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

(11) **EP 3 065 110 B1**

(12) **EUROPÄISCHE PATENTSCHRIFT**

(45) Veröffentlichungstag und Bekanntmachung des Hinweises auf die Patenterteilung:
28.08.2019 Patentblatt 2019/35

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

(21) Anmeldenummer: **16153262.7**

(22) Anmeldetag: **29.01.2016**

(54) **MODULARES HOCHSICHERHEITSSCHLOSS UND UPDATEVERFAHREN HIERFÜR**

MODULAR HIGH SECURITY LOCK AND UPDATE METHOD FOR SAME

VERROU MODULAIRE DE HAUTE SECURITE ET SON PROCEDE DE MISE A JOUR

(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: **03.03.2015 DE 102015103052**
13.11.2015 DE 102015119606

(43) Veröffentlichungstag der Anmeldung:
07.09.2016 Patentblatt 2016/36

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

(72) Erfinder:
- **Lücke, Detlef**
93164 Waldetzenberg (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:
EP-A2- 1 260 659
US-A1- 2010 057 703
US-A1- 2011 061 047
US-A1- 2012 216 726
US-B1- 7 234 636

EP 3 065 110 B1

Beschreibung

[0001] Die Erfindung betrifft ein modulares Hochsicherheitsschlosskonzept und speziell ein Hochsicherheitsschloss für ein Wertbehältnis gemäß dem Oberbegriff des Anspruchs 1.

[0002] Hochsicherheitsschlösser werden zum Beispiel für Geldautomaten bzw. Geldautomatenschränke verwendet. Dort sichern sie den Zugang zu den Geldfächern 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 autorisierter Benutzer bezeichnet) bekannt ist.

[0003] Eines oder mehrere dieser Schlösser befinden sich beispielsweise an der Hinterseite des Geldautomaten und sind somit für den Standard-Bankkunden nicht sichtbar. Zusätzlich sind sie meist durch zusätzliche Sicherheitsmaßnahmen unzugänglich angeordnet; so können sie zum Beispiel durch ein zusätzliches Blech abgedeckt sein. Nach erfolgreichem Passieren der Sicherheitsmaßnahmen kann der autorisierte Benutzer das Schloss bzw. die Schlösser öffnen und Geld nachfüllen bzw. entnehmen.

[0004] 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.

[0005] Die Schnittstellenfunktion wird zum Beispiel durch ein Bedienterminal (auch Bedieneinheit oder Bedienteil genannt) bzw. einer Eingabeeinheit als zweitem Modul oder Bedienmodul abgebildet.

[0006] 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.

[0007] Bei der Ausstattung der Geldautomaten und anderen Wertbehältnissen arbeiten die Hersteller generell mit einer hohen Anzahl von verschiedenen Hochsicherheitsschlosssystemen bzw. Schlosstypen unterschiedlicher Einbau- und Funktionsvielfalt. Dadurch entsteht ein hoher Pflege-, Logistik- bzw. Kostenaufwand. Es werden auch elektronische Hochsicherheitsschlosssysteme im Markt als Nachrüstungen vertrieben. Beim nachträglichen Einbau entstehen wiederum nicht unerhebliche Kosten für den Einbau, welche beispielsweise über externe Service-und Installationsdienstleister sowie über Wertdienstleister und Wachdienste an den Endkunden weitergegeben werden müssen. Bei der Herstellung der Geldautomaten wird seitens des Herstellers aus Kostengründen beispielsweise nur das Standardmodell des zweiten Moduls eingebaut, welches nur die geringste Anzahl an technischer Ausstattung bezogen auf seine Hardware und/oder Software aufweist.

[0008] Möchte ein Kunde erweiterte Funktionalitäten am Hochsicherheitsschlosssystem erst zu einem späteren Zeitpunkt einsetzen, ist die Nachrüstung oft schwierig. Stellt der Kunde im Betrieb beispielsweise fest, dass das eingebaute Modell seinen Anforderungen nicht gerecht wird, muss dieses notwendigerweise ausgetauscht werden. Allerdings bilden das erste und das zweite Modul gemäß derzeitigem Stand der Technik hinsichtlich des Aufbaus und/oder der Verdrahtung und/oder der Programmierung eine Einheit, d.h. dass diese nicht oder nur werksseitig bzw. beim Kunden mühsam und zeitintensiv voneinander getrennt werden können. Es muss also die komplette Einheit bestehend aus erstem und zweitem Modul ausgetauscht werden; auch wenn beispielsweise eigentlich nur die Software/Firmware des zweiten Moduls getauscht werden soll. Es versteht sich, dass eine derartige Vorgehensweise teuer und umständlich ist.

[0009] Dieser Austausch kann selbstverständlich wiederum nur nach Durchlauf verschiedener Sicherheitsmaßnahmen getätigt werden, die gleich bzw. ähnlich zu denen beim Öffnen des Geldfachs ausfallen können.

[0010] Beispielsweise offenbart die EP 1 260 659 A2 ein Schloss mit Display, Tastatur und Datenleitungsanschluss. Es ist beschrieben, dass Zusatzfunktionen des Schlosses nachträglich aktivierbar sind, indem diese entweder über den Anschluss installiert oder in einem nicht gezeigten Datenspeicher des Schlosses bereits zur Verfügung stehen und aktiviert werden.

[0011] Aus der US 2012/216726 A1 ist ebenfalls eine Möglichkeit bekannt, mittels einer Steuereinheit eines Geldautomats Zusatzfunktionen freischalten zu lassen. Dabei werden im Laufe des Verfahrens verschiedene Codes generiert, deren Zeichen unter anderem von der Seriennummer des Schlosses und dem freizuschaltenden Funktionsumfang abhängen. Auch die US 7 234 636 B1 offenbart Verfahren zur Steuerung des Funktionsumfangs eines Geldautomaten.

[0012] Gemäß der US 2010/057703 A1 und der US 2011/061047 A1 ist jeweils ein Lizenzmanagementsystem beschrieben.

[0013] Ziel der Erfindung ist es daher, ein Konzept zu entwickeln, den notwendigen Austausch so kostengünstig und so einfach wie möglich zu gestalten.

[0014] Diese Aufgabe wird durch ein Hochsicherheitsschloss (gemäß Anspruch 1) und ein Verfahren zur softwareseitigen Aktivierung oder Deaktivierung von Funktionen von Modulen eines Hochsicherheitsschlosses (gemäß Anspruch 5) gelöst.

[0015] Erfindungsgemäß ist das Hochsicherheitsschloss für ein Wertbehältnis dadurch gekennzeichnet, dass es mindestens ein mechanisch funktionierendes Schlossmodul und ein mit einer Datenempfangsschnittstelle ausgestattetes Bedienmodul umfasst. Das Schlossmodul und das Bedienmodul sind dafür einge-

richtet und dazu vorgesehen, elektronisch und mechanisch voneinander getrennt und/oder nach dem Plug-&-Play-Prinzip miteinander verbunden zu werden. Ferner umfassen das Schlossmodul und das Bedienmodul jeweils einen eigenen Programmspeicher mit vorinstallierten Unterprogrammen umfassen, welche Funktionen des Schlossmoduls und/oder des Bedienmoduls codieren. Dabei ist vorgesehen, dass die im Programmspeicher des Bedienmoduls vorinstallierten Unterprogramme nur die Funktionen des Bedienmoduls und die im Programmspeicher des Schlossmoduls vorinstallierten Unterprogramme nur die Funktionen des Schlossmoduls codieren. Ferner ist die Datenempfangsschnittstelle dafür eingerichtet und dazu vorgesehen, einen Funktionalitätscode und separat davon einen Lizenzkey an das Bedienmodul und das Schlossmodul zu übertragen. Außerdem umfassen das Schlossmodul und das Bedienmodul jeweils eine Auswerteeinheit. Beide Auswerteeinrichtungen sind dafür eingerichtet und dazu vorgesehen, einen Vergleich eines mittels eines Lizenzalgorithmus' erzeugbaren Vergleichslizenzkey mit dem Lizenzkey und eine Auswertung des Funktionalitätscodes durchzuführen und mindestens einen Bestätigungsdatensatz zur Freischaltung oder Sperrung mindestens eines Unterprogramms des Schlossmoduls an den Programmspeicher des Schlossmoduls und mindestens eines Unterprogramms des Bedienmoduls an den Programmspeicher des Bedienmoduls zu übertragen. Dabei ist der Lizenzkey ein Datensatz, welcher aus mindestens drei weiteren Datensätzen generiert ist, wobei unter den weiteren Datensätzen eine Seriennummer des Bedienmoduls, eine Seriennummer des Schlossmoduls und der Funktionalitätscode sind, wobei der Funktionalitätscode abhängig ist von den freizuschaltenden oder zu sperrenden Unterprogrammen in den Programmspeichern.

[0016] Damit ist es bei einem Hochsicherheitsschloss erstmals möglich, bei gleichbleibender Hardware unterschiedliche bzw. erweiterte Funktionsumfänge, insbesondere für das Bedienmodul und für das Schlossmodul freizuschalten. Im umgekehrten Fall können die Funktionsumfänge natürlich auch gesperrt werden. Ein umständlicher Ausbau beider Komponenten entfällt somit; der Austausch ist also wesentlich kostengünstiger als bisher.

[0017] Unterprogramme sind dabei als vorinstallierte Softwareblöcke bzw. Softwaremodule zu verstehen, welche vorteilhaft eine abgeschlossene funktionale Einheit der Betriebssoftware darstellen. Sie bestehen beispielsweise aus einer Folge von Verarbeitungsschritten und Datenstrukturen und stellen vorteilhaft eine Funktion oder Unterfunktion dar. Sie können beispielsweise über eine modulspezifische Schnittstelle aufgerufen werden. Die genaue Vorgehensweise beim Abspeichern und Aufrufen von Unterprogrammen ist allerdings aus dem Stand der Technik bestens bekannt und wird vorliegend nicht weiter erörtert.

[0018] Es ist wie oben erwähnt vorgesehen, dass die im Programmspeicher des Bedienmoduls vorinstallierten Unterprogramme nur die Funktionen des Bedienmoduls codieren. Analog dazu ist wie oben erwähnt vorgesehen, dass die im Programmspeicher des Schlossmoduls vorinstallierten Unterprogramme nur die Funktionen des Schlossmoduls codieren. Eine Ausführungsform, wonach die im Programmspeicher des Bedienmoduls vorinstallierten Unterprogramme die Funktionen des Bedienmoduls und des Schlossmoduls codieren, ist demnach nicht Teil der vorliegenden Erfindung. Ebenfalls ist eine Ausführungsform, wonach die im Programmspeicher des Bedienmoduls vorinstallierten Unterprogramme die Funktionen des Bedienmoduls und des Schlossmoduls codieren, nicht Teil der vorliegenden Erfindung.

[0019] Je nach Anforderung bzw. Kundenwunsch können nämlich verschiedene Schlossmodule und Bedienmodule zum Einsatz kommen.

[0020] Beim zweiten Modul ist es beispielsweise denkbar, dass es als Bedienterminal ähnlich wie bei einem ec-Kartenlesegerät ausgebildet ist und somit zumindest einen Ziffernblock umfasst, mittels dem beispielsweise ein Sicherheitscode eingegeben werden kann. Es gibt zweite Module ohne Display bzw. Touchscreen; allerdings ist vorteilhaft am zweiten Modul zusätzlich ein Display und/oder ein Touchscreen angeordnet. Die zweiten Module können sich also untereinander bezüglich der Hardware und/oder der Software/Firmware unterscheiden.

[0021] Als Sicherheitsmaßnahmen zum Öffnen des Hochsicherheitsschlosses kommen beispielsweise das Öffnen mit einem bestimmten Schlüssel, die Eingabe einer PIN bzw. eines Sicherheits- bzw. Einmalcodes oder die Nutzung von Tags oder RFID (engl. "radio-frequency identification", "Identifizierung mit Hilfe elektromagnetischer Wellen") in Form einer dem autorisierten Benutzer eigenen RFID-Karte in Frage. Darüber hinaus kann zusätzlich die Eingabe des Codes erst nach einer bestimmten Zeitspanne nach einer durchgeführten Aktion und dann nur für eine bestimmte Zeitspanne möglich sein. Beispielsweise ist es denkbar, dass der autorisierte Benutzer sich dem Automaten gegenüber identifiziert und den eigentlichen Sicherheitscode erst 10 Minuten nach der erfolgreichen Identifikation eingeben kann, wobei der Code aber wiederum 5 Minuten später seine Gültigkeit verliert. Weiterhin kann die Anzahl der zugelassenen autorisierten Benutzer begrenzt und/oder ein Masterbenutzer zugewiesen sein. Manche Hochsicherheitsschlösser (im Folgenden auch Schlösser genannt) verfügen zusätzlich über einen Netzwerkzugang bzw. über eine Alarmfunktion bei unautorisiertem Zugang, wobei vorteilhaft eine Überfallmeldung und anschließend eine Sperrung des Geldautomaten durch eine geeignete Sperreinrichtung erfolgen. Weiterhin ist es vorteilhaft, wenn Details des Zugangs wie Uhrzeit, Ort, Benutzer-ID usw. protokolliert werden. Das Verschließen des Geldautomaten, also das Verriegeln des mindestens einen Sicherungselementes nach Befüllen der Geldfächer kann manuell, bevorzugt allerdings automatisch erfolgen. Es sind auch Kombinationen aus den genannten Sicherheitsmaßnah-

men und/oder -ausstattungen möglich. Vorteilhaft ist die Software des Schlosses so programmiert, dass automatisch nach Voreinstellung beispielsweise abhängig von der Tageszeit unterschiedliche Programmmodule geladen werden und/oder abrufbar sind.

[0022] Die Spannungsversorgung der Schlösser bzw. Hochsicherheitsschlösser bzw. des Schlossmoduls und/oder des Bedienmoduls kann über den Geldautomaten erfolgen. Alternativ oder zusätzlich kann eine Batterieversorgung vorgesehen sein. Vorteilhaft ist das Schloss im Online- und im Offlinebetrieb nutzbar. Zur Konfiguration der Schlosseinheiten ist bevorzugt für alle Varianten, insbesondere für alle zweiten Module eine einheitliche Konfigurationssoftware verwendbar. Die Programmierung kann vorteilhaft über einen PC und/oder einen Laptop oder über mobile Endgeräte wie Smartphones und/oder Tablets erfolgen.

[0023] Gemäß einer bevorzugten Ausführungsform ist beim Hochsicherheitsschloss das erste Modul mit allen verfügbaren zweiten Modulen kompatibel. Diese Kompatibilität bezieht sich auf die Elektronik bzw. die Software und die Mechanik bzw. Hardware. Sollte also tatsächlich ein Austausch einzelner Module, insbesondere des zweiten Moduls notwendig sein, kann idealerweise dieser Austausch nach dem Plug & Play-Prinzip (PnP) erfolgen, das heißt, dass zur Inbetriebnahme der Schlosseinheit nach Hardware-Austausch des zweiten Moduls keine weiteren Treiber installiert oder Einstellungen vorgenommen werden müssen. Insofern kann nun der autorisierte Benutzer direkt vor Ort am Geldautomaten, welcher in Betrieb ist und dementsprechend beispielsweise in einem Geldinstitut steht, das notwendige Upgrade durchführen, indem er das derzeitige zweite Modul elektronisch und mechanisch vom ersten Modul trennt und anschließend ein neues zweites Modul einbaut und mit dem ersten Modul mechanisch und elektronisch verbindet.

[0024] Insofern ist es wie oben erwähnt vorgesehen, dass das Schlossmodul und das Bedienmodul elektronisch und/oder mechanisch voneinander trennbar und/oder nach dem Plug-&-Play-Prinzip miteinander verbindbar sind.

[0025] Wenn nur die Firmware bzw. Software getauscht bzw. deren Umfang erweitert werden muss, ist es denkbar, dass aus Zeitgründen dennoch ein neues zweites Modul mit vorinstallierter Firmware eingebaut wird. Wesentlich kostengünstiger ist jedoch, wenn auf das derzeitige zweite Modul vor Ort eine neue Firmware aufgespielt wird.

[0026] Die meisten Vorteile bietet jedoch schließlich die Vorgehensweise, wenn die neue Firmware bereits auf dem derzeitigen zweiten Modul blockiert vorhanden ist und nur freigeschalten werden muss, wie oben beschrieben. Dafür ist beispielsweise mindestens die Eingabe eines Lizenzkeys, also einem Buchstaben- oder Zahlencode, notwendig, wie oben beschrieben.

[0027] Gemäß einer bevorzugten Ausführungsform umfassen das Schlossmodul und das Bedienmodul jeweils mindestens eine der folgenden Einheiten: die Auswerteeinheit, eine Datenverschlüsselungseinheit, eine Datenübertragungseinheit und eine Datenspeichereinheit.

[0028] Mittels der Auswerteeinheit bzw. der Auswerteeinrichtung sind Daten verarbeitbar und Signale bzw. Datensätze an eine andere Einheit sendbar. Die Art der Verarbeitung bzw. des Sendens von Datensätzen durch die Auswerteeinrichtung kann zum Beispiel mittels eines Programms oder Software vorbestimmt werden. Die Auswerteeinrichtung kann beispielsweise in Form eines Prozessors (Central Processing Unit, CPU) vorliegen.

[0029] Mittels der Datenverschlüsselungseinheit sind, beispielsweise mittels eines Algorithmus, Datensätze verschlüsselbar, um so zu einer erhöhten Sicherheit beizutragen. Sie kann beispielsweise durch die Auswerteeinheit bzw. einen Teil der Auswerteeinheit ausgebildet werden. Alternativ kann die Datenverschlüsselungseinheit mittels einer von der Auswerteeinheit separaten Einheit ausgebildet sein.

[0030] Mittels der Datenübertragungseinheit sind Datensätze, welche beispielsweise verschlüsselt vorliegen, von einer Einheit zu einer anderen bzw. von einem Modul zum anderen übertragbar. Sie kann beispielsweise in Form eines Datenübertragungskabels zusammen mit den entsprechenden Schnittstellen vorliegen.

[0031] Mittels der Datenspeichereinheit sind Datensätze abspeicherbar. Die Datenspeichereinheit kann beispielsweise in Form eines EPROMS (Erasable Programmable Read-Only Memory), EEPROMS (Electrically Erasable Programmable Read-Only Memory) oder eines Flashspeichers vorliegen.

[0032] Aus dem Stand der Technik sind weitere Details zum Einsatz und Funktion von Auswerteeinheiten, Datenverschlüsselungseinheiten, Datenübertragungseinheiten und auch Datenspeichereinheiten bestens bekannt und werden daher hier nicht weiter erörtert.

[0033] Insgesamt wird ein Schloss erhalten, welches mittels eines intelligenten Upgrade-Verfahrens bereits bei der Erstausstattung im Werk oder später beim Kunden funktionserweiterbar ist. Gleichzeitig kann als erstes Modul ein Standard-Schlossriegel bzw. Standard-Schlossmodul verwendet werden, das ab Werk immer eingebaut wird und bei Funktionserweiterungen im Feld nicht mehr getauscht werden muss. Dieses Schlossmodul erfüllt vorteilhaft gleichzeitig auch alle gängigen Sicherheitsanforderungen wie den Normen sowie der sachgerechten Umrüstungsvorschriften nach VdS und ECB-S, welche jeweils Hinweise zu den festgelegten Sicherheitsstufen für Tresore geben. Es sei in diesem Zusammenhang erwähnt, dass eine unsachgerechte Umrüstung im schlimmsten Fall zum Verlust des Versicherungsschutzes für den Tresor bzw. für dessen Inhalt führen kann. Dies kommt natürlich vor allem dann zum Tragen, wenn nach erfolgter, unsachgerechter Umrüstung der Inhalt des Tresors bzw. Geldautomats etwa bei einem Diebstahl widerrechtlich entwendet wird.

[0034] Weiterhin kann vorteilhaft auf bewährte Technik

beim Schlossriegel als erstem Modul zurückgegriffen werden.

[0035] Ein weiterer Vorteil ist, dass bereits im Werk und beim Geldautomaten-/Tresorhersteller die Variantenvielfalt eingedämmt wird, wodurch eine enorme Kostenersparnis möglich ist. Da hohe Demontage- und Montagekosten vor Ort entfallen, kann der Preisvorteil direkt an den Kunden weitergegeben werden, wodurch sich vorteilhaft die Anzahl der Nachrüstaufträge für den Hersteller erhöhen dürfte. Dies stärkt wiederum die Kundenbindung und erhöht den Marktanteil.

[0036] Insgesamt können durch das intelligente Schlosskonzept neue und interessantere Kostenmodelle für Software und Wartungsverträge entwickelt werden. Außerdem sinkt die Abhängigkeit von zertifizierten Tresortechnikern für die Umrüstung, wodurch die Flexibilität erhöht wird.

[0037] Ein wesentliches Prinzip der vorliegenden Erfindung ist, dass vorteilhaft im Schlossriegel bzw. Schlossmodul des elektronischen Hochsicherheitsschlosses alle derzeit bekannten und notwendigen Funktionalitäten für den aktuellen und zukünftigen Betrieb bereits softwaremäßig in modularen Blöcken codiert und hinterlegt sind; jedoch sind nicht alle Blöcke, sondern beispielsweise nur die zum derzeitig aktuellen Funktionsumfang bzw. Betrieb notwendigen Blöcke bereits aktiviert.

[0038] Gleichzeitig sind in der Bedieneinheit bzw. im Bedienmodul des elektronischen Hochsicherheitsschlosses ebenso alle derzeit bekannten und gängigen Funktionalitäten und Prozesse der Kundenanwendungen des Marktes softwaremäßig in modularen Blöcken codiert und hinterlegt; auch hier sind jedoch nur die Blöcke aktiviert, die zum derzeitig aktuellen Funktionsumfang notwendig sind.

[0039] Dieser Funktionsumfang wird durch das jeweils aktuell verwendete zweite Modul bestimmt.

[0040] Das Freischalten der notwendigen Funktionalitäten bzw. Softwareblöcke wird über die Berechnung und Eingabe eines sicheren Lizenzkeys an der Bedieneinheit vollzogen. Der Lizenzkey wird auf Kundenanforderung unter Angabe von gerätespezifischen Daten, wie Seriennummer der Bedieneinheit und Seriennummer des intelligenten Schlossriegels automatisiert erstellt und dem Kunden übermittelt. Alternativ kann sich der Kunde auf der Website des Herstellers des intelligenten Schlossriegels in einem persönlichen Bereich einloggen und die erforderlichen Daten eingeben, woraufhin ein Lizenzkey automatisiert erzeugt wird. Aus Sicherheitsgründen ist es vorteilhaft, wenn dem Hersteller diese Generierungsabfrage anschließend per E-Mail mitgeteilt wird.

[0041] Zusätzlich ist zur Berechnung des Lizenzkeys vorteilhaft ein Funktionalitätscode notwendig, der abhängig ist von dem Upgradeprozess, der im speziellen Fall durchgeführt werden soll, und somit abhängig von den freizuschaltenden Funktionsblöcken im Programmspeicher.

[0042] Es ist also vorgesehen, dass der Lizenzkey ein Datensatz ist, welcher aus mindestens drei weiteren Datensätzen generiert ist, wobei unter den weiteren Datensätze eine Seriennummer des Bedienmoduls, eine Seriennummer des Schlossmoduls und der Funktionalitätscode sind.

[0043] Die Datenempfangsschnittstelle des Bedienmoduls kann dabei zum Beispiel eine Tastatur oder ein Touchscreen sein, mittels welcher eine manuelle Eingabe der Daten bzw. Datensätze möglich ist. Es ist aber insbesondere vorteilhaft, wenn die Schlosseinheit bzw. das Hochsicherheitsschloss am ersten und/oder am zweiten Modul mindestens eine Kommunikationsschnittstelle aufweist. Denkbar ist hier vor allem ein USB-Anschluss, aber auch die Nutzung der Bluetooth-Funktion oder eine Infrarotschnittstelle sind möglich. Vorteilhaft ist am ersten und/oder am zweiten Modul mindestens eine der folgenden Funktionen hardwaremäßig realisiert: Funktionen aus dem Bereich Near Field Communication (NFC), RFID oder die eines integrierten Schaltkreises wie dem "iButton". Somit ist unter dem Ausdruck "Datenempfang" das Empfangen von Daten mittels einer manuellen Eingabe, aber auch mittels einer elektronischen Übermittlung zu verstehen.

[0044] Es ist also vorteilhaft, wenn die Datenempfangsschnittstelle eine Einrichtung zur manuellen Eingabe von Datensätzen oder eine elektronische Schnittstelle zur drahtgebundenen Übermittlung von Datensätzen oder eine elektronische Schnittstelle zur drahtlosen Übermittlung von Datensätzen ist.

[0045] Zur Erhöhung der Sicherheit ist es weiterhin vorteilhaft, wenn im Schlossmodul ein Supervisorcode hinterlegbar ist, welcher mittels der Auswerteeinrichtung mit einem mittels der Datenempfangsschnittstelle an das Bedienmodul und das Schlossmodul übertragbaren Supervisorcode vergleichbar ist. Dabei ist anzumerken, dass auch bei einem Tausch des Bedienmoduls, wie er oben beschrieben ist, der im Schlossmodul abgespeicherte Supervisorcode vorteilhaft gleich bleiben kann, was den Aufwand bei der Datenverwaltung reduziert.

[0046] Die Aufgabe der Erfindung wird weiterhin gelöst von einem Verfahren zur softwareseitigen Aktivierung oder Deaktivierung von Funktionen von Modulen eines Hochsicherheitsschlosses für ein Wertbehältnis, wobei das Hochsicherheitsschloss mindestens ein mechanisch funktionierendes Schlossmodul und ein mit einer Datenempfangsschnittstelle ausgestattetes Bedienmodul umfasst. Das Schlossmodul und das Bedienmodul umfassen jeweils einen eigenen Programmspeicher mit vorinstallierten Unterprogrammen, welche die Funktionen codieren. Es ist ferner erfindungsgemäß vorgesehen, dass das Schlossmodul und das Bedienmodul dafür eingerichtet und dazu vorgesehen sind, elektronisch und mechanisch voneinander getrennt und/oder nach dem Plug-&-Play-Prinzip miteinander verbunden zu werden, und dass die im Programmspeicher des Bedienmoduls vorinstallierten Unterprogramme nur die Funktionen des Bedienmoduls und die im Programmspeicher des Schlossmoduls vorinstallierten Unterprogramme nur die Funkti-

onen des Schlossmoduls codieren. Außerdem umfassen das Schlossmodul und das Bedienmodul jeweils eine Auswerteeinheit.

[0047] Das erfindungsgemäße Verfahren weist die folgende Verfahrensschritte auf:

a) Eingabe eines Funktionalitätscodes, welcher abhängig ist von freizuschaltenden oder zu sperrenden Unterprogrammen in den Programmspeichern, und separat davon Eingabe eines Lizenzkeys an der Datenempfangsschnittstelle, wobei der Lizenzkey ein Datensatz ist, welcher aus mindestens drei weiteren Datensätzen generiert wird, wobei unter den weiteren Datensätzen eine Seriennummer des Bedienmoduls, eine Seriennummer des Schlossmoduls und der Funktionalitätscode sind,
b) Vergleich eines mittels eines Lizenzalgorithmus' erzeugbaren Vergleichslizenzkeys mit dem Lizenzkey mittels beider Auswerteeinrichtungen,
c) Auswertung des Funktionalitätscodes mittels beider Auswerteeinrichtungen,
d) Übertragung mindestens eines Bestätigungsdatensatzes an den Programmspeicher des Schlossmoduls und an den Programmspeicher des Bedienmoduls, wenn Schritt b) eine Übereinstimmung der verglichenen Datensätze ergibt,
e) Freischaltung oder Sperrung mindestens eines Unterprogramms des Schlossmoduls und mindestens eines Unterprogramms des Bedienmoduls.

[0048] Die Sicherheit wird erhöht, wenn bestimmte Verfahrensschritte nicht nur im Bedienmodul bzw. im Schlossmodul, sondern auch im jeweils anderen Modul durchgeführt werden. Es ist also wie oben erwähnt vorgesehen, dass alle drei der Schritte b), c) und d) in beiden der Module ausgeführt werden. Es ist außerdem vorteilhaft, wenn die Ausführung der Schritte jeweils in der Reihenfolge b), c) und d) aufeinander folgt und/oder die Ausführung der Schritte b), c) und/oder d) zunächst im Schlossmodul und dann im Bedienmodul erfolgt.

[0049] Weiterhin erhöht sich die Sicherheit des Verfahrens, wenn zeitlich vor Schritt a) in einem Schritt a0) eine Eingabe eines Supervisorcodes erfolgt, welcher in einem Schritt a2) vor Schritt b) mittels der Auswerteeinrichtung mit einem im Schlossmodul gespeicherten weiteren Datensatz verglichen wird.

[0050] Es ist wie oben erwähnt vorgesehen, dass der Lizenzkey ein Datensatz ist, welcher aus mindestens drei weiteren Datensätzen generiert wird, wobei unter den weiteren Datensätzen eine Seriennummer des Bedienmoduls, eine Seriennummer des Schlossmoduls und den Funktionalitätscode sind.

[0051] Dabei kann die Eingabe der Datensätze in Schritt a) und/oder Schritt a0) drahtgebunden wie über eine Hardwareschnittstelle oder drahtlos wie mittels Funkübertragung erfolgen.

[0052] Vorteile und Zweckmäßigkeiten sind der nachfolgenden Beschreibung in Verbindung mit der Zeichnung zu entnehmen.

[0053] Es zeigen:

Fig. 1 einen Geldautomaten in einer schematischen Darstellung;

Fig. 2a in einer schematischen Darstellung die Zugangstür für die Geldfächer des Geldautomaten gemäß Fig. 1;

Fig. 2b eine einzelne Schließeinheit wie gemäß Fig. 2a verwendet;

Fig. 3a Hardwarekomponenten eines Standardmodells des zweiten Moduls;

Fig. 3b Hardwarekomponenten eines erweiterten Modells des zweiten Moduls;

Fig. 4 eine Übersicht beispielhaft verfügbarer zweiter Module mit erstem Modul

Fig. 5 den Ablauf der Generierung des Lizenzkeys;

Fig. 6 einen Überblick über den Gesamt-Upgradeprozess;

Fig. 7 einen ersten Teilprozess des Gesamt-Upgradeprozesses;

Fig. 8 einen zweiten Teilprozess des Gesamt-Upgradeprozesses.

[0054] In Fig. 1 ist in einer perspektivischen Darstellung ein Geldautomat 1 abgebildet, wie er beispielsweise in einem Geldinstitut zum Abheben von Geldbeträgen den Bankkunden zur Verfügung steht. Das Bedienterminal für den Bankkunden mit Fach zum Einführen der ec-Karte, der Ziffernblock zum Eingeben der PIN sowie das Display zum Eingeben weiterer Funktionen sind hier wie üblich an der Vorderseite 1a des Geldautomaten angeordnet und spielen für die weitere Erfindung keine Rolle. Die Rückseite 1b des Geldautomaten 1 ist in Fig. 1 nicht zu sehen. Allerdings ist denkbar, dass dort beispielsweise ein bzw. zwei erfindungsgemäße Hochsicherheitsschlösser angeordnet sind. Die Schlosssysteme können je nach Ausführungsform des Geldautomaten 1 auch auf der Vorderseite 1a unter einer Abdecktür angebracht sein.

[0055] Eine mögliche Konfiguration einer Rückseite 1b des Geldautomaten 1 zeigt Fig. 2a. Dort ist eine Tür 2 mit Türgriff 2a zu sehen, welche mit zwei Schließeinheiten 6 als ersten Modulen 3 ausgestattet ist und mit diesen den Zugang zu den Geldfächern sichert. Die mechanische und/oder elektronische Anbindung der Schließeinheiten 6 an der Tür 2 ist hier lediglich beispielhaft veranschaulicht. Vorliegend sind die Schließeinheiten 6 als intelligente Schlossriegel 6 ausgebildet.

[0056] Fig. 2b zeigt die Schließeinheit 6 gemäß Fig. 2a in vergrößerter Darstellung. Ein elektronisches Hochsicherheitsschlosssystem besteht unter anderem aus einer Eingabeeinheit (siehe Bedienteil 5 gemäß Fig. 3a/3b), mindestens einer Auswerteeinheit 18a und einer Betätigungseinheit 17 (Riegelelement). Eine Auswerteeinheit 18a und die Betätigungseinheit 17 sind beispielsweise in dem Schlossriegel 6 zusammengefasst, weshalb dieser auch als intelligenter Schlossriegel 6 bezeichnet wird. Vorliegend kann beispielsweise mittels einer Verlagerung der Betätigungseinheit 17 die Tür 2 entriegelt und verriegelt werden. Allerdings spielen weder die Mechanik dieses Schlossriegels 6 bzw. der Betätigungseinheit oder des Riegelelements 17 noch die Abfolge der Schritte, welche das Verschließen und das Öffnen der Tür 2 erlauben, für die vorliegende Erfindung eine Rolle. Sie erfahren daher in der weiteren Beschreibung keine weitere Beachtung.

[0057] Die Figuren 3a und 3b zeigen verschiedene zweite Module 4, welche die Schnittstellenfunktion zum Benutzer abbilden und vorliegend jeweils als Bedienterminal bzw. Bedieneinheit 5 ausgebildet sind. Fig. 3a zeigt das Standardmodell 7a des zweiten Moduls 4, welches über einen Ziffernblock 8 mit Zifferntasten 8a (hier anhand einer Zifferntaste beispielhaft gekennzeichnet), eine Bestätigungstaste 8b und eine Löschtaste 8c verfügt. Fig. 3b zeigt ein erweitertes Modell des zweiten Moduls 4, welches zusätzlich zu den beim Standardmodell 7a vorhandenen Elementen 8, 8a, 8b, 8c über ein Display 9 und Scroll- bzw. Cursortasten 8d verfügt, mittels welchen ein Benutzermenü abrufbar und mittels des Displays 9 anzeigbar ist. Die Hardwareausstattung des in Fig. 3b abgebildeten erweiterten Modells entspricht damit der Hardwareausstattung der Modelle 7b, 7c und 7d.

[0058] In Fig. 4 sind beispielhaft vier zweite Module 4 als Modelle 7a, 7b, 7c, 7d gezeigt, wobei die Module 7b, 7c, 7d jeweils die gleiche Hardwareausstattung zeigen, sich hinsichtlich ihrer Softwareausstattung jedoch unterscheiden. Beispielsweise weisen die Modelle bzw. Module von 7a bis 7d ansteigende Funktionalitäten auf. Das Modul 7a ist beispielsweise werksseitig verbaut. Um Modul 7a gegen Modul 7b auszutauschen, mithin ein Upgrade 10a von Modell 7a auf 7b durchzuführen, ist somit ein Tausch der gesamten Tastatur bzw. des Ziffernblocks 8 notwendig. Dahingegen erfordert ein Tausch des Moduls 7b gegen 7c oder 7d bzw. 7c gegen 7d (Upgrade mittels Pfeil 10b1 bzw. 10b2 bzw. 10b3 dargestellt) nur jeweils ein Softwareupgrade mit Hilfe eines Lizenzkeys 15 (siehe Fig. 5). Das gezeigte erste Modul 3 kann jedoch in Kombination mit allen vier gezeigten zweiten Modulen 7a, 7b, 7c, 7d verwendet werden.

[0059] Fig. 5 veranschaulicht die Generierung 100 eines Lizenzkeys 15. Hierfür werden die Daten bezüglich der Seriennummer 12 des intelligenten Schlossriegels 6, der Seriennummer 13 der Bedieneinheit 5 sowie ein Funktionalitätscode 14 kombiniert (Schritt 101) und mittels Anwendung eines geeigneten Lizenzalgorithmus ein beispielsweise 8-stelliger Lizenzkey 15 generiert (Schritt 102).

[0060] Fig. 6 beschreibt den gesamten Upgradeprozess 200 zum Beispiel von Modell 7b auf 7c in einzelnen Verfahrensschritten 201 bis 214, wobei die einzelnen Schritte in einer bevorzugten zeitlichen Reihenfolge abgebildet sind. Wie bereits oben erwähnt, muss bei diesem Upgradeprozess kein Tausch des Bedienteils 5 erfolgen, sondern nur eine Freischaltung codierter Softwareblöcke 36a, 36b, 36c bzw. 46a, 46b, 46c.

[0061] Zum Start des Upgradeprozesses 200 gibt der autorisierte Benutzer an der Bedieneinheit 5 in einem bestimmten Menüpunkt des Bedienmenüs den Supervisorcode 57 (Schritt 201) und anschließend den Funktionscode 14 und den Lizenzkey 15 ein (Schritt 202). Eine Aufforderung zur Eingabe dieser Daten 57, 14 und/oder 15 kann beispielsweise auf dem Display 9 angezeigt werden. Diese Daten werden in der Bedieneinheit 5 zwischengespeichert sowie verschlüsselt (Schritt 203) und im Schritt 204 verschlüsselt an den Schlossriegel 6 übertragen. Dieser entschlüsselt die Daten (Schritt 205), wertet den Supervisorcode aus (Schritt 206) und vergleicht den berechneten Lizenzkey mit dem empfangenen Lizenzkey (Schritt 207). Ist dieser Vergleich zufriedenstellend, wird der bzw. werden die entsprechenden Funktionsblöcke freigeschalten (Schritt 208). Es erfolgt eine Bestätigung der Freischaltung (Schritt 209) sowie eine Verschlüsselung der Daten (Schritt 210). Die verschlüsselten Daten werden dann an die Bedieneinheit 5 übertragen (Schritt 211) und dort entschlüsselt (Schritt 212). Anschließend wird der entsprechende Funktionsblock im Bedienteil 5 freigeschalten (Schritt 213), womit der Upgradeprozess abgeschlossen ist (mit 214 veranschaulicht).

[0062] In jedem intelligentem Schlossriegel 6 ist mind. ein sogenannter Supervisorcode 39 für das Aktivieren der neuen Funktionsblöcke 36a, 36b, 36c (siehe Fig. 7) im Schlossriegel 6 bzw. 46a, 46b, 46c (siehe Fig. 8) in der Bedieneinheit 5 hinterlegt. Diese Supervisorcodes 39 können bei der Installation eines Systems durch den Bediener bzw. den autorisierten Benutzer verändert werden. Durch die Tatsache, dass nur die Bedieneinheit 5 getauscht werden muss, kann der Code 39 jedoch vorteilhaft gleich bleiben.

[0063] Fig. 7 veranschaulicht einen Teilprozess 200a des Upgradeprozesses 200 gemäß Fig. 6 sowie die Beteiligung verschiedener Einheiten beim Ablauf der Freischaltung der Funktionsblöcke 36a, 36b, 36c im Programmspeicher 36 des intelligenten Schlossriegels 6. Die im Schritt 203 verschlüsselten Daten 31 werden gemäß Schritt 204 an eine Empfangseinrichtung 32 des Schlossriegels 6 übertragen und gemäß Schritt 204a an die Entschlüsselungseinrichtung 33 übertragen. Dort werden die Daten 31 in Klartext 40a entschlüsselt (Schritt 205), wodurch sie sich wieder mit dem empfangenen Lizenzkey 15 und dem Funktionalitätscode 14 vergleichen lassen. Anschließend werden die Klartextdaten 40a im Schritt 205b an die Auswerteeinrichtung 18a übertragen. Mittels des implementierten Lizenzgenerators 37a wird

ein Vergleichslizenzkey 38a berechnet (Schritt 205a) und im Schritt 205c an die Auswerteeinrichtung 18a übertragen. Ebenfalls wird ausgehend vom Codespeicher 34 der Supervisorcode 39 an die Auswerteeinrichtung 18a übertragen (Schritt 205d). In der Auswerteeinrichtung 18a werden die empfangenen Daten 38a, 39, 40a bzw. 38a, 39, 14, 15 auf Basis der im intelligenten Schlossriegel 6 gespeicherten gerätespezifischen Daten aufbereitet und verglichen. Stimmt der aktuell berechnete Lizenzkey 38a mit dem empfangenen, entschlüsselten Lizenzkey 15 überein, wird der entsprechende Softwarefunktionsblock (hier drei Blöcke 36a, 36b, 36c) im Programmspeicher 36 über eine Übertragung eines oder mehrerer Bestätigungsdatensätze 48a, 48b, 48c bzw. -signale von der Auswerteeinheit 18a an den Programmspeicher 36 dauerhaft freigeschaltet.

[0064] Die Bestätigung der Freischaltung wird anhand von Bestätigungsdaten 41 verschlüsselt an die Bedieneinheit 5 zurückgesendet (siehe Fig. 8). Diese Daten 41 werden von einer Empfangseinrichtung 42 des Bedienteils 5 im Schritt 210a empfangen bzw. im Schritt 211 verschlüsselt an eine Entschlüsselungseinrichtung 43 der Bedieneinheit 5 übertragen. Die restlichen folgenden Schritte erfolgen jeweils analog zu denen aus Fig. 7, wobei allerdings jeweils der Bedieneinheit 5 zugeordnete separate Einheiten wie Auswerteeinrichtung 18b oder Lizenzgenerator 37b verwendet werden: 212 analog zu 205, 212a analog zu 205a, 212b analog zu 205b (mit Klartextdaten 40b), 212c analog zu 205c, 212d analog zu 207, 213 analog zu 208. Es ist davon auszugehen, dass der Lizenzkey 38a dem Lizenzkey 38b entspricht. In der Bedieneinheit 5 wird also im gleichen Zuge die neue Funktionalität entsprechend freigeschalten (über eine Übertragung eines oder mehrerer Bestätigungsdatensätze 49a, 49b, 49c bzw. -signale von der Auswerteeinheit 18b an den Programmspeicher 46).

[0065] Nicht alle gemäß Fig. 6 gezeigten Schritte sind gemäß Fig. 7 und Fig. 8 dargestellt. Dies gilt auch umgekehrt.

Bezugszeichenliste

[0066]

1	Geldautomat
1a	Vorderseite
1b	Rückseite
2	Tür
2a	Türgriff
3	erstes Modul
4	zweites Modul
5	Bedieneinheit
6	Schließeinheit
7a	Standardmodell
7b, 7c, 7d	erweitertes Modell
8	Ziffern block
8a	Nummerntaste
8b	Bestätigungstaste
8c	Löschtaste
8d	Cursortaste
9	Display
10a	Tausch des Ziffernblocks
10b1, 10b2, 10b3	Softwareupgrade
11	Kombination
12, 13	Seriennummer
14	Funktionalitätscode
15	Lizenzkey
17	Betätigungseinheit
18a, b	Auswerteeinheit
31	Verschlüsselte Daten
32, 42	Empfangseinrichtung
33, 43	Entschlüsselungseinrichtung
34	Codespeicher des Supervisorcodes
36, 46	Programmspeicher
36a, 46a	Funktionsblock A
36b, 46b	Funktionsblock B
36c, 46c	Funktionsblock C
37a, 37b	Lizenzgenerator
38a, 38b	Vergleichs-Lizenzkey
39	Supervisorcode
40, 40a, 40b	Klartextdaten
41	Bestätigungsdaten
45	Hochsicherheitsschloss
48a, 48b, 48c	Bestätigungsdatensatz
49a, 49b, 49c	Bestätigungsdatensatz
52a, 52b, 52c	Funktion
53a, 53b	Datenverschlüsselungseinheit
54a, 54b	Datenübertragungseinheit
55a, 55b	Datenspeichereinheit
56	Datenempfangsschnittstelle
57	Supervisorcode
100	Erzeugung des Lizenzkeys
101	Kombinationsschritt
102	Lizenzalgorithmus
200	Upgradeprozess
200a	Upgrade-Teilprozess im intelligenten Schlossriegel
200b	Upgrade-Teilprozess in der Bedieneinheit
201	Eingabe des Supervisorcodes
202	Eingabe des Funktionscodes und des Lizenzkeys
203	Verschlüsselung des Funktionscodes und des Lizenzkeys
204	Verschlüsselte Übertragung an den Schlossriegel
204a	Weiterleitung der Daten
205	Entschlüsselung der Daten
205a	Berechnung des Vergleichslizenzkeys
205b	Übertragung der Klartextdaten
205c	Übertragung des Vergleichslizenzkeys
205d	Übertragung des Supervisorcodes
206	Auswertung des Supervisorcodes

207	Vergleich berechneter Lizenzkey mit empfangenem Lizenzkey
208	Freischaltung des entsprechenden Funktionsblocks
209	Bestätigung der Freischaltung
210	Verschlüsselung der Daten
210a	Dateneingabe
211	Verschlüsselte Übertragung an die Bedieneinheit
212	Entschlüsselung der Freigabedaten
212a	Berechnung Vergleichslizenzkey
212b	Übertragung der Klartextdaten
212c	Übertragung des Vergleichslizenzkeys
212d	Vergleich berechneter Lizenzkey mit empfangenem Lizenzkey
213	Freischaltung des entsprechenden Funktionsblocks
214	Abschluss des Upgradeprozesses

Patentansprüche

1. Hochsicherheitsschloss (45) für ein Wertbehältnis (1),
umfassend mindestens ein mechanisch funktionierendes Schlossmodul (3) und ein mit einer Datenempfangsschnittstelle ausgestattetes Bedienmodul (4),
wobei das Schlossmodul (3) und das Bedienmodul (4) dafür eingerichtet und dazu vorgesehen sind, elektronisch und mechanisch voneinander getrennt und/oder nach dem Plug-&-Play-Prinzip miteinander verbunden zu werden,
wobei das Schlossmodul (3) und das Bedienmodul (4) jeweils einen eigenen Programmspeicher (36; 46) mit vorinstallierten Unterprogrammen (36a, 36b, 36c; 46a, 46b, 46c) umfassen, welche Funktionen des Schlossmoduls (3) und/oder des Bedienmoduls (4) codieren,
wobei die im Programmspeicher (46) des Bedienmoduls (4) vorinstallierten Unterprogramme (46a, 46b, 46c) nur die Funktionen des Bedienmoduls (4) und die im Programmspeicher (36) des Schlossmoduls (3) vorinstallierten Unterprogramme (36a, 36b, 36c) nur die Funktionen des Schlossmoduls (3) codieren,
wobei die Datenempfangsschnittstelle dafür eingerichtet und dazu vorgesehen ist, einen Funktionalitätscode (14) und separat davon einen Lizenzkey (15) an das Bedienmodul (4) und das Schlossmodul (3) zu übertragen,
wobei das Schlossmodul (3) und das Bedienmodul (4) jeweils eine Auswerteeinheit (18a; 18b) umfassen,
und wobei beide Auswerteeinheiten (18a; 18b) dafür eingerichtet und dazu vorgesehen sind, einen Vergleich eines mittels eines Lizenzalgorithmus' erzeugbaren Vergleichslizenzkey (38a; 38b) mit dem Lizenzkey (15) und eine Auswertung des Funktionalitätscodes (14) durchzuführen und mindestens einen Bestätigungsdatensatz (48a, 48b, 48c) zur Freischaltung oder Sperrung mindestens eines Unterprogramms (36a, 36b, 36c) des Schlossmoduls (3) an den Programmspeicher (36) des Schlossmoduls (3) und mindestens eines Unterprogramms (46a, 46b, 46c) des Bedienmoduls (4) an den Programmspeicher (46) des Bedienmoduls (4) zu übertragen, wobei der Lizenzkey (15) ein Datensatz ist, welcher aus mindestens drei weiteren Datensätzen (12, 13, 14) generiert ist, wobei unter den weiteren Datensätzen eine Seriennummer (12) des Bedienmoduls (4), eine Seriennummer (13) des Schlossmoduls (3) und der Funktionalitätscode (14) sind, wobei der Funktionalitätscode (14) abhängig ist von den freizuschaltenden oder zu sperrenden Unterprogrammen (36a, 36b, 36c; 46a, 46b, 46c) in den Programmspeichern (36; 46).

2. Hochsicherheitsschloss (45) nach Anspruch 1,
dadurch gekennzeichnet, dass
das Schlossmodul (3) und das Bedienmodul (4) jeweils mindestens eine der folgenden Einheiten umfassen: eine Datenverschlüsselungseinheit (53a; 53b), eine Datenübertragungseinheit (54a; 54b) und eine Datenspeichereinheit (55a; 55b).

3. Hochsicherheitsschloss (45) nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet, dass
die Datenempfangsschnittstelle eine Einrichtung (8) zur manuellen Eingabe von Datensätzen oder eine elektronische Schnittstelle zur drahtgebundenen Übermittlung von Datensätzen oder eine elektronische Schnittstelle zur drahtlosen Übermittlung von Datensätzen ist.

4. Hochsicherheitsschloss (45) nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet, dass
das Schlossmodul (3) dafür eingerichtet und dazu vorgesehen ist, dass ein Supervisorcode (39) im Schlossmodul (3) hinterlegt wird, wobei die Auswerteeinheit (18a) dafür eingerichtet und dazu vorgesehen ist, den Supervisorcode (39) mit einem mittels der Datenempfangsschnittstelle an das Bedienmodul (4) und das Schlossmodul (3) übertragenen Supervisorcode (57) zu vergleichen.

5. Verfahren (200) zur softwareseitigen Aktivierung oder Deaktivierung von Funktionen von Modulen (3, 4) eines Hochsicherheitsschlosses (45) für ein Wertbehältnis (1),
wobei das Hochsicherheitsschloss (45) mindestens ein mechanisch funktionierendes Schlossmodul (3)

und ein mit einer Datenempfangsschnittstelle ausgestattetes Bedienmodul (4) umfasst,
wobei das Schlossmodul (3) und das Bedienmodul (4) jeweils einen eigenen Programmspeicher (36; 46) mit vorinstallierten Unterprogrammen (36a, 36b, 36c; 46a, 46b, 46c) umfassen, welche die Funktionen codieren,
dadurch gekennzeichnet, dass
das Schlossmodul (3) und das Bedienmodul (4) dafür eingerichtet und dazu vorgesehen sind, elektronisch und mechanisch voneinander getrennt und/oder nach dem Plug-&-Play-Prinzip miteinander verbunden zu werden, und dass
die im Programmspeicher (46) des Bedienmoduls (4) vorinstallierten Unterprogramme (46a, 46b, 46c) nur die Funktionen des Bedienmoduls (4) und die im Programmspeicher (36) des Schlossmoduls (3) vorinstallierten Unterprogramme (36a, 36b, 36c) nur die Funktionen des Schlossmoduls (3) codieren, und dass
das Schlossmodul (3) und das Bedienmodul (4) jeweils eine Auswerteeinheit (18a; 18b) umfassen,
aufweisend folgende Verfahrensschritte:

a) Eingabe eines Funktionalitätscodes (14), welcher abhängig ist von freizuschaltenden oder zu sperrenden Unterprogrammen (36a, 36b, 36c; 46a, 46b, 46c) in den Programmspeichern (36; 46), und separat davon Eingabe eines Lizenzkeys (15) an der Datenempfangsschnittstelle, wobei der Lizenzkey (15) ein Datensatz ist, welcher aus mindestens drei weiteren Datensätzen (12, 13, 14) generiert wird, wobei unter den weiteren Datensätzen eine Seriennummer (12) des Bedienmoduls (4), eine Seriennummer (13) des Schlossmoduls (3) und der Funktionalitätscode (14) sind,
b) Vergleich eines mittels eines Lizenzalgorithmus' erzeugbaren Vergleichslizenzkeys (38a; 38b) mit dem Lizenzkey (15) mittels beider Auswerteeinheiten (18a; 18b),
c) Auswertung des Funktionalitätscodes (14) mittels beider Auswerteeinheiten (18a; 18b),
d) Übertragung mindestens eines Bestätigungsdatensatzes (48a, 48b, 48c; 49a, 49b, 49c) an den Programmspeicher (36) des Schlossmoduls (3) und an den Programmspeicher (46) des Bedienmoduls (4), wenn Schritt b) eine Übereinstimmung der verglichenen Datensätze (38a, 15; 38b, 15) ergibt,
e) Freischaltung oder Sperrung mindestens eines Unterprogramms (36a, 36b, 36c) des Schlossmoduls (3) und mindestens eines Unterprogramms (46a, 46b, 46c) des Bedienmoduls (4).

6. Verfahren (200) nach Anspruch 5,
dadurch gekennzeichnet, dass
die Ausführung der Schritte jeweils in der Reihenfolge b), c) und d) aufeinander folgt und/oder die Ausführung der Schritte b), c) und/oder d) zunächst im Schlossmodul (3) und dann im Bedienmodul (4) erfolgt.

7. Verfahren (200) nach Anspruch 5 oder 6,
dadurch gekennzeichnet, dass
zeitlich vor Schritt a) in einem Schritt a0) eine Eingabe eines Supervisorcodes (57) erfolgt, welcher in einem Schritt a2) vor Schritt b) mittels der Auswerteeinheit (18a; 18b) mit einem im Schlossmodul (3) gespeicherten weiteren Datensatz (39) verglichen wird.

8. Verfahren (200) nach einem der Ansprüche 5-7,
dadurch gekennzeichnet, dass
die Eingabe der Datensätze (14, 15) in Schritt a) und/oder Schritt a0) drahtgebunden wie über eine Hardwareschnittstelle oder drahtlos wie mittels Funkübertragung erfolgt.

Claims

1. High-security lock (45) for a secure storage unit (1), comprising at least one mechanically functioning lock module (3) and a control module (4) equipped with a data receiving interface,
wherein the lock module (3) and the control module (4) are designed and provided to be electronically and mechanically separated from one another and/or connected to one another according to the plug-and-play principle,
wherein the lock module (3) and the control module (4) each comprise their own program memory (36; 46) having preinstalled subprograms (36a, 36b, 36c; 46a, 46b, 46c) which encode functions of the lock module (3) and/or the control module (4), wherein the subprograms (46a, 46b, 46c) preinstalled in the program memory (46) of the control module (4) only encode the functions of the control module (4) and the subprograms (36a, 36b, 36c) preinstalled in the program memory (36) of the lock module (3) only encode the functions of the lock module (3),
wherein the data receiving interface is designed and provided to transmit a functionality code (14) and, separately from that, a licence key (15) to the control module (4) and the lock module (3),
wherein the lock module (3) and the control module (4) each comprise an evaluation unit (18a; 18b),
and wherein the two evaluation units (18a; 18b) are designed and provided to compare a comparison licence key (38a; 38b) which can be generated by a licence algorithm with the licence key (15) and evaluate the functionality code (14), and to transfer at least one confirmation data record (48a, 48b, 48c) to the program memory (36) of the lock module (3)

in order to unlock or lock at least one subprogram (36a, 36b, 36c) of the lock module (3), and to the program memory (46) of the control module (4) in order to unlock or lock at least one subprogram (46a, 46b, 46c) of the control module (4),
wherein
the licence key (15) is a data record which is generated from at least three further data records (12, 13, 14), wherein the further data records include a serial number (12) of the control module (4), a serial number (13) of the lock module (3) and the functionality code (14), wherein the functionality code (14) is dependent on the subprograms (36a, 36b, 36c; 46a, 46b, 46c) to be unlocked or locked in the program memories (36; 46).

2. High-security lock (45) according to claim 1,
characterised in that
the lock module (3) and the control module (4) each comprise at least one of the following units: a data encryption unit (53a; 53b), a data transmission unit (54a; 54b) and a data storage unit (55a; 55b).

3. High-security lock (45) according to either of the preceding claims,
characterised in that
the data receiving interface is a device (8) for manually entering data records or an electronic interface for wired transfer of data records or an electronic interface for wireless transfer of data records.

4. High-security lock (45) according to any of the preceding claims,
characterised in that
the lock module (3) is designed and provided such that a supervisor code (39) is stored in the lock module (3), the evaluation unit (18a) being designed and provided to compare the supervisor code (39) with a supervisor code (57) transmitted to the control module (4) and the lock module (3) by means of the data receiving interface.

5. Method (200) for the software-side activation or deactivation of functions of modules (3, 4) of a high-security lock (45) for a secure storage unit (1),
the high-security lock (45) comprising at least one mechanically functioning lock module (3) and a control module (4) equipped with a data receiving interface,
the lock module (3) and the control module (4) each comprising their own program memory (36; 46) with preinstalled subprograms (36a, 36b, 36c; 46a, 46b, 46c) which encode the functions,
characterised in that
the lock module (3) and the control module (4) are designed and provided to be electronically and mechanically separated from one another and/or connected to one another according to the plug-and-play principle, and **in that** the subprograms (46a, 46b, 46c) preinstalled in the program memory (46) of the control module (4) only encode the functions of the control module (4) and the subprograms (36a, 36b, 36c) preinstalled in the program memory (36) of the lock module (3) only encode the functions of the lock module (3), and **in that**
the lock module (3) and the control module (4) each comprise an evaluation unit (18a; 18b),
comprising the following method steps:

a) inputting a functionality code (14) which is dependent on subprograms which are to be unlocked or locked (36a, 36b, 36c; 46a, 46b, 46c) in the program memories (36; 46), and separately from that inputting a licence key (15) at the data receiving interface, the licence key (15) being a data record which is generated from at least three further data records (12, 13, 14), the further data records including a serial number (12) of the control module (4), a serial number (13) of the lock module (3) and the functionality code (14),
b) comparing a comparison licence key (38a; 38b) which can be generated by a licence algorithm with the licence key (15) by means of the two evaluation units (18a; 18b),
c) evaluating the functionality code (14) by means of the two evaluation units (18a; 18b),
d) transmitting at least one confirmation data record (48a, 48b, 48c; 49a, 49b, 49c) to the program memory (36) of the lock module (3) and to the program memory (46) of the control module (4) if step b) results in a match of the compared records (38a, 15; 38b, 15),
e) unlocking or locking at least one subprogram (36a, 36b, 36c) of the lock module (3) and at least one subprogram (46a, 46b, 46c) of the control module (4).

6. Method (200) according to claim 5,
characterised in that
the steps are in each case carried out one after the other in the order b), c) and d), and/or steps b), c) and/or d) are first carried out in the lock module (3) and then in the control module (4).

7. Method (200) according to either claim 5 or claim 6,
characterised in that
a supervisor code (57) is input in a step a0) temporally before step a) and, in a step a2) before step b), is compared, by means of the evaluation unit (18a; 18b), with a further data record (39) stored in the lock module (3).

8. Method (200) according to any of claims 5-7,
characterised in that
the data records (14, 15) are input in step a) and/or

step a0) via wire, such as via a hardware interface, or wirelessly, such as via radio transmission.

Revendications

1. Verrou de haute sécurité (45) pour un coffre-fort (1), comportant au moins un module de verrou à fonctionnement mécanique (3) et un module de commande (4) équipé d'une interface de réception de données,
dans lequel le module de verrou (3) et le module de commande (4) sont agencés et prévus pour être séparés l'un de l'autre électroniquement et mécaniquement et/ou connectés l'un à l'autre selon le principe Plug & Play,
dans lequel le module de verrou (3) et le module de commande (4) comportent respectivement une mémoire de programme propre (36 ; 46) ayant des sous-programmes préinstallés (36a, 36b, 36c ; 46a, 46b, 46c), lesquels codent des fonctions du module de verrou (3) et/ou du module de commande (4),
dans lequel les sous-programmes (46a, 46b, 46c) préinstallés dans la mémoire de programme (46) du module de commande (4) codent seulement les fonctions du module de commande (4) et les sous-programmes (36a, 36b, 36c) préinstallés dans la mémoire de programme (36) du module de verrou (3) codent seulement les fonctions du module de verrou (3),
dans lequel l'interface de réception de données est agencée et prévue pour transférer un code de fonctionnalité (14) et de façon séparée une clé de licence (15) au module de commande (4) et au module de verrou (3),
dans lequel le module de verrou (3) et le module de commande (4) comportent respectivement une unité d'évaluation (18a ; 18b),
et dans lequel les deux unités d'évaluation (18a ; 18b) sont agencées et prévues pour réaliser une comparaison d'une clé de licence de comparaison (38a ; 38b) apte à être réalisée au moyen d'un algorithme de licence avec la clé de licence (15) et une évaluation du code de fonctionnalité (14) et pour transférer au moins un ensemble de données de confirmation (48a, 48b, 48c) pour l'activation ou le blocage d'au moins un sous-programme (36a, 36b, 36c) du module de verrou (3) à la mémoire de programme (36) du module de verrou (3) et d'au moins un sous-programme (46a, 46b, 46c) du module de commande (4) à la mémoire de programme (46) du module de commande (4),
dans lequel la clé de licence (15) est un ensemble de données, lequel est généré à partir d'au moins trois autres ensembles de données (12, 13, 14),
dans lequel par les autres ensembles de données, on entend un numéro de série (12) du module de commande (4), un numéro de série (13) du module de verrou (3) et le code de fonctionnalité (14), le code de fonctionnalité (14) étant dépendant des sous-programmes (36a, 36b, 36c ; 46a, 46b, 46c) à activer ou à bloquer dans les mémoires de programme (36 ; 46).

2. Verrou de haute sécurité (45) selon la revendication 1,
caractérisé par le fait que
le module de verrou (3) et le module de commande (4) comportent respectivement au moins l'une des unités suivantes : une unité de chiffrement de données (53a ; 53b), une unité de transfert de données (54a ; 54b) et une unité de mémorisation de données (55a ; 55b).

3. Verrou de haute sécurité (45) selon l'une des revendications précédentes,
caractérisé par le fait que
l'interface de réception de données est un dispositif (8) pour l'entrée manuelle d'ensembles de données ou une interface électronique pour la communication filaire d'ensembles de données ou une interface électronique pour la communication sans fil d'ensembles de données.

4. Verrou de haute sécurité (45) selon l'une des revendications précédentes,
caractérisé par le fait que
le module de verrou (3) est agencé et prévu de sorte qu'un code superviseur (39) est déposé dans le module de verrou (3), l'unité d'évaluation (18a) étant agencée et prévue pour comparer le code superviseur (39) à un code superviseur (37) transféré au module de commande (4) et au module de verrou (3) au moyen de l'interface de réception de données.

5. Procédé (200) pour l'activation ou la désactivation côté logiciel de fonctions de modules (3, 4) d'un verrou de haute sécurité (45) pour un coffre-fort (1),
dans lequel le verrou de haute sécurité (45) comporte au moins un module de verrou (3) à fonctionnement mécanique et un module de commande (4) équipé d'une interface de réception de données,
dans lequel le module de verrou (3) et le module de commande (4) comportent respectivement une mémoire de programme propre (36 ; 46) ayant des sous-programmes préinstallés (36a, 36b, 36c ; 46a, 46b, 46c), lesquels codent les fonctions,
caractérisé par le fait que
le module de verrou (3) et le module de commande (4) sont agencés et prévus pour être séparés l'un de l'autre électroniquement et mécaniquement et/ou connectés l'un à l'autre selon le principe Plug & Play,
et **par le fait que**
les sous-programmes (46a, 46b, 46c) préinstallés dans la mémoire de programme (36) du module de commande (4) codent seulement les fonctions du

module de commande (4) et les sous-programmes (36a, 36b, 36c) préinstallés dans la mémoire de programme (36) du module de verrou (3) codent seulement les fonctions du module de verrou (3) et **par le fait que**
le module de verrou (3) et le module de commande (4) comportent respectivement une unité d'évaluation (18a ; 18b),
présentant les étapes de procédé suivantes :

a) entrée d'un code de fonctionnalité (14), lequel est dépendant de sous-programmes (36a, 36b, 36c ; 46a, 46b, 46c) à activer ou à bloquer dans les mémoires de programme (36 ; 46), et séparément entrée d'une clé de licence (15) sur l'interface de réception de données, la clé de licence (15) étant un ensemble de données, lequel est généré à partir d'au moins trois autres ensembles de données (12, 13, 14), où, par les autres ensembles de données, on entend un numéro de série (12) du module de commande (4), un numéro de série (13) du module de verrou (3) et le code de fonctionnalité (14) ;
b) comparaison d'une clé de licence de comparaison (38a ; 38b) apte à être générée au moyen d'un algorithme de licence avec la clé de licence (15) au moyen des deux unités d'évaluation (18a ; 18b) ;
c) évaluation du code de fonctionnalité (14) au moyen des deux unités d'évaluation (18a ; 18b) ;
d) transfert d'au moins un ensemble de données de confirmation (48a, 48b, 48c ; 49a, 49b, 49c) à la mémoire de programme (36) du module de verrou (3) et à la mémoire de programme (46) du module de commande (4), lorsque l'étape b) donne une coïncidence des ensembles de données comparés (38a, 15 ; 38b, 15),
e) activation ou blocage d'au moins un sous-programme (36a, 36b, 36c) du module de verrou (3) et d'au moins un sous-programme (46a, 46b, 46c) du module de commande (4).

6. Procédé (200) selon la revendication 5,
caractérisé par le fait que
la réalisation des étapes se succède à chaque fois dans l'ordre b), c) et d) et/ou la réalisation des étapes b), c) et/ou d) a lieu tout d'abord dans le module de verrou (3) et ensuite dans le module de commande (4).

7. Procédé (200) selon l'une des revendications 5 ou 6,
caractérisé par le fait que
antérieurement à l'étape a) une entrée d'un code superviseur (57) a lieu dans une étape a0), qui est comparée dans une étape a2) avant l'étape b) au moyen de l'unité d'évaluation (18a ; 18b) avec un autre ensemble de données (39) mémorisé dans le module de verrou (3).

8. Procédé (200) selon l'une des revendications 5 à 7,
caractérisé par le fait que
l'entrée des ensembles de données (14, 15) à l'étape a) et/ou à l'étape a0) a lieu de façon filaire comme par l'intermédiaire d'une interface matérielle ou sans fil comme au moyen d'une transmission radio.

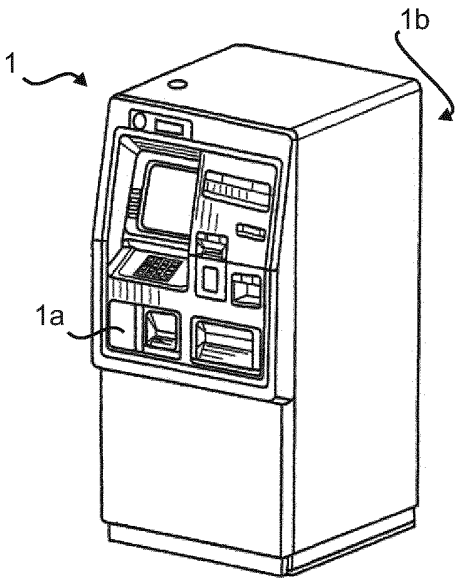

Fig. 1

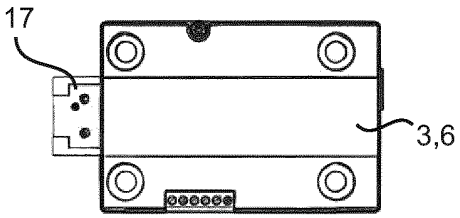

Fig. 2b

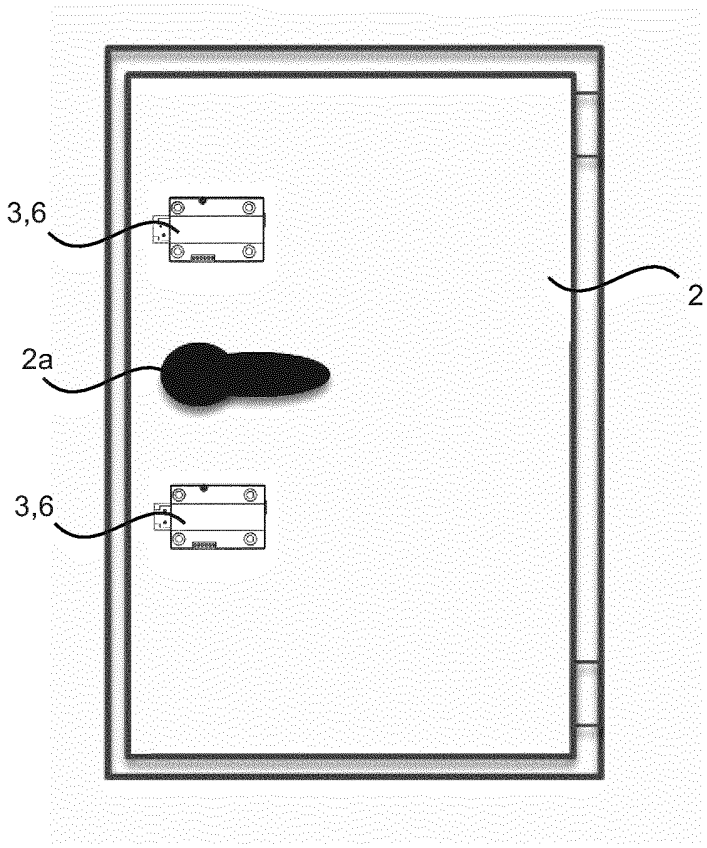

Fig. 2a

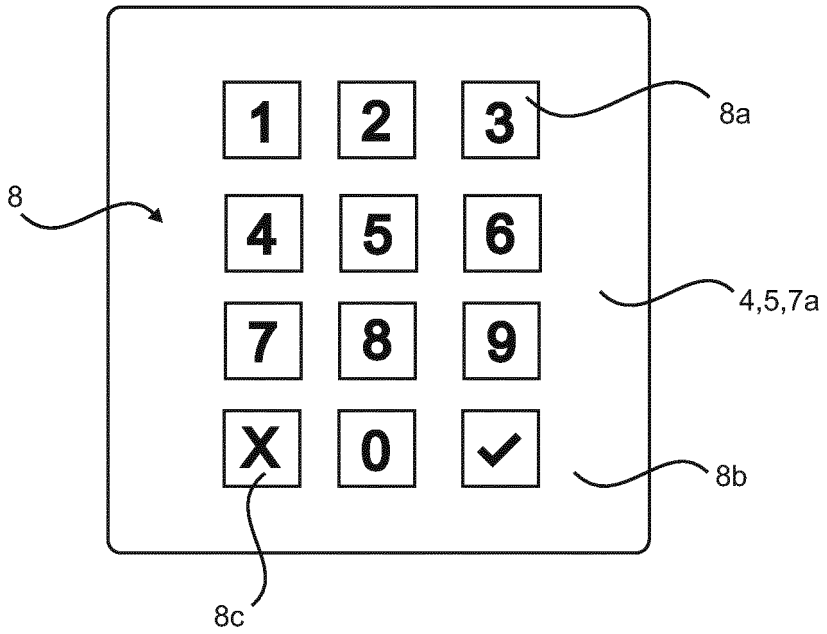
1
2
3
8a
8
4
5
6
4,5,7a
7
8
9
X
0
8b
8c

Fig. 3a

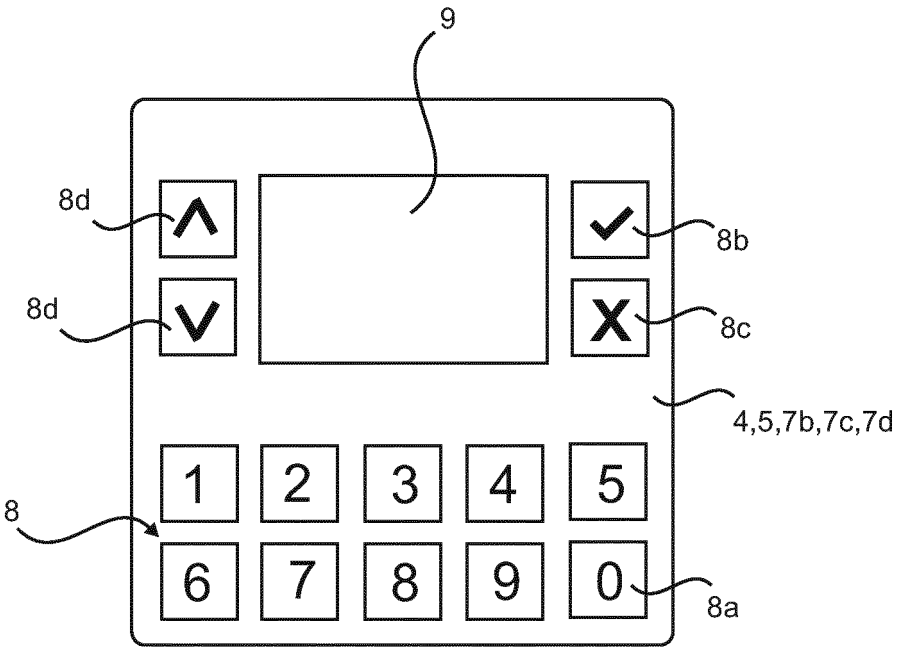
9
8d
8b
8d
8c
4,5,7b,7c,7d
1
2
3
4
5
8
6
7
8
9
0
8a

Fig. 3b

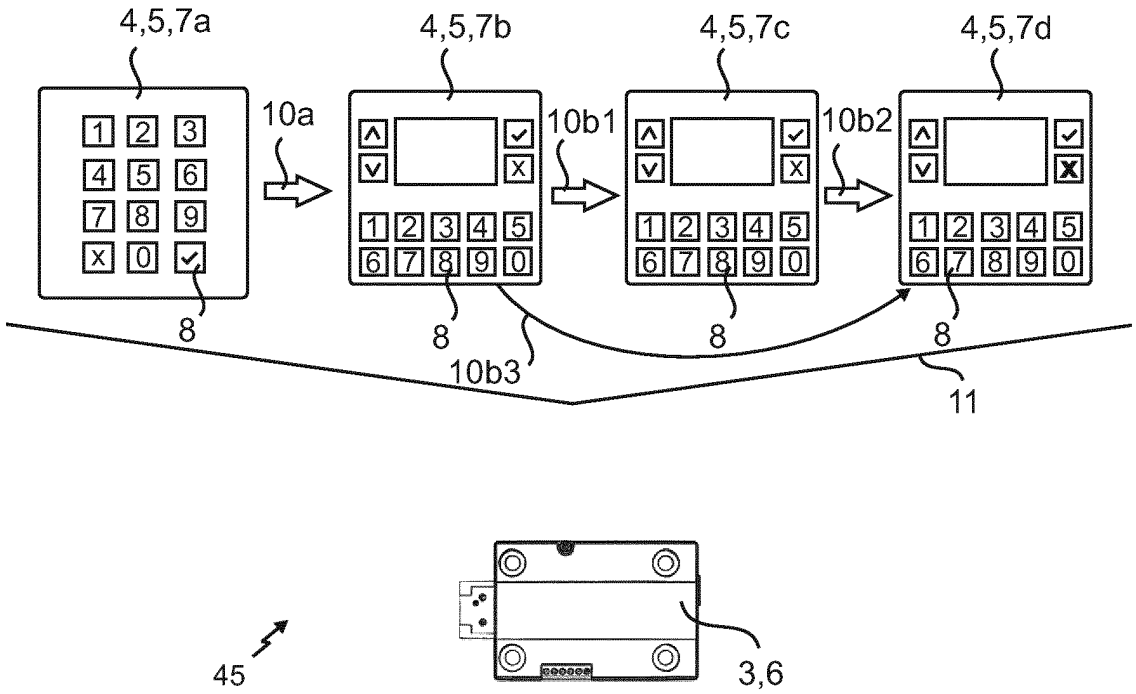
4,5,7a
4,5,7b
4,5,7c
4,5,7d
10a
10b1
10b2
10b3
8
11
45
3,6

Fig. 4

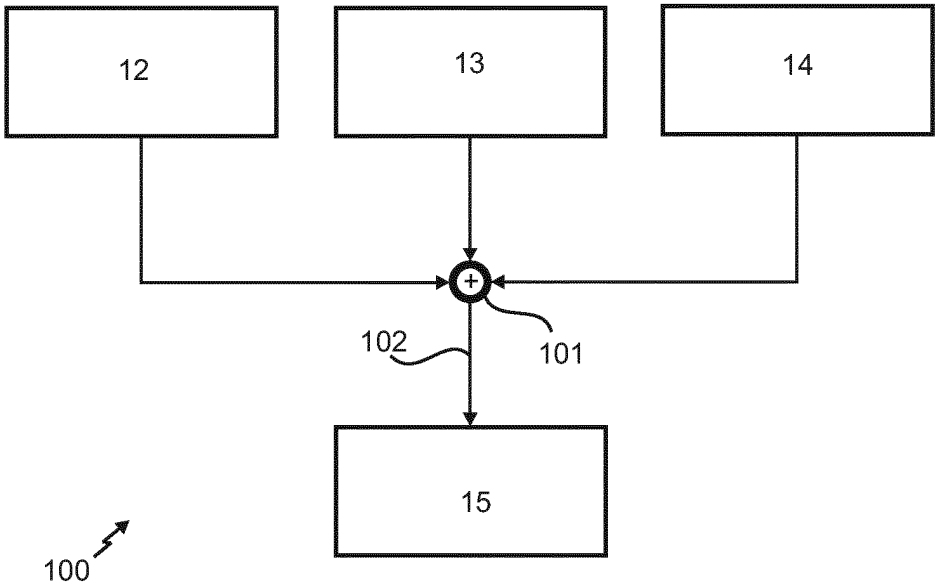
12
13
14
102
101
15
100

Fig. 5

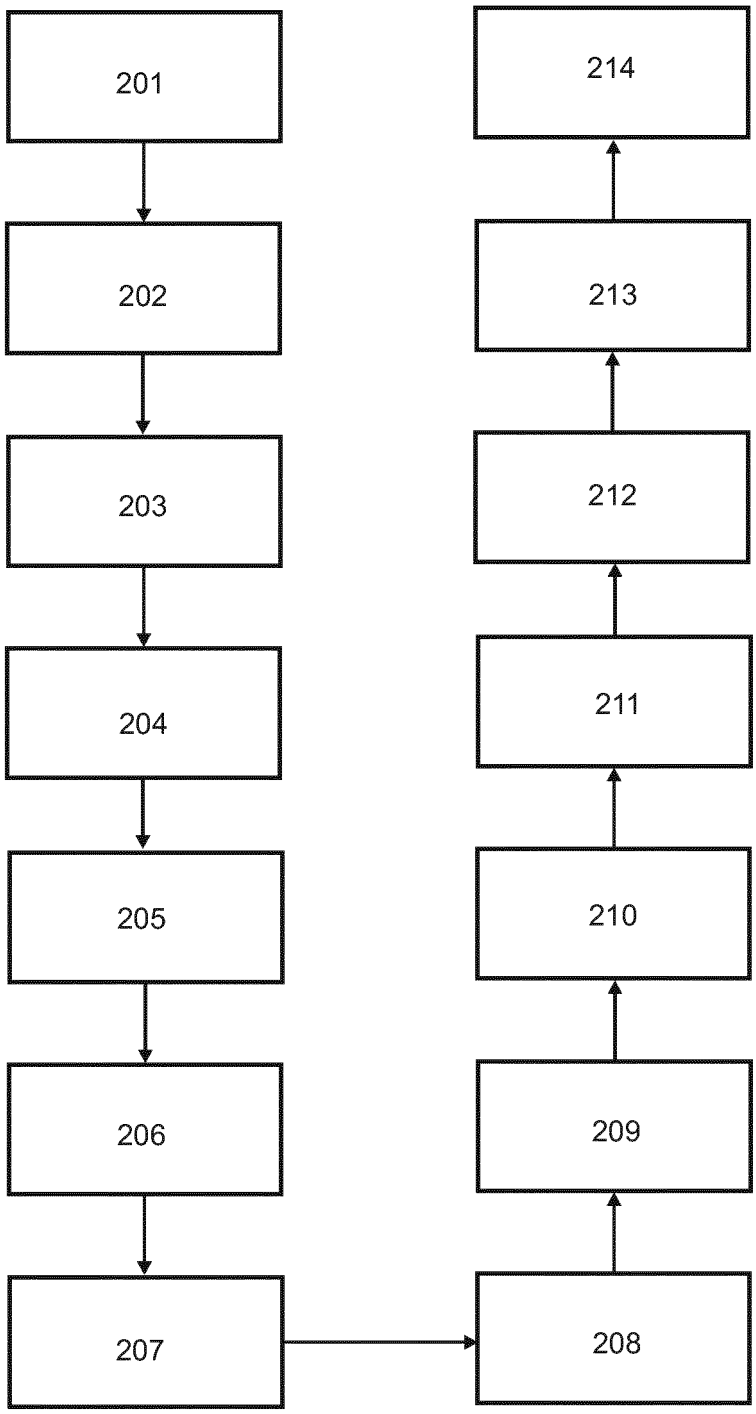

Fig. 6

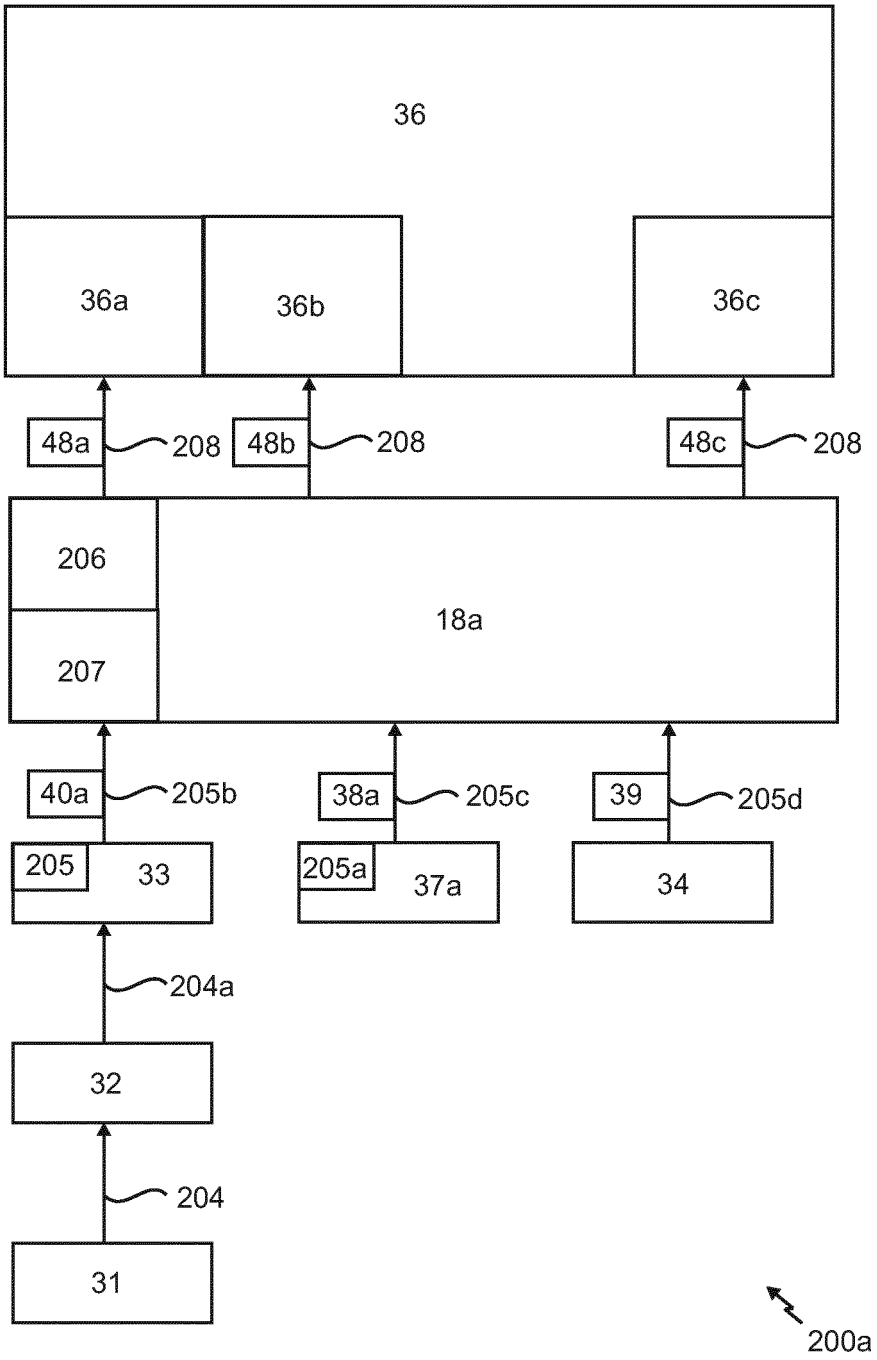
36
36a
36b
36c
48a
208
48b
208
48c
208
206
207
18a
40a
205b
38a
205c
39
205d
205
33
205a
37a
34
204a
32
204
31
200a

Fig. 7

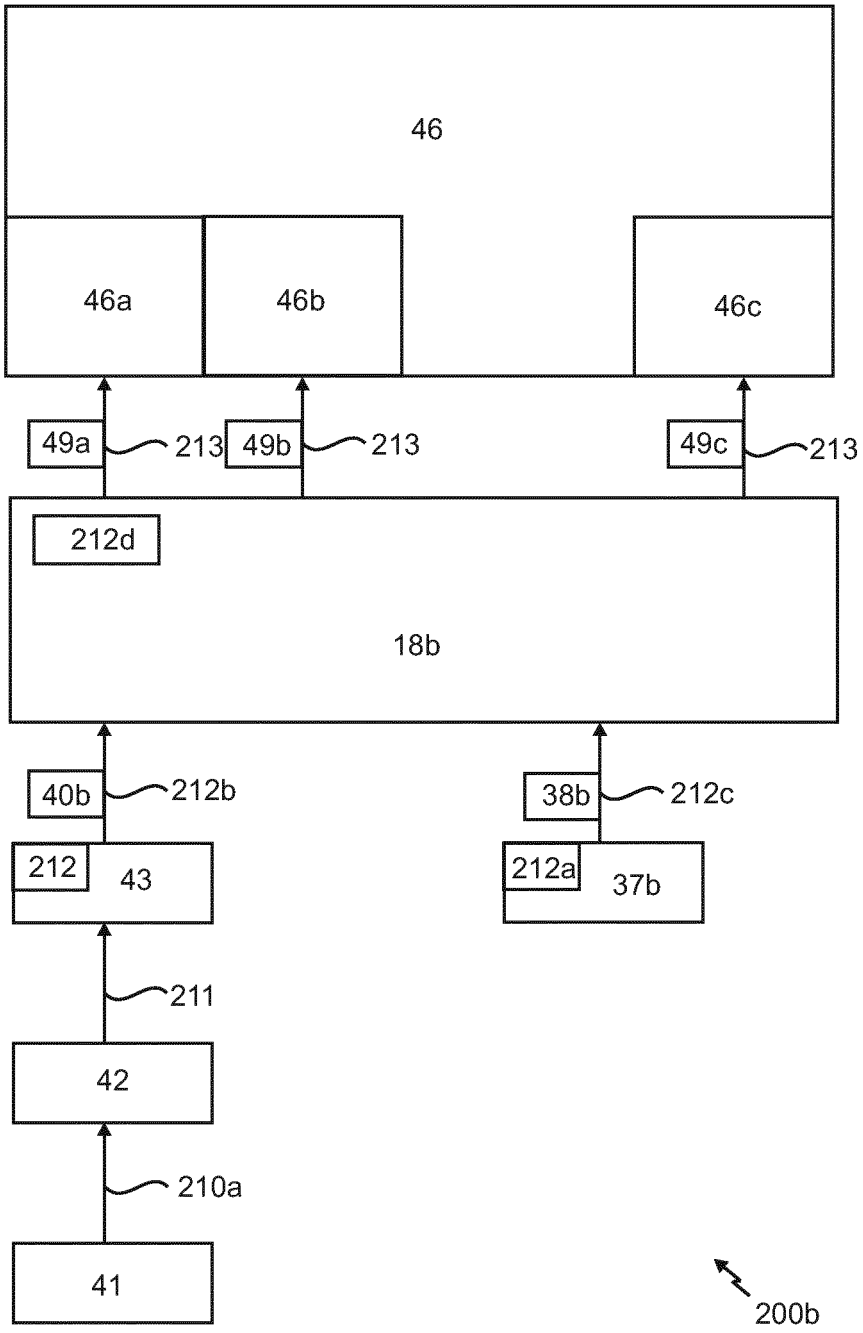
46
46a
46b
46c
49a
213
49b
213
49c
213
212d
18b
40b
212b
38b
212c
212
43
212a
37b
211
42
210a
41
200b

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

- EP 1260659 A2 **[0010]**
- US 2012216726 A1 **[0011]**
- US 7234636 B1 **[0011]**
- US 2010057703 A1 **[0012]**
- US 2011061047 A1 **[0012]**