach einem versuchten Start des Verfahrens (100) bei einem anderen Wertbehältnis und/oder in einem anderen Zeitraum, nach dem Scan des ersten Anzeigecodes (104) eine Fehlermeldung auf dem Endgerät (7) angezeigt und/oder an den Server (8) gesendet wird.

2. Verfahren (100) nach Anspruch 1,
dadurch gekennzeichnet, dass

alle Schritte außer die Schritte Starten des Verfahrens über eine Eingabevorrichtung (4a, 4c) der Bedieneinheit (4), Starten einer vorinstallierten Anwendung auf einem Endgerät (7), Erfassen des ersten Anzeigecodes mittels eines des Endgeräts (7), Eingabe des Öffnungscodes (9) an das Wertbehältnis (1) über die Eingabevorrichtung (4a, 4c) der Bedieneinheit (4), Entriegeln des mindestens einen mechanischen und/oder elektrischen Schlosses des Wertbehältnisses (1), Verriegeln des mindestens einen mechanischen und/oder elektrischen Schlosses des Wertbehältnisses (1) und Erfassen des zweiten Anzeigecodes mittels des Endgeräts (7) automatisch
erfolgen und/ oder durch eine Durchführung oder ein Beenden eines vorhergehenden Schrittes ausgelöst/gestartet werden.

3. Verfahren (100) nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet, dass
der Öffnungscode (9) ein Einmalcode ist und anhand eines auf dem Server (8) abgespeicherten Algorithmus' generiert wird.

4. Verfahren (100) nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet, dass

der Server (8) eine Auswerteeinheit (81), einen Codegenerator (82), eine Datenbank (83), eine Managementsoftware (84) und/ oder ein Zugriffsmanagement (85) umfasst,
wobei mittels der Auswerteeinheit (81) die Anzeigecodes (5a, 5b) ausgewertet und/ oder verglichen werden,
wobei mittels des Codegenerator (82) der Öffnungscode (9) generiert wird,
wobei mittels der Datenbank (83) Datensätze wie Angaben zu Benutzern (6) und/ oder Angaben zum Wertbehältnis (1) gespeichert werden und aus der Datenbank (83) abgerufen werden,
wobei mittels der Managementsoftware (84) Eingangssignale und Ausgangssignale verarbeitet werden, und
wobei mittels des Zugriffsmanagements (85) Zugriffsberechtigungen auf das System (300) und/ oder auf das Verfahren (100) gesteuert werden.

5. Verfahren (100) nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet, dass
das Verfahren (100) mittels einer Log-Datei (30) protokolliert wird, welche mindestens einen der folgenden Datensätze umfasst:

eine Identifikation (31) des dem Verfahren (100) zugrundeliegenden Vorgangs und/ oder
eine weitere Beschreibung (32) des Vorgangs,
eine Identifikation (33) des Wertbehältnisses (1), bevorzugt in Form einer Seriennummer,
eine Nummer der Schlossriegel oder Schlösser (34, 37, 40) des Wertbehältnisses (1), eine Identifikation von beteiligten Benutzern (35, 38),
eine Identifikation von verwendeten Öffnungscodes (36, 39, 41),
Zeitangaben (42, 43).

6. Verfahren (100) nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet, dass
das Verfahren (100) mittels eines einem einzelnen Wertbehältnis (1) zugeordneten Vorgangsprotokolls (50) protokolliert wird, welches mindestens einen der folgenden Datensätze umfasst:

eine oder mehrere Zeitangaben (57, 58),
am jeweiligen Wertbehältnis (1) durchgeführte Vorgänge (51-56), welche bevorzugt einer der Zeitangaben (57, 58) zugeordnet sind,
die Identifikation von an den Vorgängen (51-56) beteiligten Benutzern (35, 38),
die Identifikation von verwendeten Öffnungscodes (36, 39, 41),
Angaben über eine Dauer des Verfahrens (100),
Angaben darüber, ob der Schritt (110) durchgeführt wurde.

7. System (300) zur Verwaltung eines Öffnungszustandes eines Wertbehältnisses (1) mittels eines Verfahrens nach einem der Ansprüche 1-6,
umfassend

ein Wertbehältnis (1) mit einer Bedieneinheit (4) und mindestens einem mechanischen und/ oder elektrischen und entriegelbaren Schloss, wobei mittels einer Anzeigeeinrichtung (4b) der Bedieneinheit (4) Anzeigecodes anzeigbar sind, und wobei mittels einer Eingabevorrichtung (4a, 4c) der Bedieneinheit (4) Öffnungscodes (9) eingebbar sind,
ein Endgerät (7), mittels welchem die Anzeigecodes erfassbar und die Öffnungscodes empfangbar sind,
einen Server (8), an welchen die Anzeigecodes übermittelbar sind und mittels welchem die Öffnungscodes an das Endgerät (7) übermittelbar sind,
eine Funkverbindung (23) zwischen Endgerät (7) und Server (8),
eine Netzwerkumgebung für den Server (8).

8. System (300) nach Anspruch 7,
dadurch gekennzeichnet, dass
der Server (8) ferner umfasst:

eine Auswerteeinheit (81), mittels welcher die Anzeigecodes (5a, 5b) auswertbar und/ oder vergleichbar sind, und/ oder
einen Codegenerator (82), mittels welchem der Öffnungscode (9) generierbar ist,
eine Datenbank (83), mittels welcher Datensätze wie Angaben zu Benutzern (6) und/ oder Angaben zum Wertbehältnis (1) speicherbar und aus der Datenbank (83) abrufbar sind, und/ oder
eine Managementsoftware (84), mittels welcher Eingangssignale und Ausgangssignale verarbeitbar sind, und/ oder
ein als ausführbares Programm abgespeichertes Zugriffsmanagement (85), mittels welchem Zugriffsberechtigungen auf das System (300) und/ oder auf das Verfahren (100) steuerbar sind.

Claims

1. Method (100) for managing an opening state of a value container (1),
wherein the value container (1) comprises an operating unit (4) and at least one mechanical and/or electrical lock,
characterised by the following steps:

(101) Starting the method via an input device (4a, 4c) of the operating unit (4),
(102) starting a pre-installed application on a terminal device (7),
(103) displaying a first display code, preferably in the form of a QR code (5a), by means of a display device (4b) of the operating unit (4), the first display code being generated on the basis of at least three different data records, the at least three data records being selected from data records which encode a current date, a current time (42), a serial number (33) of the value container (1) or a location of the value container (1),
(104) acquiring the first display code by means of the terminal device (7),
(105) transmitting the first display code to a server (8) by means of the terminal device (7),
(107) transmitting an opening code (9) to the terminal device (7) by the server (8), the opening code (9) being generated on the basis of the at least three data records encoded on the basis of the first display code, the at least three data records being the serial number (33) of the value container (1), the current date and the current time (42),
(108) Receiving the opening code (9) on the terminal device (7),
(109) inputting the opening code (9) to the value container (1) via the input device (4a, 4c) of the operating unit (4),
(110) unlocking the at least one mechanical and/or electrical lock of the value container (1),
(111) locking the at least one mechanical and/or electrical lock of the value container (1),
(111a) detection of the locking of the at least one mechanical and/or electrical lock of the value container (1) by a sensor on the value container (1) and transmission of a corresponding sensor signal to a control unit of the value container (1),
(111b) sending an output signal to the display device (4b) of the control unit (4) by the control unit,
(112) displaying a second display code in response to the received output signal from the control unit, preferably in the form of a QR code (5b), by means of the display device (4b) of the operating unit (4), the second display code being generated on the basis of at least one third data record, the at least one third data record being selected from data records which encode a current date, a current time (42), a serial number (33) of the value container (1) or a location of the value container (1),
(113) acquiring the second display code by means of the terminal device (7),
(114) transmitting the second display code to the server (8) by means of the terminal device (7),
(114a) storing a confirmation on the server (8) for software-side completion of the method,
(115) end of the method,
wherein a compatibility between the value container (1), the terminal device (7), which can be assigned or is assigned to a specific user, and the server is checked after steps acquiring the first display code by means of the terminal device (7), transmitting the first display code to a server (8) by means of the terminal device (7) and/or transmitting an opening code (9) to the terminal device (7) by the server (8), inputting the opening code (9) to the value container (1) via the input device (4a, 4c) of the operating unit (4), and/or acquiring the second display code by means of the terminal device (7), transmitting the second display code to the server (8) by means of the terminal device (7) on the basis of the data records on the basis of which the first and/or the second display code is generated,
wherein a start of the method (100) by means of the pre-installed application on the terminal device (7) is enabled only for a predetermined, limited period of time and/or temporarily limited

only for a specific value container (1) and wherein, after an attempted start of the method (100) for another value container and/or in another period of time, an error message is displayed on the terminal device (7) and/or sent to the server (8) after the scanning of the first display code (104).

2. Method (100) according to claim 1,
characterised in that
all steps except steps starting the method via an input device (4a, 4c) of the operating unit (4), starting a pre-installed application on a terminal device (7), acquiring the first display code by means of the terminal device (7), inputting the opening code (9) to the value container (1) via the input device (4a, 4c) of the operating unit (4), unlocking the at least one mechanical and/or electrical lock of the value container (1), locking the at least one mechanical and/or electrical lock of the value container (1) and acquiring the second display code by means of the terminal device (7) are automatic and/or triggered/started by an execution or termination of a preceding step.

3. Method (100) according to any one of the preceding claims,
characterized in that
the opening code (9) is a one-time code and is generated on the basis of an algorithm stored on the server (8).

4. Method (100) according to any one of the preceding claims,
characterized in that

the server (8) comprises an evaluation unit (81), a code generator (82), a database (83), management software (84) and/or access management (85),
wherein the display codes (5a, 5b) are evaluated and/or compared by means of the evaluation unit (81),
wherein the opening code (9) is generated by means of the code generator (82),
wherein by means of the database (83) data records such as details of users (6) and/or details of the value container (1) are stored and retrieved from the database (83),
wherein input signals and output signals are processed by means of the management software (84), and
wherein access authorisations to the system (300) and/or to the method (100) are controlled by means of the access management (85).

5. Method (100) according to any one of the preceding claims,
characterized in that
the method (100) is logged by means of a log file (30) comprising at least one of the following data sets:

an identification (31) of a process underlying the method (100) and/or a further description (32) of the process,
an identification (33) of the value container (1), preferably in the form of a serial number,
a number of the lock bolts or locks (34, 37, 40) of the value container (1), an identification of users involved (35, 38),
an identification of opening codes used (36, 39, 41), time information (42, 43).

6. Method (100) according to any one of the preceding claims,
characterised in that
the method (100) is logged by means of an event log (50) associated with a single value container (1), comprising at least one of the following records:

one or more pieces of time information (57, 58),
events (51-56) carried out on the respective value container (1), which are preferably assigned to one of the time information (57, 58),
the identification of users (35, 38) involved in the events (51-56),
the identification of opening codes used (36, 39, 41),
indications of a duration of the method (100),
information on whether the step (110) has been carried out.

7. System (300) for managing an opening state of a value container (1) by means of a method according to any of claims 1-6,
comprising

a value container (1) with an operating unit (4) and at least one mechanical and/or electrical and unlockable lock, wherein display codes can be displayed by means of a display device (4b) of the operating unit (4), and wherein opening codes (9) can be entered by means of an input device (4a, 4c) of the operating unit (4),
a terminal device (7) by means of which the display codes can be detected and the opening codes can be received,
a server (8) to which the display codes can be transmitted and by means of which the opening codes can be transmitted to the terminal device (7),
a radio communication (23) between the terminal device (7) and the server (8),
a network environment for the server (8).

8. System (300) according to claim 7,

characterised in that
the server (8) further comprises:

an evaluation unit (81) by means of which the display codes (5a, 5b) can be evaluated and/or compared, and/or
a code generator (82) by means of which the opening code (9) can be generated,
a database (83) by means of which data records such as details of users (6) and/or
details of the value container (1) can be stored and retrieved from the database (83), and/or
a management software (84) by means of which input signals and output signals can be processed, and/or
an access management (85) stored as an executable program, by means of which access authorisations to the system (300) and/or to the method (100) can be controlled.

Revendications

1. Procédé (100) pour la gestion d'un état d'ouverture d'un coffre-fort (1), le coffre-fort (1) comportant une unité de commande (4) et au moins une serrure mécanique et/ou électrique,
caractérisé par les étapes suivantes :

(101) Démarrage du procédé par l'intermédiaire d'un dispositif d'entrée (4a, 4c) de l'unité de commande (4) ;
(102) Démarrage d'une application préinstallée sur un terminal (7) ;
(103) Affichage d'un premier code d'affichage, de préférence sous la forme d'un QR code (5a), au moyen d'un dispositif d'affichage (4b) de l'unité de commande (4), le premier code d'affichage étant généré sur la base d'au moins trois ensembles de données différents, lesdits au moins trois ensembles de données étant choisis parmi des ensembles de données qui codent une date actuelle, une heure actuelle (42), un numéro de série (33) du coffre-fort (1) ou un emplacement du coffre-fort (1) ;
(104) Saisie du premier code d'affichage au moyen du terminal (7) ;
(105) Transmission du premier code d'affichage à un serveur (8) par le terminal (7) ;
(107) Transmission d'un code d'ouverture (9) au terminal (7) par le serveur (8), le code d'ouverture (9) étant généré sur la base desdits au moins trois ensembles de données codés à partir du premier code d'affichage, lesdits au moins trois ensembles de données étant le numéro de série (33) du coffre-fort (1), la date actuelle et l'heure actuelle (42) ;
(108) Réception du code d'ouverture (9) sur le terminal (7) ;
(109) Entrée du code d'ouverture (9) sur le coffre-fort (1) par l'intermédiaire du dispositif d'entrée (4a, 4c) de l'unité de commande (4) ;
(110) Déverrouillage de ladite au moins une serrure mécanique et/ou électrique du coffre-fort (1) ;
(111) Verrouillage de ladite au moins une serrure mécanique et/ou électrique du coffre-fort (1) ;
(111a) Détection du verrouillage de ladite au moins une serrure mécanique et/ou électrique du coffre-fort (1) par un capteur sur le coffre-fort (1) et envoi d'un signal de capteur correspondant à une unité de contrôle du coffre-fort (1) ;
(111b) Envoi d'un signal de sortie au dispositif d'affichage (4b) de l'unité de commande (4) par l'unité de contrôle ;
(112) Affichage d'un second code d'affichage en réponse au signal de sortie reçu de l'unité de contrôle, de préférence sous la forme d'un QR code (5b), au moyen du dispositif d'affichage (4b) de l'unité de commande (4), le second code d'affichage étant généré sur la base d'au moins un troisième ensemble de données, ledit au moins un troisième ensemble de données étant choisi parmi des ensembles de données qui codent une date actuelle, une heure actuelle (42), un numéro de série (33) du coffre-fort (1) ou un emplacement du coffre-fort (1) ;
(113) Saisie du second code d'affichage au moyen du terminal (7) ;
(114) Transmission du second code d'affichage au serveur (8) par le terminal (7) ;
(114a) Stockage d'une confirmation sur le serveur (8) pour la fin côté logiciel du procédé;
(115) Fin du procédé,
une compatibilité entre le coffre-fort (1), le terminal (7), qui est attribuable ou attribué à un utilisateur déterminé, et le serveur étant vérifiée après les étapes de saisie du premier code d'affichage au moyen du terminal (7), transmission du premier code d'affichage à un serveur (8) par le terminal (7) et/ou transmission d'un code d'ouverture (9) au terminal (7) par le serveur (8), entrée du code d'ouverture (9) sur le coffre-fort (1) par l'intermédiaire du dispositif d'entrée (4a, 4c) de l'unité de commande (4), et/ou saisie du second code d'affichage au moyen du terminal (7), transmission du second code d'affichage au serveur (8) par le terminal (7) à partir des ensembles de données, sur la base desquels le premier et/ou le second code d'affichage sont générés,
un démarrage du procédé (100) n'étant débloqué par l'application préinstallée sur le terminal (7) que pour une période de temps limitée prédéterminée et/ou de façon temporairement limi-

tée que pour un coffre-fort défini (1) et, après une tentative de démarrage du procédé (100) dans le cas d'un autre coffre-fort et/ou dans une autre période de temps, un message d'erreur étant affiché sur le terminal (7) et/ou envoyé au serveur (8) après le balayage du premier code d'affichage (104).

2. - Procédé (100) selon la revendication 1,
caractérisé par le fait que
toutes les étapes, à l'exception des étapes de démarrage du procédé par l'intermédiaire d'un dispositif d'entrée (4a, 4c) de l'unité de commande (4), de démarrage d'une application préinstallée sur un terminal (7), de saisie du premier code d'affichage au moyen du terminal (7), d'entrée du code d'ouverture (9) sur le coffre-fort (1) par l'intermédiaire du dispositif d'entrée (4a, 4c) de l'unité de commande (4), de déverrouillage de ladite au moins une serrure mécanique et/ou électrique du coffre-fort (1), de verrouillage de ladite au moins une serrure mécanique et/ou électrique du coffre-fort (1) et de saisie du second code d'affichage au moyen du terminal (7) ont lieu automatiquement et/ou sont déclenchées/démarrées par une exécution ou une fin d'une étape précédente.

3. Procédé (100) selon l'une des revendications précédentes,
caractérisé par le fait que
le code d'ouverture (9) est un code à usage unique et est généré à partir d'un algorithme stocké sur le serveur (8).

4. Procédé (100) selon l'une des revendications précédentes,
caractérisé par le fait que

le serveur (8) comporte une unité d'évaluation (81), un générateur de code (82), une base de données (83), un logiciel de gestion (84) et/ou une gestion d'accès (85) ; les codes d'affichage (5a, 5b) étant évalués et/ou comparés au moyen de l'unité d'évaluation (81) ;
le code d'ouverture (9) étant généré au moyen du générateur de code (82) ; des ensembles de données tels que des indications concernant des utilisateurs (6) et/ou des indications concernant le coffre-fort (1) étant stockés au moyen de la base de données (83) et étant récupérés à partir de la base de données (83) ;
des signaux d'entrée et des signaux de sortie étant traités au moyen du logiciel de gestion (84) ; et
des autorisations d'accès au système (300) et/ou au procédé (100) étant commandées au moyen de la gestion d'accès (85).

5. Procédé (100) selon l'une des revendications précédentes,
caractérisé par le fait que
le procédé (100) est consigné au moyen d'un fichier journal (30), lequel comporte au moins l'un des ensembles de données suivants :

une identification (31) de l'opération à la base du procédé (100) et/ou une autre description (32) de l'opération ;
une identification (33) du coffre-fort (1), de préférence sous la forme d'un numéro de série ;
un numéro des verrous ou serrures (34, 37, 40) du coffre-fort (1) ;
une identification des utilisateurs impliqués (35, 38) ;
une identification des codes d'ouverture utilisés (36, 39, 41) ;
des indications de temps (42, 43).

6. Procédé (100) selon l'une des revendications précédentes,
caractérisé par le fait que
le procédé (100) est consigné au moyen d'un journal des opérations (50) associé à un coffre-fort individuel (1), lequel journal comporte au moins l'un des ensembles de données suivants :

une ou plusieurs indications de temps (57, 58) ;
des opérations (51-56) effectuées sur le coffre-fort respectif (1), lesquelles sont, de préférence, associées à l'une des indications de temps (57, 58) ;
l'identification des utilisateurs (35, 38) impliqués dans les opérations (51-56) ;
l'identification des codes d'ouverture utilisés (36, 39, 41) ;
des indications sur une durée du procédé (100) ;
des informations indiquant si l'étape (110) a été effectuée ou non.

7. Système (300) pour la gestion d'un état d'ouverture d'un coffre-fort (1) au moyen d'un procédé selon l'une des revendications 1 à 6,
comportant

un coffre-fort (1) avec une unité de commande (4) et au moins une serrure mécanique et/ou électrique et déverrouillable, des codes d'affichage étant affichables au moyen d'un dispositif d'affichage (4b) de l'unité de commande (4), et des codes d'ouverture (9) étant aptes à être entrés au moyen d'un dispositif d'entrée (4a, 4c) de l'unité de commande (4) ;
un terminal (7) au moyen duquel les codes d'affichage sont aptes à être saisis et les codes d'ouverture sont aptes à être reçus ;
un serveur (8) auquel les codes d'affichage sont

aptes à être transmis et au moyen duquel les codes d'ouverture sont aptes à être transmis au terminal (7) ;
une liaison radio (23) entre le terminal (7) et le serveur (8) ;
un environnement réseau pour le serveur (8).

8. Système (300) selon la revendication 7, **caractérisé par le fait que**
le serveur (8) comprend en outre :

une unité d'évaluation (81), au moyen de laquelle les codes d'affichage (5a, 5b) sont aptes à être évalués et/ou comparés, et/ou
un générateur de code (82), au moyen duquel le code d'ouverture (9) est apte à être généré,
une base de données (83), au moyen de laquelle des ensembles de données tels que des indications concernant des utilisateurs (6) et/ou des indications concernant le coffre-fort (1) sont aptes à être stockés et à être récupérés à partir de la base de données (83), et/ou
un logiciel de gestion (84), au moyen duquel des signaux d'entrée et des signaux de sortie sont aptes à être traités, et/ou
une gestion d'accès (85) stockée sous forme de programme exécutable, au moyen de laquelle des autorisations d'accès au système (300) et/ou au procédé (100) sont aptes à être commandées.

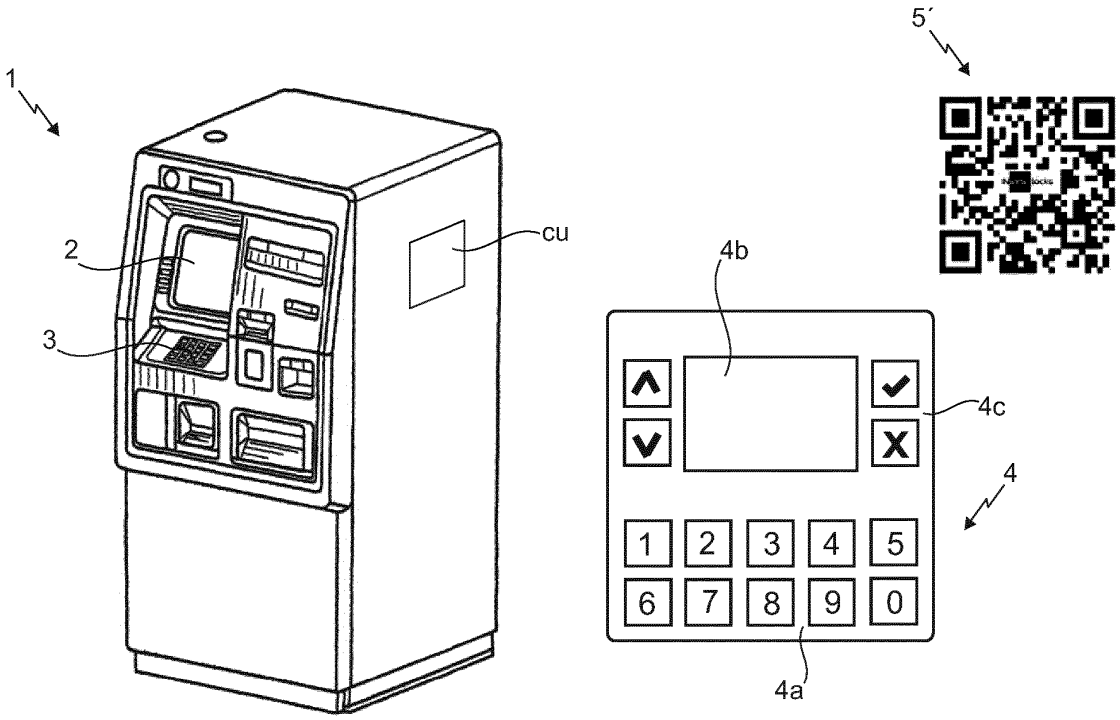


Fig. 1

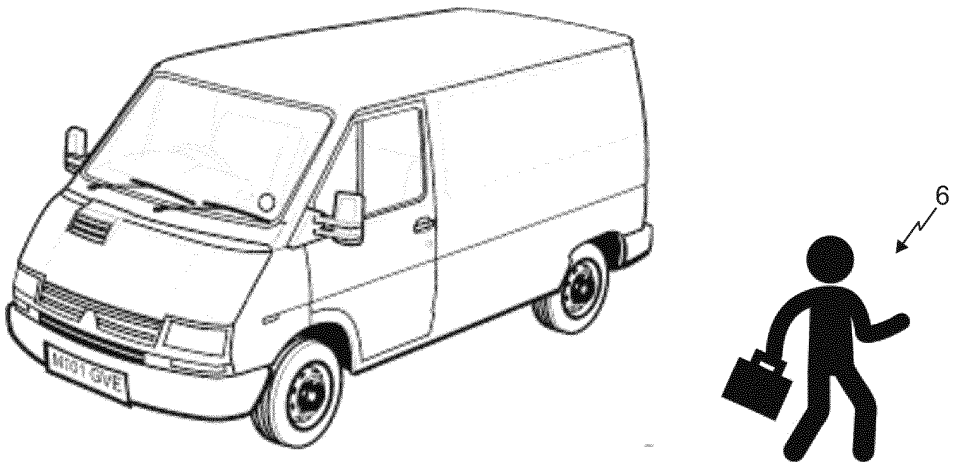
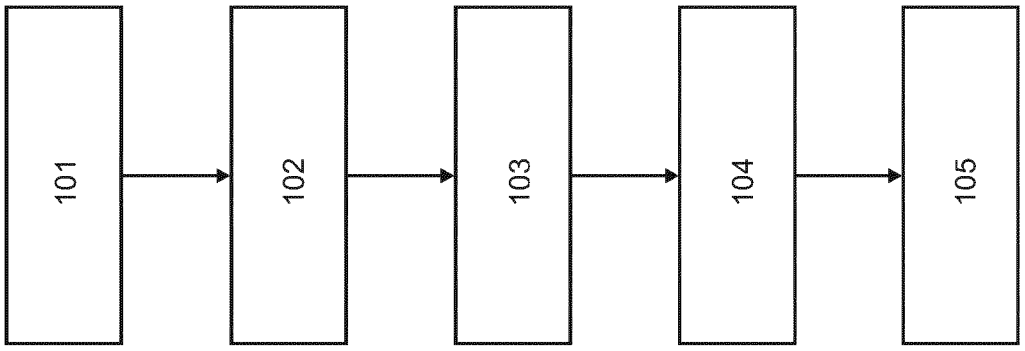


Fig. 2



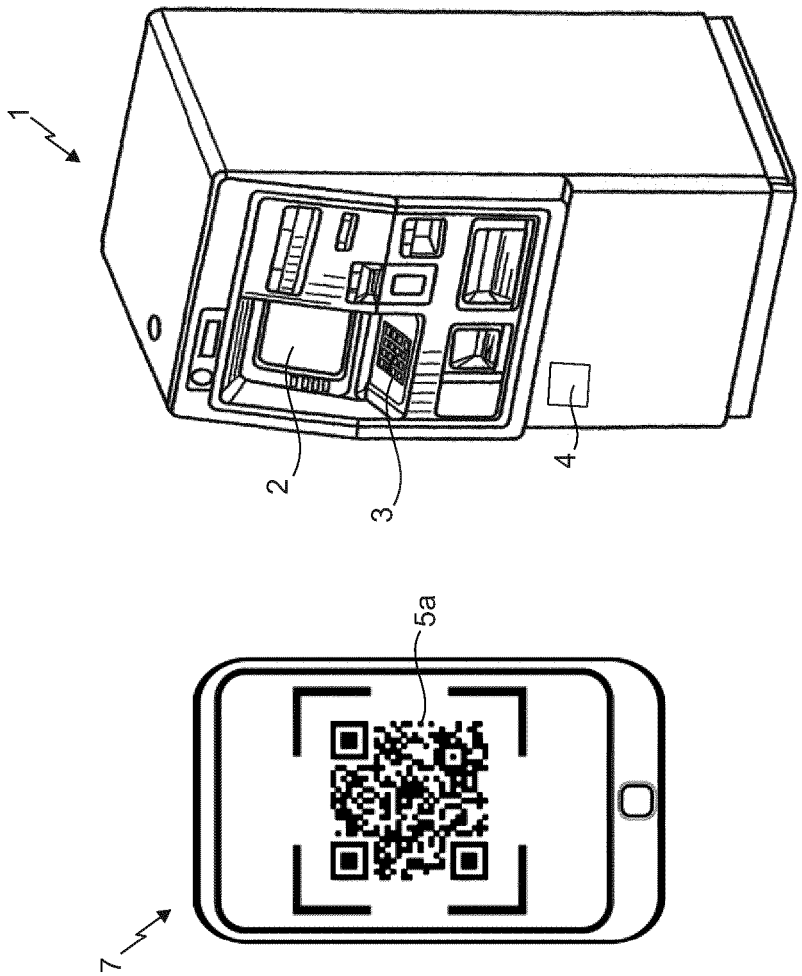


Fig. 3

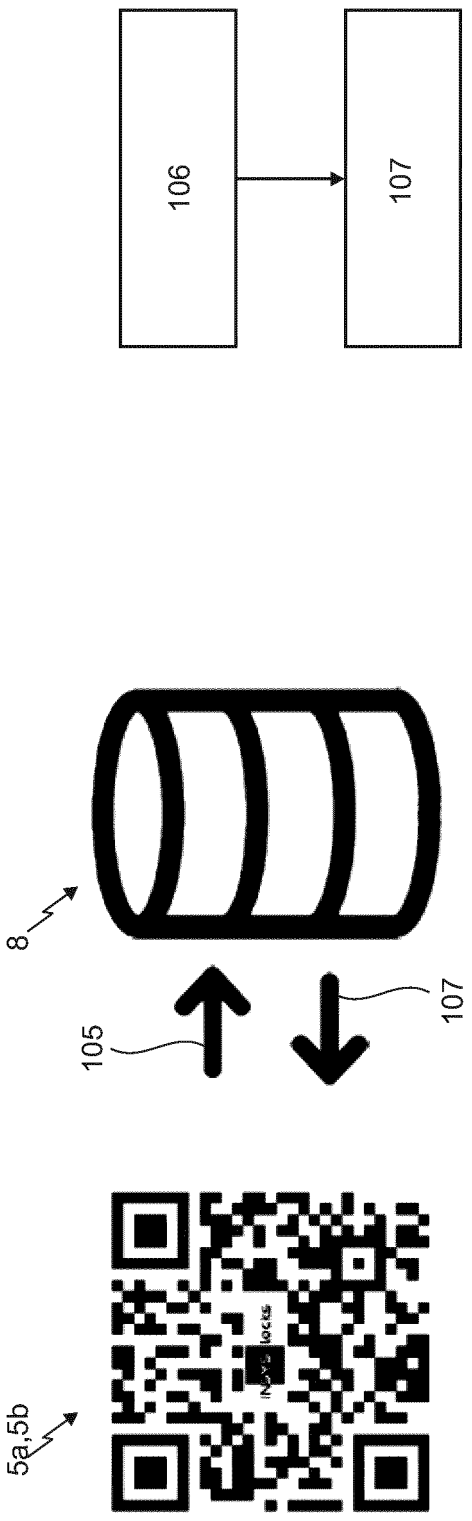
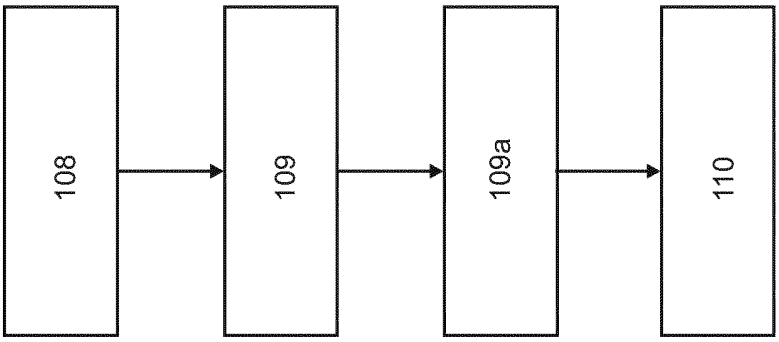
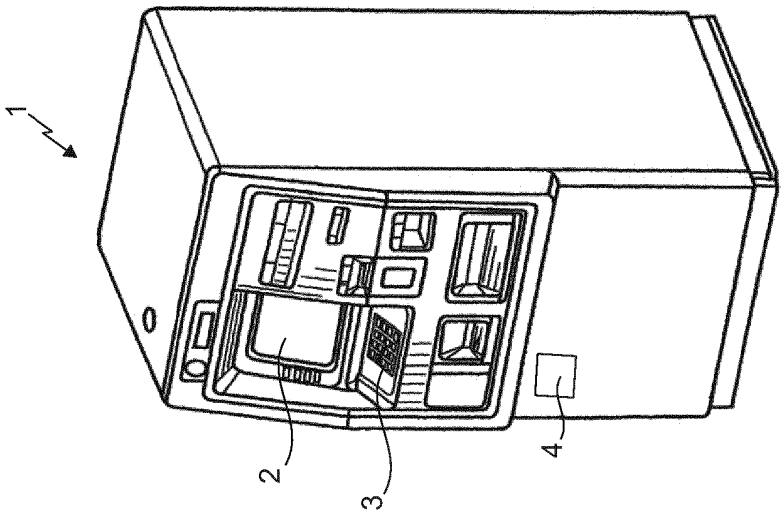


Fig. 4





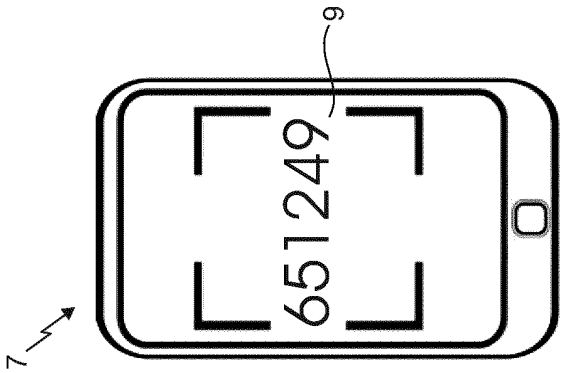
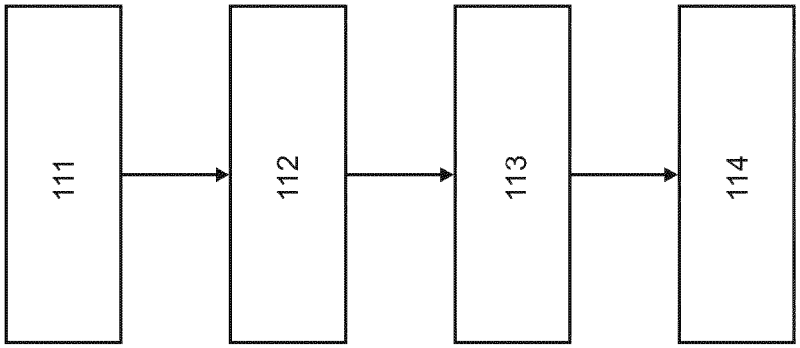
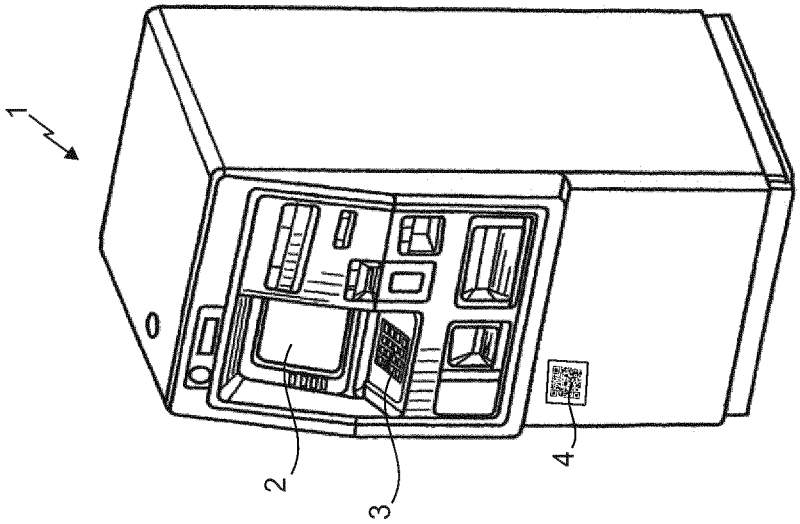


Fig. 5





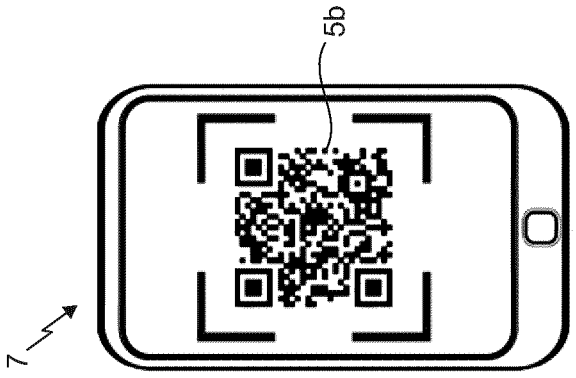


Fig. 6

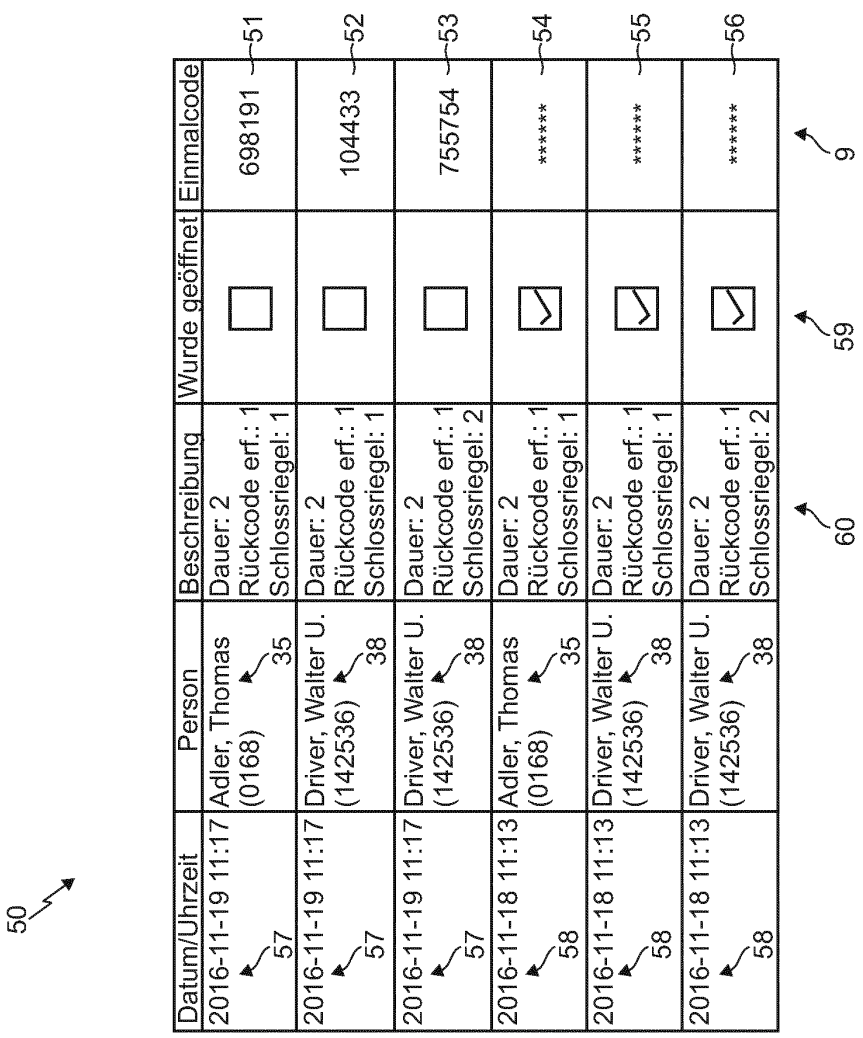

30
50
Feld
Wert
Neuer Wert
Transaktions-ID
- - -
13936
Beschreibung
- - -
Vorgang 1 Tour 1
Objekt
- - -
JZE: 081-32 | 11018586
Schlossriegel
- - -
1
Person
- - -
Adler, Thomas | 0168
Einmalcode
- - -
******
Schlossriegel
- - -
1
Person
- - -
Driver, Walter U. | 142536
Einmalcode
- - -
******
Schlossriegel
- - -
2
Person
- - -
Driver, Walter U. | 142536
Einmalcode
- - -
******
Datum Zeit
- - -
2016-11-18 11:13
Dauer
- - -
2
Rückcode erforderlich
- - -
1
31
32
33
34
35
36
37
38
39
40
38
41
42
43
44
Datum/Uhrzeit
Person
Beschreibung
Wurde geöffnet
Einmalcode
2016-11-19 11:17
57
Adler, Thomas (0168)
35
Dauer: 2 Rückcode erf.: 1 Schlossriegel: 1
698191
51
2016-11-19 11:17
57
Driver, Walter U. (142536)
38
Dauer: 2 Rückcode erf.: 1 Schlossriegel: 1
104433
52
2016-11-19 11:17
57
Driver, Walter U. (142536)
38
Dauer: 2 Rückcode erf.: 1 Schlossriegel: 2
755754
53
2016-11-18 11:13
58
Adler, Thomas (0168)
35
Dauer: 2 Rückcode erf.: 1 Schlossriegel: 1
******
54
2016-11-18 11:13
58
Driver, Walter U. (142536)
38
Dauer: 2 Rückcode erf.: 1 Schlossriegel: 1
******
55
2016-11-18 11:13
58
Driver, Walter U. (142536)
38
Dauer: 2 Rückcode erf.: 1 Schlossriegel: 2
******
56
60
59
9

Fig. 7

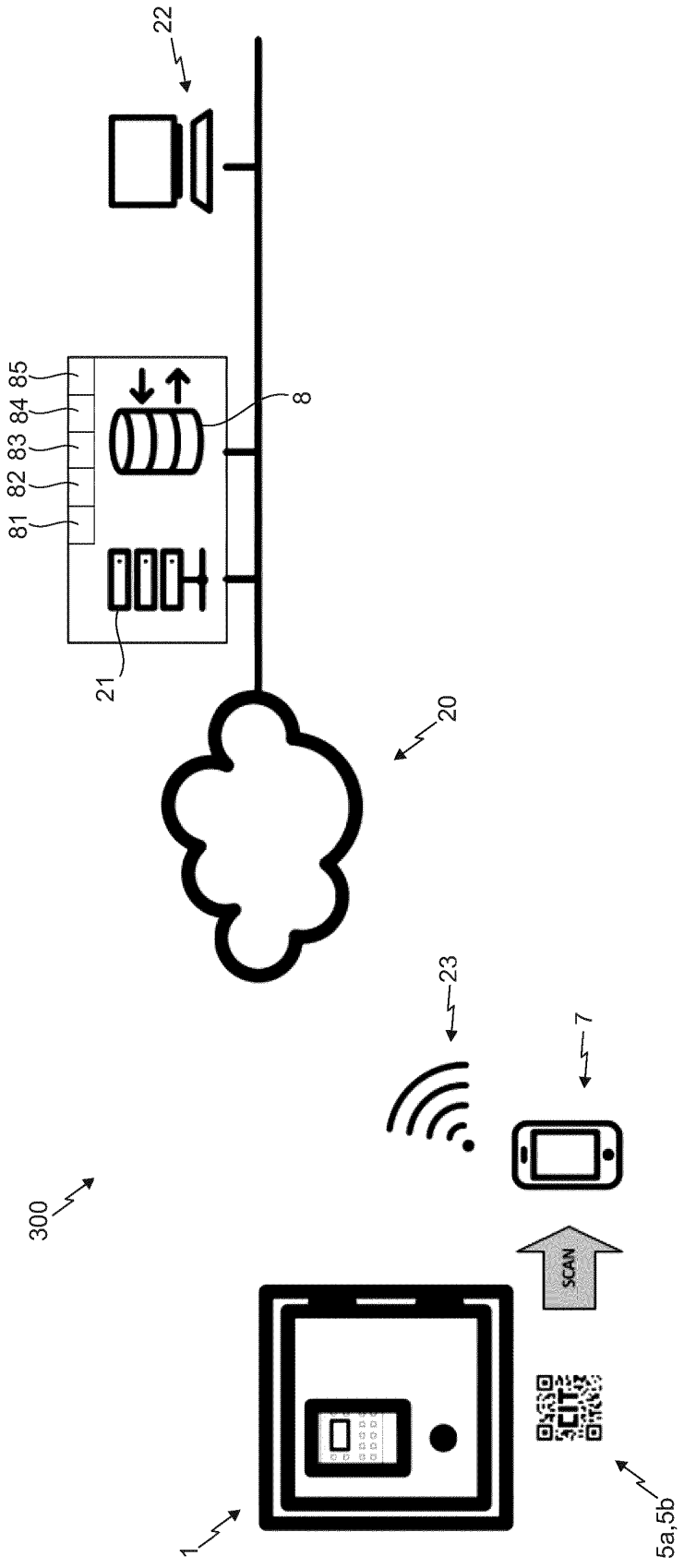


Fig. 8

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 2012229251 A1 **[0010]**
- US 2015102906 A1 **[0011]**
- US 2014375422 A1 **[0012]**
- DE 102012008395 A1 **[0013]**
- US 2016145904 A1 **[0014]**
- US 2013187756 A1 **[0015]**