

(19)



Europäisches Patentamt

European Patent Office

Office européen des brevets



(11)

EP 1 703 473 A2

(12)

EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
20.09.2006 Patentblatt 2006/38

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

(21) Anmeldenummer: **06001068.3**

(22) Anmeldetag: **19.01.2006**

(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**
Benannte Erstreckungsstaaten:
AL BA HR MK YU

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

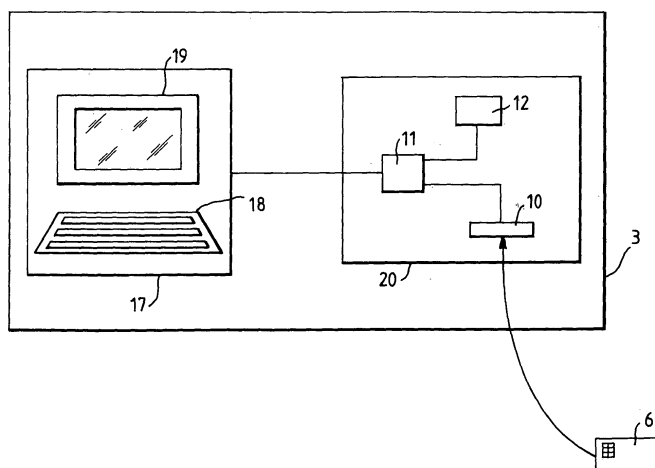
(74) Vertreter: **Jungblut, Bernhard Jakob et al**
Albrecht, Lüke & Jungblut,
Patentanwälte,
Gelfertstrasse 56
14195 Berlin (DE)

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

(71) Anmelder: **INSYS MICROELECTRONICS GMBH**
98047 Regensburg (DE)

(54) Schlosssystem

(57) Die Erfindung betrifft ein Schlosssystem mit zumindest einem Schloss (2), und mit einem Zentralenrechner (3), wobei das Schloss (2) mittels einer elektronischen Schaltung (4) über ein elektrisch ansteuerbares Stellglied (14) in eine Offenstellung ansteuerbar ist, wobei die elektronische Schaltung (4) Mittel (5) zum Auslesen eines Datenträgers (6), einen Schlossprozessor (7) mit einer internen Schlossprozessoruhr (8) sowie ein Schlossspeicherelement (9), worin ein Decodierprogramm sowie ein Festcode gespeichert sind, aufweist, wobei der Zentralenrechner (3) Mittel (10) zum Beschreiben des mobilen Datenträgers (6), einen Zentralenprozessor (11) sowie ein Zentralspeicherelement (12), worin ein Codierprogramm und der Festcode gespeichert sind, aufweist, wobei ein Datensatz erzeugbar und auf den Datenträger (6) schreibbar ist, wobei der Datensatz durch Auslesen des Festcodes und dessen Kombination mit einem eingegebenen Sollzeitfenster erzeugbar ist, wobei der Datensatz mittels der Mittel (5) zum Auslesen des Datenträgers (6) auslesbar ist, wobei im Schlossprozessor (7) mittels des Decodierprogramms durch Auslesen des Festcodes aus dem Schlossspeicherelement (9) das Sollzeitfenster bestimmbar ist, und wobei durch Auslesen der Schlossprozessoruhr (8) und Vergleich der Uhrzeit mit dem Sollzeitfenster das Schloss (2) in die Offenstellung ansteuerbar ist, wenn die Uhrzeit innerhalb des Sollzeitfensters liegt.

FIG.2**EP 1 703 473 A2**

Beschreibung

Gebiet der Erfindung

5 **[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

15 **[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 typischerweise um einen Festcode, i.e. der Code ist einem Schloss zugeordnet und wird im normalen Betrieb nicht geändert.

25 **[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.

30 **[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 verbesserungsfähig.

Technisches Problem der Erfindung

35 **[0005]** 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

40 **[0006]** Zur Lösung dieses technischen Problems lehrt die Erfindung ein Schlosssystem mit zumindest einem an einem Wertbehältnis angebrachten und dieses verschließenden Schloss, mit einem von dem Schloss beabstandeten und mit dem Schloss nicht verbundenen Zentralenrechner, 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 Decodierprogramm sowie ein dem 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 dem 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 Schlossprozessor mittels des Decodierprogramms durch Auslesen des dem Schloss zugeordneten Festcodes aus dem Schlossspeicherelement das Sollzeitfenster bestimmbar ist und wobei durch Auslesen der 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.

55 **[0007]** Der Zentralenrechner ist mit dem Schloss nicht verbunden in dem Sinne, dass keinerlei unmittelbare Verbin-

dung, 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 Auslese-schutz und Sabotageschutz auszustatten.

[0008] Dagegen ist die elektronische Schaltung unmittelbar mit dem Schloss verbunden, beispielsweise mittels elek-trischer Leitungen oder drahtloser Übermittlung von Signalen. Typischerweise bildet sie sogar ein Bauteil des Schlosses.

[0009] Als Datenträger kommen grundsätzlich alle fachüblichen Datenträger in Frage. Beispiele hierfür sind: Magnet-karte, Chipkarte, mobiler Speicherbaustein usw.. Im Falle der Chipkarte, welche bevorzugt ist, kann diese passwortge-schützt 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.

[0010] 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 Schlos-sprozessoruhren nahezu synchron zueinander. Im Rahmen beispielsweise jährlicher Wartungen kann eine Synchroni-sierung eventueller Abweichungen durch Drift erfolgen, falls einzelne Schlossprozessoruhren gegenüber einer Referenzzeit um mehr als ein definiertes Divergenzzeitintervall vor- oder nachgehen.

[0011] 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. Entspre-chendes gilt für die Schlossprozessoruhr, welche in der Regel integraler Bestandteil des Prozessors i.V. mit dem Be-triebsprogramm des Prozessors ist.

[0012] Ein einem Schloss zugeordneter Festcode ist einzigartig, ausschließlich für das betreffende Schloss eingerichtet und im Schlossspeicherelement sowie im Zentralenspeicherelement gespeichert. Die Festcodes verschiedener Schlös-ser 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..

[0013] 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 Zeit-intervall, in welchem eine Öffnung des dem Festcode zugeordneten Wertbehältnisses durch eine autorisierte Person zulässig und möglich sein soll. Eine Öffnung außerhalb dieses Sollzeitfensters ist dagegen nicht möglich. Das einzuge-bende Sollzeitfenster entspricht einem Wechselcode, da bei jeder zulässigen Öffnung dies zu jeweils anderen Zeitpunk-ten 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 an-dere 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 An-fangszeitpunkt 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 Verschlüs-selungscode ebenfalls sowohl im Zentralenspeicherelement als auch im Schlossspeicherelement gespeichert. Durch Änderung des Verschlüsselungscodes kann dann - bei Beibehaltung des eigentlichen Verschlüsselungsalgorithmus - 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.

[0014] Mit einem erfindungsgemäßen Schlosssystem wird eine erhebliche Verbesserung der Sicherheit dadurch er-reicht, 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 Schlossprozessor-Uhrzeit mit dem ausgelesenen Sollzeitfenster nicht in die Offenstellung ansteuerbar ist.

[0015] Bevorzugt ist es, wenn auf den Datenträger eine Mehrzahl von verschiedenen Datensätzen schreibbar ist, 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 Zentralenrechners ein Abholplan für eine Person eines Werttransportunternehmens erstellt werden, in welchem die Reihenfolge, mit Zeitintervallangaben, der Öffnung der Wertbehältnisse vorgegeben ist.

[0016] 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 zeitnahe 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.

[0017] 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.

[0018] In einer Weiterbildung der Erfindung ist es möglich, bei Betätigung des Schlosses aus der Offenstellung in die Geschlossenstellung einen Quittierdatensatz durch den Schlossprozessor auf den Datenträger schreiben zu lassen. 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 offenbaren 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 den Schaltzuständen detektierbar und unterscheidbar. Wird vom Schlossprozessor die Flanke der Betätigung des Schlosses in die Geschlossenstellung detektiert, erfolgt dann die Quittierung, wie vorstehend beschrieben.

[0019] In der Ausführungsform mit Quittierdatensätzen können diese nach Abarbeitung des Abholplanes wiederum in den Zentralenrechner eingelesen werden, wodurch der gesamte Abholvorgang dann abgeschlossen und protokolliert ist.

[0020] In der Ausführungsform 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.

[0021] Die Erfindung betrifft des Weiteren ein Verfahren zum Betrieb eines erfindungsgemäßen Schlosssystems, a) wobei durch den Zentralenprozessor (11) ein Datensatz oder eine 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 eines oder mehrerer verschiedener Wertbehältnisse (1) erhält, wobei jedem Wertbehältnis (1) ein Sollzeitfenster zugeordnet ist, c) wobei die Bedienperson das 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 Datenträger (6) auslesen lässt, d) wobei im Schlossprozessor (7) die Datensätze decodiert werden und bei Übereinstimmung der aus der Schlossprozessoruhr (8) ausgelesenen 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 das Wertbehältnis (1) durch die Bedienperson entleert und/oder befüllt wird, f) wobei das geöffnete Schloss (2) durch Schließen des Wertbehältnisses (1) in die Geschlossenstellung gebracht wird, g) wobei optional durch den Schlossprozessor (7) ein Quittierdatensatz auf den Datenträger (6) geschrieben wird und/oder der dem Schloss (2) zugeordnete Datensatz auf dem Datenträger (6) gelöscht wird, und h) wobei sich in der Alternative mit einer Mehrzahl von Datensätzen die Verfahrensschritte c) bis g) jeweils für verschiedene Wertbehältnisse (1) bzw. Schlösser (2) wiederholen. Bevorzugt ist es, wenn die Bedienperson bei jedem Schloss zusätzlich einen Identifikationscode eingeben muss.

[0022] 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 einsetztem Schloss,

Figur 2: eine schematische Darstellung eines erfindungsgemäß eingesetzten Zentralenrechners,

Figur 3: ein Ablaufdiagramm eines erfindungsgemäßen Betriebsverfahrens.

[0023] In der Figur 1 erkennt man als eine erste Komponenten 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 Sperr-
element 15 aus einer Geschlossenstellung in eine Offenstellung bewegt. In der gezeigten Darstellung ist das Sperr-
glied 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
einggegebenen PIN durch den Schlossprozessor 7 gesperrt. Schließlich erkennt man ein Display 19, welcher der Dia-
logführung 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 Sperr-
element 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.

[0024] In der Figur 2 erkennt man als weitere Komponente des erfindungsgemäßen Schlosssystems einen Zentra-
lenrechner 3. Dieser umfasst Mittel 10 zum Beschreiben der Chipkarte 6, einen Zentralenprozessor 11 sowie ein Zentra-
lenspeicherelement 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.

[0025] 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.

[0026] In der Figur 3 sind die Abläufe einer einfachen Variante eines erfindungsgemäßen Verfahrens dargelegt. 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).

[0027] 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).

[0028] 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 abgespeichert.

[0029] 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 Auslesen 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.

[0030] 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.

[0031] 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 zumindest einem an einem Wertbehältnis (1) angebrachten und dieses verschließenden Schloss (2), und
 mit einem von dem Schloss (2) beabstandeten und mit dem Schloss (2) nicht verbundenen Zentralenrechner (3),
 wobei das Schloss (2) mittels einer elektronischen Schaltung (4) über ein elektrisch ansteuerbares Stellglied (14)
 aus einer Geschlossenstellung in eine Offenstellung ansteuerbar ist,
 wobei die elektronische Schaltung (4) Mittel (5) zum Auslesen eines mobilen Datenträgers (6), einen Schlosspro-
 zessor (7) mit einer internen Schlossprozessoruhr (8) sowie ein Schlossspeicherelement (9), worin ein Decodier-
 programm sowie ein dem Schloss (2) zugeordneter Festcode gespeichert sind, aufweist,
 wobei der Zentralenrechner (3) Mittel (10) zum Beschreiben des mobilen Datenträgers (6), einen Zentralenprozessor
 (11) sowie ein Zentralenspeicherelement (12), worin ein Codierprogramm und der 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 Festcodes aus dem Zentralenspeicherelement (12) und dessen Kombi-
 nation mit einem dem Zentralenprozessor (11) eingegebenen Sollzeitfenster erzeugbar ist,
 wobei der Datensatz des Datenträgers (6) mittels der Mittel (5) zum Auslesen des Datenträgers (6) auslesbar ist,
 wobei im Schlossprozessor (7) mittels des Decodierprogramms durch Auslesen des dem Schloss (2) zugeordneten
 Festcodes aus dem Schlossspeicherelement (9) das Sollzeitfenster bestimmbar ist, und wobei durch Auslesen der
 Schlossprozessoruhr (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.

2. Schlosssystem nach Anspruch 1, wobei auf den Datenträger (6) eine Mehrzahl von verschiedenen Datensätzen
 schreibbar ist, wobei jeder Datensatz eine Kombination eines einem Schloss (2) zugeordneten Festcodes und eines
 Sollzeitfensters ist, wobei die Datensätze sich durch verschiedene, verschiedenen Schlössern (2) zugeordnete
 Festcodes und/oder durch verschiedene Sollzeitfenster unterscheiden.

3. Schlosssystem nach einem der Ansprüche 1 oder 2, wobei 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 sperrbar ist und/oder der Datensatz durch den Schlossprozessor (7)
 von dem Datenträger (6) gelöscht wird.

4. Schlosssystem nach einem der Ansprüche 1 bis 3, wobei das Schloss (2) Mittel (13) zum Eingeben eines Identifi-
 kationscodes aufweist, wobei in dem Schlossspeicherelement (9) ein Identifikationscode eingespeichert ist, und
 wobei eine Ansteuerung des Schlosses (2) in die Offenstellung bei Nichtübereinstimmung des gespeicherten Iden-
 tifikationscodes mit dem eingegebenen Identifikationscode durch den Schlossprozessor (7) sperrbar ist.

5. Schlosssystem nach einem der Ansprüche 1 bis 4, wobei bei Betätigung des Schlosses (2) aus der Offenstellung
 in die Geschlossenstellung ein Quittierdatensatz durch den Schlossprozessor (7) auf den Datenträger (6) schreibbar
 ist.

6. Schlosssystem nach Anspruch 5 in der Ausführungsform mit mehreren verschiedenen Datensätzen, wobei 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 Sollzeit-
 fenster ein Quittierdatensatz auf den Datenträger (6) geschrieben ist.

7. Verfahren zum Betrieb eines Schlosssystems nach einem der Ansprüche 1 bis 6,

a) wobei durch den Zentralenprozessor (11) ein Datensatz oder eine 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
 eines oder mehrerer verschiedener Wertbehältnisse (1) erhält, wobei jedem Wertbehältnis (1) ein Sollzeitfenster
 zugeordnet ist,

c) wobei die Bedienperson das 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 Datenträger (6) auslesen lässt,

d) wobei im Schlossprozessor (7) die Datensätze decodiert werden und bei Übereinstimmung der aus der

Schlossprozessoruhr (8) ausgelesenen 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 das Wertbehältnis (1) durch die Bedienperson entleert und/oder befüllt wird,

f) wobei das geöffnete Schloss (2) durch Schließen des Wertbehältnisses (1) in die Geschlossenstellung gebracht wird,

g) wobei optional durch den Schlossprozessor (7) ein Quittierdatensatz auf den Datenträger (6) geschrieben wird und/oder der dem Schloss (2) zugeordnete Datensatz auf dem Datenträger (6) gelöscht wird, und

h) wobei sich in der Alternative mit einer Mehrzahl von Datensätzen die Verfahrensschritte c) bis g) jeweils für verschiedene Wertbehältnisse (1) bzw. Schlösser (2) wiederholen.

8. Verwendung nach Anspruch 7, wobei die Bedienperson bei jedem Schloss zusätzlich einen Identifikationscode eingibt.

FIG.1

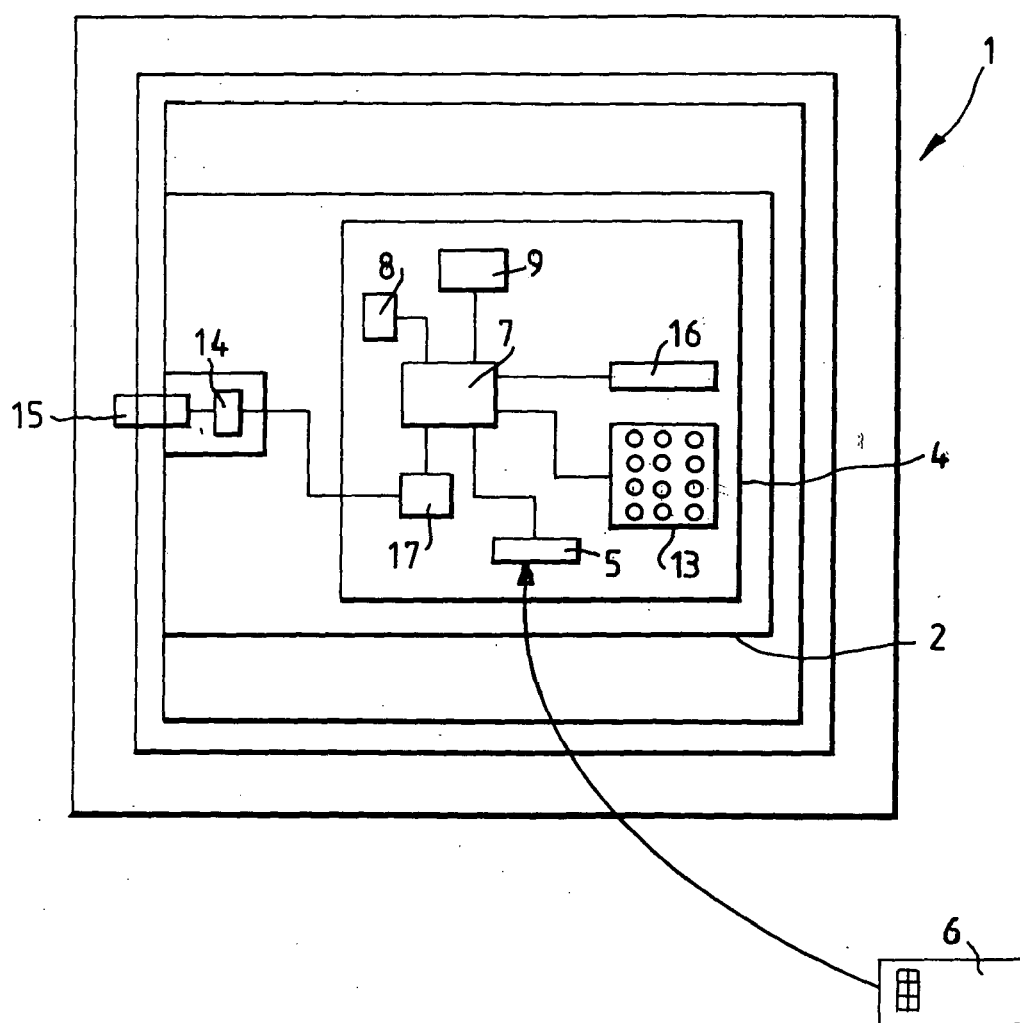


FIG.2

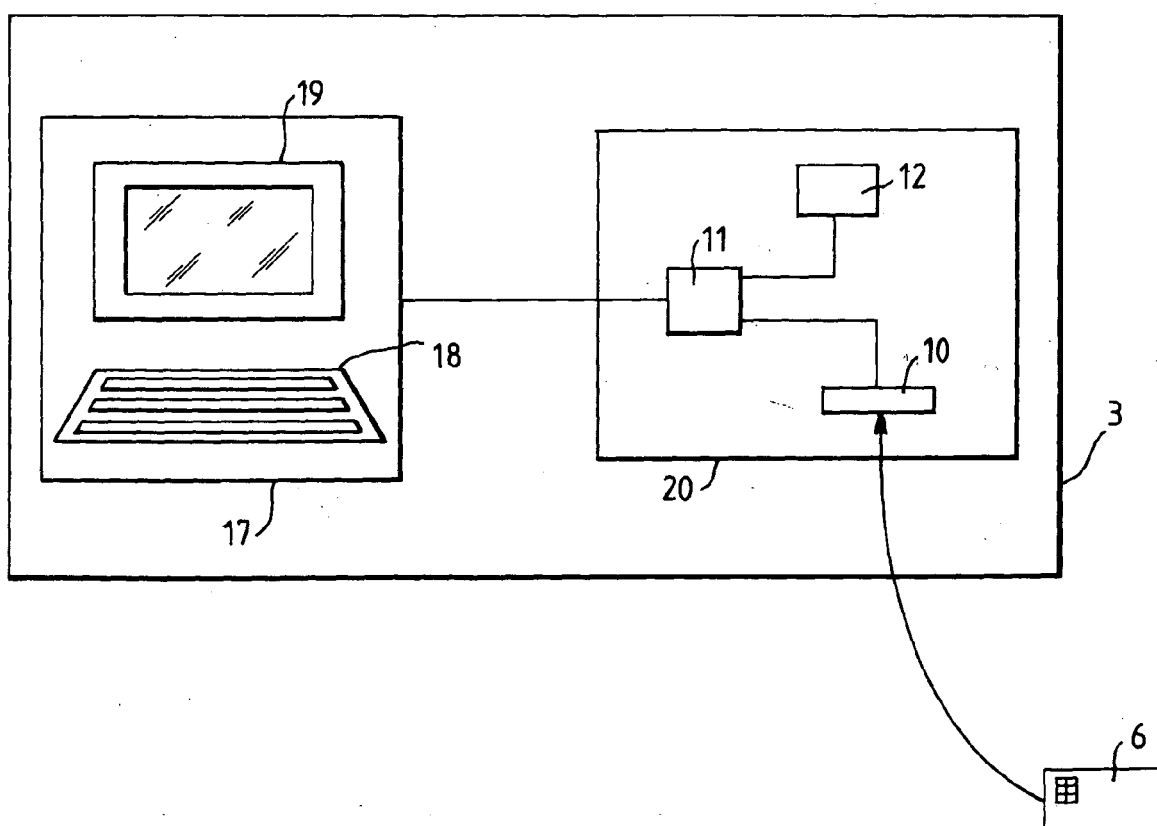


FIG.3

A

B

C

D

E

F

G

H

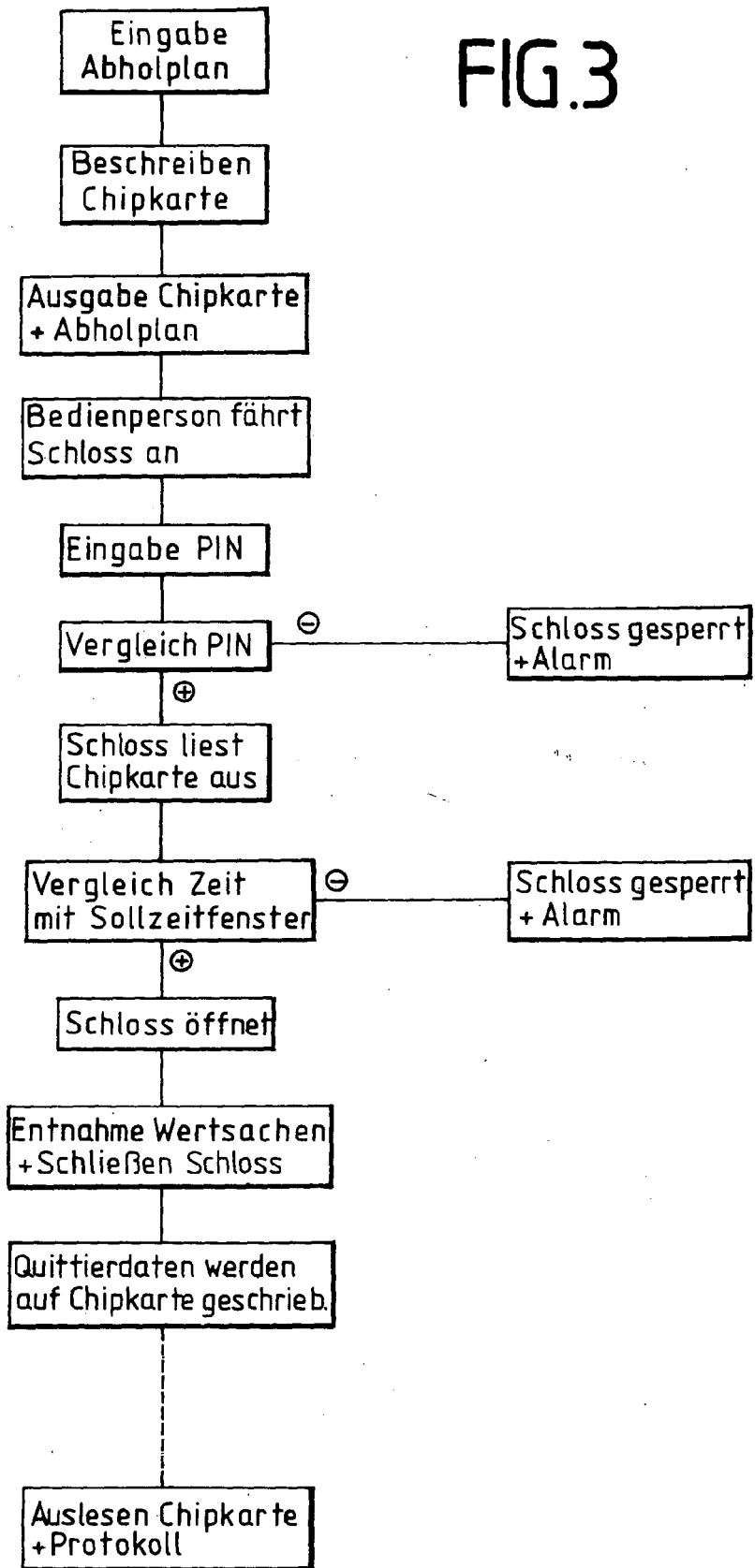
I

J

K

D-K

L



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 19535065 A [0023]