

(19)



(11)

EP 1 703 473 B1

(12)

EUROPÄISCHE PATENTSCHRIFT

(45) Veröffentlichungstag und Bekanntmachung des
Hinweises auf die Patenterteilung:
18.03.2015 Patentblatt 2015/12

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

(21) Anmeldenummer: **06001068.3**

(22) Anmeldetag: **19.01.2006**

(54) **Schlosssystem**

Lock system

Système de serrures

(84) Benannte Vertragsstaaten:
**AT BE BG CH CY CZ DE DK EE ES FI FR GB GR
HU IE IS IT LI LT LU LV MC NL PL PT RO SE SI
SK TR**

(30) Priorität: **18.03.2005 DE 102005013098**

(43) Veröffentlichungstag der Anmeldung:
20.09.2006 Patentblatt 2006/38

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

(72) Erfinder: **Wagner, Eduard B.
98047 Regensburg (DE)**

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

(56) Entgegenhaltungen:
**EP-A2- 0 282 339 WO-A-01/40605
DE-A1- 3 711 746 DE-U1- 29 807 184
FR-A- 2 566 823 US-A- 5 768 379**

EP 1 703 473 B1

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).

Beschreibung

Gebiet der Erfindung

[0001] Die Erfindung betrifft ein Schlosssystem mit zumindest einem an einem Wertbehältnis angebrachten und dieses verschließenden Schloss, wobei das Schloss mittels einer elektronischen Schaltung über ein elektrisch ansteuerbares Stellglied aus einer Geschlossenstellung in eine Offenstellung ansteuerbar ist, wobei die elektronische Schaltung Mittel zum Auslesen eines mobilen Datenträgers, einen Schlossprozessor mit einer internen Schlossprozessoruhr sowie ein Schlossspeicherelement, worin ein Programm gespeichert ist, aufweist. Die Erfindung betrifft des Weiteren ein Betriebsverfahren für ein solches Schlosssystem.

Stand der Technik und Hintergrund der Erfindung

[0002] Aus der Praxis ist ein Schlosssystem der eingangs genannten Art bekannt. Bei den Wertbehältnissen handelt es sich beispielsweise um automatische Kassentresore, Geldautomaten und andere Wertbehältnisse. Bei solchen Wertbehältnissen ist es regelmäßig erforderlich, Wertinhalte zu entfernen oder auch aufzufüllen. Dies erfolgt in der Regel durch autorisierte Personen, welche mit geeigneten Mitteln ausgestattet sind, das Schloss in die Offenstellung zu betätigen. Solche Mittel umfassen beispielsweise die manuelle Eingabe eines Öffnungscodes, eines Berechtigungscodes oder dergleichen. Auch können elektronisch auslesbare Datenträger gleichsam wie ein mechanischer Schlüssel verwendet werden. In letzterem Fall wird das Schloss nur dann in die Offenstellung angesteuert, wenn die aus dem Datenträger ausgelesenen Daten die notwendigen Codes für einen berechtigten Zugriff enthalten. Hierbei handelt es sich typischerweise um einen Festcode, i.e. der Code ist einem Schloss zugeordnet und wird im normalen Betrieb nicht geändert.

[0003] Das Befüllen und Entleeren von Wertbehältnissen wird üblicherweise von Werttransportunternehmen und ähnlichen Dienstleistern besorgt. Dabei fährt ein Werttransportfahrzeug gemäß einem Fahrplan verschiedene Wertbehältnisse nacheinander an und die Bedienpersonen entleeren und/oder befüllen das jeweils angefahrte Wertbehältnis. Aufgrund der regelmäßig hohen Werte sind dabei an die Sicherheitsaspekte sehr hohe Anforderungen zu stellen.

[0004] Bei dem vorstehend beschriebenen und aus der Praxis bekannten Betriebsverfahren reicht der Besitz eines Öffnungscodes, Identifikationscodes oder Datenträgers zur Öffnung eines Wertbehältnisses aus. Wird beispielsweise ein solcher Datenträger unbefugt kopiert, so kann mittels der Kopie eine Öffnung des Wertbehältnisses erfolgen, ohne dass dies durch beispielsweise das Werttransportunternehmen oder den Betreiber des Wertbehältnisses ohne weiteres verhindert werden kann. Insofern sind die bekannten Schlosssysteme verbesserte

rungsfähig.

[0005] DE 37 11 746 offenbart ein Schlosssystem mit einem elektronischen Schloss und einem von dem Schloss beabstandeten und mit dem Schloss nicht verbundenen Zentralrechner, wobei das Schloss mittels einer elektronischen Schaltung über ein elektrisch ansteuerbares Stellglied aus einer Geschlossenstellung in eine Offenstellung ansteuerbar ist. Es wird auch eine interne Schlossprozessoruhr sowie ein Schlossspeicherelement, worin ein Decodierprogramm sowie ein dem Schloss zugeordneter Festcode gespeichert sind, gezeigt.

Technisches Problem der Erfindung

[0006] Der Erfindung liegt daher das technische Problem zugrunde, ein Schlosssystem anzugeben, welches eine erhöhte Sicherheit aufweist, insbesondere gegen unbefugte Zugriffe besser gesichert ist.

Grundzüge der Erfindung und bevorzugte Ausführungsformen

[0007] Zur Lösung dieses technischen Problems lehrt die Erfindung ein Schlosssystem gemäß Anspruch 1 und ein Verfahren gemäß Anspruch 4. Das Schlosssystem ist ausgestattet mit einer Mehrzahl von einem an einem Wertbehältnis angebrachten und dieses verschließenden Schlössern, mit von den Schlössern beabstandeten und mit den Schlössern nicht verbundenen Zentralenrechner und mit einem mobilen Datenträger, wobei jedes der Schlösser jeweils mittels einer elektronischen Schaltung über ein elektrisch ansteuerbares Stellglied aus einer Geschlossenstellung in eine Offenstellung ansteuerbar ist, wobei jede elektronische Schaltung Mittel zum Auslesen des mobilen Datenträgers, einen Schlossprozessor mit einer internen Schlossprozessoruhr sowie ein Schlossspeicherelement, worin ein Decodierprogramm sowie ein dem jeweiligen Schloss zugeordneter Festcode gespeichert sind, aufweist, wobei der Zentralenrechner Mittel zum Beschreiben des mobilen Datenträgers, einen Zentralenprozessor sowie ein Zentralenspeicherelement, worin ein Codierprogramm und der jedem Schloss zugeordnete Festcode gespeichert sind, aufweist, wobei mittels des Codierprogramms ein Datensatz erzeugbar und auf den Datenträger schreibbar ist, wobei der Datensatz durch Auslesen des Festcodes aus dem Zentralenspeicherelement und dessen Kombination mit einem dem Zentralenprozessor eingegebenen Sollzeitfenster erzeugbar ist, wobei der Datensatz des Datenträgers mittels der Mittel zum Auslesen des Datenträgers auslesbar ist, wobei im zugeordneten Schlossprozessor mittels des Decodierprogramms durch Auslesen des dem jeweiligen Schloss zugeordneten Festcodes aus dem zugeordneten Schlossspeicherelement das Sollzeitfenster bestimmbar ist und wobei durch Auslesen der zugeordneten Schlossprozessoruhr und Vergleich der ausgelesenen Uhrzeit mit dem bestimmten

Sollzeitfenster das Schloss in die Offenstellung ansteuerbar ist, wenn die Uhrzeit innerhalb des Sollzeitfensters liegt. Wenn die ausgelesene Uhrzeit nicht innerhalb des Sollzeitfensters liegt, versteht es sich, dass eine Ansteuerung in die Offenstellung nicht stattfindet.

[0008] Der Zentralenrechner ist mit dem Schloss nicht verbunden in dem Sinne, dass keinerlei unmittelbare Verbindung, sei es durch elektrische Leitungen oder durch drahtlose Übermittlung, besteht. Es wird sich empfehlen, den Zentralenrechner, oder zumindest jenen Prozessor, mittels welchem die Codierung erfolgt, mit fachüblichem Ausleseschutz und Sabotageschutz auszustatten.

[0009] Dagegen ist die elektronische Schaltung unmittelbar mit dem Schloss verbunden, beispielsweise mittels elektrischer Leitungen oder drahtloser Übermittlung von Signalen. Typischerweise bildet sie sogar ein Bauteil des Schlosses.

[0010] Als Datenträger kommen grundsätzlich alle fachüblichen Datenträger in Frage. Beispiele hierfür sind: Magnetkarte, Chipkarte, mobiler Speicherbaustein usw.. Im Falle der Chipkarte, welche bevorzugt ist, kann diese passwortgeschützt sein, i.e. auf das Speicherelement des Chips kann nur mittels eines Passwortes zugegriffen werden. Dann versteht es sich, dass im Rahmen des Schlossspeicherelementes das Passwort gespeichert ist und zur Auslesung der Chipkarte zunächst an diese übertragen wird. Die für die vorstehenden Datenträger benötigten Mittel zum Auslesen und Mittel zum Beschreiben sind dem Fachmann im übrigen wohl vertraut und brauchen daher nicht näher beschrieben zu werden.

[0011] Die interne Schlossprozessoruhr stellt eine Systemuhrzeit zur Verfügung, deren Struktur und Ablauf innerhalb des Schlosssystems definiert und einheitlich ist. Das Format kann hierbei grundsätzlich beliebig sein. Im einfachsten Fall umfasst das Format Jahr, Monat, Tag, Stunde, Minute und ggf. Sekunde. Diese Zeitinformation kann verschlüsselt sein, wobei der Verschlüsselungsalgorithmus dann im Zentralenrechner in analoger Weise eingerichtet ist. Da bei einem erfindungsgemäßen Schlosssystem regelmäßig eine Vielzahl von Schlössern umfasst sind, laufen die jeweiligen Schlossprozessoren nahezu synchron zueinander. Im Rahmen beispielsweise jährlicher Wartungen kann eine Synchronisierung eventueller Abweichungen durch Drift erfolgen, falls einzelne Schlossprozessoren gegenüber einer Referenzzeit um mehr als ein definiertes Divergenzzeitintervall vor- oder nachgehen.

[0012] Es versteht sich, dass die jeweiligen Speicherelemente in der Regel nicht baulich separat von den Prozessoren ausgebildet sind, sondern Speicherbereiche innerhalb eines im Prozessor integrierten Speichers sein können. Entsprechendes gilt für die Schlossprozessoren, welche in der Regel integraler Bestandteil des Prozessors i.V. mit dem Betriebsprogramm des Prozessors ist.

[0013] Ein einem Schloss zugeordneter Festcode ist einzigartig, ausschließlich für das betreffende Schloss

eingerichtet und im Schlossspeicherelement sowie im Zentralenspeicherelement gespeichert. Die Festcodes verschiedener Schlösser unterscheiden sich folglich. Insofern entspricht der Festcode gleichsam einem Namen für das zugeordnete Schloss. Im Zentralenspeicher sind alle Festcodes jeweils mit Zuordnung zu dem betreffenden Schloss, in welchem ein Festcode abgespeichert ist, gespeichert, gleichsam einem Adressbuch mit dem Festcode als Name und zumindest einer weiteren individualisierenden Information, wie beispielsweise Standort, Betreiber, Laufnummer, Seriennummer etc..

[0014] Der mittels des Codierprogramms erzeugbare und mittels des hierzu komplementären Decodierprogramms zerlegbare Datensatz enthält neben dem Festcode ein Sollzeitfenster. Dieses Sollzeitfenster ist zur Erzeugung dem Zentralenprozessor beispielsweise durch eine Bedienperson eingegeben worden. Das Sollzeitfenster steht für das Zeitintervall, in welchem eine Öffnung des dem Festcode zugeordneten Wertverhältnisses durch eine autorisierte Person zulässig und möglich sein soll. Eine Öffnung außerhalb dieses Sollzeitfensters ist dagegen nicht möglich. Das einzugebende Sollzeitfenster entspricht einem Wechselcode, da bei jeder zulässigen Öffnung dies zu jeweils anderen Zeitpunkten und folglich in verschiedenen Sollzeitfenstern erfolgt. Im Ergebnis weist der Datensatz einen Festcodeanteil und einen Wechselcodeanteil auf. Im einfachsten Fall besteht ein Datensatz dabei aus einer Zeichenfolge, die den Festcode definiert, einer hieran angeschlossenen Zeichenfolge, die den Anfangszeitpunkt des Sollzeitfensters definiert, und einer angeschlossenen Zeichenfolgen, welche die Endzeit des Sollzeitfensters definiert. Dann ist der Datensatz durch schlichte Aneinanderreihung von Festcode und zwei variablen Codes gegeben. Die Decodierung umfasst dann lediglich eine Auftrennung der Zeichenfolge des Festcodes an vorgegeben Zeichenstellen, wodurch wiederum die vorstehenden Komponenten separiert sind. Anstelle einer solchen einfachen Aneinanderreihung können selbstverständlich auch andere Algorithmen der Kombination verwendet werden. Beispielsweise kann beim Codieren eine Multiplikation einer den Festcode bildenden Binärzahl mit einer Binärzahl, die durch die Aneinanderreihung von Binärzahlen, welche den Anfangszeitpunkt und den Endzeitpunkt des Sollzeitfensters darstellen, durchgeführt werden. Das Decodieren erfolgt dann durch Division des Datensatzes durch den im Schlossspeicherelement gespeicherten Festcode und folgender Zerlegung bzw. Separierung des Divisionsergebnisses, wodurch wiederum die Binärzahlen des Anfangs- und des Endzeitpunktes erhalten werden. Weiterhin ist es möglich, dass mittels eines Verschlüsselungsalgorithmus, welcher beispielsweise mit einem Verschlüsselungscode arbeitet, der Festcode mit dem Sollzeitfenster verknüpft wird. Dann ist der Verschlüsselungscode ebenfalls sowohl im Zentralenspeicherelement als auch im Schlossspeicherelement gespeichert. Durch Änderung des Verschlüsselungscode kann dann - bei Beibehaltung des eigentlichen Ver-

schlüsselungsalgorithmus - eine Umstellung im Falle einer festgestellten Sicherheitslücke, beispielsweise Abhandenkommen des Datenträgers, erfolgen. Damit ein Vergleich der aus der Schlossprozessoruhr ausgelesenen Uhrzeit mit dem Sollzeitfenster erfolgen kann, ist es ansonsten grundsätzlich lediglich erforderlich, dass das Codierprogramm im Zentralenspeicherelement komplementär zum Decodierprogramm im Schlossspeicherelement ist.

[0015] Mit einem erfindungsgemäßen Schlosssystem wird eine erhebliche Verbesserung der Sicherheit dadurch erreicht, dass nicht nur ein Festcode zur Öffnung eines Schlosses erforderlich ist, sondern dass vielmehr diese Öffnung auch innerhalb eines vorgegebenen Sollzeitfensters erfolgen muss. Wird der Datenträger beispielsweise unbefugterweise kopiert und mit dieser Kopie zu einem späteren Zeitpunkt ein Öffnungsversuch unternommen, so ist ein solcher Öffnungsversuch zum Scheitern verurteilt, weil das Schloss aufgrund der Nichtübereinstimmung der ausgelesenen Schlossprozessoruhrzeit mit dem ausgelesenen Sollzeitfenster nicht in die Offenstellung ansteuerbar ist.

[0016] Auf dem Datenträger sind eine Mehrzahl von verschiedenen Datensätzen geschrieben, wobei jeder Datensatz eine Kombination eines einem Schloss zugeordneten Festcodes und eines Sollzeitfensters ist, wobei die Datensätze sich durch verschiedene, verschiedenen Schlössern zugeordnete Festcodes und/oder durch verschiedene Sollzeitfenster unterscheiden. Durch die Gruppe der Datensätze ist folglich gleichsam ein Öffnungszeitplan für die Vielzahl verschiedener Schlösser eingerichtet. So kann beispielsweise mittels des Zentralrechners ein Abholplan für eine Person eines Werttransportunternehmens erstellt werden, in welchem die Reihenfolge, mit Zeitintervallangaben, der Öffnung der Wertbehältnisse vorgegeben ist.

[0017] In Weiterbildung der Erfindung ist es möglich, dass nach Auslesung eines Datensatzes und Ansteuerung des Schlosses in die Offenstellung im Schlossprozessor eine erneute Ansteuerung des Schlosses durch erneutes Auslesen desselben Datensatzes sperrbar ist und/oder der Datensatz durch den Schlossprozessor von dem Datenträger gelöscht wird. In dieser Ausführungsform wird verhindert, dass innerhalb des Sollzeitfensters eine zweite Öffnung eines Wertbehältnisses erfolgt. Hierdurch ist beispielsweise sichergestellt, dass durch Beobachtung einer berechtigten Person und zeitnaher Entwendung des Datenträgers mit sofortigem erneutem Öffnungsversuch dieser misslingen muss. In der ersten Alternative kann dies beispielsweise dadurch realisiert werden, dass im Schlossprozessor der bei der ersten Öffnung ausgelesene Datensatz gespeichert wird. Im Rahmen einer Zusatzroutine wird ein (erneut) ausgelesener Datensatz mit zuvor ausgelesenen und im Schlossprozessor gespeicherten Datensätzen verglichen und bei Identität die Ansteuerung in die Offenstellung gesperrt. Mit einer Auslesung wird ein Datensatz folglich gleichsam verbraucht. In der zweiten Alternative umfasst

die elektronische Schaltung auch Mittel zum Beschreiben des mobilen Datenträgers. Dann wird ein verbrauchter Datensatz auf dem Datenträger beispielsweise mit einem Null-Datensatz überschrieben, wobei andere Datensätze selbstverständlich erhalten bleiben.

[0018] Eine zusätzliche Erhöhung der Sicherheit wird erreicht, wenn das Schloss Mittel zum Eingeben eines Identifikationscodes aufweist, wobei in dem Schlossspeicherelement der Identifikationscode eingespeichert ist, und wobei eine Ansteuerung des Schlosses in die Offenstellung bei Nichtübereinstimmung des gespeicherten Identifikationscodes mit dem eingegebenen Identifikationscode durch den Schlossprozessor sperrbar ist. Ein Identifikationscode kann grundsätzlich beliebiger Natur sein und ist individuell für einen Datenträger, eine Bedienperson oder eine Bedienpersonengruppe und diesen zugeordnet. Beispielsweise kann es sich hierbei um eine (vorzugsweise, aber nicht zwingend, auf einem separaten Datenträger) abgespeicherte Zeichenfolge handeln. Ebenso kann es sich um eine Zeichenfolge handeln, die die Bedienperson sich gemerkt hat (sog. PIN-Code). In diesen Fällen ist der Identifikationscode dem jeweiligen Datenträger zugeordnet. Als Identifikationscodes kommen aber auch beispielsweise biometrische Merkmale, wie Fingerabdruck, Irismuster oder Gesichtserkennung, in Frage. Die Mittel zum Eingeben des Identifikationscodes umfassen jeweils entsprechende technische Baugruppen. Im Falle eines Datenträgers handelt es sich dann um Mittel zum Auslesen des Datenträgers. Dies können die gleichen Mittel sein, welche vorstehend im Rahmen der Erfindung verwendet werden. Im Falle eines PIN-Codes umfassen die Mittel zum Eingeben beispielsweise eine mit dem Schlossprozessor verbundene Tastatur. Im Falle der biometrischen Daten umfassen die Mittel zum Auslesen des Datenträgers hierzu fachübliche Scanner in Verbindung mit einem geeigneten Datenverarbeitungsprogramm zur Umsetzung der gescannten optischen Informationen in den Identifikationscode. In dieser Ausführungsform der Erfindung versteht es sich, dass einer oder mehrere Identifikationscodes von autorisierten Bedienpersonen im Schlossspeicherelement gespeichert sein können. Die Eingabe des Identifikationscodes kann vor oder nach dem Auslesen des Datenträgers erfolgen.

[0019] Erfindungsgemäß wird bei Betätigung des Schlosses aus der Offenstellung in die Geschlossenstellung einen Quittierdatensatz durch den Schlossprozessor auf den Datenträger geschrieben.

[0020] In diesem Zusammenhang, aber auch in allgemeinen Zusammenhängen der vorliegenden Erfindung kann eine Sensorik eingerichtet sein, die auf das Öffnen und Schließen des Wertbehältnisses reagiert und mit dem Schlossprozessor verbunden ist. Im einfachsten Fall kann es sich beispielsweise um einen Mikroschalter handeln, welcher im Bereich des öffnbaren Bauteils des Wertbehältnisses oder auch im Bereich eines Sperrelementes des Schlosses angeordnet ist, wobei der Mikroschalter in der Geschlossenstellung in einem ersten

Schaltzustand und in der Offenstellung in einem zweiten Schaltzustand ist. Das Öffnen und Schließen ist dann durch verschiedene Flanken zwischen des Schaltzuständen detektier- und unterscheidbar. Wird vom Schlossprozessor die Flanke der Betätigung des Schlosses in die Geschlossenstellung detektiert, erfolgt dann die Quittierung, wie vorstehend beschrieben.

[0021] Die Quittierdatensätzen können nach Abarbeitung des Abholplanes wiederum in den Zentralenrechner eingelesen werden, wodurch der gesamte Abholvorgang dann abgeschlossen und protokolliert ist.

[0022] Mit mehreren verschiedenen Datensätzen und der Einrichtung von Quittierdatensätzen ist es möglich, dass durch den Schlossprozessor eine Ansteuerung des Schlosses in die Offenstellung sperrbar ist, wenn zu einem Datensatz für ein anderes Schloss mit zeitlich früherem Sollzeitfenster kein Quittierdatensatz auf dem Datenträger geschrieben ist und/oder wenn zu einem Datensatz für ein anderes Schloss mit zeitlich späterem Sollzeitfenster ein Quittierdatensatz auf den Datenträger geschrieben ist. Hierdurch wird erreicht, dass eine Betätigung des Schlosses trotz positivem Vergleich von Festcode- und Wechselcodeanteil, i. e. des Datensatzes, nicht möglich ist, wenn von dem vorgegebenen Abholplan gemäß der Gruppe abgespeicherter Datensätze abgewichen worden ist. Hierdurch wird die Sicherheit zusätzlich erhöht.

[0023] Die Erfindung betrifft des Weiteren ein Verfahren zum Betrieb eines erfindungsgemäßen Schlosssystems gemäß Anspruch 4. Bevorzugt behältnisses (1) in die Geschlossenstellung wird, ist es, wenn die Bedienperson bei jedem Schloss zusätzlich einen Identifikationscode eingeben muss.

[0024] Im Folgenden wird die Erfindung anhand von lediglich ein Ausführungsbeispiel darstellenden Figuren näher erläutert. Es zeigen:

Figur 1: eine schematische Darstellung eines Wertbehältnisses mit erfindungsgemäß einsetzbarem Schloss,

Figur 2: eine schematische Darstellung eines erfindungsgemäß eingesetzten Zentralenrechners,

Figur 3: ein Ablaufdiagramm eines erfindungsgemäßen Betriebsverfahrens.

[0025] In der Figur 1 erkennt man als eine erste Komponente des Schlosssystems, die typischerweise in einer Mehrzahl eingerichtet ist, ein an einem Wertbehältnis 1 angebrachten und dieses verschließenden Schloss 2. Das Schloss 2 weist ein mittels einer elektronischen Schaltung 4 elektrisch ansteuerbares Stellglied 14, welches ein Sperrelement 15 aus einer Geschlossenstellung in eine Offenstellung bewegt. In der gezeigten Darstellung ist das Sperrglied in der Geschlossenstellung und wird in die Offenstellung nach rechts bewegt. Die

Ausführung der elektromechanischen Komponenten des Schlosses 2 ist grundsätzlich beliebig. In Frage kommt beispielsweise eine Ausführung, wie in der Literaturstelle DE 195 35 065.0 A beschrieben. Die elektronische Schaltung 4 weist einen Kartenleser 5 zum Auslesen einer Chipkarte 6 auf. Der Kartenleser 5 kann die Chipkarte 6 nicht nur auslesen, sondern auch beschreiben. Die Chipkarte 6 ist mit einer an sich bekannten passwortgeschützten Auslesesperre versehen, die hier nicht näher erläutert zu werden braucht. Des Weiteren sind ein Schlossprozessor 7 mit einer internen Schlossprozessoruhr 8 sowie ein Schlossspeicherelement 9, worin ein Decodierprogramm sowie ein dem Schloss 2 zugeordneter Festcode gespeichert sind, eingerichtet. Weiterhin erkennt man eine Tastatur 13 zum Eingeben eines Identifikationscodes bzw. einer PIN. Die PIN (neben anderen PIN für andere autorisierte Bedienpersonen) ist in dem Schlossspeicherelement 9 eingespeichert. Eine Ansteuerung des Schlosses 2 in die Offenstellung ist bei Nichtübereinstimmung der gespeicherten PINs mit der eingegebenen PIN durch den Schlossprozessor 7 gesperrt. Schließlich erkennt man ein Display 19, welcher der Dialogführung mit einer Bedienperson dient, sowie einen Treiber 17 für das Stellglied 14. Der Übersichtlichkeit halber nicht dargestellt ist, dass eine Handhabe zur Bewegung des Wertbehältnisverschlusses zwischen einer Offenstellung und einer Geschlossenstellung eingerichtet ist. Auch ist es möglich, dass das Stellglied 14 nicht unmittelbar auf das Sperrelement 15 wirkt, sondern auf ein Verriegelungselement, welches in der Geschlossenstellung das Sperrelement in seiner Geschlossenstellung fixiert. In der Offenstellung des Verriegelungselementes gibt dieses dann das Sperrelement 15 frei, welches dann entweder mittels des gleichen oder eines weiteren Stellgliedes oder durch manuelle Betätigung über eine Handhabe in seine Offenstellung gebracht werden kann.

[0026] In der Figur 2 erkennt man als weitere Komponente des erfindungsgemäßen Schlosssystems einen Zentralenrechner 3. Dieser umfasst Mittel 10 zum Beschreiben der Chipkarte 6, einen Zentralenprozessor 11 sowie ein Zentralenspeicherelement 12, worin ein Codierprogramm und der dem in der Figur 1 dargestellten Schloss 2 zugeordnete Festcode gespeichert sind. Für andere Schlösser sind ebenfalls (verschiedene) Festcodes eingespeichert. Weiterhin erkennt man ein Terminal 17 mit Tastatur 18 und Display 19, mittels welchem eine Bedienperson Daten, beispielsweise einen Abholplan, eingeben kann. In Einzelnen erkennt man, dass der Zentralenprozessor 11, das Zentralenspeicherelement 12 und das Mittel 10 zum Beschreiben der Chipkarte 6 in einer separaten baulichen Einheit, einer Sicherheitsbox 20, eingerichtet sind. Diese Sicherheitsbox 20 ist mechanisch und/oder elektrisch gegen unbefugte Eingriffe (beispielsweise Manipulation oder Sabotage) mit üblichen und nicht näher dargestellten Maßnahmen der Sicherungstechnik gesichert. Das Mittel 10 zum Beschreiben der Chipkarte 6 kann alternativ zur Darstellung auch außerhalb der Sicherheitsbox 20 eingerichtet sein.

[0027] Aus einer vergleichenden Betrachtung der Figuren 1 und 2 erkennt man, dass zwischen dem Schloss 1 und dem Zentralenrechner keinerlei elektrische oder drahtlose Datenübertragung stattfindet. Die Datenübertragung erfolgt ausschließlich durch Transport des Datenträgers 6.

[0028] In der Figur 3 sind die Abläufe einer einfachen Variante eines erfindungsgemäßen Verfahrens dargestellt. In Stufe A wird dem Zentralenprozessor 3 mittels des Terminals 17 ein Abholplan eingegeben. Ein Abholplan umfasst dabei die Zuordnung jeweils eines Sollzeitfensters zu einem anzufahrenden Schloss 2, welches beispielsweise durch den Standort identifiziert ist. Mittels des Codierprogramms wird dann für jedes Schloss 2 ein Datensatz erzeugt und auf den Datenträger 6 geschrieben (Stufe B). Jeder Datensatz wird dabei durch Auslesen des jeweiligen Festcodes eines Schlosses 2 aus dem Zentralenspeicherelement 12 und dessen Kombination mit dem eingegebenen Sollzeitfenster erzeugt. Der eingegebene Abholplan wird zudem in Klartext ausgedruckt und an eine Bedienperson zusammen mit der beschriebenen Chipkarte 6 übergeben (Stufe C).

[0029] Die Bedienperson fährt sodann in Stufe D das erste Schloss 2 mit der Maßgabe an, dass die Ankunftszeit innerhalb des zugeordneten Sollzeitfensters liegt. Die Chipkarte 6 wird dann in den Kartenleser 5 eingeführt. Hierauf wird die Bedienperson mittels des Display 16 zur Eingabe ihrer PIN aufgefordert. Dies erfolgt dann über die Tastatur 13 in üblicher Weise (Stufe E). Es erfolgt in Stufe F ein Vergleich der eingegebenen PIN mit allen gespeicherten PINs durch den Schlossprozessor 7. Ist dieser Vergleich negativ, so erfolgt ein Abbruch des Vorganges, eine Sperrung des Schlosses 2 in der Geschlossenstellung sowie optional ein Alarm. Die Chipkarte 6 wird nicht wieder ausgegeben. Ist der Vergleich positiv, so wird die Chipkarte 6 ausgelesen (Stufe G). Der Schlossprozessor 7 bestimmt dann mittels des Decodierprogramms durch Auslesen des dem Schloss 2 zugeordneten Festcodes aus dem Schlossspeicherelement 9 das Sollzeitfenster. Dann erfolgt ein Auslesen der Schlossprozessoruhr 8 und Vergleich der ausgelesenen Uhrzeit mit dem bestimmten Sollzeitfenster (Stufe H). Ist dieser Vergleich negativ, so erfolgt ein Abbruch des Vorganges, eine Sperrung des Schlosses 2 in der Geschlossenstellung sowie optional ein Alarm. Wenn die Uhrzeit innerhalb des Sollzeitfensters liegt, so wird das Schloss 2 in die Offenstellung angesteuert (Stufe I). Es erfolgt dann das Ent- oder Beladen des Wertbehältnisses 1 durch die Bedienperson (Stufe K). Bei Betätigung des Schlosses 2 aus der Offenstellung in die Geschlossenstellung wird durch den Kartenleser 5 auf die immer noch eingeführte Chipkarte 6 ein Quittierdatensatz geschrieben (Stufe K).

[0030] Sodann wiederholen sich die Stufen D bis K nach Maßgabe des Abholplanes. Nach Abarbeitung des Abholplanes werden dann mittels des Kartenlesers 10 des Zentralenprozessors 3 die Quittierdatensätze ausgelesen und zu Dokumentationszwecken abgespei-

chert.

[0031] In der Figur 3 der Übersichtlichkeit halber nicht dargestellt ist, dass nach Auslesung eines Datensatzes und Ansteuerung des Schlosses 2 in die Offenstellung im Schlossprozessor 7 eine erneute Ansteuerung des Schlosses 2 durch erneutes Auslesen desselben Datensatzes gesperrt ist. Dies verhindert, dass sofort nach Stufe K die Stufen D bis K beim gleichen Schloss nochmals durchlaufen werden. Die Sperrung kann auf verschiedenste Weise erfolgen. Beispielsweise kann das Schloss 2 eine übliche Zeitsteuerung aufweisen, die ein erneutes Öffnen nach einer Öffnung für einen vorgegebenen Zeitraum, beispielsweise 1 bis 24 Stunden, seit der letzten Öffnung, sperrt. Auch kann eine Sperrung erfolgen im Falle des Auslesens eines Quittierdatensatzes von der Chipkarte 6, deren Quittierzeit im Sollzeitfenster liegt. In einer besonders einfachen Variante wird der Datensatz durch den Schlossprozessor 7 in einer der Stufen G bis K von der Chipkarte 6 gelöscht.

[0032] Zusätzlich Sicherheit wird gewährleistet, wenn über die Darstellung der Figur 3 hinaus durch den Schlossprozessor 7 eine Ansteuerung des Schlosses 2 in die Offenstellung sperrbar ist, wenn zu einem Datensatz für ein anderes Schloss 2 mit zeitlich früherem Sollzeitfenster kein Quittierdatensatz auf den Datenträger 6 geschrieben ist und/oder wenn zu einem Datensatz für ein anderes Schloss 2 mit zeitlich späterem Sollzeitfenster ein Quittierdatensatz auf den Datenträger 6 geschrieben ist. Anschließend an die Stufe E prüft dabei der Schlossprozessor 7 alle Datensätze sowie alle Quittierdatensätze. Datensätze mit bereits geendeten Sollzeitfenstern müssen dabei mit Quittierdatensätzen korreliert sein. Datensätze mit noch nicht begonnenen Sollzeitfenstern dürfen nicht mit einem Quittierdatensatz korreliert sein. Ist eine dieser Bedingungen nicht erfüllt, so erfolgt Abbruch.

[0033] Als allgemeine Vorteile der Erfindung ergeben sich: i) Es brauchen keine Codes mehr über drahtgebundene oder drahtlose Telekommunikationsverbindungen übertragen werden, ii) keine offenen Listen mit "Einmalcodes" sind mehr erforderlich, und iii) die Verwaltungssoftware des Zentralenprozessors ist sehr einfach und effizient gestaltbar. Vorteile der konkreten Ausführungsformen sind: i) Die Datensätze sind auslese- und kopiergeschützt auf dem Datenträger gesichert, ii) die Datensätze werden automatisch in der Sicherheitsbox und somit extern von dem Terminal erzeugt, und iii) die Software und Datenspeicher des zentralenprozessors sind wirksam gegen unbefugte Eingriffe gesichert.

Patentansprüche

1. Schlosssystem mit einer Mehrzahl von jeweils an einem Wertbehältnis (1) angebrachten und dieses verschließenden Schlössern (2), mit einem von den Schlössern (2) beabstandeten und mit den Schlössern (2) nicht verbundenen Zen-

tralenrechner (3), und
mit einem mobilen Datenträger,
wobei jedes der Schlösser (2) jeweils mittels einer
elektronischen Schaltung (4) über ein elektrisch an-
steuerbares Stellglied (14) aus einer Geschlossen-
stellung in eine Offenstellung ansteuerbar ist,
wobei jede elektronische Schaltung (4) Mittel (5) zum
Auslesen des mobilen Datenträgers (6), einen
Schlossprozessor (7) mit einer internen Schlosspro-
zessoruhr (8) sowie ein Schlossspeicherelement (9),
worin ein Decodierprogramm sowie ein dem jewei-
ligen Schloss (2) zugeordneter Festcode gespei-
chert sind, aufweist,
wobei der Zentralenrechner (3) Mittel (10) zum Be-
schreiben des mobilen Datenträgers (6), einen Zen-
tralprozessor (11) sowie ein Zentralenspeichere-
lement (12), worin ein Codierprogramm und der je-
dem Schloss (2) zugeordnete Festcode gespeichert
sind, aufweist,
wobei mittels des Codierprogramms ein Datensatz
erzeugbar und auf den Datenträger (6) schreibbar
ist, wobei der Datensatz durch Auslesen des Fest-
codes aus dem Zentralenspeicherelement (12) und
dessen Kombination mit einem dem Zentralenpro-
zessor (11) eingegebenen Sollzeitfenster erzeugbar
ist,
wobei der Datensatz des Datenträgers (6) mittels
der Mittel (5) zum Auslesen des Datenträgers (6)
auslesbar ist, wobei im zugeordneten Schlosspro-
zessor (7) mittels des Decodierprogramms durch
Auslesen des dem jeweiligen Schloss (2) zugeord-
neten Festcodes aus dem zugeordneten Schloss-
speicherelement (9) das Sollzeitfenster bestimmbar
ist, wobei durch Auslesen der zugeordneten Schlos-
sprocessoruhr (8) und Vergleich der ausgelesenen
Uhrzeit mit dem bestimmten Sollzeitfenster das
Schloss (2) in die Offenstellung ansteuerbar ist,
wenn die Uhrzeit innerhalb des Sollzeitfensters liegt,
und wobei auf den Datenträger (6) eine Mehrzahl
von verschiedenen Datensätzen geschrieben ist,
wobei jeder Datensatz eine Kombination eines ei-
nem Schloss (2) zugeordneten Festcodes und eines
Sollzeitfensters ist, wobei die Datensätze sich durch
verschiedene, verschiedenen Schlössern (2) zuge-
ordnete Festcodes und durch verschiedene Sollzeit-
fenster unterscheiden,
dadurch gekennzeichnet,
dass jeder Schlossprozessor so angepasst ist,
dass bei Betätigung des Schlosses (2) aus der Of-
fenstellung in die Geschlossenstellung ein Quittier-
datensatz durch den Schlossprozessor (7) auf den
Datenträger (6) geschrieben wird, und
dass durch den Schlossprozessor (7) eine Ansteu-
erung des Schlosses (2) in die Offenstellung ge-
sperrt wird, wenn zu einem Datensatz für ein ande-
res Schloss (2) mit zeitlich früherem Sollzeitfenster
kein Quittierdatensatz auf den Datenträger (6) ge-
schrieben ist und/oder wenn zu einem Datensatz für

ein anderes Schloss (2) mit zeitlich späterem Soll-
zeitfenster ein Quittierdatensatz auf den Datenträger
(6) geschrieben ist.

- 5 2. Schlosssystem nach Anspruch 1, wobei nach Aus-
lesung eines Datensatzes und Ansteuerung des
Schlosses (2) in die Offenstellung im Schlosspro-
zessor (7) eine erneute Ansteuerung des Schlosses
(2) durch erneutes Auslesen desselben Datensatzes
sperrbar ist und/oder der Datensatz durch den
Schlossprozessor (7) von dem Datenträger (6) ge-
löscht wird.
- 10 3. Schlosssystem nach einem der Ansprüche 1 oder
2, wobei das Schloss (2) Mittel (13) zum Eingeben
eines Identifikationscodes aufweist, wobei in dem
Schlossspeicherelement (9) ein Identifikationscode
eingespeichert ist, und wobei eine Ansteuerung des
Schlosses (2) in die Offenstellung bei Nichtüberein-
stimmung des gespeicherten Identifikationscodes
mit dem eingegebenen Identifikationscode durch
den Schlossprozessor (7) sperrbar ist.
- 15 4. Verfahren zum Betrieb eines Schlosssystems nach
einem der Ansprüche 1 bis 3,
 - a) wobei durch den Zentralenprozessor (11) ei-
ne Mehrzahl verschiedener Datensätze codiert
und auf den Datenträger (6) geschrieben wird,
 - b) wobei eine Bedienperson den Datenträger (6)
sowie einen Abholplan für die Entleerung
und/oder Befüllung mehrerer verschiedener
Wertbehältnisse (1) erhält, wobei jedem Wert-
behältnis (1) ein Sollzeitfenster zugeordnet ist,
 - c) wobei die Bedienperson ein Wertbehältnis (1)
nach Maßgabe des Abholplans aufsucht und
durch den Schlossprozessor (7) des im Rahmen
des Wertbehältnisses (1) eingerichteten
Schlosses (2) die Datensätze aus dem Daten-
träger (6) auslesen lässt,
 - d) wobei im Schlossprozessor (7) die Datensät-
ze decodiert werden und bei Übereinstimmung
der aus der Schlossprocessoruhr (8) ausgele-
senen Uhrzeit mit einem Sollzeitfenster das
Schloss (2) in die Offenstellung angesteuert
wird,
 - e) wobei nach Ansteuerung des Schlosses (2)
des Wertbehältnisses (1) in die Offenstellung
die Wertbehältnisse (1) durch die Bedienperson
entleert und/oder befüllt werden,
 - f) wobei das geöffnete Schloss (2) durch Schlie-
ßen des Wertbehältnisses (1) in die Geschlos-
senstellung gebracht wird,
 - g) wobei durch den Schlossprozessor (7) ein
Quittierdatensatz auf den Datenträger (6) ge-
schrieben wird, und
 - h) wobei sich die Verfahrensschritte c) bis g) je-
weils für verschiedene Wertbehältnisse (1) bzw.
- 20
- 25
- 30
- 35
- 40
- 45
- 50
- 55

Schlösser (2) wiederholen, wobei durch den Schlossprozessor (7) eine Ansteuerung des Schlosses (2) in die Offenstellung gesperrt wird, wenn zu einem Datensatz für ein anderes Schloss (2) mit zeitlich früherem Sollzeitfenster kein Quittierdatensatz auf den Datenträger (6) geschrieben ist und/oder wenn zu einem Datensatz für ein anderes Schloss (2) mit zeitlich späterem Sollzeitfenster ein Quittierdatensatz auf den Datenträger (6) geschrieben ist.

5. Verfahren nach Anspruch 4, wobei die Bedienperson bei jedem Schloss zusätzlich einen Identifikationscode eingibt.

Claims

1. Lock system with a plurality of locks (2), each of which is fixed to and locks a valuables container (1), a central computer (3) at a distance from the locks (2) and not connected to the locks (2), and a mobile data medium, each of the locks (2) being actuatable in each case by means of an electronic circuit (4) via an electrically actuatable actuator (14) from a closed position into an open position, each electronic circuit (4) comprising means (5) for reading the mobile data medium (6), a lock processor (7) with an internal lock processor clock (8) and a lock storage element (9) in which a decoding program and a secure code assigned to the respective lock (2) are stored, the central computer (3) comprising means (10) for writing to the mobile data medium (6), a central processor (11) and a central storage element (12) in which a coding program and the secure code assigned to each lock (2) are stored, it being possible to generate a data record and write said record to the data medium (6) by means of the coding program, it being possible to generate the data record by reading the secure code from the central storage element (12) and combining said code with a desired time window which is entered in the central processor (11), the data record of the data medium (6) being readable by the means (5) for reading the data medium (6), it being possible to determine the desired time window in the assigned lock processor (7) using the decoding program by reading the secure code assigned to the respective lock (2) from the assigned lock storage element (9), it being possible, by means of reading the assigned lock processor clock (8) and comparing the read time with the specified desired time window, to actuate the lock (2) into the open position if the time is within the desired time window, and a plurality of different data records being written to the data medium (6), each data record being a combination of a secure code, assigned to a lock (2), and a desired time window, the data records differing from one another by different secure codes assigned to different

locks (2) and by different desired time windows, **characterised in that** each lock processor is adapted such that, when the lock (2) is actuated from the open position into the closed position, an acknowledgement data record is written to the data medium (6) by the lock processor (7), and **in that** actuation of the lock (2) into the open position is blocked by the lock processor (7) if no acknowledgement data record is written to the data medium (6) for a data record for another lock (2) having an earlier desired time window and/or if an acknowledgement data record is written to the data medium (6) for a data record for another lock (2) having a later desired time window.

2. Lock system according to claim 1, wherein, following the reading of a data record and the actuation of the lock (2) into the open position, re-actuation of the lock (2) resulting from the same data record being read again can be blocked in the lock processor (7) and/or the data record is erased from the data medium (6) by the lock processor (7).
3. Lock system according to either claim 1 or claim 2, wherein the lock (2) comprises means (13) for entering an identification code, wherein an identification code is stored in the lock storage element (9), and wherein actuation of the lock (2) into the open position can be blocked by the lock processor (7) in the event of a mismatch between the stored identification code and the entered identification code.
4. Method for operating a lock system according to any of claims 1 to 3,
 - a) wherein a plurality of different data records are coded and written to the data medium (6) by the central processor (11),
 - b) wherein an operator receives the data medium (6) and a collection plan for emptying and/or filling a plurality of different valuables containers (1), wherein a desired time window is assigned to each valuables container (1),
 - c) wherein the operator searches for a valuables container (1) in accordance with the collection plan and, by means of the lock processor (7), initiates reading the data records from the data medium (6) for the lock (2) fitted in the frame of the valuables container (1),
 - d) wherein the data records are decoded in the lock processor (7) and the lock (2) is actuated into the open position if the time read from the lock processor clock (8) corresponds to a desired time window,
 - e) wherein, after actuation of the lock (2) of the valuables container (1) into the open position, the valuables containers (1) are emptied and/or filled by the operator,

f) wherein the opened lock (2) is moved into the closed position by closing the valuables container (1),

g) wherein an acknowledgement data record is written to the data medium (6) by the lock processor (7), and

h) wherein the method steps c) to g) are each repeated for different valuables container (1) or locks (2) respectively, wherein actuation of the lock (2) into the open position is blocked by the lock processor (7) if no acknowledgement data record is written to the data medium (6) for a data record for another lock (2) having an earlier desired time window and/or if an acknowledgement data record is written to the data medium (6) for a data record for another lock (2) having a later desired time window.

5. Method according to claim 4, wherein the operator additionally enters an identification code for each lock.

Revendications

1. Système de verrou

avec une pluralité de verrous (2) respectivement montés sur un coffre-fort (1) et fermant celui-ci, avec un ordinateur central (3) éloigné des verrous (2) et non relié aux verrous (2), et avec un support de données mobile,

chacun des verrous (2) pouvant être commandé respectivement à l'aide d'un circuit électronique (4) par l'intermédiaire d'un organe de réglage (14) à commande électrique d'une position fermée vers une position ouverte,

chaque circuit électronique (4) comprenant des moyens (5) permettant de lire le support de données mobile (6), un processeur de verrou (7) avec une horloge de processeur de verrou interne (8) ainsi qu'un élément de mémoire de verrou (9), dans lequel un programme de décodage et un code fixe, respectivement correspondant au verrou (2), sont stockés, l'ordinateur central (3) comprenant des moyens (10) permettant d'écrire sur le support de données mobile (6), un processeur central (11) et un élément de mémoire centrale (12), dans lequel un programme de codage et le code fixe correspondant à chaque verrou (2) sont stockés,

un ensemble de données pouvant être générés à l'aide du programme de codage et pouvant être écrits sur le support de données (6), l'ensemble de données pouvant être généré par la lecture du code fixe provenant de l'élément de mémoire centrale (12) et de sa combinaison avec une fenêtre de temps de consigne entrée dans le processeur central (11), l'ensemble de données du support de données (6) pouvant être lu à l'aide des moyens (5) de lecture

du support de données (6), la fenêtre de temps de consigne pouvant être déterminée dans le processeur de verrou (7) correspondant à l'aide du programme de décodage par la lecture du code fixe correspondant au verrou (2) et provenant de l'élément de mémoire centrale (9) correspondant, la lecture de l'horloge de processeur de verrou (8) correspondante et la comparaison entre l'heure lue et la fenêtre de temps de consigne déterminée permettant de commander le passage du verrou (2) à la position ouverte si l'heure se trouve à l'intérieur de la fenêtre de temps de consigne et, sur le support de données (6), sont écrits une pluralité d'ensembles de données, chaque ensemble de données étant une combinaison d'un code fixe correspondant à un verrou (2) et d'une fenêtre de temps de consigne, les ensembles de données se différenciant par différents codes fixes correspondant à différents verrous (2) et par différentes fenêtres de temps de consigne,

caractérisé en ce que

chaque processeur de verrou est conçu de façon à ce que, lors de l'actionnement du verrou (2) pour le passage de la position ouverte vers la position de fermeture, un ensemble de données d'acquiescement est écrit par le processeur de verrou (7) sur le support de données (6) et

grâce au processeur de verrou (7), une commande du verrou (2) pour le passage vers la position ouverte est bloquée lorsque, pour un ensemble de données pour un autre verrou (2), avec une fenêtre de temps de consigne antérieur dans le temps, aucun ensemble de données d'acquiescement n'est écrit sur le support de données (6) et/ou si, pour un ensemble de données pour un autre verrou (2), avec une fenêtre de temps de consigne plus tardive dans le temps, un ensemble de données d'acquiescement est écrit sur le support de données (6).

2. Système de verrou selon la revendication 1, une nouvelle commande du verrou (2) pouvant être bloquée, après la lecture d'un ensemble de données et la commande du verrou (2) vers la position de fermeture dans le processeur de verrou (7), par une nouvelle lecture du même ensemble de données et/ou l'ensemble de données étant effacé du support de données (6) par le processeur de verrou (7).

3. Système de verrou selon l'une des revendications 1 ou 2, le verrou (2) comprenant des moyens (13) d'entrée d'un code d'identification, un code d'identification étant stocké dans l'élément de mémoire de verrou (9) et une commande du verrou (2) vers la position ouverte si le code d'identification stocké ne correspond pas au code d'identification entrée peut être bloquée par le processeur de verrou (7).

4. Procédé d'utilisation d'un système de verrou selon

l'une des revendications 1 à 3

- a) le processeur central (11) permettant de coder une pluralité de différents ensembles de données et de les écrire sur le support de données (6), 5
- b) un opérateur recevant le support de données (6) ainsi qu'un plan de ramassage pour le vidage et/ou le remplissage de différents coffres-forts (1), une fenêtre de temps de consigne correspondant à chaque coffre-fort (1), 10
- c) l'opérateur recherchant un coffre-fort (1) selon le plan de ramassage et ordonnant au processeur de verrou (7) du verrou (2) inséré dans le cadre du coffre-fort (1) de faire lire les ensembles de données sur le support de données (6), 15
- d) les ensembles de données étant décodés dans le processeur de verrou (7) et si l'heure lue sur l'horloge du processeur de verrou (8) correspond à une fenêtre de temps de consigne, le verrou (2) est commandé vers la position ouverte, 20
- e) suite à la commande du verrou (2) du coffre-fort (1) vers la position ouverte, les coffres-forts (1), étant vidés et/ou remplis par l'opérateur, 25
- f) le verrou (2) ouvert étant mis en position fermée par la fermeture du coffre-fort (1),
- g) le processeur de verrou (7) permettant d'écrire un ensemble de données d'acquiescement sur le support de données (6), et 30
- h) les étapes du procédé c) à g) étant respectivement répétées pour différents coffres-forts (1) ou verrous (2) respectivement, le processeur de verrou (7) bloquant une commande du verrou (2) vers la position ouverte si, pour un ensemble de données, pour un autre verrou (2) avec une fenêtre de temps de consigne plus tôt dans le temps, aucun ensemble de données d'acquiescement n'est écrit sur le support de données (6) et/ou si, pour un ensemble de données, pour un autre verrou (2) avec une fenêtre de temps de consigne plus tard dans le temps, un ensemble de données d'acquiescement est écrit sur le support de données (6). 40

45

5. Procédé selon la revendication 4, l'opérateur entrant en outre pour chaque verrou un code d'identification.

50

55

FIG.1

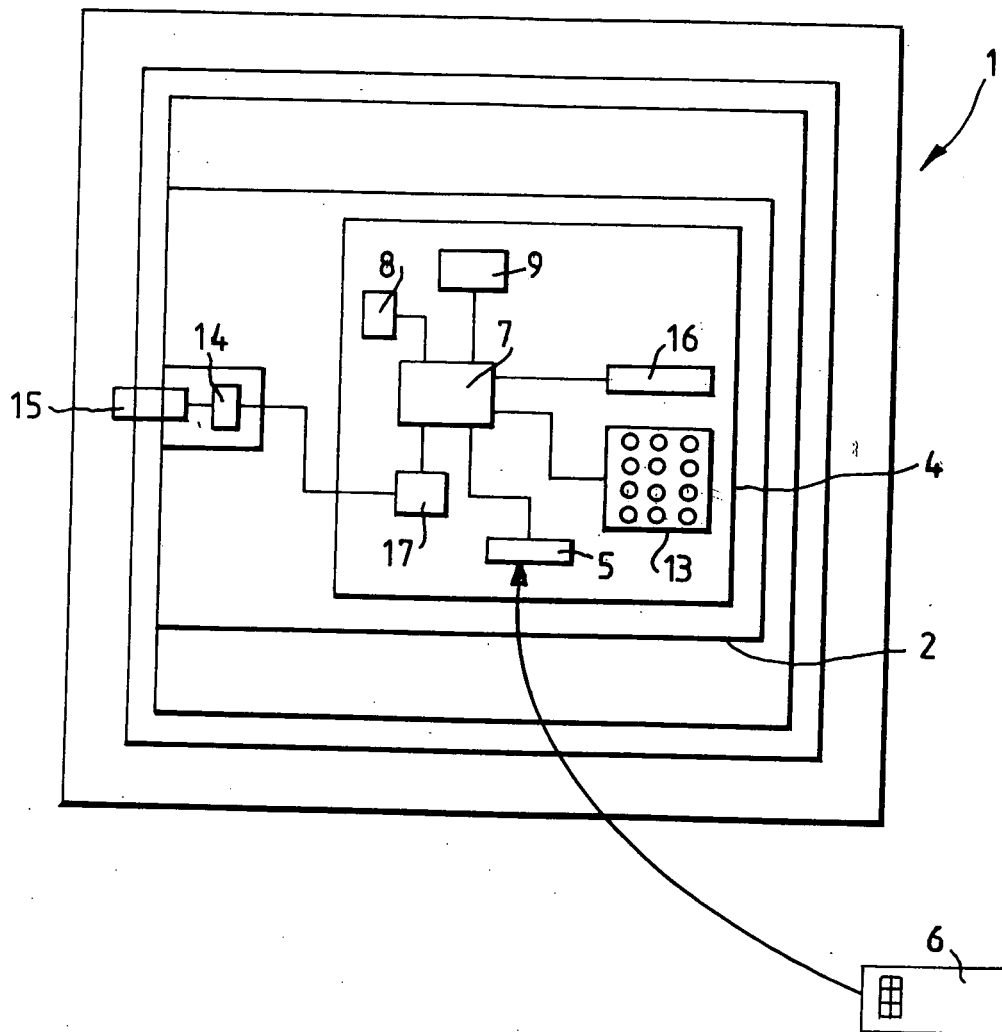


FIG.2

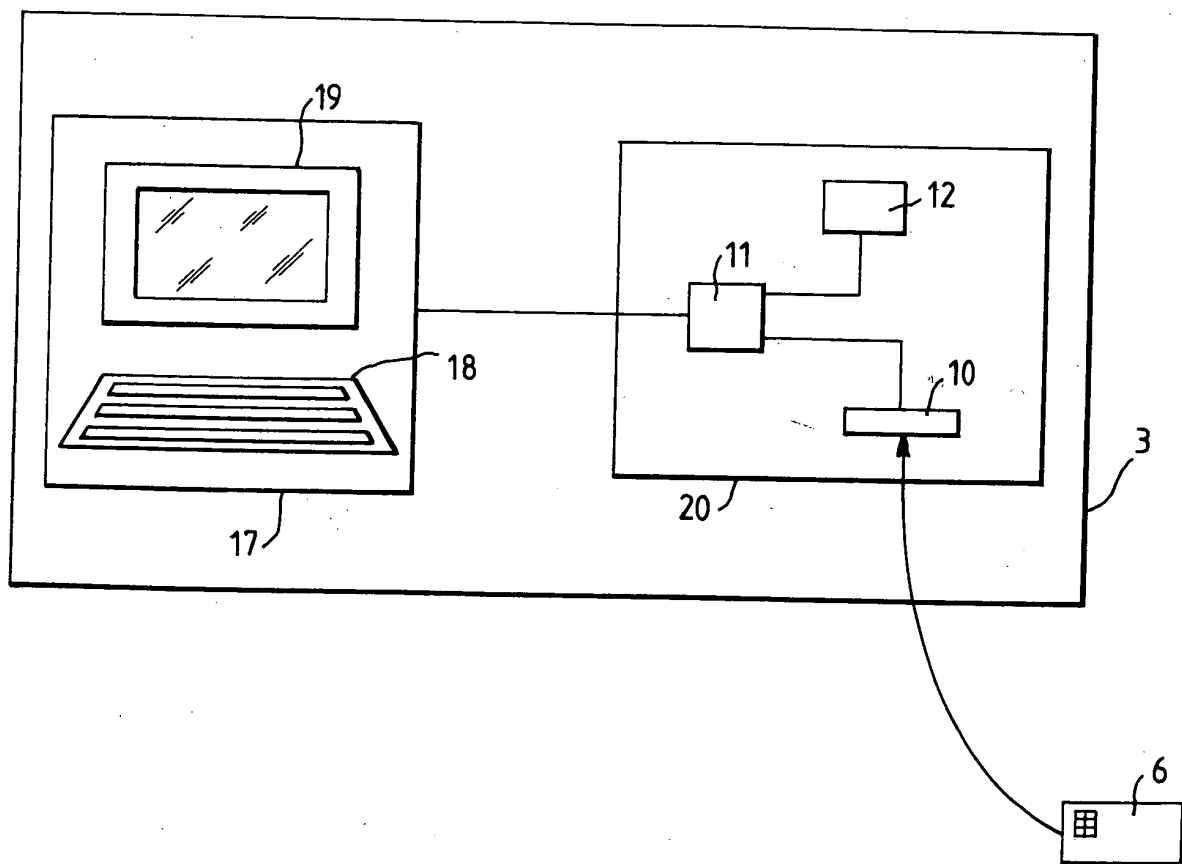
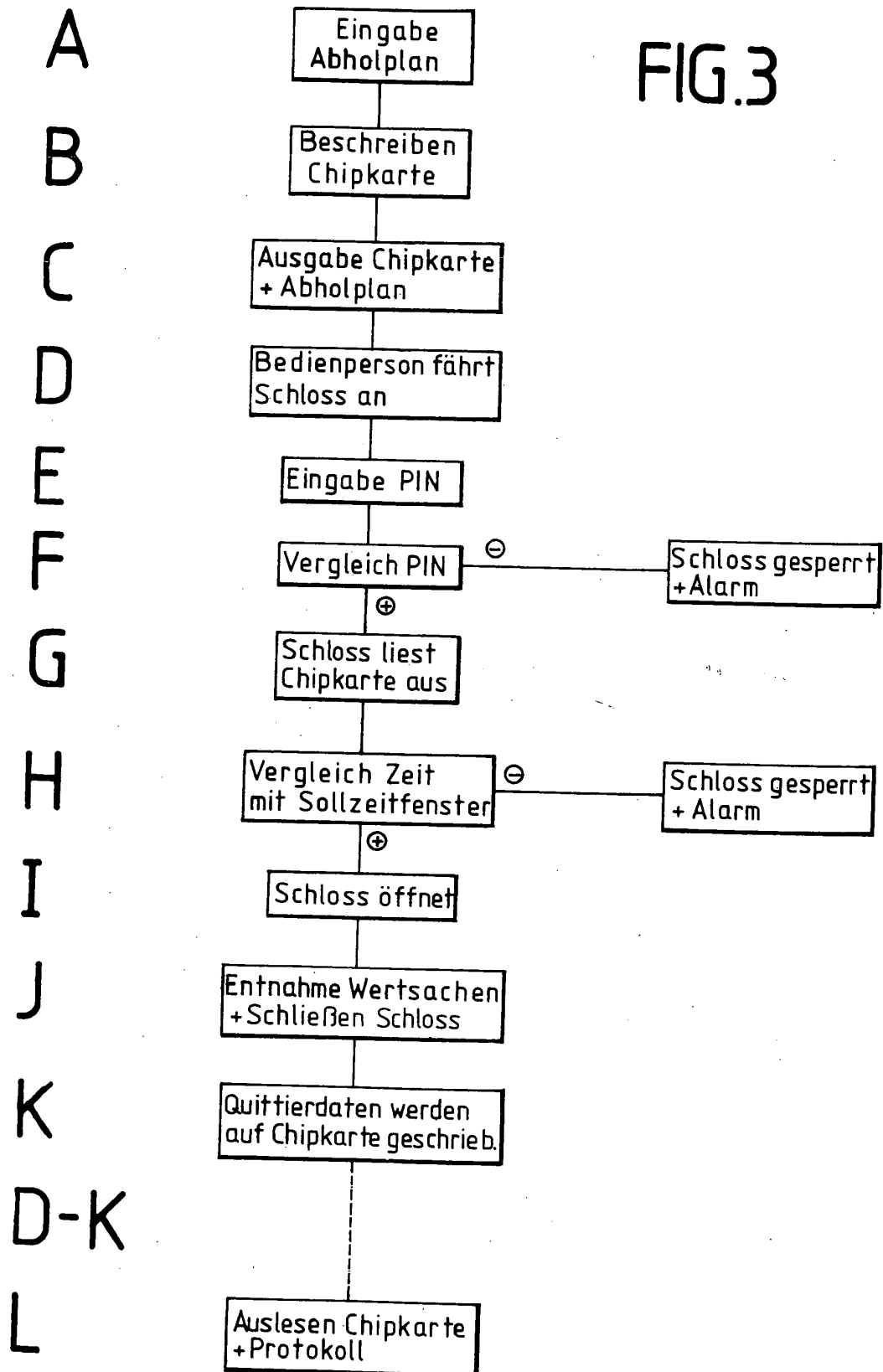


FIG.3



IN DER BESCHREIBUNG AUFGEFÜHRTE DOKUMENTE

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

In der Beschreibung aufgeführte Patentdokumente

- DE 3711746 [0005]
- DE 19535065 A [0025]