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

(11) EP 1 321 901 A2

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
25.06.2003 Patentblatt 2003/26

(51) Int Cl.[7]: **G07C 9/00**

(21) Anmeldenummer: **02406101.2**

(22) Anmeldetag: **16.12.2002**

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

(30) Priorität: **21.12.2001 CH 234701**

(71) Anmelder: **Kaba AG**
8620 Wetzikon (CH)

(72) Erfinder: **Dütschler, Urs**
8610 Uster (CH)

(74) Vertreter: **Frei, Alexandra Sarah et al**
Frei Patentanwaltsbüro
Postfach 768
8029 Zürich (CH)

(54) Verfahren zur Regelung des Zutrittsregimes zu einem Objekt

(57) Die Erfindung betrifft Schliesssysteme mit mobilen Einheiten (2) ("Schlüsseln") und ortsfesten Einheiten ("Schliesszylindern"), wobei die ortsfesten Einheiten ein Objekt in Abhängigkeit von einem Informationsaustausch mit einer mit ihnen in Verbindung stehenden ortsfesten Einheit freigeben können. Die mobilen Einheiten (2) sind variabel programmierbar und mit Kommunikationsmitteln sowie mit Speichermitteln ausgestattet. In ihnen ist die Information speicher- und umprogrammierbar, welche über gültige Berechtigung bzw. fehlende oder falsche Berechtigung entscheidet. Sie sind als die aktiven, intelligenten, kommunikationsfähigen Komponenten ausgebildet und weisen bspw. selbst Energieversorgungsmittel auf. Um eine Freigebe durch die ortsfesten Einheiten zu erhalten, lassen sich die mobilen Einheiten von einer Zentrale ein Zertifikat übermitteln. Dieses beinhaltet bspw. einen Code, welcher an die ortsfeste Einheit zu übergeben ist. Die ortsfesten Einheiten ("Schliesszylinder") sind hingegen von der Aufgabe befreit, die Information über Zugangsberechtigungen etc. zu verwalten. Die Übergabe eines Codes, der über die Zutrittsberechtigung entscheidet, von der mobilen Einheit an die ortsfeste Einheit erfolgt offline und es ist nicht notwendig, dass während der Verifikation die ortsfeste oder die mobile Einheit mit einer Zentrale in Kommunikationsverbindung steht.

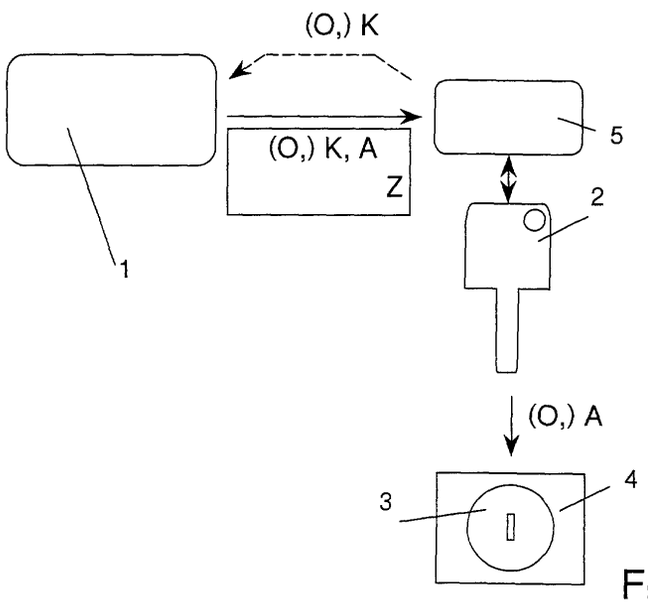

Fig. 2

EP 1 321 901 A2

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zur Regelung des Zutrittsregimes zu einem Objekt, ein Schliesssystem eine mobile Einheit, eine ortsfeste Einheit, ein Computerprogramm und ein Computerprogrammprodukt gemäss den unabhängigen Ansprüchen.

[0002] Traditionelle Schliesssysteme beruhen, auch wenn sie mit neusten Technologien verwirklicht sind, auf einem einheitlichen Prinzip. Mit mobilen Einheiten ("Schlüsseln") wird eine Freigabe in festen Einheiten ("Schliesszylindern") erwirkt. Die mobilen Einheiten besitzen eine fixe mechanische oder elektronische Codierung, während die feste Einheiten mechanisch oder elektronisch programmiert sind, so dass nur bei mobilen Einheiten mit bestimmten Codierungen eine Freigabe durch die ortsfesten Einheiten erfolgt. Moderne, elektronische Schliesssysteme sehen dabei vor, dass die Programmierung der ortsfesten Einheiten immer wieder abgeändert und aktualisiert werden kann.

[0003] Traditionelle Schliesssysteme bieten einen guten Schutz für einzelne Objekte mit klar geregelten Zugangsberechtigungen. Es können aber Probleme entstehen, wenn die zu schützenden, mit einem bestimmten Schlüssel zugänglichen Objekte territorial verteilt sind. Ebenfalls können Probleme entstehen, wenn die Gruppe der Zugangsberechtigten nicht von vornherein definiert ist und rasche und wiederholte Änderungen der Zutrittsberechtigungen zu erwarten sind. Dies gilt insbesondere auch, wenn die Freigabe jeweils nur für kurze Zeitabschnitte erfolgen soll.

[0004] Solche Schliesssysteme sind sicher die beste Wahl wenn viele Partizipienten mit zentral zu vergebenden Zugangsberechtigungen Zugang zu einem Objekt haben, das durch verhältnismässig wenige Schlösser geschützt ist. Dies ist bspw. bei einem Firmengebäude der Fall, wo einige Türen von vielen Angestellten benutzt werden.

[0005] Es gibt aber immer mehr Anwendungen, wo Zutrittsberechtigungen variabel vergeben werden sollen. Auch gibt es Anwendungen, wo viele potentielle Zylinder, die auch räumlich verteilt sein können, durch wenige Schlüsselbesitzer bedient werden sollen.

[0006] Ein Beispiel: Im Mobiltelefonbereich werden Anlagen in bisher durch staatliche oder halbstaatliche Institutionen kontrollierten Objekten zunehmend von Mobiltelefonbetreibern gewartet. Es kommt auch vor, dass die Anlagen Dritten gegen Miete zur Verfügung gestellt werden. Die Objekte, bspw. Tunnelanlagen, Kirchtürme, Gemeindehäuser etc. sind auf einem grossen territorialen Gebiet verteilt und lassen sich aus wirtschaftlichen oder technischen Gründen nicht durch Kabel oder Funk in ein Netz einbinden. Sie weisen eine Vielzahl von Systemen auf, welche von externen und internen Technikern gewartet werden müssen. Das Schlüsselmanagement wird daher zunehmend schwieriger. Auch muss eine Vielzahl von Schliesszylindern ausgewechselt werden, wenn eine einzige Person einen Schlüssel oder gar einen Generalschlüssel verliert. Die Absicherung von unter Sicherheitsaspekten kritischen Anlagen ist nicht vollständig gewährleistet, insbesondere in der Zeit zwischen einem Schlüsselverlust und dem Abschluss des Schliesszylinder-Austauschs.

[0007] Weitere Beispiele für Zugangsberechtigungen zu territorial weit verteilten Objekten finden sich bei der Tätigkeit von Überwachungsfirmen und Transportunternehmen, im Tiefbau etc. Eine ähnliche Problemstellung ist im Bereich Online-Shopping mit Hauslieferung denkbar. Es wäre wünschenswert, wenn bei Abwesenheit des Belieferten die Lieferung in ein abschliessbares Objekt erfolgen könnte.

[0008] Ebenfalls komplizierte und variable Zugansberechtigungen ergeben sich für die Zugangsberechtigung zu Chemieschränken (in Spitälern, Laboratorien etc.). Ähnliches gilt - auf einer anderen Sicherheitsstufe - für Schulen, wo die Zugangsberechtigung zu Klassen- und Vorbeiteitungszimmern häufigen Wechseln unterworfen ist.

[0009] Variable Vergaben von Zutrittsberechtigungen beziehen sich auch immer öfter auf verschiedene Systeme. So gibt es Anwendungen, wo einige wenige Schlüsselbesitzer Zugang zu verschiedenen Objekten haben sollten, die verschiedenen Systemen angehören. So sollte beispielsweise ein Lieferant möglicherweise Zugang zu Lagerräumen verschiedener Firmen haben, wobei natürlich jede Firma ein eigenes Schliesssystem hat.

[0010] Bereits existieren Ansätze zu technischen Lösungen, die diesen geänderten Umständen Rechnung tragen. Beispielsweise gibt es Systeme mit elektronischen Schlüsseln und elektronischen Schlössern, bei denen der Schlüssel eine unter Umständen zeitlich begrenzte Freigabe erhalten kann. Jeder Zugang zum geschützten Objekt wird schloss- und schlüsselseitig online protokolliert. Aspekte eines solchen Systems sind bspw. in der US-Patentschrift 4,988, 987 beschrieben. Sowohl die Zylinder als auch die Schlüssel müssen in diesen Systemen von einer Zentrale programmiert werden. Das ist nachteilig in den Fällen der oben erwähnten Anwendungen, wo die mit Schlössern versehenen Objekte geografisch weit verstreut und unter Umständen auch schwer zugänglich sind. Ausserdem stellt ein solcher online-Ansatz hohe Anforderungen an Kommunikationsverbindungen, deren Verfügbarkeit, Protokolle etc.

[0011] Eine weiterer Ansatz wird bspw. in der schweizerischen Patentanmeldung 01365/00 beschrieben. Feststationen eines bspw. berührungslosen Systems fungieren als Schliesszylinder. Die Feststationen werden über ein Kommunikationsmedium, bspw. das Internet, aufdatiert. Die mobilen Einheiten können dann über eine Feststation initialisiert werden. Dieser Ansatz bedingt aber, dass die Schlösser vernetzt sind und je nach Ausgestaltung als Feststation auch technisch aufwändig konstruiert und gross sind.

[0012] Lösungen dieser Art stellen eine Erweiterung des konventionellen Konzepts durch Sicherheits- und Überwachungsfeatures dar. Durch einen erheblichen technischen Aufwand erlauben sie eine verbesserte Kontrolle über erfolgte Zugänge. Sie sind aber in der Herstellung relativ kompliziert und daher teuer. Auch ist ihre Bedienung umständlich, wodurch sie wenig geeignet sind für einen alltäglichen Gebrauch durch Nicht-Fachleute. Ausserdem bedingen Sie, dass die ortsfesten Einheiten Energiequellen besitzen. Wenn solche durch Batterien gebildet werden, benötigen sie viel Platz, wenn die Funktionsfähigkeit über eine längere Zeit gewährleistet werden soll und viele Zutritte zu erwarten sind.

[0013] Die internationale Offenlegungsschrift WO 93/21712 zeigt ein elektronisches Sicherheitssystem für Münztelefone und andere Automaten mit Münzeinwurf. Bei solchen Systemen stellt sich das Problem, dass verschiedene Personen für das Einsammeln des angesammelten Geldes verantwortlich sind. Es besteht die Gefahr von Missbrauch, und die Schlüsselverwaltung ist aufwändig. Daher wird gemäss der genannten Offenlegungsschrift ein mit dem Schlüssel verbundenes tragbares Gehäuse vorgestellt, welchem über das öffentliche Telefonnetz und eine Modemverbindung eine Liste von ID-Codes zugeteilt werden; wenn einer der ID-Codes einem ID-Code eines Schliesszylinders entspricht erfolgt eine Freigabe. Die Übermittlung der ID-Codes kann verschlüsselt geschehen. Ausserdem kann dem Speicher im Schlüssel ein Zeitfenster zugeteilt werden, während dem der Schlüssel zum Betätigen des Schliesszylinders berechtigt. Der Schlüssel kann über das tragbare Gehäuse mit Energie versorgt werden und auch die Schliesszylinder mit Energie versorgen. Dieses System löst das Problem der aufwendigen Schlüsselverwaltung. Es ist aber verhältnismässig umständlich und in erster Linie nur für Telefonkabinen geeignet, bedingt es doch das unmittelbare Vorhandensein eines öffentlichen Telefonanschlusses. Ausserdem ist das System sehr anfällig für Manipulationen, und daher nicht geeignet für Anwendungen, welche eine höhere Sicherheit erfordern. Eine Person, die den Schlüssel manipulieren will muss lediglich verhindern, dass einmal gespeicherte ID-Codes wieder gelöscht werden und dann dem Schlüssel ein aktuelles Zeitfenster zuteilen.

[0014] Weitere elektronische Sicherheitssysteme sind in der französischen Offenlegungsschrift 2 722 596 und in der europäischen Offenlegungsschrift 0 282 339 offenbart. Beide diese Systeme beruhen darauf, dass ein Code auf einen als Schlüssel dienenden Datenträger geladen wird; die französische Offenlegungsschrift 2 722 596 zeigt ausserdem Verfahren auf, wie ein solcher Code durch Kryptographiemittel im Schliesszylinder verifiziert werden kann.

[0015] Alle diese Schicherheitssysteme haben die Eigenschaft, dass der Schlüssel im Wesentlichen nur noch aus einem elektronischen Code (ID-Code, "Fingerabdruck" bestehen) Wenn ein korrekter solcher Code an den Schliesszylinder übergeben wird, erfolgt Freigabe. Dies hat Nachteile, wenn die Sicherheitsanforderungen hoch sind. So ist bekannt, dass elektronische Daten mit geeigneten Mitteln kopiert oder manipuliert werden können.

[0016] Es ist daher eine Aufgabe der Erfindung, ein Verfahren zur Regelung eines Zutritts-Regimes sowie ein entsprechendes Schliesssystem und entsprechende Hardware- und Softwarekomponenten zur Verfügung zu stellen, welches Nachteile von konventionellen Verfahren und Systemen überwinden und welches insbesondere eine variablere Regelung von Zutrittsberechtigungen ermöglichen und dabei hohen Sicherheitsanforderungen genügen.

[0017] Diese Aufgabe wird gelöst durch die Erfindung, wie sie in den Patentansprüchen definiert ist.

[0018] Die Erfindung wählt einen im Vergleich zum Stand der Technik grundsätzlich anderen Ansatz. Die mobilen Einheiten ("Schlüssel") sind variabel programmierbar und mit Kommunikationsmitteln sowie mit Speichermitteln ausgestattet. In ihnen ist die Information speicher- und umprogrammierbar, welche über gültige, fehlende oder falsche Berechtigung entscheidet. Sie sind als die aktiven, kommunikationsfähigen Komponenten ausgebildet und weisen bspw. selbst Energieversorgungsmittel auf. Um eine Freigebe durch die ortsfesten Einheiten zu erhalten, lassen sich die mobilen Einheiten von einer Zentrale ein Zertifikat übermitteln. Dieses beinhaltet bspw. einen Code, welcher an die ortsfeste Einheit zu übergeben ist und von dieser anhand von gespeicherten Informationen verifiziert wird.

[0019] Diese Verifikation erfolgt aber mit schlüsselspezifischen Algorithmen (wobei mit "schlüsselspezifisch" gemeint ist, dass bei jeder physisch vorhandenen ortsfesten anders verifiziert wird, bspw. indem Daten mit einer in einem nicht überschreibbaren Datenspeicher gespeicherten Schlüssel-Identifikationsnummer ID als , Seed-Nummer' verschlüsselt wird). Zugangsberechtigungen werden also nicht rein aufgrund von elektronischen Daten mit dem Schlüssel als Datenträger vergeben, sondern der Schlüssel ist auch physisch ein Sicherheitselement, und das individuell.

[0020] Die ortsfesten Einheiten ("Schliesszylinder") sind hingegen von der Aufgabe befreit, die Information über Zugangsberechtigungen etc. zu verwalten. Die Übergabe eines Codes, der über die Zutrittsberechtigung entscheidet, von der mobilen Einheit an die ortsfeste Einheit erfolgt offline. D.h. es ist nicht notwendig, dass während der Verifikation die ortsfeste oder die mobile Einheit mit einer Zentrale in Kommunikationsverbindung steht.

[0021] Die Erfindung beinhaltet also Sicherheitselemente in drei beteiligten Komponenten: Der Zentrale, welche die Zugangsberechtigungen verwaltet, dem Schlüssel, welcher mit charakteristischen Informationen versehen ist und der Schliesszylinder, in welchem Informationen gespeichert sind, anhand welcher Stimmigkeit überprüft wird. Alle diese drei Sicherheitsele-

mente sind relevant. Man kann bspw. nicht ohne die aktuelle Autorisierung der Zentrale vorgehen. Man kann auch nicht ein einmal übermitteltes Zertifikat durch Manipulation auf einen anderen Schlüssel übertragen und mit diesem den Zugang erwirken. Schliesslich kann auch nicht ein Zertifikat in irgend einer Weise für die Erwirkung des Zugangs für einen anderen als den vorgesehenen Schliesszylinder verwenden. Es muss Stimmigkeit - nicht nur von flüchtig gespeicherten Codes, sondern der physischen Elemente - aller drei Komponenten herrschen.

[0022] Auf diese Weise kombiniert die Erfindung eine maximale Flexibilität von Systemen mit rein elektronischen Schlüsseln - wie bspw. demjenigen der internationalen Offenlegungsschrift WO 93/21712 - mit einer hohen Sicherheit gegenüber Manipulationsversuchen. Durch die Voraussetzung, dass nur beim physischen Vorhandensein des richtigen Schlüssels überhaupt eine Freigabe erfolgen kann, hat die Erfindung insbesondere auch ein Sicherheitselement von traditionellen, mechanischen Schliessystemen. Im Gegensatz zu diesen ist das Sicherheitselement aber nicht durch mechanisches Kopieren umgehbar.

[0023] Die offline-Regelung der Freigabe hat massive Vorteile. Eine Versorgung der ortsfesten Einheit mit aktuellen Daten ist nicht zwingend erforderlich. Das ganze System kann sehr einfach um zusätzliche Einheiten erweitert werden. Die ortsfesten Einheiten müssen auch nicht online mit einer zentralen Einheit verbindbar sein. Trotzdem kann ein dynamisches, laufend den Begebenheiten angepasstes Management der Zutrittsberechtigungen erfolgen. Dies ist ein Vorteil im Hinblick auf die eingangs erwähnten Anwendungsbeispiele, wo der Zugang zu möglicherweise sehr vielen Objekten mit eventuell schwieriger Zugänglichkeit geregelt werden muss.

[0024] Die Bedingung, dass die Verifikation schlüsselspezifisch erfolgt, ist eine wichtige Voraussetzung für die Gewährleistung der Sicherheit des Systems. So kann bspw. bei den eingangs beschriebenen elektronischen Sicherheitssystemen die auf einem Schlüssel vorhandene Information auf einen anderen Datenträger kopiert und dieser anschliessend manipuliert werden, bspw. um die ‚Zeitfenster'-Bedingung zu überwinden. Ein Manipulierender muss sich lediglich irgend wann einmal Zugang zu einen Schlüssel gehabt haben, um dann möglicherweise viel später und unerkannt Manipulationen vornehmen zu können. Dies ist bei einem erfindungsgemässen Vorgehen nicht möglich. Wenn die auf einem Schlüssel vorhandenen Informationen auf einen anderen Datenträger - bspw. auf einen gestohlenen anderen Schlüssel - kopiert werden, sind sie wertlos. Ausserdem erlaubt die schlüsselspezifische Verifikation auch eine eindeutige schliesszylinderseitige Protokollierung des Zugangs.

[0025] Obwohl also wie erwähnt die Schlüssel die aktiven Einheiten des erfindungsgemässen Systems sind, beruht die Sicherheit nicht einzig auf einem dem Schlüssel übermittelten Code, der stimmen muss und dann kraft seiner Stimmigkeit zum Zugang berechtigt, wie das aus dem Stand der Technik bekannt ist. Vielmehr muss gemäss dem Stand der Technik der Schliesszylinder auf Basis von für den Schlüssel charakteristischen Daten und auf Basis eines Zertifikates bestimmen, ob eine Berechtigung vorliegt. Im Gegensatz zum Stand der Technik, wo die Sicherheitselemente entweder einseitig im Schliesszylinder programmiert sind oder einseitig im Schlüssel vorliegen, gilt hier das Konzept der 'vernetzten' oder 'verschränkten' Sicherheit: es muss eine Stimmigkeit zwischen Schlüssel - als physisch vorhandene Entität - Zertifikat und Schlosszylinder vorliegen: nur dann kann eine Freigabe erfolgen.

[0026] Das erfindungsgemässe Verfahren und das entsprechende System bringen Vorteile in Punkto Variabilität. Wie erläutert kann das System als Ganzes ohne jegliches Umstrukturieren laufend den Begebenheiten angepasst werden. Zutrittsberechtigungen können ohne Weiteres auch an mobile Einheiten vergeben werden, welche bisher noch nicht Teile des Systems waren. Daraus ergibt sich sofort ein weiterer Vorteil: die Skalierbarkeit. Das System ermöglicht die Verwaltung von sehr wenigen oder sehr vielen ortsfesten und mobilen Einheiten, ohne dass die Systemarchitektur geändert werden muss.

[0027] Damit verbunden ist der Vorteil der Mobilität. Im Gegensatz zu auch elektronischen Schiesssystemen gemäss dem Stand der Technik sind keine Komponenten des Systems - auch nicht die ‚ortsfesten' Einheiten - an bestimmte Standorte gebunden.

[0028] Ein weiterer Vorteil ist die Vielseitigkeit. Das System erlaubt gleichermassen die Übermittlung und Verwaltung von sehr einfachen Zugangs-Zertifikaten wie auch von komplexen, hierarchischen Zertifikaten. In jedem Fall können die ortsfesten Einheiten sehr einfach und immer gleich ausgestaltet und auf der Basis von immer den gleichen Algorithmen programmiert sein.

[0029] Schliesslich ist das System inhärent dynamisch. Obwohl, oder gerade weil die Zertifizierung, also die Übergabe des Zertifikats an die ortsfeste Einheit, offline erfolgt, können Zugangsberechtigungen jederzeit neu erteilt oder aufgehoben werden.

[0030] Ortsfeste Einheiten des erfindungsgemässen Systems können so ausgestaltet sein, dass sie einfach in vorhandene Türen oder Schränke eingebaut werden, welche bisher mit Standard- Schliesszylindern versehen waren. Dies stellt einen grossen und entscheidenden Vorteil im Vergleich zu bestehenden Verfahren und Systemen dar, die eine variable, also dynamische Kontrolle des Zutrittsregimes einzuführen versuchen. Die Erfindung bietet damit eine in der Implementation und Handhabung sehr einfache Lösung für die sich ihr stellende Aufgabe.

[0031] Dadurch, dass die Regelung des Zutritts-Regimes offline erfolgt, müssen die ortsfesten Einheiten nicht auf aktuelle Zugangsberechtigungsinformationen aufdatierbar und daher gar nicht vernetzt sein. Vorzugsweise und in konsequenter Weiterentwicklung sind zu-

sätzlich die mobilen Einheiten mit Energieversorgungsmitteln, bspw. einer Batterie, ausgestattet. Die Energieversorgung der ortsfesten Einheiten während der Zugangskontrolle kann dann durch die Schlüssel erfolgen. Die mobilen Einheiten müssen damit nicht einmal am Stromnetz hängen. Auch eine Wartung der ortsfesten Einheiten, bspw. ein Auswechseln von Batterien etc. ist kaum nötig.

[0032] Die von einer zentralen Einheit zu übermittelnden Zertifikate können verschieden ausgestaltet sein. In einer einfachen Version der Erfindung bestehen sie lediglich aus dem Code, welchen die ortsfeste Einheit erkennen muss, sowie bspw. einem Zeitfenster oder einem Zutrittskontingent. Ein Zeitfenster legt eine gewisse Zeit fest, während der der Zutritt möglich ist. Ein Zutrittskontingent bestimmt eine gewisse Anzahl von Zutritten, welche gewährt werden (bspw. wird ein einziger Zutritt gewährt). Der Code wird bswp. verschlüsselt an die ortsfeste Einheit übergeben, wobei für die Entschlüsselung eine schlüsselspezifische Daten (ID) als , Seed Number' verwendet werden.

[0033] Das Zertifikat kann zusätzlich weitere Informationen beinhalten. Beispiele für solche Daten sind eine Berechtigungs-Hierarchie bei komplexeren Systemen, die aber im Kontrast zu konventionellen Systemen nicht durch die Schlüssel-Mechanik implementiert ist. Beispielsweise kann gleichzeitig mit einer Zugangsberechtigung zu einem bestimmten Objekt automatisch auch eine Zugangsberechtigung mit zugeordneten Objekten einer tieferen Hierarchiestufe verbunden sein. Das Zertifikat kann auch eine Objekt-Identifikation und eine Schlüssel-Identifikation beinhalten.

[0034] Eine Objekt-Identifikation kann als unveränderbares und einmaliges Objekt-Identifikationszeichen ausgebildet sein, das dem Objekt bzw. der ortsfesten Einheit eindeutig zugeordnet werden kann. Es ist bspw. so festgelegt, dass es nicht einmal von einer zentralen Einheit geändert werden kann. Das Objekt-Identifikationszeichen kann dazu dienen, Manipulationen an den Schliesszylindem zu verhindern, die bspw. nicht von einer zentralen Einheit überwacht werden können.

[0035] Schliesslich können mit dem Zertifikat je nach Ausgestaltung des Systems und dessen Hardware-Komponenten auch noch individuell abgestimmte Daten wie zu hinterlegende PINs, Informationen für den Benützer etc. übermittelt werden. Auf diese Weise ermöglicht die Erfindung ‚Sicherheit nach Mass'.

[0036] Ein Schlüssel-Identifikationszeichen dient dazu, die Schlüssel zu identifizieren und sicherzustellen, dass die Zertifikate an die gewünschte mobile Einheit übermittelt werden. Das Schlüssel-Identifikationszeichen muss nicht zwingend an den Schliesszylinder übergeben werden.

[0037] Gemäss einem ersten Ausführungsbeispiel muss keine Information vom Schliesszylinder an den Schlüssel fliessen. Der Schlüssel übermittelt dann nach Erhalt des Zertifikats einen verschlüsselten, dem Schliesszylinder zugeordneten und in diesem gespeicherten Code zusammen mit den schlüsselspezifischen Daten (ID) an diesen. In diesem wird die Stimmigkeit überprüft und es erfolgt ggf. eine Freigabe. Der zu übermittelnde Code kann auch anstelle eines festen Zeichens als Funktionswert $f_{ID}(A, t)$ einer im Wesentlichen unumkehrbaren Funktion der Zeit und eines Funktionsparamters A vorhanden sein, wobei A den Schliesszylinder charakterisiert. Dem Schlüssel wird nur $f_{ID}(A, t)$ übermittelt, er hat keine Möglichkeit zur Bestimmung von A. Im Schliesszylinder wird zur Verifikation ebenfalls $f_{ID}(A, t)$ berechnet, bei Stimmigkeit erfolgt eine Freigabe. Zur zusätzlichen Sicherheit kann hardwaremässig sichergestellt sein, dass keine Information vom Schliesszylinder an den Schlüssel fliesst, womit ein ‚Datenklau' - ein schlüsselseitiges Bestimmen von A - verunmöglicht wird. Die schlüsselspezifischen Daten (ID) - sie werden hier als eine Art ‚Seed number' für die Datenenverschlüsselung verwendet - können bei der Herausgabe des Schlüssels von der zentralen Einheit bestimmt worden sein, sie sind aber keinesfalls veränderbar.

[0038] Gemäss einem weiteren Ausführungsbeispiel erfolgt die Regelung des Zutrittsregimes in einem zweistufigen Autorisierungsverfahren. Der Schlüssel erhält ein Zertifikat von der zentralen Einheit, welches ihn zum Zutritt zu einem Objekt oder einer Gruppe von Objekten berechtigt. Das Zertifikat kann zusätzlich regeln, dass dem Schlüssel nur ein beschränktes Zutrittsfenster bzw. Zutrittskontingent zugeteilt wird. Wenn der Schlüssel Kontakt mit einem Schliesszylinder hat, wird in einer ersten Stufe ein den Schliesszylinder identifizierendes Zeichen vom Schliesszylinder an den Schlüssel übermittelt. Dieser überprüft dann anhand der in ihm vorhandenen Zertifikate - er kann ja mehr als ein Zertifikat erhalten haben und speichern - ob er zu einem Zugang zum Objekt mit diesem Schliesszylinder berechtigt ist. Wenn das nicht der Fall ist, bleibt der Schlüssel passiv und übermittelt bspw. keine weiteren Informationen an den Schliesszylinder. Wenn ein Zertifikat des Schlüssels eine Berechtigung bejaht, übermittelt der Schlüssel als zweite Stufe des Verfahrens den Code an den Schliesszylinder, worauf dieser bei Stimmigkeit den Zugang freigibt.

[0039] Das erfindungsgemässe Schliesssystem bzw. seine Ausführungsformen erfüllen folgende Anforderungen:

- Flexible Erteilung des Zutritts, und zwar als einmaliger Zutritt, als periodischer (täglicher, wöchentlicher etc.) Zutritt, als Zutritt während eines definierbaren Zeitfensters (Zutrittsfenster) oder als Zutritt ohne zeitliche Beschränkungen.

- Jeder Zutritt kann registriert werden, und zwar nach Person resp. Schlüssel, Objekt, Zylinder und Zeit.

- Der Zutritt ist kurzfristig fernkonfigurierbar, d.h. einer Person, welche ein Schlüsselmedium besitzt, kann sofort ein Zutritt zugeteilt werden.

- Innerhalb eines Objektes können im Rahmen einer Berechtigungs-Hierarchie verschiedene Zonen definierbar sein, bspw. Hochspannungen, Leitsystem, Lager etc.. Innerhalb der Zonen kann auch die Zutrittsberechtigung von einzelnen Teilobjekten (Schränken, Räumen etc.) flexibel zuteilbar sein.

- Das Schliesssystem kann einfach in vorhandene Türen oder Schränke eingebaut werden, welche bisher mit Standard- Schliesszylindern versehen waren.

- Die ortsfesten Einheiten benötigen keine Energieversorgung.

- Der Dialog mit einer zentralen Einheit, welche den Zutritt zum Objekt gewähren kann, kann mit modernen Standard-Kommunikationsmittel erfolgen, bspw. mit Internet-basierenden Kommunikationseinheiten. Auch die Übertragung der Zutritt verschaffenden Signale selbst kann in standardisierter Form erfolgen, z.B. mit dem TCP/IP-Protokoll und ggf. verschlüsselt.

- Die zentrale Einheit kann die Möglichkeit haben, vorbereitete Zutrittsprofile zu erstellen.

- Die zentrale Einheit kann ihrerseits in ein übergeordnetes System eingebunden sein, über welches Konfigurationen und Zuständigkeitsbereiche von mehreren zentralen Systemen verwaltet werden, wobei aber bspw. vom übergeordneten System keine direkten Zutritte gewährbar sind.

- Eine Fluchtwegfunktion von Innen nach Aussen kann auch bei Energieausfall gewährleistet werden.

- Der Inhaber des Objekts hat die Kontrolle über die zentrale Einheit und kann selbst entscheiden, dass ein beliebiger anderer System-Partizipient oder auch ein Partizipient eines anderen Systems Zugang erhält, er muss das nicht vordefinieren.

[0040] Im Folgenden werden noch Ausführungsbeispiele der Erfindung anhand von Figuren etwas detaillierter beschrieben. In den Figuren zeigen:

- Figur 1 ein Schema erfindungsgemässen Verfahrens anhand von Komponenten des erfindungsgemässen Systems in einer ersten Ausführungsform.

- Figur 2 ein analoges Schema mit Komponenten einer weiteren Ausführungsform des erfindungsgemässen Systems.

- Figur 3 eine Ansicht einer mobilen Einheit für die Ausführung des erfindungsgemässen Verfahrens.

- Figur 4 ein Schema von Einheiten des erfindungsgemässen Systems im Zusammenspiel.

- Figur 5 ein Schema eines erfindungsgemässen Systems.

[0041] Das System gemäss **Figur 1** besitzt verschiedene Komponenten: die zentrale Einheit 1 ist die Kontrollinstanz. Sie kann bspw. identisch sein mit einer Zentrale einer das erfindungsgemässe System anwendenden Überwachungsfirma, einer Verteilerfirma etc. Sie kann durch Personen bedient oder als Software implementiert sein. Sie besitzt Mittel zur Kommunikation mit den mobilen Einheiten 2 (im Folgenden: Schlüssel). Die mobilen Einheiten besitzen je eine Energiequelle bzw. einen Energiespeicher sowie Datenverarbeitungs- und Datenspeicherungsmittel. Ausserdem sind sie mit Kommunikationsmitteln zum Übermitteln von Daten an die ortsfesten Einheiten 3 (Schliesszylinder) ausgestattet. Der Begriff ‚ortsfest' bedeutet im Kontext dieser Anmeldung übrigens, dass die Einheiten im Betrieb in Relation zu einem zu sichernden Objekt im wesentlichen stationär sind. Der Begriff schliesst weder aus, das die Schliesszylinder an einem mobilen Objekt (Fahrzeug, Schiff etc.) befestigt sind noch dass sie zur Montage von einem Objekt zum anderen transportierbar sind.

[0042] Das Objekt, in das die ortsfesten Einheiten integriert sind, ist in der Zeichnung durch einen Kasten 4 symbolisiert. Die ortsfesten Einheiten 3 können bspw. äusserlich wie konventionelle Schliesszylinder ausgebildet sein und an deren Stelle treten. Sie besitzen Speichermittel sowie eine Datenverarbeitungs- und Übertragungseinheit zur Kommunikation mit den Schlüsseln. Hingegen ist sowohl die Integration von Energiequellen bzw. -speichern als auch die Beschreibbarkeit des Speichers fakultativ und nur je nach Ausgestaltung des Systems vorhanden.

[0043] Jeder Schlüssel 2 besitzt bspw. ein Identifikationszeichen K. Dieses Identifikationszeichen K kann gleichzeitig als schlüsselspezifischer Datensatz (ID) in der eingangs geschilderten Art verwendet werden; er kann aber auch von diesem verschieden sein. Wenn Zugang zu einem Objekt 4 gewünscht wird, so wird vom Schlüssel aus dieses Identifikationszeichen übermittelt. In der Zentrale wird darauf hin festgestellt oder festgelegt, ob der Inhaber des Schlüssels die Berechtigung für einen Zugang zum Objekt hat oder erhalten soll. Wenn ein Zutritt erfolgen soll, wird anschliessend ein Zertifikat Z mit dem Autorisierungs-Code A (im Folgenden meist kurz Code genannt) an den Schlüssel übermittelt. Gemäss einer Ausführungsform des Verfahrens ist der Code A im Zertifikat immer in einem festen Paket zusammen mit dem Schlüssel-Identifikationszeichen K enthalten. (Dann ist dieses vorzugsweise nicht identisch mit dem schlüsselspezifischen Datensatz (ID)). So wird sichergestellt, dass der Code A nur bei Stimmigkeit der Schlüssel-Identifikation zum Zugang berechtigen kann. Der Code A wird an den Schliesszylinder übergeben

und dort verifiziert. Dann erfolgt gegebenenfalls eine Freigabe.

[0044] Gemäss einer speziellen Ausführungsform wird der Code immer zusammen mit einer Objekt-Identifikation O übermittelt. Dieser dient als eindeutiges und unveränderbares Objekt-Identifikationzeichen und wird dem Schliesszylinder zusammen mit dem Code A zur Verifikation übergeben. Er ist hardwaremässig im Objekt so implementiert, dass er nicht durch Umprogrammieren abgeändert werden kann.

[0045] Die Kommunikationsmittel, über welche Daten zwischen der zentralen Einheit und dem Schlüssel übermittelt werden, können verschieden ausgestaltet sein. In der **Figur 2** ist schematisch zusätzlich zu den Komponenten der Figur 1 ein mobiles Übermittlungsgerät 5 gezeichnet. Dieses besitzt ein Modem oder ein anderes Kommunikationsmittel zur Kommunikation über ein Datennetzwerk, bspw. das Internet. Es kann bspw. als batteriebetriebenes, tragbares Gerät ausgebildet sein oder in einem Fahrzeug oder dergleichen installiert sein. Es kann über eine Radiofrequenz-Verbindung berührungslos mit dem Schlüssel Informationen austauschen. Alternativ dazu kann auch direkte (Kabel- etc.) Verbindung zwischen dem Schlüssel 2 und dem Übermittlungsgerät 5 vorhanden sein. Schliesslich kann das Übermittlungsgerät auch im Schlüssel 2 integriert sein. In der **Figur 2** ist auch dargestellt, wie das vorstehend erwähnte Objekt-Identifikationszeichen O gehandhabt wird, wobei das Übermittlungsgerät natürlich nicht nur in Systemen benutz werden kann, die sich des Objekt-Identifikationszeichens bedienen.

[0046] In der **Figur 3** ist noch ein Beispiel für einen Schlüssel 2 schematisch dargestellt. Der Schlüssel besitzt eine Schlüsselblatt 2.1, welcher wie bei konventionellen Schlüsseln ausgearbeitet sein kann und bspw. die mechanische Kodierung eines Passschlüssels besitzt. Er kann auch anders ausgestaltet sein, und bspw. gar keine mechanische Kodierung aufweisen. Je nach Ausgestaltung des Schliesszylinders könnte das Schliesssystem auch berührungslos funktionieren und der Schlüssel also gar kein Schlüsselblatt aufweisen. Zusätzlich besitzt der Schlüssel eine Leiterplatte 2.2, auf welcher Prozessormittel 2.3 und Leiterbahnen 2.4 sowie eventuell zusätzliche elektronische Komponenten angebracht sind. Weiter sind im Schlüssel Energieversorgungsmittel 2.5, also eine Batterie angeordnet. Die Batterie, Leiterplatte sowie die Leiterbahnen sind so angeordnet, dass die Batterie die Prozessormittel mit elektrischer Energie versorgen kann. Ausserdem besitzt der Schlüssel noch einen Kontaktpfad 2.6 zur Kommunikation, mit einem Schliesszylinder und/oder zu dessen Energieversorgung. Ferner sind noch Kommunikationsmittel 2.7 vorhanden, mit welchen berührungslos mit einem Übermittlungsgerät oder Zylinder Daten ausgetauscht werden können.

[0047] In der **Figur 4** ist ein Schema dargestellt, welches einige Elemente eines erfindungsgemässen Systems und ihr Zusammenspiel darstellt. In der Figur dargestellt sind eine zentrale Einheit 1, ein Übermittlungsgerät 5, ein Schlüssel 2 und ein Schliesszylinder 3. Das Datenübertragungsgerät, der Schlüssel und der Schliesszylinder besitzen je eine Prozessoreinheit 5.3, 2.3 resp. 3.3. und eine Datenspeicher- und Verschlüsselungseinheit 5.9, 2.9 resp. 3.3. Die Prozessoreinheit und/oder die Datenspeicher- und Verschlüsselungseinheit können bspw. in an sich bekannter Art gefertigt sein. Sie können bspw., was hier lediglich als Beispiel zur Illustration erwähnt sei, ein LEGIC® -Sicherheitsmodul enthalten. An diese Datenspeicher- und Verschlüsselungseinheit 5.9, 2.9 resp. 3.3 angeschlossen sind Mittel 5.7, 2.7 resp. 3.7 zur berührungslosen Kommunikation. Der Schlüssel besitzt wie bereits beschrieben Energieversorgungsmittel 2.5. Die Energieversorgungsmittel versorgen den die Mikroprozessoreinheit 2.3 sowie einen daran angeschlossenen Zeitgeber 2.8.

[0048] Das Übermitteln von Daten von der zentralen Einheit an das Übertragungsgerät erfolgt bspw. mit bekannten und gängigen Datenübertragungsleitungen, Schnittstellen Protokollen, etc. unter Zuhilfenahme des Internets. Selbstverständlich erfolgt die Datenübertragung vorzugsweise verschlüsselt. Der Kanal für das Übermitteln von Daten zwischen der Software 1.1 der zentralen Einheit 1 und dem Übertragungsgerät 5 ist in der Figur durch einen Doppelpfeil 11 symbolisiert. Zwischen dem Übertragungsgerät 5 und dem Schlüssel 2 sind zwei Interfaces eingerichtet: Das Mikroprozessorinterface 12 als Kontaktinterface und das Programminterface 13. Das Mikroprozessorinterface 12 dient der Synchronisation der Mikroprozessoren 5.3, 2.3 der Übertragungsgerätes und des Schlüssels. Die Zeit ist ein bedeutender Parameter bei der Regelung des Zutrittsregimes, bspw. wenn nur ein Zeitfenster für einen Zutritt zur Verfügung steht. Sie kann auch bedeutend sein bezüglich Daten- und Manipulationssicherheit, wie das anhand von Beispielen noch erläutert werden wird. Das Programminterface 13 dient dem Austausch der erwähnten Daten. Das Programminterface und das Mikroprozessorinterface brauchen sich nicht physisch verschiedener Datenübertragungskanäle zu bedienen.

[0049] Zwischen dem Schlüssel und dem Schliesszylinder sind zwei Interfaces vorgesehen. Das Dateninterface 14 dient der Übergabe von Daten vom Schlüssel an den Schliesszylinder und eventuell auch in die umgekehrte Richtung vom Schliesszylinder an den Schlüssel. Über das Leistungsinterface 15 wird der Schliesszylinder mit der während der Übergabe des Zertifikats an den Schliesszylinder und während der Verifikation benötigten elektrischen Energie versorgt. Dies kann kontinuierlich oder zu Beginn der Aktion in einen Kurzzeit-Energiespeicher des Schliesszylinders erfolgen.

[0050] Das Schema von **Figur 5** zeigt eine zentrale Einheit 1, einige Schlüssel 2 und einige Objekte 4 mit Schliesszylindern 3.

[0051] Wie vorstehend erwähnt gibt es - durch Pfeile symbolisiert - einen Informationsfluss zwischen der zentralen Einheit und den Schlüsseln sowie von der zentra-

len Einheit autorisiert und eingeschränkt von den Schlüsseln zu den Schliesszylindern und je nach dem zurück. Zwischen der zentralen Einheit und den Schliesszylindern muss keine Information fliessen. Ebenso ist ein Informationsfluss zwischen den Schliesszylindern zwar nicht ausgeschlossen, aber im Allgemeinen nicht nötig. Zwischen den Schlüsseln untereinander darf keine Information fliessen.

[0052] Die zentrale Einheit 1 besitzt Informationen, die zur Kontrolle über das ganze System befähigen. In der Figur sind zwei Datenbanken 1.1 und 1.2 symbolisch dargestellt. Die erste Datenbank enthält laufend aufdatierte Informationen über die Objekte, die zweite Datenbank 1.2 über die Schlüssel.

[0053] Jeder Schlüssel und jeder Schliesszylinder ist anhand eines entsprechenden Identifikationszeichens K_i bzw. P_i identifizierbar. Die Daten über die Objekte können eine Datenstruktur aufweisen, welche Beziehungen der Objekte untereinander widerspiegeln. Ein sehr simples Beispiel ist in der Figur dargestellt: Die Objekte mit den der Identifikation P_3, P_4 und P_9 sind bspw. Teile eines übergeordneten Gebildes. Das Objekt P_9 ist dabei in einem einfachen Modell einem inneren Kreis angeordnet (übergeordnet), die Objekte P_3 und P_4 in einem äusseren Kreis (untergeordnet). Als Beispiel zur Illustration kann das Objekt P_9 ein Tresor sein, der in einem durch Türen P_3 und P_4 zu erreichenden Raum steht. Ein Zugang zum Objekt im inneren Kreis bedingt eine Zugangsberechtigung zu einem Objekt im äusseren Kreis, umgekehrt aber nicht. Diese hierarchische Beziehung findet in den Daten in der zentralen Einheit ihren Niederschlag.

[0054] Die Schlüsselinhaber erfüllen unterschiedliche Funktionen und werden daher auch mit unterschiedlichen Zertifikaten ausgestattet: Ein Sicherheitsdienstmitarbeiter erhält vielleicht Zugang nur zu untergeordneten Objekten, dafür aber in vielen verschiedenen Gebilden, ein Filialleiter hat Zugang zu allen Objekten eines einzigen Gebildes.

[0055] Entsprechend sind in den Datenbanken Archetypen angelegt. Die Objekt-Datenbank 1.1 enthält Hierarchie-Archetypen B;. So kann bspw. mit einer Zugangsberechtigung zu einem Objekt inhärent oder zumindest defaultmässig eine Zugangsberechtigung zu einem hierarchisch untergeordneten Objekt verbunden sein. Die Hierarchie-Archetypen können bspw. den Code A der hierarchisch untergeordneten Objekte direkt enthalten. Den Hierarchie-Archetypen entsprechende Hierarchien werden in die Zertifikate übernommen. Die Schlüssel-Datenbank 1.2 enthält Zertifikat-Archetypen C_i. Typischerweise erhält ein Sicherheitsdienstmitarbeiter immer wieder Zugang zu denselben Objekten, aber nur einmal pro Nacht. Die Zertifikate Z werden anhand der Archetypen und ggf. aktuellen Daten gefertigt. Die Zertifikat-Archetypen enthalten bspw. Verweise auf Hierarchie-Archetypen und nicht den gesamten Inhalt der Zertifikat-Archetypen.

[0056] Gemäss einem Ausführungsbeispiel können einzelne Elemente der Archetypen sogar im Schlüssel selbst angelegt sein. Sie müssen aber auf jeden Fall durch ein von der zentralen Einheit übermitteltes Zertifikat aktiviert werden.

[0057] Es folgen einige Beispiele für das erfindungsgemässe Verfahren:

Beispiel 1:

[0058]

a. Der Schlüssel wird von seinem Inhaber aktiviert und fragt bei der Zentrale um einen Berechtigung an. Diese Anfrage in der Form eines Request-Signals kann individuell auf einen einzelnen Zugang hin oder pauschal (bspw. morgens, wenn der Inhaber als Monteur die Arbeit aufnimmt und eine Zugangsberechtigung für sämtliche an diesem Tag zugänglichen Objekte erhalten möchte) erfolgen. Das Request-Signal beinhaltet ein Schlüssel-Identifikationszeichen K.

b. Der in der zentralen Einheit vorhandene Computer prüft anhand einer laufend aktualisierbaren Datenbank die Berechtigung und stellt ein Zertifikat zusammen. Dieses beinhaltet für jedes Objekt einen für dieses charakteristischen Code A sowie ein Zeitfenster bzw. ein Zutrittskontingent. Zusätzlich enthält das Zertifikat das Schlüssel-Identifikationszeichen des Empfängers.

c. Der zentrale Computer übersendet das Zertifikat an das Übermittlungsgerät bzw. an die mobile Einheit verschlüsselt.

d. Die mobile Einheit empfängt das Zertifikat ggf. vom Übermittlungsgerät (in dem es zwischengespeichert sein kann, bis zwischen dem Übermittlungsgerät und der mobilen Einheit eine Verbindung besteht) und speichert es auf ihrem Speicherchip ab.

e. Der Inhaber des Schlüssels begibt sich zum Objekt und steckt den Schlüssel in den Schliesszylinder.

f. Der Schlüssel versorgt den Schliesszylinder mit elektrischer Energie. Dies kann in einen Kurzzeit-Energiespeicher oder kontinuierlich während der folgenden Verfahrensschritte erfolgen.

g. Der Schlüssel übergibt den im Zertifikat enthaltenen Code, bspw. weitere Informationen wie ein Schlüssel-Identifikationszeichen K über die Datenschnittstelle 14 an den Schliesszylinder. Die Übergabe ist bspw. ebenfalls verschlüsselt, wobei die , Seed Number' von der zur Übersendung des Zertifikats verwendeten ‚Seed Number' verschieden ist

und bspw. dem schlüsselspezifischen Datensatz ID entspricht.

h. Die im Schliesszylinder enthaltenen Prozessormitteln führen eine Verifikation durch, d.h. einen Abgleich zwischen dem übermittelten und einem gespeicherten Code durch. Ggf. wird der übermittelte Code vorher entschlüsselt. Entsprechende Verfahren, wie das Public Key/Private Key-System, welche bspw. gleichzeitig auch noch eine nicht manipulierbare Verifikation des Absenders der verschlüsselten Botschaft (hier des Schlüssels) erlauben, sind an sich bekannt und werden hier nicht weiter im Detail erläutert.

i. Durch die Prozessormittel des Schliesszylinders wird bei Stimmigkeit eine Freigabe ausgelöst. Nach der Freigabe hat der Schlüsselinhaber eine gewisse Zeit, typischerweise einige Sekunden, zur Verfügung um den Schlüssel zu drehen. Durch Kontakte im Zylinder wird festgestellt, in welcher Stellung sich der Schlüssel befindet. Damit Schlüssel und Schliesszylinder erkennen können, wann der Kontakt unterbrochen wird, sendet der Schlüssel bspw. dauernd Testbits.

j. Bei fehlender Stimmigkeit (entsprechend einer fehlenden oder falschen Berechtigung) erfolgt ein nicht-Freigabe-Ereignis. Dieses kann bspw. einfach ein akustisches Signal sein. Ein dem nicht-Freigabe-Ereignis ähnliches Ereignis kann auch ausgelöst werden, wenn innerhalb einer bestimmten Schwellenzeit keine Kommunikationsverbindung zwischen Schlüssel und Schliesszylinder aufgebaut werden konnte oder wenn bspw. die Batterie 2.5 entladen ist und die Energie nicht ausreicht.

Beispiel 2:

[0059] Schritte a, c-f, i und j bspw. gleich wie beim Beispiel 1, aber das Zertifikat enthält nicht den eigentlichen Code A sondern einen Wert $f_{ID}(A,t_0)$, wobei t_0 ein Zeitpunkt ist, um den Schlüsselinhaber zum Zugang berechtigt ist. Beim Kontakt zwischen Schlüssel und Schliesszylinder, d.h. nach dem Schritt e werden die Prozessormittel des Schliessszylinders durch einen Zeitgeber 2.8 im Schlüssel mit der aktuellen Uhrzeit t versorgt. Der Abgleich erfolgt dann zwischen $f_{ID}(A,t_0)$ und $f_{ID}(A, t)$. Dabei kann die für eine Freigabe zu erfüllende Bedingung diejenige sein, dass die Differenz der Werte $f_{ID}(A,t_0)$ und $f_{ID}(A, t)$ einen gewissen Schwellwert nicht überschreitet, wobei die Funktion f dann stetig und normierbar sein muss.

Beispiel 3:

[0060] Wie Beispiel 2, aber die Berechtigung erfolgt nicht nur zu einem Zeitpunktes t_0 (bzw. in einem diesen umgebenden Zeitfenster) sondern periodisch wiederkehrend, bspw. täglich um eine bestimmte Zeit. Dies kann damit bewirkt werden, dass das Zertifikat eine Reihe von Funktionswerten $f_{ID}(A,t_i)$ enthält mit i=1, 2, ... oder mit der Verwendung einer speziellen, in t periodischen Funktion.

Beispiel 4:

[0061] Wie Beispiel 2, aber anstelle eines Wertes $f_{ID}(A,t_0)$ wird ein Wert $f_{ID}(A,n)$ übermittelt, wobei n die Zahl der bisher erfolgten Zutritte des Schlüsselinhabers darstellt. Dieses Beispiel funktioniert gewissermassen analog zu einem Streichlisten-Prinzip.

Beispiel 5:

[0062] Wie Beispiel 1 bis 4, aber anstelle des Schrittes a wird das Zertifikat von der zentralen Einheit ohne ein vorgängiges Request-Signal übermittelt. Das kann bspw. sinnvoll sein, wenn der Schlüssel-Inhaber einem Sicherheitsdienst oder einem Lieferanten angehört und gleichzeitig mit der Berechtigung von der Zentralen Einheit ein Auftrag ausgegeben wird.

Beispiel 6:

[0063] Der Inhaber des Schlüssels begibt sich zum Objekt, zu dem er Zugang erhalten möchte. In einem ersten Schritt steckt er den Schlüssel in den Schliesszylinder dieses Objekts. Im Allgemeinen wird der Schlüssel kein Zertifikat aufweisen, welches ihn zum Zugang des Objektes berechtigt, und es erfolgt auch keine Freigabe. Der Schliesszylinder übergibt aber eine ihn charakterisierende Angabe - bspw. ein Objekt-Identifikationszeichen O - an den Schlüssel. Dieser übermittelt die charatkterisierende Angabe an die Zentrale, wofür noch gegebenenfalls ein Kommunikationsmodul wie das mobile Übermittlungsgerät 5 eingesetzt wird. In der Zentrale wird entschieden, ob der Schlüsselträger zu diesem Zeitpunkt zu einem einmaligen Zugang berechtigt sein soll. Dies kann in einer unbemannten Zentrale anhand von Tabellenwerten oder anderen Charakteristika geschehen. Zur zusätzlichen Sicherheit kann die Zentrale - ggf. automatisiert - den vermuteten Inhaber des Schlüssels anrufen, bspw. auf sein Mobiltelefon , und seine Identität und Absichten überprüfen. Eine unbemannte Zentrale kann die Identität überprüfen, indem es und eine bestimmte Aussage - bspw. ein vereinbartes Codewort - von ihm abfragt und die Stimme des angerufenen mit gespeicherten Stimmaufnahmen vergleicht. Dann übermittelt die Zentrale ein Zertifikat an den Schlüssel, und es wird wie in einem der vorstehend erläuterten Beispiele vorgegangen.

[0064] Je nach Ausgestaltung des Systems kann in irgendeinem der Beispiele bei der Freigabe/nicht-Freigabe oder nach dieser der Zutritt bzw. Zutrittsversuch zum Objekt protokolliert werden. Dies folgt bspw. in ei-

nen Speicher im Schlüssel. Beim nächsten Kontakt mit der zentralen Einheit oder direkt von sich aus kann der Schlüssel das Protokoll an die zentrale Einheit übermitteln, wo es in einer Datenbank gespeichert und/oder ausgewertet wird. Protokolle von erfolgten Zutritten/Zutrittsversuchen können natürlich bei der Erstellung von neuen Zertifikaten verwendet werden. Alternativ oder als Ergänzung dazu kann ein Zutritt/Zutrittsversuch auch in nichtflüchtigen Datenspeichern der ortsfesten Einheiten protokolliert werden.

[0065] Natürlich gehören auch beliebige Kombinationen von Merkmalen der vorstehend Beschriebenen Beispiele, sofern sie im Rahmen der Definition der unabhängigen Ansprüche und nicht widersprüchlich sind.

[0066] Es versteht sich, dass die Erfindung noch unzählige andere Ausführungsformen umfasst und sich nicht auf die vorstehend beschriebenen Beispiele beschränkt.

Patentansprüche

1. Verfahren zur Regelung des Zutrittsregimes zu einem Objekt, oder zu einer Gruppe von Objekten, wobei eine mobile Einheit (2) mit einer ortsfesten Einheit (3) in Kontakt tritt und diese in Abhängigkeit von einer Verifikation das Objekt freigibt oder ein nicht-Freigabe-Ereignis auslöst, wobei vorgängig zum Kontakt zwischen der ortsfesten und der mobilen Einheit eine zentrale Einheit ein Zertifikat an die mobile Einheit übermittelt und die Verfikation auf Basis von im Zertifikat enthaltenen Daten und offline erfolgt, **dadurch gekennzeichnet, dass** die mobile Einheit einen spezifischen Identitätscode (ID) aufweist, und dass ein zur Freigabe eines bestimmten Objekts berechtigender Code auf Basis dieses spezifischen Identitätscodes und des Zertifikates ermittelt wird.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, dass** der spezifische Identitätscode (ID) als ‚Seed Number' bei einer Verschlüsselung von im Zertifikat enthaltenen Daten dient.

3. Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet, dass** das Zertifikat einen Code enthält, welcher von der mobilen Einheit (2) an die ortsfeste Einheit (3) übergeben wird, und dass die Verifikation eine Prüfung des Codes auf Übereinstimmung mit Daten ist, welche auf Basis von in Speichermitteln der ortsfesten Einheit (3) fest gespeicherten Daten ermittelt werden.

4. Verfahren nach Anspruch 3, **dadurch gekennzeichnet, dass** zwischen der zentralen Einheit und der ortsfesten Einheit kein direkter Informationsfluss stattfindet.

5. Verfahren nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet, dass** die Freigabe/nicht-Freigabe von einem im Zertifikat enthaltenen Zutritts-Zeitfenster oder eine Zutrittskontingent abhängig gemacht werden kann.

6. Verfahren nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet, dass** der zur Freigabe eines bestimmten Objekts berechtigende Code von der Zeit und/oder von einer Statusinformation abhängig ist.

7. Verfahren nach Anspruch 6, **dadurch gekennzeichnet, dass** das Zertifikat einen Funktionsparameter enthält, dass der Code als im Wesentlichen unumkehrbare Funktion der Zeit und dieses Funktionsparameters berechnet wird, und dass in der ortsfesten Einheit durch Prozessormittel der Code durch Evaluation einer ebenfalls im Wesentlichen unumkehrbaren Funktion der Zeit verifiziert wird.

8. Verfahren nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet, dass** keine für das Zertifikat nützlichen Information von den ortsfesten Einheiten (3) an die mobilen Einheiten fliesst.

9. Verfahren nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet, dass** die Übermittlung des Zertifikats an die mobile Einheit online erfolgt.

10. Verfahren nach einem der Ansprüche 1 bis 8, **dadurch gekennzeichnet, dass** das Zertifikat an ein Übertragungsgerät (5) übermittelt und von diesem an die mobile Einheit weiter übermittelt wird.

11. Verfahren nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet, dass** vorgängig zur Verifikation und/oder während der Verifikation Energie von der mobilen Einheit an die ortsfeste Einheit übertragen wird.

12. Verfahren nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet, dass** zur Autorisierung die ortsfeste Einheit ein das Objekt identifizierendes Zeichen an die mobile Einheit übergibt und dass eine Verifikation auf Basis des Zertifikates durch Prozessormittel der mobilen Einheit erfolgt.

13. Elektronisches Schliesssystem mit ortsfesten Einheiten (3) und mobilen Einheiten (2), wobei die mobilen Einheiten codierbar sind und die ortsfesten Einheiten Freigabemittel besitzen, um ein Objekt freizugeben, wenn eine mobile Einheit mit ihnen Verbindung steht und nachdem eine Verifikation als Abgleich zwischen Daten durchgeführt wurde, wobei die mobilen Einheiten mit Kommunikationsmitteln zur Kommunikation mit einer zentralen Einheit

(1) und mit Speichermitteln zum Speichern eines von der zentralen Einheit übermittelten Zertifikats ausgestattet sind, dass in den mobilen Einheiten und den ortsfesten Einheiten Mittel zur offline-Durchführung der Verifikation als Abgleich von im Zertifikat enthaltenen und mit in Speichermitteln der ortsfesten Einheiten vorhandenen Daten vorhanden sind **dadurch gekennzeichnet, dass** jede mobile Einheit einen spezifischen Identitätscode (ID) aufweist, und dass ein zur Freigabe eines bestimmten Objekts berechtigender Code auf Basis dieses spezifischen Identitätscodes und des Zertifikates ermittelbar ist.

14. Schliesssystem nach Anspruch 13, **dadurch gekennzeichnet, dass** die mobilen Einheiten Energieversorgungsmittel (2.5) besitzen, und dass eine Leistungsschnittstelle (15) zur Übertragung von Energie an die ortsfesten Einheiten vorhanden ist, während die ortsfesten Einheiten und die mobilen Einheiten in Verbindung stehen, so dass für die Verfikation die ortsfesten Einheiten (3) von den mobilen Einheiten (2) mit elektrischer Energie versorgt werden können.

15. Schliesssystem nach Anspruch 13 oder 14, **dadurch gekennzeichnet, dass** die ortsfesten Einheiten frei von fest installierten Kommunikationsleitungen und frei von Energieversorgungsmitteln sind.

16. Mobile Einheit (2) zur Durchführung des Verfahrens nach einem der Ansprüche 1 bis 12 als Teil eines Systems nach einem der Ansprüche 13 bis 15, **gekennzeichnet durch** Kommunikations- und Prozessormittel zum Austausch von Informationen mit einer zentralen Einheit, **durch** Speichermittel zum Speichern von von der zentralen Einheit empfangenen Zertifikaten und **durch** eine Schnittstelle (14, 15) zum offline-Austausch von Informationen mit einer ortsfesten Einheit (3), und **durch** einen fest gespeicherten Identitätscode (ID).

17. Mobile Einheit nach Anspruch 16, **gekennzeichnet durch** Energieversorgungsmittel (2.5) sowie eine Leistungsschnittstelle (15) zum Übertragen von Energie auf eine ortsfeste Einheit.

18. Ortsfeste Einheit (3) zur Durchführung des Verfahrens nach einem der Ansprüche 1 bis 12 als Teil eines Systems nach einem der Ansprüche 13 bis 15, **gekennzeichnet durch** Speichermitteln zum nichtflüchtigen Speichern von für die ortsfeste Einheit charakteristischen Informationen, eine Schnittstelle (14) zum offline-Austausch von Informationen mit einer mit ihr in Verbindung stehenden mobilen Einheit, und **durch** Mittel zum Betätigen eines Freigabemechanismus in Abhängigkeit von einer Verifikation von mit der Schnittstelle ausgetauschten und in den Speichermitteln gespeicherten Informationen.

19. Ortsfeste Einheit nach Anspruch 18, **gekennzeichnet durch** eine Leistungsschnittstelle (15) zum Empfangen von elektrischer Energie von einer mobilen Einheit für das Durchführen der Verfikation.

20. Ortsfeste Einheit nach Anspruch 19, **dadurch gekennzeichnet, dass** die Mittel zum Betätigen eines Freigabemechanismus so ausgebildet und verschaltet sind, dass sie ebenfalls mit von der ortsfesten Einheit empfangener elektrischer Energie betätigt werden können.

21. Computerprogramm mit Mitteln, einen über Kommunikationsmittel mit einer mobilen Einheit eines Systems nach einem der Ansprüche 13 bis 15 verbindbaren Computer eine Zentrale Einheit im Verfahren nach einem der Ansprüche 1 bis 12 bilden zu lassen, mit Mitteln, den Computer in Abhängigkeit eines von einer mobilen Einheit abgesandten Request-Signals ein Zertifikat auszustellen und verschlüsselt an die mobile Einheit zu versenden.

22. Computerprogrammprodukt enthaltend computerlesbare Programmcodemittel, einen über Kommunikationsmittel mit einer mobilen Einheit eines Systems nach einem der Ansprüche 13 bis 15 verbindbaren Computer eine Zentrale Einheit im Verfahren nach einem der Ansprüche 1 bis 12 bilden zu lassen, wobei die computerlesbaren Programmcodemittel Mittel beinhalten, den Computer in Abhängigkeit eines von einer mobile Einheit abgesandten Request-Signals ein Zertifikat auszustellen und verschlüsselt an die mobile Einheit zu versenden

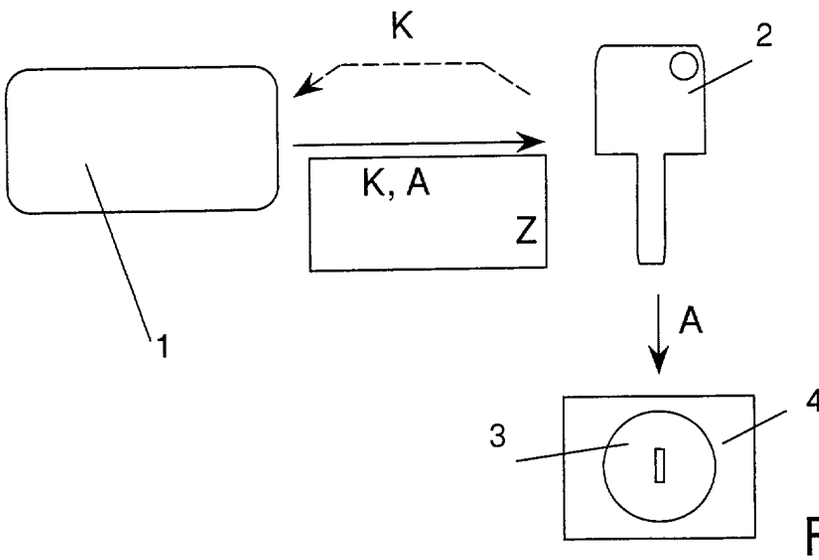

Fig. 1

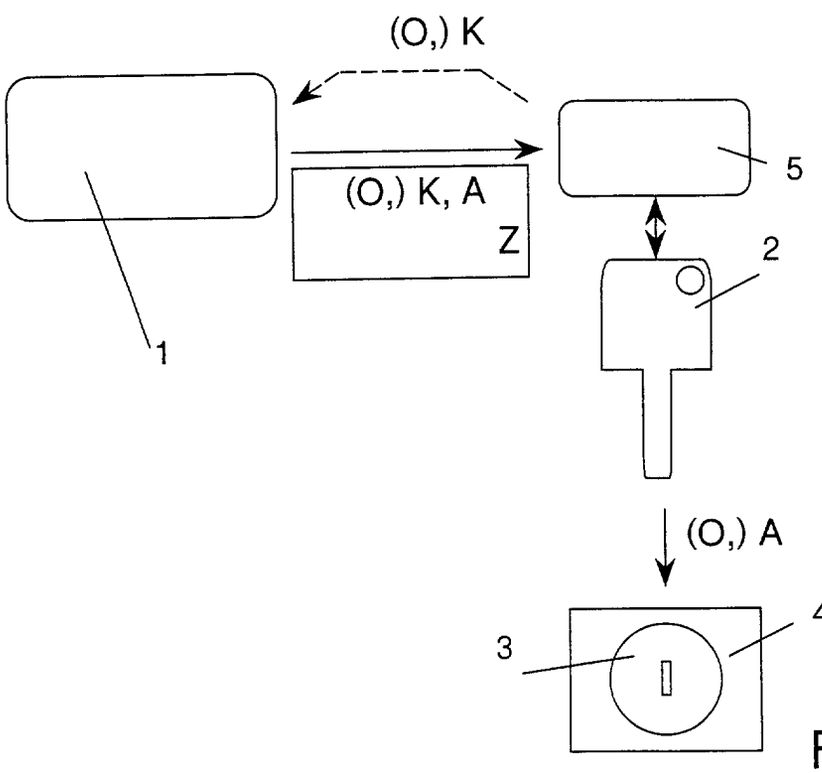

Fig. 2

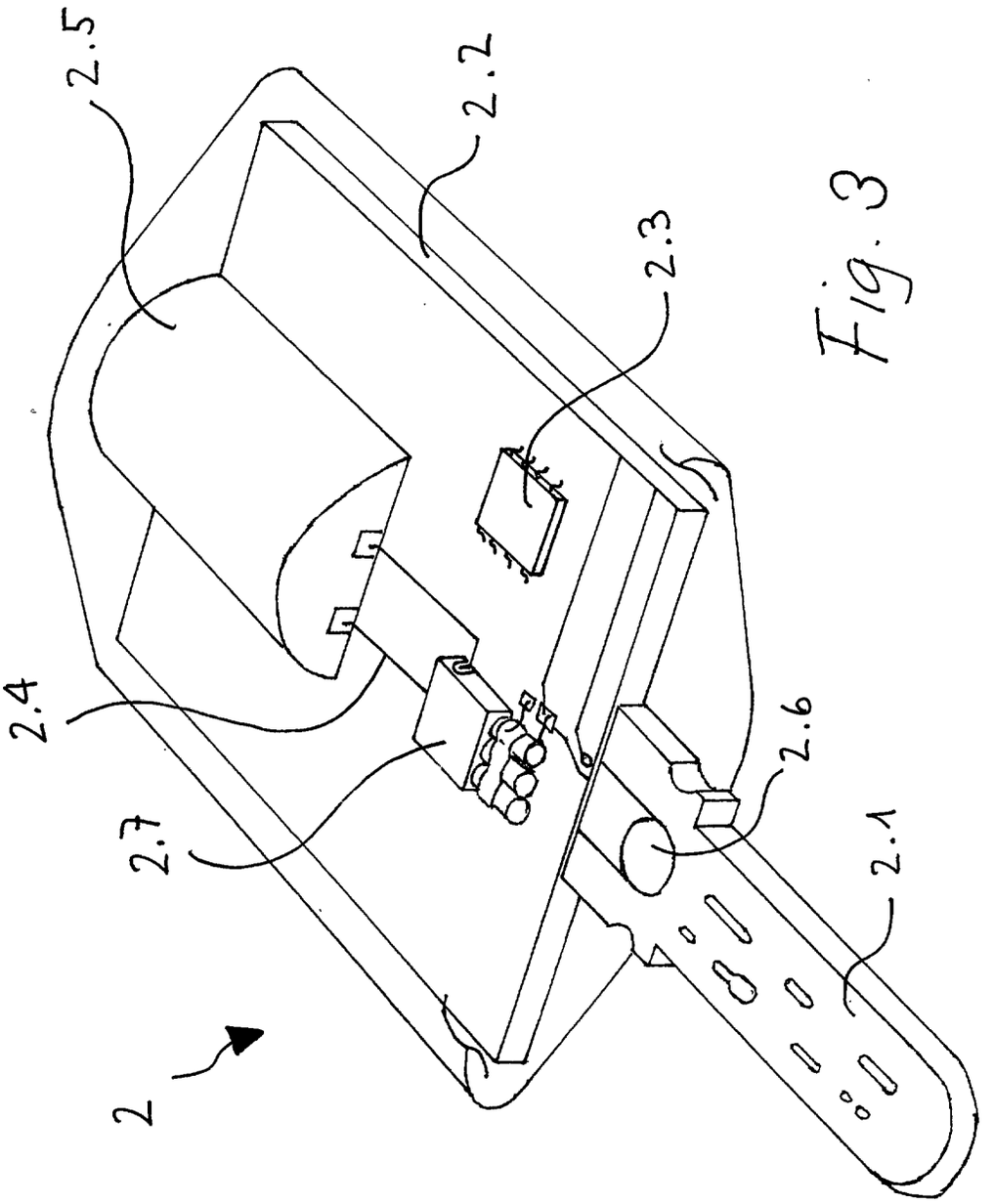

Fig. 3

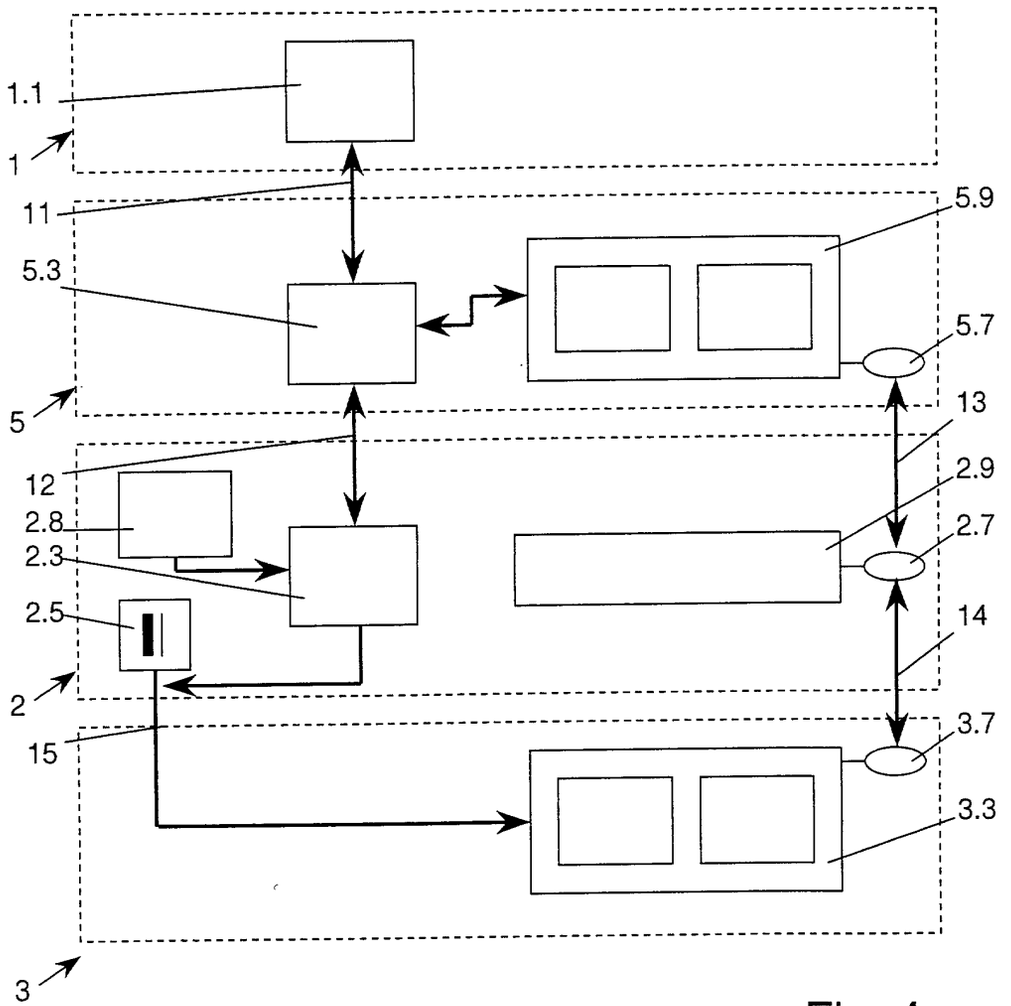

Fig. 4

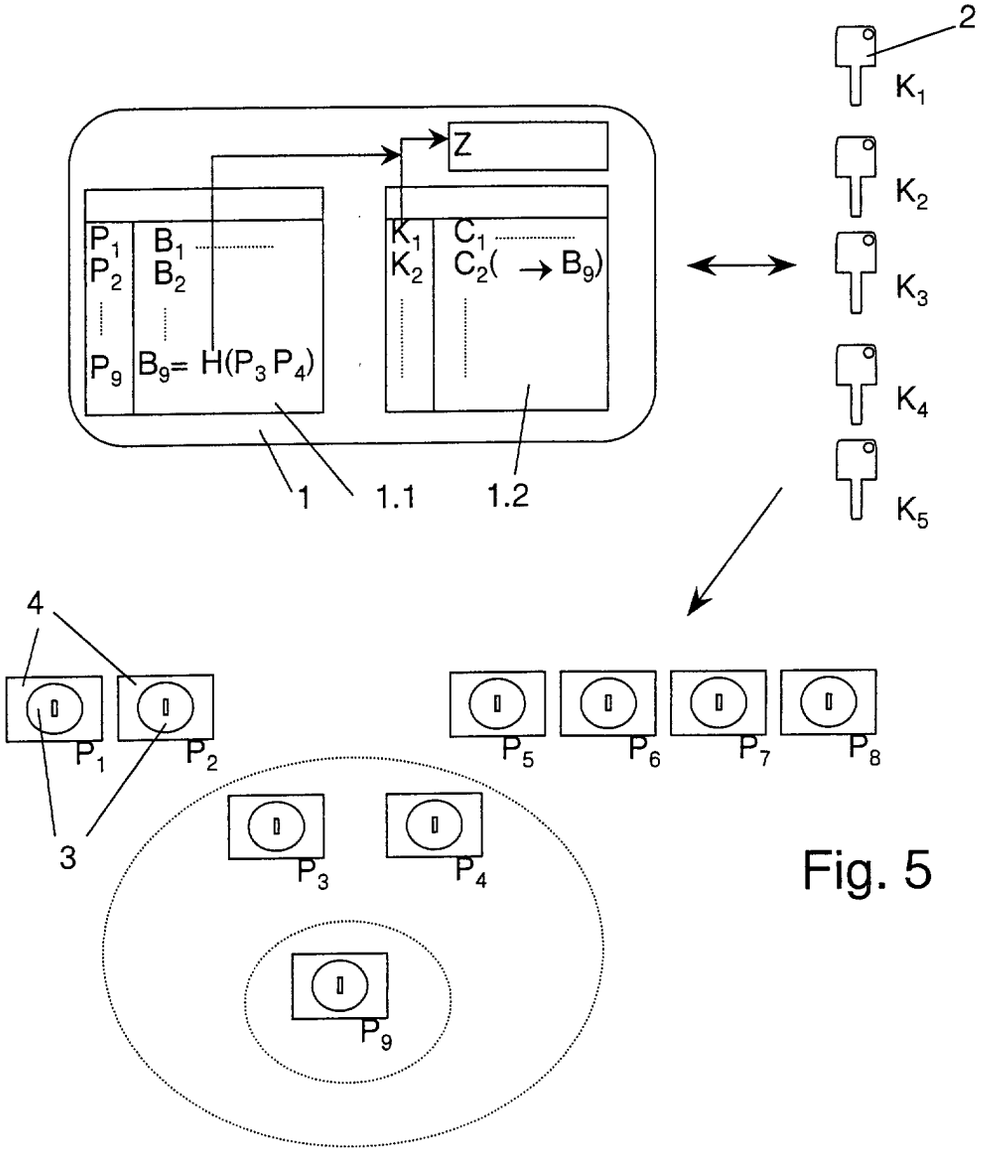
2
K1
K2
K3
K4
K5
Z
P1
P2
P9
B1
B2
B9= H(P3 P4)
K1
K2
C1
C2(→ B9)
1
1.1
1.2
4
3
P1
P2
P3
P4
P5
P6
P7
P8
P9

Fig. 5