



(12) **EUROPÄISCHE PATENTANMELDUNG**

(43) Veröffentlichungstag:
09.09.2009 Patentblatt 2009/37

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

(21) Anmeldenummer: **09002830.9**

(22) Anmeldetag: **27.02.2009**

(84) Benannte Vertragsstaaten:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO SE SI SK TR
Benannte Erstreckungsstaaten:
AL BA RS

(30) Priorität: **03.03.2008 DE 102008012249**
04.03.2008 DE 102008012574

(71) Anmelder: **DORMA GmbH + Co. KG**
58256 Ennepetal (DE)

(72) Erfinder:
• **Hirtsiefer, Werner**
53343 Wachtberg (DE)
• **Gerdemann, Helmut**
78554 Aldingen (DE)
• **Wolf, Martin, Dr.**
53115 Bonn (DE)
• **Klein, Thomas**
50321 Brühl (DE)
• **Debus, Michael**
53179 Bonn (DE)

(54) **Zutrittskontrollsystem und Verfahren zum Betrieb eines solchen Systems**

(57) Die Erfindung betrifft ein Zutrittskontrollsystem (1), mit zumindest einer Kontrollzentrale (3), einem ersten Zutrittskontrollmodul (9), welches wenigstens ein Lesemodul (9.1) und ein Stellmodul (9.2) aufweist, wobei das Lesemodul (9.1) dazu dient, Daten von einem ID-Geber (8) auszulesen, und das Stellmodul (9.2) einen Zutritt zu einem Objekt freigibt, falls die richtigen Daten vom ID-Geber (8) ausgelesen worden sind. Erfindungsgemäß

ist vorgesehen, dass Identifikationsdaten sowie Zutrittskontrolldaten auf dem ID-Geber (8) gespeichert sind, die von dem Lesemodul (9.1) auslesbar sind, anhand dessen über den Zutritt zu dem Objekt und somit über eine Freigabe durch das Stellmodul (9.2) entschieden wird.

Ferner ist die Erfindung auch auf ein Verfahren zum Betrieb eines erfindungsgemäßen Zutrittskontrollsystems (1) gerichtet.

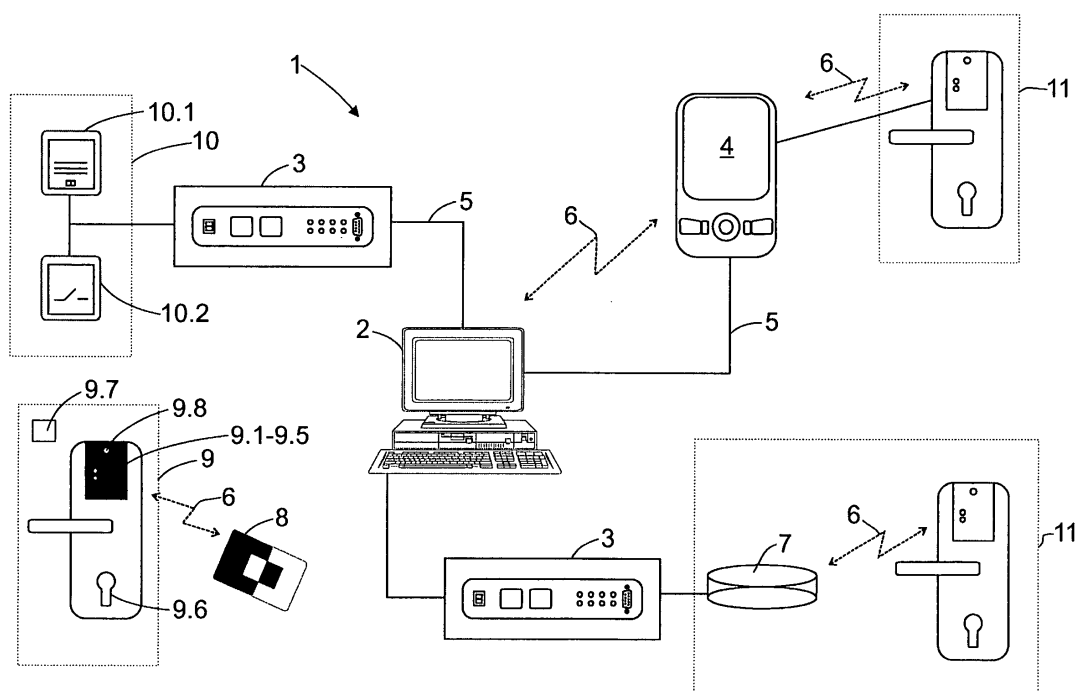


Fig. 1

Beschreibung

[0001] Die Erfindung richtet sich auf ein Zutrittskontrollsystem gemäß dem Oberbegriff von Anspruch 1, welches dazu dient, einem Benutzer den Zutritt zu einem geschützten Objekt freizugeben oder zu versperren. Zu diesem Zweck muss der Benutzer sich mit einem ID-Geber ausweisen, um den Zutritt zu dem Objekt zu erhalten. Hierfür sind auf dem ID-Geber zumindest Identifikationsdaten gespeichert, die magnetisch, optisch, kontaktlos bzw. drahtlos oder durch elektrische Verbindungen ausgelesen werden können. Das durch das Zutrittskontrollsystem geschützte Objekt ist selbst mit einem Zutrittskontrollmodul versehen, welches den Zutritt zum Objekt freigibt oder versperrt. Üblicherweise weist das Zutrittskontrollmodul wenigstens ein Lesemodul und ein Stellmodul auf, wobei das Lesemodul dazu dient, die Daten von dem ID-Geber auszulesen, und das Stellmodul bei einem positiven Ergebnis dazu dient, den Zutritt zum Objekt freizugeben.

[0002] Derartige Zutrittskontrollsysteme werden bei einer Vielzahl von zu sichernden Objekten eingesetzt, wie z. B. bei einer Industrieanlage, einem Bürogebäude oder dergleichen. Dabei können nicht nur Räume sondern auch Parkplätze, Laboratorien und/oder ganze Bereiche zentral durch das Zutrittskontrollsystem gesichert und der Zutritt verwaltet werden.

[0003] Ferner ist die vorliegende Erfindung auch auf ein Verfahren gemäß dem Oberbegriff von Anspruch 22 gerichtet, welches zum Betrieb eines erfindungsgemäßen Zutrittskontrollsystems dient.

[0004] Aus dem Stand der Technik sind zahlreiche Zutrittskontrollsysteme bekannt, die auf verschiedene Art und Weise den Zutritt zu einem oder mehreren geschützten Objekten sichern. Aus der Druckschrift DE 102 46 664 A1 ist beispielsweise bekannt, dass sich ein Besitzer eines ID-Gebers an einem Zutrittskontrollmodul des Zutrittskontrollsystems zusätzlich durch seine biometrischen Daten, wie z. B. einen Fingerabdruck, ausweisen muss, damit das im Zutrittskontrollmodul vorhandene Stellmodul den Zutritt zu dem Objekt freigibt.

[0005] Ferner ist beispielsweise aus der Druckschrift WO 2006/056085 A1 bekannt, dass sich der Benutzer an einem Zutrittskontrollmodul nicht nur durch den entsprechenden ID-Geber ausweisen muss, sondern gleichzeitig auch ein mechanisches Sicherheitselement, wie z. B. einen mechanischen Sicherheitsschlüssel, aufweisen muss, um somit den Zutritt zu dem gesicherten Objekt zu erlangen. Dabei kann der ID-Geber mit dem mechanischen Sicherheitselement zu einer Einheit verbunden sein, sodass bei einer Betätigung des mechanischen Sicherheitselements gleichzeitig auch die Daten des ID-Gebers von einem Lesemodul des Zutrittskontrollmoduls ausgelesen werden können, um somit den Zutritt bei einem positiven Ergebnis zu erhalten.

[0006] Bei den beiden zuvor genannten Zutrittskontrollsystemen ist die Kontrollzentrale in der Regel mit dem jeweiligen Zutrittskontrollmodul über eine Datenleitung

verbunden, sodass ein Datenaustausch problemlos möglich ist. Darüber hinaus existieren Zutrittskontrollsysteme, bei denen eine Verdrahtung der Zutrittskontrollmodule nicht ohne Weiteres möglich ist, da beispielsweise das Zutrittskontrollsystem in einem bereits bestehenden Gebäude angebracht wird. In diesem Fall werden die beiden folgenden Varianten unterschieden, die jeweils als drahtlose Zutrittskontrollmodule ausgestaltet sind.

[0007] Bei der ersten Variante ist das jeweilige Zutrittskontrollmodul über eine Funkverbindung mit einem sogenannten Traffic-Point verbunden, um einen permanenten Datenaustausch zwischen der Kontrollzentrale und dem Zutrittskontrollmodul zu ermöglichen. Sofern das Zutrittskontrollmodul Daten von einem ID-Geber auslesen kann, sendet es diese gelesenen Daten über die Funkverbindung und den Traffic-Point an die Kontrollzentrale des Zutrittskontrollsystems, die über eine Freigabe oder eine Sperrung des Zutritts zu dem Objekt des jeweiligen Zutrittskontrollmoduls entscheidet. Zu diesem Zweck sendet die Kontrollzentrale das positive oder negative Ergebnis an das jeweilige Zutrittskontrollmodul per Funk über den Traffic-Point zurück, woraufhin ein Stellmodul des Zutrittskontrollmoduls den Zutritt zum Objekt freigibt oder weiterhin versperrt, je nach empfangenem Ergebnis.

[0008] Bei der zweiten Variante steht das Zutrittskontrollmodul nicht permanent mit der Kontrollzentrale in Verbindung. Aus diesem Grund werden die drahtlosen Zutrittskontrollmodule vorher mit den jeweiligen Zutrittskontrollregeln und -daten programmiert, sodass diese Zutrittskontrollmodule selbstständig nach dem Auslesen der Identifikationsdaten vom ID-Geber entscheiden, ob ein Zutritt zum Objekt durch das Stellmodul freigegeben werden kann oder nicht. Diese ebenfalls drahtlosen Zutrittskontrollmodule werden beispielsweise durch einen Taschencomputer (PDA) im Vorfeld mit den entsprechenden Zugangsregeln und Zutrittskontrolldaten programmiert.

[0009] Bei der ersten Variante ist es von Nachteil, dass das drahtlose Zutrittskontrollmodul eine Funkverbindung mit dem Traffic-Point aufbauen muss, um somit den permanenten Datenaustausch mit der Kontrollzentrale zu ermöglichen. Bei großen Industrieanlagen muss dann entweder eine lange Verdrahtung zum Traffic-Point oder eine spezielle Funkstrecke aufgebaut werden, um den Datenaustausch über weite Distanzen zwischen dem Traffic-Point und der Kontrollzentrale zu ermöglichen. Hierdurch kommt es auch zu längeren Antwortzeiten an dem Zutrittskontrollmodul. Ferner ist es denkbar, dass die Funkverbindung z. B. durch einen Störsender gezielt unterbrochen wird, was zu Fehlfunktionen führt. Bei der zweiten Variante hat sich dagegen als Nachteil herausgestellt, dass die jeweiligen drahtlosen Zutrittskontrollmodule beispielsweise umprogrammiert werden müssen, falls ein ID-Geber abhanden gekommen ist. Ebenfalls muss ein häufiger, zeitaufwändiger Abgleich der Zutrittskontrolldaten mit dem Zentralrechner stattfinden, da-

mit auch geänderte Zutrittsregeln z. B. für einen neuen ID-Geber oder geänderte Zugangszeiten in dem jeweiligen Zutrittskontrollmodul abgespeichert sind.

[0010] Folglich unterscheidet man die oben genannten Zutrittskontrollsysteme einerseits nach ihrer Art der Anbindung mit den Zutrittskontrollmodulen, d. h. verdrahtet und unverdrahtet, und andererseits nach der Lokalität der Zutrittsregeln und dem jeweiligen Informationsabgleich, z. B. ob dieser permanent oder nur auf Anforderung stattfindet.

[0011] Aufgabe der vorliegenden Erfindung ist es, den Aufbau und den Betrieb eines Zutrittskontrollsystems zu vereinfachen. Dabei sollen u. a. auch die Nachteile aus dem Stand der Technik, insbesondere bei einem drahtlosen Datenaustausch zwischen der Kontrollzentrale und einem Zutrittskontrollmodul, vermieden werden. Die vorliegende Aufgabe wird durch ein Zutrittskontrollsystem gemäß dem Anspruch 1, insbesondere mit den technischen Merkmalen des kennzeichnenden Teils gelöst, denen folgende besondere Bedeutungen zukommen.

[0012] Bei dem erfindungsgemäßen Zutrittskontrollsystem werden in dem ID-Geber nicht nur die Identifikationsdaten gespeichert sondern zusätzlich auch Zutrittskontrolldaten, die von dem Lesemodul eines ersten Zutrittskontrollmoduls auslesbar sind. Anhand der ausgelesenen Daten kann dann ein erstes Zutrittskontrollmodul, welches drahtlos zur Kontrollzentrale ausgestaltet ist, über den Zutritt zu dem Objekt und somit selbstständig über eine Freigabe durch das Stellmodul entscheiden. Folglich besteht der wesentliche Unterschied zu den beschriebenen drahtlosen Zutrittskontrollmodulen darin, dass die Zutrittskontrolldaten nicht in der Kontrollzentrale oder in dem Zutrittskontrollmodul gespeichert werden sondern vielmehr auf dem ID-Geber hinterlegt sind. Hierdurch lassen sich der Aufbau und der Betrieb des erfindungsgemäßen Zutrittskontrollsystems vereinfachen.

[0013] Weitere zweckmäßige Ausgestaltungen der vorliegenden Erfindung ergeben sich aus den abhängigen Unteransprüchen.

[0014] Zweckmäßigerweise ist das erste Zutrittskontrollmodul drahtlos mit dem übrigen Zutrittskontrollsystem, insbesondere der Kontrollzentrale, verbunden, um einen Datenaustausch zu ermöglichen. Hierbei findet insbesondere ein Datenaustausch zum Informationsabgleich nur auf Anforderung statt. Folglich ist das erste Zutrittskontrollmodul nicht über einen Traffic-Point, wie die bekannten drahtlosen Zutrittskontrollmodul, mit der Kontrollzentrale verbunden. Auch sind bei dem ersten Zutrittskontrollmodul nicht die Zutrittskontrolldaten in dem ersten Zutrittskontrollmodul gespeichert. Vielmehr befinden sich diese Zutrittskontrolldaten zusätzlich auf dem ID-Geber. Zu diesem Zweck wird der ID-Geber vor seinem ersten Einsatz mit den notwendigen Daten, insbesondere den Zutrittskontrolldaten, versehen, um dem jeweiligen Benutzer die entsprechenden Rechte zum Zutritt zu den jeweiligen Objekten zu ermöglichen. In diesem Zusammenhang wird auch von einer Vorbereitung

des ID-Gebers für die nachfolgende Verwendung gesprochen. Somit muss nicht das erste Zutrittskontrollmodul durch einen Informationsabgleich mit der Kontrollzentrale an den neu verwendeten ID-Geber angepasst werden, wie es aus dem Stand der Technik bei drahtlosen Zutrittskontrollmodulen der Fall ist.

[0015] Das erste Zutrittskontrollmodul kann ein Logikmodul aufweisen, welches die von dem ID-Geber gelesenen Daten mit vorgegebenen Solldaten vergleicht und bei einem positiven Ergebnis das Stellmodul entsprechend ansteuert, um den Zutritt zu dem Objekt freizugeben. Ferner kann das erste Zutrittskontrollmodul ein Zeitmodul enthalten, welches konkrete Zeitdaten liefert, die zum Vergleich mit den ausgelesenen Zutrittskontrolldaten vom ID-Geber dienen. Somit ist es denkbar, dass das Logikmodul zusätzlich die Zeitdaten vom Zeitmodul erhält, wobei es die Solldaten und die Zeitdaten mit den von dem ID-Geber gelesenen Daten vergleicht und bei einem positiven Ergebnis das Stellmodul entsprechend ansteuert, um den Zutritt zu dem Objekt freizugeben.

[0016] Die zusätzlich in dem ID-Geber gespeicherten Zutrittskontrolldaten können z. B. die Informationen enthalten, wo (welche Tür, welchen Bereich, welchen Parkplatz etc.), wann (zu welcher Uhrzeit) und/oder wie oft (Häufigkeit des Zugangs) ein Benutzer mit dem ID-Geber einen speziellen Zutritt passieren darf. Zusätzlich ist es denkbar, auch biometrische Daten wie z. B. den Fingerabdruck, Netzhautinformationen oder eine Stimmenerkennung oder dergleichen als Personendaten auf dem ID-Geber zu speichern. Diese Personendaten können dann mit den jeweiligen Personendaten eines Benutzers verglichen werden, indem z. B. ein zusätzliches Sensorelement diese Daten messtechnisch erfasst und an das Logikmodul des ersten Zutrittskontrollmoduls liefert. Nur wenn die Personendaten auf dem ID-Geber mit den messtechnisch erfassten Daten vom Benutzer übereinstimmen sowie die Zutrittskontrolldaten und die Identifikationsdaten ein positives Ergebnis bei einem Vergleich mit den Sollwerten liefern, kann der Zutritt zu einem Objekt freigegeben werden. In diesem Fall weist das Logikmodul das Stellmodul an, den Zutritt zu dem Objekt freizugeben. Dabei kann es optional vorgesehen sein, dass die Identifikationsdaten des ID-Gebers unterschiedlich zu den Zutrittskontrolldaten gespeichert sind, wobei insbesondere die Identifikationsdaten unveränderbar und die Zutrittskontrolldaten veränderbar im ID-Geber vorgegeben sind.

[0017] Dabei ist auch denkbar, dass die Daten des ID-Gebers verschlüsselt gespeichert sind, wobei insbesondere eine Entschlüsselung der Daten von dem Logikmodul des ersten Zutrittskontrollmoduls vorgenommen wird. Hierbei können die Identifikationsdaten andersartig verschlüsselt werden als die Zutrittskontrolldaten. Auch ist es denkbar, dass die Identifikationsdaten durch ein anderes Schnittstellensystem ausgelesen werden als die Zutrittskontrolldaten. Das Lesen der Identifikationsdaten kann z. B. durch die folgenden Schnittstellenformate stattfinden: Hitag-1, Hitag-2, EM4102, EM4450, Mifare-

ID, LEGIC-ID, Trovan oder Indala. Zusätzlich ist es denkbar, dass auch Zustandsdaten von dem Zutrittskontrollmodul durch ein Schreibmodul auf dem ID-Geber gespeichert werden. Zu diesem Zweck kann das Zutrittskontrollmodul zusätzlich ein Schreibmodul aufweisen. Diese Zustandsdaten können z. B. den erfolgreichen oder abgewiesenen Zutritt an dem ersten Zutrittskontrollmodul enthalten. Ebenfalls können die Zustandsdaten auch die Häufigkeit und Uhrzeit und die konkrete Nummer des ersten Zutrittskontrollmoduls und den Energiezustand eines Energiespeichers des ersten Zutrittskontrollmoduls enthalten. Das Schreiben dieser Zustandsdaten kann z. B. über die folgenden Formate erfolgen: Mifare, LEGIC, Hitag-2, EM4102 oder EM4450. Ferner ist es denkbar, dass z. B. die Identifikationsdaten magnetisch von dem ID-Geber ausgelesen werden, wohingegen die Zutrittskontrolldaten drahtlos über einen sogenannten RFID-Chip ausgelesen werden können. Dabei sind auch andere Konstellationen denkbar. Ebenfalls kann der ID-Geber mit einem mechanischen Sicherheitselement, wie z. B. einem Schlüssel, versehen sein, um den Sicherheitsstandard am ersten Zutrittskontrollmodul zu erhöhen. Folglich müssen einerseits eine elektromechanische und andererseits eine rein mechanische Überprüfung des ID-Gebers erfolgreich stattfinden, bevor der Zutritt zu dem Objekt freigegeben werden kann.

[0018] Das bisher beschriebene Zutrittskontrollsystem weist den Vorteil auf, dass ein verlorengegangener ID-Geber z. B. nach Ablauf einer vorgegebenen Zeitspanne selbstständig unbrauchbar wird, da die Zutrittskontrolldaten einen Zutritt nicht mehr ermöglichen. Zu diesem Zweck weisen die Zutrittskontrolldaten eine Zutrittsregel auf, wobei die Zutrittsregel insbesondere auch wenigstens eine Gültigkeitsdauer beinhaltet. Dabei können auch mehrere Zutrittsregeln vorhanden sein, die unterschiedliche Gültigkeitsdauern aufweisen. So kann z. B. ein ID-Geber einerseits eine Zutrittsregel enthalten, um den Zutritt zu einer Parkschanke genau einmal an einem Vormittag freizugeben. Ferner kann in dem ID-Geber eine weitere Zutrittsregel gespeichert sein, um z. B. einen Haupteingang an dem Tag mehrfach passieren zu können. Geht nun der entsprechende ID-Geber verloren, so läuft automatisch seine Gültigkeit ab, womit der ID-Geber unbrauchbar wird. Wird der ID-Geber von dem Benutzer ordnungsgemäß zurück gebracht, so kann der ID-Geber z. B. für eine nächste Verwendung vorbereitet werden.

[0019] Sollte der ID-Geber jedoch eine größere Restgültigkeitsdauer aufweisen, so müsste der entsprechende ID-Geber von der Kontrollzentrale gesperrt werden, wobei die entsprechenden Daten (gemeint sind die Identifikationsdaten) manuell in das erste Zutrittskontrollmodul gespeichert werden müssten.

[0020] Die Vorbereitung des ID-Gebers kann z. B. durch die Kontrollzentrale erfolgen, in der die individuellen Zutrittskontrolldaten für einen Benutzer erstellt werden und mittels einer Lese-Schreibeinheit, die mit der Kontrollzentrale verbunden ist, auf dem ID-Geber gespeichert werden. Die Kontrollzentrale selbst stellt einen

speziellen Computer oder Microcontroller für das Zutrittskontrollsystem dar, welches mit einer Vielzahl von Zutrittskontrollmodulen in Verbindung stehen kann. Innerhalb eines Zutrittskontrollsystems können mehrere unterschiedliche oder gleichartige Kontrollzentralen vorgesehen sein.

[0021] Ebenfalls ist es denkbar, dass der ID-Geber einen Transponder aufweist, mit dem Energie insbesondere drahtlos von dem ID-Geber auf das erste Zutrittskontrollmodul übertragbar ist. Somit kann das erste Zutrittskontrollmodul ausreichend mit Energie von dem ID-Geber gespeist werden, um den Zutritt zu einem Objekt freizugeben. Gerade bei größeren Zutrittskontrollsystemen, wie z. B. in einem Hotel, kann somit die Energieversorgung des ersten Zutrittskontrollmoduls unproblematisch bewerkstelligt werden. Wie bereits erwähnt wurde, ist es auch denkbar, dass die Energiezustandsinformationen von dem ersten Zutrittskontrollmodul auf dem ID-Geber bei einem Zutrittsversuch gespeichert werden, wobei diese Informationen anschließend wieder ausgewertet werden können, sobald der ID-Geber mit einem fest verdrahteten Zutrittskontrollmodul in Kontakt bzw. im Informationsabgleich steht.

[0022] Bei einer zweckmäßigen Ausgestaltung des ersten Zutrittskontrollmoduls bildet dieses wenigstens mit dem Lese- und/oder Schreibmodul, dem Logik- und/oder Zeitmodul und dem Stellmodul eine bauliche Einheit. Dabei kann das erste Zutrittskontrollmodul z. B. in einem Türbeschlag integriert sein. Ebenfalls ist es denkbar, dass das erste Zutrittskontrollmodul die Form eines normalen mechanischen Schließzylinders aufweist und in einem Türschloss steckt. Die sonst von dem Schließzylinder durchgeführte mechanische Bewegung wird dann automatisch von dem ersten Zutrittskontrollmodul ausgeführt, falls eine positive Zutrittskontrolle stattgefunden hat.

[0023] Das Stellmodul des Zutrittskontrollmoduls weist optional ein ansteuerbares, elektromechanisches Sperrglied auf, womit der Zutritt zu dem Objekt versperrt oder freigegeben werden kann, wobei das Stellmodul insbesondere an einer Tür, einem Fenster, einer Schranke, einer Klappe, einem Tresor oder dergleichen vorgesehen ist.

[0024] Ebenfalls ist es denkbar, das erfindungsgemäße Zutrittskontrollsystem in ein Zeiterfassungssystem und/oder ein Zeitwirtschaftssystem zu integrieren oder einzubinden. Auf diese Weise können die Zutrittsinformationen ohne weiteren Aufwand auch zur Zeiterfassung verwendet werden.

[0025] Um eine hohe Flexibilität des erfindungsgemäßen Zutrittskontrollsystems zu ermöglichen, kann dieses auch mit weiteren Zutrittskontrollmodulen versehen sein, die von dem ersten Zutrittskontrollmodul abweichen. Hierzu kann z. B. ein zweites Zutrittskontrollmodul vorgesehen sein, welches permanent mit einer Datenleitung mit dem Zutrittskontrollsystem verbunden ist, um einen Datenaustausch zu ermöglichen. Der Datenaustausch kann dabei insbesondere permanent oder nur auf Anfor-

derung stattfinden. Bei diesem zweiten Zutrittskontrollmodul ist es ausreichend, wenn nur die Identifikationsdaten aus dem ID-Geber ausgelesen werden, da die Zutrittsdaten bzw. die Zutrittsregeln von der Kontrollzentrale an das zweite Zutrittskontrollmodul über die Datenleitung gesendet werden können. Auch ist es denkbar, dass das zweite Zutrittskontrollmodul selber keine Entscheidung über einen Zutritt zu dem gewünschten Objekt vornimmt, da nur die Identifikationsdaten des ID-Gebers ausgelesen werden und mit den Daten des zweiten Zutrittskontrollmoduls an die Kontrollzentrale weitergeleitet werden, die dann selbst die Entscheidung für den Zutritt fällt. Diese Entscheidung wird dann über die Datenleitung wieder an das zweite Zutrittskontrollmodul gesendet, wobei das vorgesehene Stellmodul den Zutritt zum Objekt freigibt, sofern das Vergleichsergebnis positiv war.

[0026] An dieser Stelle sei erwähnt, dass unter dem Vergleich der Daten auch komplexe Berechnungsmethoden oder Algorithmen verstanden werden sollen, die ein zuverlässiges Entscheidungsergebnis liefern.

[0027] Ferner ist es denkbar, dass das erfindungsgemäße Zutrittskontrollsystem auch mit zumindest einem dritten Zutrittskontrollmodul drahtlos verbunden ist, um einen Datenaustausch zu ermöglichen, wobei die Zutrittskontrolldaten für einen ID-Geber in dem Zutrittskontrollmodul gespeichert sind. Ein entsprechender Informationsabgleich zwischen dem Zutrittskontrollsystem und dem dritten Zutrittskontrollmodul kann permanent oder nur auf Aufforderung stattfinden. Auch bei diesem dritten Zutrittskontrollmodul werden nur die Identifikationsdaten aus dem ID-Geber gelesen, um über einen Zutritt zu dem gesperrten Objekt zu entscheiden.

[0028] Bei einem permanenten Informationsabgleich zwischen dem dritten Zutrittskontrollmodul und dem Zutrittskontrollsystem werden die ausgelesenen Identifikationsdaten drahtlos z. B. über einen Traffic-Point zu dem Zutrittskontrollsystem geschickt, welches die entsprechende Kontrolle oder den Vergleich vornimmt. Sofern der Vergleich oder die Kontrolle positiv verläuft, wird ein entsprechendes Steuersignal an das dritte Zutrittskontrollmodul zurück geschickt, wobei wieder eine drahtlose Verbindung über den bereits erwähnten Traffic-Point stattfinden kann.

[0029] Bei der zweiten Variante werden die Zutrittskontrolldaten nur auf Anforderung in dem dritten Zutrittskontrollmodul gespeichert. Somit nimmt das dritte Zutrittskontrollmodul bei dieser Variante selbst den Vergleich zwischen den ausgelesenen Identifikationsdaten und den Zutrittskontrolldaten vor. Bei diesem Zutrittskontrollmodul muss ein häufiger Abgleich zwischen einer Kontrollzentrale und dem Zutrittskontrollmodul stattfinden, damit die Zutrittskontrolldaten aktuell bleiben.

[0030] Ebenfalls ist es Aufgabe der folgenden Erfindung, ein einfaches Verfahren zum Betrieb eines Zutrittskontrollsystems bereitzustellen, bei dem nicht ein häufiger Datenaustausch zwischen einer Kontrollzentrale und einem drahtlos verbundenem ersten Zutrittskontrollmodul stattfinden muss. Die vorliegende Aufgabe wird durch

ein Verfahren zum Betrieb eines Zutrittskontrollsystems gemäß Anspruch 22, insbesondere den kennzeichnenden Merkmalen gelöst, denen folgende besondere Bedeutung zukommt.

[0031] Ausgehend von einem Zutrittskontrollsystem gemäß der Ansprüche 1 bis 21 laufen die folgenden Schritte zur Vorbereitung des ID-Gebers in dem Verfahren ab:

- a) Lesen von Identifikationsdaten des ID-Gebers durch eine Lese-/Schreibeinheit
- b) Weiterleiten der gelesenen Identifikationsdaten an eine Kontrollzentrale
- c) Erstellen von individuellen Zutrittskontrolldaten, insbesondere mit wenigstens einer Zutrittsregel und einer Gültigkeitsdauer, für einen durch den ID-Geber identifizierbaren Besitzer
- d) Weiterleiten der erstellten Zutrittskontrolldaten an die Lese-/ Schreibeinheit
- e) Schreiben der Zutrittskontrolldaten auf den ID-Geber.

[0032] Die zuvor genannten Schritte können teilweise hintereinander oder parallel ablaufen und dienen ausschließlich zur Vorbereitung des ID-Gebers zum Einsatz in dem Zutrittskontrollsystem. Nach der Vorbereitung des ID-Gebers können die nachfolgenden Schritte zur Identifikation und Freigabe, sprich die Verwendung des ID-Gebers, an einem ersten Zutrittskontrollmodul ablaufen:

- f) Lesen der Identifikationsdaten sowie der Zutrittskontrolldaten des ID-Gebers durch das Lesemodul
- g) Weiterleiten der gelesenen Daten an das Logikmodul
- h) Vergleich der gelesenen Daten mit vorgegebenen Solldaten des Logikmoduls
- i) Ermitteln eines positiven oder negativen Ergebnisses durch den Datenvergleich
- j) bei einem positiven Ergebnis, Ansteuerung des Stellmoduls zur Freigabe des Objektes
- k) bei einem negativen Ergebnis, ggf. Aussenden eines Warnhinweises an die Kontrollzentrale.

[0033] Ferner ist es denkbar, dass ein Schritt I), nämlich eine erste Inbetriebnahme des ersten Zutrittskontrollmoduls durch Speichern von Konfigurationsdaten im Zutrittskontrollmodul, vorgenommen wird, wobei insbesondere die Konfigurationsdaten drahtlos oder per Datenleitung übertragbar sind. Für diese Konfiguration kann das erste Zutrittskontrollmodul entweder direkt über eine Datenleitung mit einer Kontrollzentrale verbunden werden, um die Konfigurationsdaten zu erhalten. Ebenfalls ist es denkbar, dass die Konfigurationsdaten von der Kontrollzentrale zunächst in einem Handgerät (einem sogenannten PDA - Personal Digital Assistant) zwischengespeichert werden, um von dort aus die Konfigurationsdaten beispielsweise drahtlos an das erste Zutrittskontrollmodul zu senden. Bei dieser Inbetriebnahme ist zu erwäh-

nen, dass die Konfigurationsdaten eben nicht die Zutrittsregeln für einzelne ID-Geber enthalten. Vielmehr sind diese erfindungsgemäß auf dem ID-Geber gespeichert.

[0034] Darüber hinaus ist es denkbar, dass nach einem Lesen der Identifikationsdaten sowie der Zutrittskontrolldaten des ID-Gebers durch einen Schritt m) Zustandsdaten des ersten Zutrittskontrollmoduls auf dem ID-Geber gespeichert werden. Diese Zustandsdaten des ersten Zutrittskontrollmoduls können z. B. Lese-, Freigabe-, Sperrvorgänge sowie den Energiezustand eines Energiespeichers des Zutrittskontrollmoduls enthalten. Damit ist eine umfassende Auswertung über die Freigabe oder Sperrvorgänge und die Zutrittsstatistik an dem ersten Zutrittskontrollmodul möglich, auch wenn eben kein permanenter Datenaustausch zwischen dem Zutrittskontrollsystem und dem ersten Zutrittskontrollmodul stattfindet.

[0035] Zusätzlich können auf dem ID-Geber Personendaten von einem Besitzer, insbesondere biometrische Daten des Besitzers, gespeichert sein, die insbesondere durch ein zusätzliches Sensorelement von dem Besitzer an dem ersten Zutrittskontrollmodul erfasst werden und an das Logikmodul weitergeleitet werden, um somit einen Vergleich der Solldaten mit den gelesenen Daten des ID-Gebers vorzunehmen. Die Personendaten von dem Besitzer können bei der Vorbereitung des ID-Gebers durch die Kontrollzentrale auf dem ID-Geber gespeichert werden.

[0036] Weitere Merkmale und Vorteile der Erfindung ergeben sich aus den nachfolgenden Figuren und der folgenden Beschreibung, wobei verschiedene Ausführungsbeispiele in den Figuren dargestellt sind.

[0037] Es zeigen:

- Figur 1 eine schematische Darstellung von einem erfindungsgemä- ßen Zutrittskontrollsystem mit verschiedenen Zutrittskontroll- modulen,
- Figur 2 eine schematische Darstellung zur Inbetriebnahme eines ersten Zutrittskontrollmoduls innerhalb eines Zutrittskontroll- systems,
- Figur 3 eine schematische Darstellung einer Vorbereitung eines ID- Gebers, der mit einem ersten Zutrittskontrollmodul zusam- menwirkt und der zu den Identifikationsdaten auch Zutrittskontrolldaten speichert, und
- Figur 4 eine schematische Darstellung eines Zutrittsversuches bei einem ersten Zutrittskontrollmodul sowie bei einem drahtge- bundenen zweiten Zutrittskontrollmodul.

[0038] In der Figur 1 ist schematisch ein Zutrittskontrollsystem 1 mit verschiedenen Zutrittskontrollmodulen 9, 10, 11 dargestellt. Grundsätzlich ist zu bemerken, dass ein Zutrittskontrollsystem 1 mehrere erste, zweite und dritte Zutrittskontrollmodule 9, 10, 11 aufweisen kann.

Ebenfalls ist es denkbar, dass auch mehr als eine Kontrollzentrale 3 vorgesehen ist, um die einzelnen Zutrittskontrollmodule 9, 10, 11 untereinander zu verbinden. Ebenfalls kann ein Computer 2 vorgesehen sein, der zum Speichern und Verwalten der Daten des Zutrittskontrollsystems 1 dient. Dieser Computer 2 kann über elektrische Datenleitungen 5 mit den jeweiligen Kontrollzentralen 3 verbunden sein. Üblicherweise enthält ein Zutrittskontrollmodul 9, 10, 11 zumindest ein Lesemodul 9.1, 10.1 und ein Stellmodul 9.2, 10.2, wodurch der Zutritt zu einem gesperrten Objekt freigebbar ist. Außerdem kann zumindest das erste Zutrittskontrollmodul 9 auch ein Logikmodul 9.3, ein Zeitmodul 9.4 und ein Schreibmodul 9.5 aufweisen. Ebenfalls kann ein zusätzliches Sensorelement 9.7 oder ein mechanisches Sicherheitselement 9.6 an dem ersten Zutrittskontrollmodul vorgesehen sein. Auch kann ein Anzeigeelement 9.8 an dem ersten Zutrittskontrollmodul 9 vorgesehen sein. Dieses Anzeigeelement 9.8 kann beispielsweise den Freigabe- oder Sperrzustand des Stellmoduls 9.2 anzeigen. Auch ist es denkbar, dass das Anzeigeelement 9.8 dazu dient, Störzustände, Energiezustand oder dergleichen anzuzeigen. In der Figur 1 ist ein erstes Zutrittskontrollmodul 9 als bauliche Einheit in einem Türbeschlag dargestellt. Dieses erste Zutrittskontrollmodul 9 ist mit einem mechanischen Sicherheitselement 9.6 versehen, was aus einem Schließzylinder besteht. Das gezeigte Zutrittskontrollsystem 1 kann mit mehreren ersten Zutrittskontrollmodulen 9 ausgestattet sein. Ebenfalls kann das Zutrittskontrollsystem 1 auch ein zweites Zutrittskontrollmodul 10 aufweisen, welches über eine permanente Datenleitung 5 verbunden ist, um einen Datenaustausch zu ermöglichen. Das zweite Zutrittskontrollmodul 10 weist dabei im Wesentlichen nur ein Lesemodul 10.1 und ein Stellmodul 10.2 auf. Die eigentliche Entscheidung über einen erfolgreichen Zutritt wird von einer Kontrollzentrale 3 getroffen, die mit dem zweiten Zutrittskontrollmodul 10 in Verbindung steht, um einen Informationsabgleich vorzunehmen. Ferner kann auch ein drittes Zutrittskontrollmodul 11 innerhalb des Zutrittskontrollsystems 1 vorgesehen sein, welches drahtlos eingebunden ist, um einen Datenaustausch mit dem Kontrollsystem 1 zu ermöglichen. Hierbei gibt es die Variante, dass ein permanenter Informationsabgleich zwischen dem Zutrittskontrollsystem 1 und dem dritten Zutrittskontrollmodul 11 stattfindet, wie unten rechts in Figur 1 dargestellt ist. Der Datenaustausch kann bei der erwähnten Variante über einen Traffic-Point 7 stattfinden. Ebenfalls kann auch nur ein Informationsabgleich auf Anforderung stattfinden, wie es z. B. bei dem dritten Zutrittskontrollmodul 11 oben rechts in Figur 1 angedeutet ist.

[0039] Das dritte Zutrittskontrollmodul 11 mit einem permanenten Informationsabgleich unterscheidet sich unwesentlich von dem zweiten Zutrittskontrollmodul 10, wobei der Datenaustausch über z. B. eine Funkverbindung stattfindet. Hierzu kann der dargestellte Traffic-Point 7 dienen, um z. B. mehrere dritte Zutrittskontrollmodule 11 mit einem Traffic-Point 7 zu verbinden, die an

einer gemeinsamen Kontrollzentrale 3 einen Informationsabgleich vornehmen. Bei der anderen Variante des dritten Zutrittskontrollmoduls 11 werden die erforderlichen Zutrittskontrolldaten z. B. über ein Handgerät 4 in dem Zutrittskontrollmodul 11 gespeichert. Somit kann auf einen permanenten Informationsabgleich zwischen diesem Zutrittskontrollmodul 11 und einer Kontrollzentrale 3 verzichtet werden, da das Zutrittskontrollmodul 11 selber die Entscheidung für einen ausgelesenen ID-Geber 8 trifft, ob ein Zutritt gewährt werden kann.

[0040] Wie in der Figur 1 ferner optional dargestellt ist, kann der Informationsabgleich zwischen dem Zutrittskontrollsystem 1 und dem dritten Zutrittskontrollmodul 11 oben rechts auch drahtlos über das Handgerät 4 stattfinden. Dabei kann einerseits die Verbindung Zutrittskontrollsystem 1 und Handgerät 4 drahtlos oder per Datenleitung 5 erfolgen, sowie die anschließende Verbindung zum Informationsaustausch Handgerät 4 drittes Zutrittskontrollmodul 11 drahtlos oder per Datenleitung 5 erfolgen.

[0041] Da der ID-Geber 8 auch einen Transponder zum Energietransfer für zumindest das erste Zutrittskontrollmodul 9 aufweisen kann, kann der ID-Geber 8 mit einem wiederaufladbaren Energiespeicher in Form von einem Akku oder einem Kondensator oder dergleichen ausgestattet sein. Dieser Energiespeicher kann z. B. nachts auf einer Ladestation wiederaufgeladen werden, damit wieder ausreichend Energie vorhanden ist, um über den Transponder im ID-Geber 8 und somit ein oder mehrere erste Zutrittskontrollmodule 9 mit Energie zu versorgen. Der Transponder im ID-Geber 8 kann z. B. aus einer Spule bestehen, die Strom über Induktion in eine Spule im ersten Zutrittskontrollmodul 9 überträgt. Wie aus Figur 1 weiter ersichtlich ist, ist das erste Zutrittskontrollmodul 9 nach einer ersten Inbetriebnahme (s. Schritt I)) selbstständig tätig, sodass es dann als Stand-Alone-System arbeiten kann, um den Zutritt zu einem Objekt freizugeben oder weiterhin zu versperren.

[0042] In der Figur 2 ist eine erste Inbetriebnahme (s. Schritt I)) des ersten Zutrittskontrollmoduls 9 dargestellt. Hierbei sind zwei unterschiedliche Ausführungsvarianten des ersten Zutrittskontrollmoduls 9 dargestellt. In der ersten Variante oben rechts ist das erste Zutrittskontrollmodul 9 als ein Türbeschlag ausgestaltet, in dem die weiteren Module 9.1 ff in einer Baueinheit integriert sind. Optional kann das erste Zutrittskontrollmodul 9 auch als ein Schließzylinderersatz, wie in Figur 2 unten rechts dargestellt, ausgestaltet sein. Die beiden Handhaben können dann die entsprechenden Module 9.1 ff. des ersten Zutrittskontrollmoduls 9 beinhalten. Ein solches erstes Zutrittskontrollmodul 9 kann anstelle eines mechanischen Schließzylinders innerhalb eines Türschlosses integriert werden, wobei es dann die gleiche Funktionalität wie der mechanische Schließzylinder übernimmt. Allerdings dient nicht ein mechanischer Schlüssel zur Betätigung des vergleichbaren Schließzylinders, sondern vielmehr der ID-Geber 8 mit den Identifizierungs- und Zutrittskontrolldaten. Die beiden dargestellten ersten Zu-

trittskontrollmodule 9 werden zur ersten Inbetriebnahme (s. Schritt I)) durch ein Handgerät 4 programmiert, welches die entsprechenden Daten z. B. von dem Computer 2 oder einer Kontrollzentrale 3 des Zutrittskontrollsystems 1 erhält. Hierbei werden durch das Handgerät 4 nicht die Zutrittskontrolldaten in dem ersten Zutrittskontrollmodul 9 gespeichert sondern vielmehr nur beispielsweise eine Liste von gültigen Identifikationsdaten von ID-Gebern 8, die grundsätzlich berechtigt sind, einen Zutritt an dem ersten Zutrittskontrollmodul 9 zu erhalten. Ebenfalls kann jedem ersten Zutrittskontrollmodul 9 eine unverwechselbare Modulnummer zugeordnet werden, um damit eine eindeutige Zuordnung in dem Zutrittskontrollsystem 1 zu ermöglichen.

[0043] Der Datenaustausch zwischen dem Handgerät 4 und dem Zutrittskontrollsystem 1 kann per Datenleitung 5 oder drahtlos stattfinden. Ebenfalls kann der Datenaustausch (s. Pfeil 13) zwischen dem Handgerät 4 und dem ersten Zutrittskontrollmodul 9 drahtlos oder per Datenleitung 5 erfolgen. Nach der ersten Inbetriebnahme ist ein weiterer direkter Datenaustausch zwischen dem Zutrittskontrollsystem 1 und dem ersten Zutrittskontrollmodul 9 nicht mehr unbedingt erforderlich.

[0044] In Figur 3 ist die Vorbereitung eines ID-Gebers 8 dargestellt, siehe hierzu Schritte a) bis e). Hierbei werden zunächst die Identifikationsdaten aus dem ID-Geber 8 durch eine Lese- und Schreibeinheit 12 des Zutrittskontrollsystems 1 ausgelesen, siehe Schritt a). Diese Daten können dann an einen zentralen Computer 2 oder eine Kontrollzentrale 3 gesendet werden (s. Schritt b)), in der die Zutrittskontrolldaten für einen Benutzer erstellt werden (s. Schritt c)). Diese Zutrittskontrolldaten können z. B. enthalten, wo, wann, wie häufig ein Benutzer ein Zutrittskontrollmodul 9 passieren darf. Zusätzlich können die Zutrittskontrolldaten auch personenbezogene Daten, wie z. B. biometrische Daten enthalten. Diese Daten werden nun nach der Identifikation des ID-Gebers 8 von dem Zutrittskontrollsystem 1 auf den ID-Geber 8 geschrieben (s. Schritt e)), nach dem die Daten zuvor an die Lese-/Schreibeinheit 12 gesendet worden sind (s. Schritt d)). Nach dieser Vorbereitung kann der ID-Geber 8 an den Benutzer ausgehändigt werden, der somit nun an den gewünschten Stellen einen Zugang bei den entsprechenden Zutrittskontrollmodulen 9, 10, 11 erhält.

[0045] In der Figur 4 wird noch einmal der Unterschied in dem Verfahrensablauf bei der Identifikation beim ersten Zutrittskontrollmodul 9 und dem zweiten Zutrittskontrollmodul 10 deutlich. Beim zweiten Zutrittskontrollmodul 10 werden die Identifikationsdaten aus dem ID-Geber 8 ausgelesen und über Draht 5 an das Zutrittskontrollsystem 1 gesendet. Eine nicht dargestellte Kontrollzentrale 3 entscheidet dann, ob dem ID-Geber 8 an dem zweiten Zutrittskontrollmodul 10 der Zutritt gewährt wird. Sofern das Ergebnis positiv ist, weist die Kontrollzentrale 3 das Stellmodul 10.2 des zweiten Zutrittskontrollmoduls 10 an, den Zutritt freizugeben. Folglich sind sämtliche Zutrittskontrolldaten für den ID-Geber 8 bei dem zweiten Zutrittskontrollmodul 10 in der Kontrollzentrale 3 hinterlegt.

[0046] Im Gegensatz dazu werden bei dem ersten Zutrittskontrollmodul 9 nicht nur die Identifikationsdaten, sondern auch die Zutrittskontrolldaten durch das Lesemodul 9.1 ausgelesen (s. Schritt f)). Anhand dieser Zutrittskontrolldaten entscheidet das Logikmodul 9.3 über einen Zutritt, indem es die ausgelesenen Daten des ID-Gebers mit vorgegebenen Solldaten vergleicht (s. Schritt h)) und bei einem positiven Ergebnis das Stellmodul 9.2 ansteuert (s. Schritt j)), um den Zutritt zu dem Objekt freizugeben. Der erfolgreiche Zutritt oder der abgewiesene Zutritt (s. Schritt k)) zu diesem ersten Zutrittskontrollmodul 9 kann als Zustandsdaten über ein Schreibmodul 9.5 auf dem ID-Geber 8 gespeichert werden, siehe hierzu Schritt m)).

Bezugszeichenliste

[0047]

1	Zutrittskontrollsystem
2	Computer
3	Kontrollzentrale
4	Handgerät (PDA)
5	Datenleitungen / Verbindungen
6	Drahtlose Verbindungen
7	Traffic-Point / Verteilerpunkt
8	ID-Geber mit Identifizierungsdaten
9	erstes Zutrittskontrollmodul
9.1	Lesemodul
9.2	Stellmodul
9.3	Logikmodul
9.4	Zeitmodul
9.5	Schreibmodul
9.6	mechanisches Sicherheitselement
9.7	Sensorelement, insbesondere für biometrische Messdaten
9.8	Anzeigeelement
10	zweites Zutrittskontrollmodul
10.1	Lesemodul

10.2	Stellmodul
11	drittes Zutrittskontrollmodul
5 12	Lese-/Schreibeinheit
13	Pfeil für Datenrichtung

10 Patentansprüche

1. Zutrittskontrollsystem (1), mit zumindest einer Kontrollzentrale (3), einem ersten Zutrittskontrollmodul (9), welches wenigstens ein Lesemodul (9.1) und ein Stellmodul (9.2) aufweist, wobei das Lesemodul (9.1) dazu dient, Daten von einem ID-Geber (8) auszulesen, und das Stellmodul (9.2) einen Zutritt zu einem Objekt freigibt, falls die richtigen Daten vom ID-Geber (8) ausgelesen worden sind,
dadurch gekennzeichnet,
dass Identifikationsdaten sowie Zutrittskontrolldaten auf dem ID-Geber (8) gespeichert sind, die von dem Lesemodul (9.1) auslesbar sind, anhand dessen über den Zutritt zu dem Objekt und somit über eine Freigabe durch das Stellmodul (9.2) entschieden wird.
2. Zutrittskontrollsystem (1) nach Anspruch 1,
dadurch gekennzeichnet,
dass das Zutrittskontrollsystem (1) drahtlos mit dem ersten Zutrittskontrollmodul (9) verbindbar ist, um einen Datenaustausch zu ermöglichen, wobei insbesondere ein Datenaustausch zum Informationsabgleich nur auf Anforderung stattfindet.
3. Zutrittskontrollsystem (1) nach Anspruch 1 oder 2,
dadurch gekennzeichnet,
dass das erste Zutrittskontrollmodul (9) ein Logikmodul (9.3) aufweist, welches die von dem ID-Geber (8) gelesenen Daten mit vorgegebenen Solldaten vergleicht, und bei einem positiven Ergebnis das Stellmodul (9.2) entsprechend ansteuert, um den Zutritt zu dem Objekt freizugeben.
4. Zutrittskontrollsystem (1) nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet,
dass das erste Zutrittskontrollmodul (9) ein Zeitmodul (9.4) enthält, welches konkrete Zeitdaten liefert, die zum Vergleich mit den ausgelesenen Zugangskontrolldaten vom ID-Geber (8) dienen.
5. Zutrittskontrollsystem (1) nach Anspruch 4,
dadurch gekennzeichnet,
dass das Logikmodul (9.3) zusätzlich die Zeitdaten vom Zeitmodul (9.4) erhält, wobei es die Solldaten und die Zeitdaten mit den von dem ID-Geber (8) gelesenen Daten vergleicht und bei einem positiven

Ergebnis das Stellmodul (9.2) entsprechend ansteuert, um den Zutritt zu dem Objekt freizugeben.

6. Zutrittskontrollsystem (1) nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet,
dass das erste Zutrittskontrollmodul (9) auch ein Schreibmodul (9.5) enthält, um damit Zustandsdaten auf dem ID-Geber (8) zu speichern. 5
7. Zutrittskontrollsystem (1) nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet,
dass der ID-Geber (8) mit einem mechanischen Sicherheitselement (9.6) gekoppelt ist. 10
8. Zutrittskontrollsystem (1) nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet,
dass die Identifikationsdaten des ID-Gebers (8) unterschiedlich zu den Zutrittskontrolldaten gespeichert sind, wobei insbesondere die Identifikationsdaten unveränderbar und die Zutrittskontrolldaten veränderbar im ID-Geber (8) vorgesehen sind. 15
9. Zutrittskontrollsystem (1) nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet,
dass die Daten des ID-Gebers (8) verschlüsselt gespeichert sind, wobei insbesondere eine Entschlüsselung der Daten von dem Logikmodul (9.3) des ersten Zutrittskontrollmoduls (9) vorgenommen wird. 20
10. Zutrittskontrollsystem (1) nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet,
dass die Zutrittskontrolldaten Zutrittsregeln aufweisen, wobei insbesondere die Zutrittsregeln auch wenigstens eine Gültigkeitsdauer beinhalten. 25
11. Zutrittskontrollsystem (1) nach einem der vorhergehenden Ansprüche und nach Anspruch 3,
dadurch gekennzeichnet,
dass die Zutrittskontrolldaten zusätzliche Personendaten, wie z. B. biometrische Daten enthalten, wobei ein zusätzliches Sensorelement (9.7) vorgesehen ist, welches die entsprechenden Personendaten von einem Besitzer des ID-Gebers (8) automatisch erfasst und an das Logikmodul (9.3) des ersten Zutrittskontrollmoduls (9) liefert. 30
12. Zutrittskontrollsystem (1) nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet,
dass das erste Zutrittskontrollmodul (9) ein mechanisches Sicherheitselement (9.6) enthält. 35
13. Zutrittskontrollsystem (1) nach einem der vorhergeh-

henden Ansprüche,

- dadurch gekennzeichnet,**
dass für eine nachfolgende Verwendung des ID-Gebers (8) eine Vorbereitung erforderlich ist, in dem zumindest die individuellen Zutrittskontrolldaten für einen Besitzer des ID-Gebers (8) auf dem ID-Geber (8) gespeichert werden. 40
14. Zutrittskontrollsystem (1) nach Anspruch 13,
dadurch gekennzeichnet,
dass die Kontrollzentrale (3) zur Vorbereitung eines ID-Gebers (8) dient, in dem die individuellen Zutrittskontrolldaten erstellt werden und mittels einer Lese-/Schreibeinheit (12), die mit der Kontrollzentrale (3) verbunden ist, auf dem ID-Geber (8) gespeichert werden. 45
15. Zutrittskontrollsystem (1) nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet,
dass der ID-Geber (8) einen Transponder aufweist, mit dem Energie, insbesondere drahtlos, von dem ID-Geber (8) auf zumindest das erste Zutrittskontrollmodul (9) übertragbar ist. 50
16. Zutrittskontrollsystem (1) nach einem der vorhergehenden Ansprüche und nach Anspruch 3, 4 und/oder 6,
dadurch gekennzeichnet,
dass das erste Zutrittskontrollmodul wenigstens mit dem Lese- und/oder Schreibmodul (9.1, 9.5), dem Logik- und/oder Zeitmodul (9.3, 9.4) und dem Stellmodul (9.2) eine bauliche Einheit bildet, wobei insbesondere das erste Zutrittskontrollmodul (9) in einem Türbeschlag integriert ist. 55
17. Zutrittskontrollsystem (1) nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet,
dass das Stellmodul (9.2) ein ansteuerbares, elektromechanisches Sperrglied aufweist, womit der Zutritt zu dem Objekt versperrt oder freigegeben werden kann, wobei das Stellmodul (9.2) insbesondere an einer Tür, einer Schranke, einer Klappe, einem Tresor oder dergleichen vorgesehen ist.
18. Zutrittskontrollsystem (1) nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet,
dass die Daten des ID-Gebers (8) magnetisch, optisch, kontaktlos, drahtlos oder durch eine elektrische Verbindung von dem Lesemodul (9.1) auslesbar sind.
19. Zutrittskontrollsystem (1) nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet,
dass das Zutrittskontrollsystem (1) mit zumindest

- einem zweiten Zutrittskontrollmodul (10) über eine Datenleitung (5) verbunden ist, um einen Datenaustausch zu ermöglichen, wobei insbesondere ein Informationsabgleich permanent oder nur auf Anforderung stattfindet. 5
20. Zutrittskontrollsystem (1) nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet,
dass das Zutrittskontrollsystem (1) mit zumindest einem dritten Zutrittskontrollmodul (11) drahtlos verbunden ist, um einen Datenaustausch zu ermöglichen, wobei die Zutrittskontrolldaten für einen ID-Geber (8) in dem dritten Zutrittskontrollmodul (11) gespeichert sind, und wobei insbesondere ein Informationsabgleich zwischen dem Zutrittskontrollsystem (1) und dem dritten Zutrittskontrollmodul (11) permanent oder nur auf Anforderung stattfindet. 10 15
21. Zutrittskontrollsystem (1) nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet,
dass das Zutrittskontrollsystem (1) in ein Zeiterfassungssystem und/oder ein Zeitwirtschaftssystem integriert oder eingebunden ist. 20 25
22. Verfahren zum Betrieb eines Zutrittskontrollsystems (1), insbesondere nach einem der vorhergehenden Ansprüche, mit zumindest einer Kontrollzentrale (3), einem ersten Zutrittskontrollmodul (9), welches wenigstens ein Lesemodul (9.1) und ein Stellmodul (9.2) aufweist, wobei das Lesemodul (9.1) dazu dient, Daten von einem ID-Geber (8) auszulesen, und das Stellmodul (9.2) einen Zutritt zu einem Objekt freigibt, falls die richtigen Daten vom ID-Geber (8) ausgelesen worden sind, 30 35
dadurch gekennzeichnet,
dass die folgenden Schritte zur Vorbereitung des ID-Gebers (8) ablaufen: 40
- a) Lesen von Identifikationsdaten des ID-Gebers (8) durch eine Lese-/Schreibeinheit (12)
 - b) Weiterleiten der gelesenen Identifikationsdaten an eine Kontrollzentrale (3)
 - c) Erstellen von individuellen Zutrittskontrolldaten, insbesondere mit wenigstens einer Zutrittsregel und einer Gültigkeitsdauer, für einen durch den ID-Geber (8) identifizierbaren Besitzer 45
 - d) Weiterleiten der erstellten Zutrittskontrolldaten an die Lese-/ Schreibeinheit (12) 50
 - e) Schreiben der Zutrittskontrolldaten auf den ID-Geber (8).
23. Verfahren zum Betrieb eines Zutrittskontrollsystems (1) nach Anspruch 22,
dadurch gekennzeichnet,
dass nach der Vorbereitung des ID-Gebers (8) die nachfolgenden Schritte zu Identifikation und Freigabe 55
- be an einem ersten Zutrittskontrollmodul (9) ablaufen:
- f) Lesen der Identifikationsdaten sowie der Zutrittskontrolldaten des ID-Gebers (8) durch das Lesemodul (9.1)
 - g) Weiterleiten der gelesenen Daten an das Logikmodul (9.3)
 - h) Vergleich der gelesenen Daten mit vorgegebenen Solldaten des Logikmoduls (9.3)
 - i) Ermitteln eines positiven oder negativen Ergebnisses durch den Datenvergleich
 - j) bei einem positiven Ergebnis, Ansteuerung des Stellmoduls zur Freigabe des Objektes
 - k) bei einem negativen Ergebnis, ggf. Aussenden eines Warnhinweises an die Kontrollzentrale (3).
24. Verfahren zum Betrieb eines Zutrittskontrollsystems (1) nach Anspruch 22 oder 23,
dadurch gekennzeichnet,
dass Schritt l) eine erste Inbetriebnahme des ersten Zutrittskontrollmoduls (9) durch Speichern von Konfigurationsdaten im Zutrittskontrollmodul (9) vorgenommen wird, wobei insbesondere die Konfigurationsdaten drahtlos oder per Datenleitung (5) übertragbar sind.
25. Verfahren zum Betrieb eines Zutrittskontrollsystems (1) nach einem der Ansprüche 22 bis 24,
dadurch gekennzeichnet,
dass bei einem positiven und/oder negativen Ergebnis die speziellen Zutrittsinformationen des ersten Zutrittskontrollmoduls (9) auf dem ID-Geber (8) gespeichert werden.
26. Verfahren zum Betrieb eines Zutrittskontrollsystems (1) nach einem der Ansprüche 22 bis 25,
dadurch gekennzeichnet,
dass in einem Schritt m) nach dem Lesen der Identifikationsdaten sowie der Zutrittskontrolldaten des ID-Gebers (8) Zustandsdaten des ersten Zutrittskontrollmoduls (9), wie insbesondere Anzahl der Lese-, Freigabe-, Sperrvorgänge, Energiezustand eines Energiespeichers etc., auf dem ID-Geber (8) gespeichert werden.
27. Verfahren zum Betrieb eines Zutrittskontrollsystems (1) nach einem der Ansprüche 22 bis 26,
dadurch gekennzeichnet,
dass auf dem ID-Geber (8) Personendaten von einem Besitzer, insbesondere biometrische Daten, gespeichert sind, die insbesondere durch ein zusätzliches Sensorelement (9.7) von dem Besitzer erfasst werden und an das Logikmodul (9.3) weitergeleitet werden.

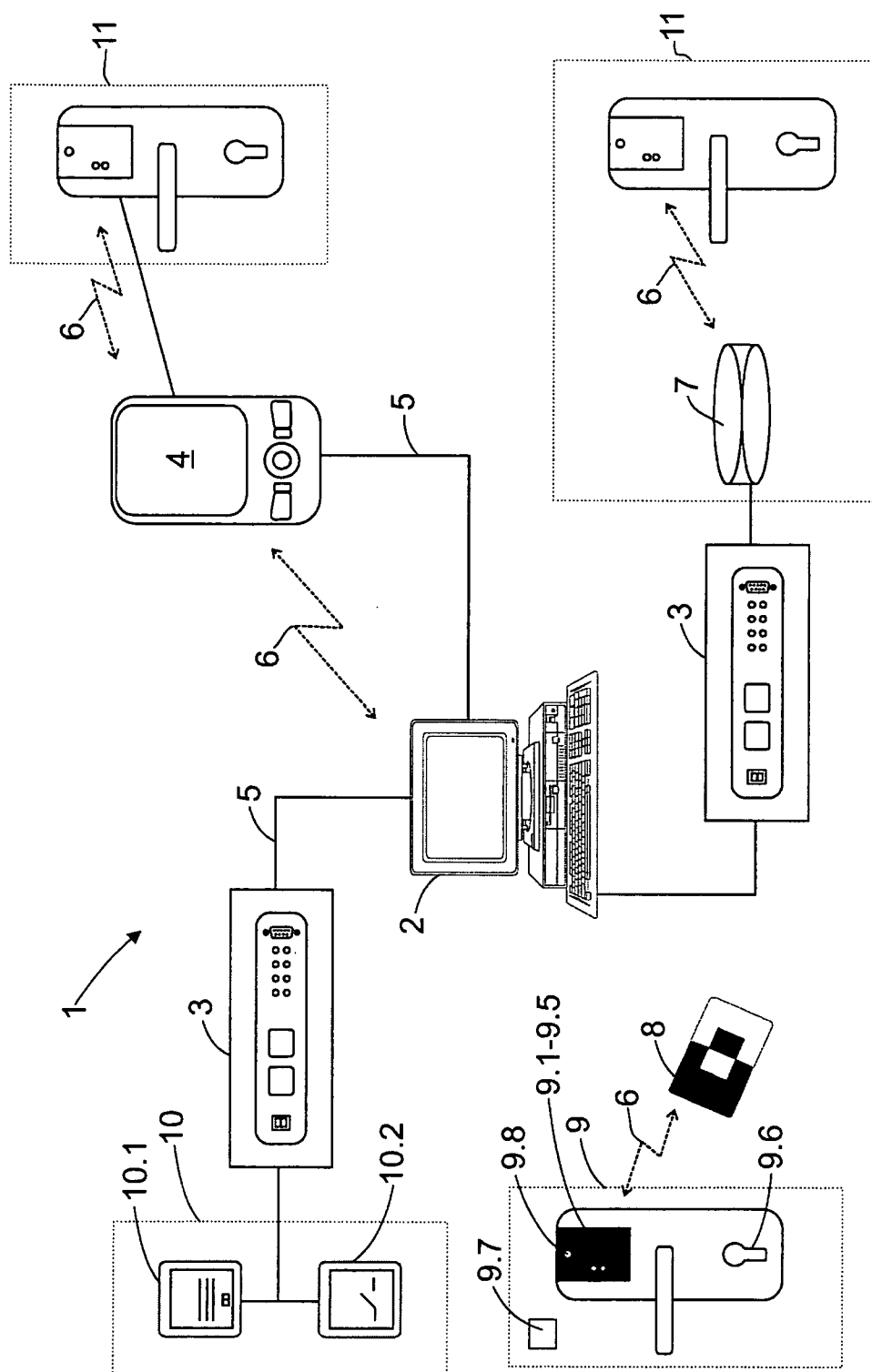


Fig. 1

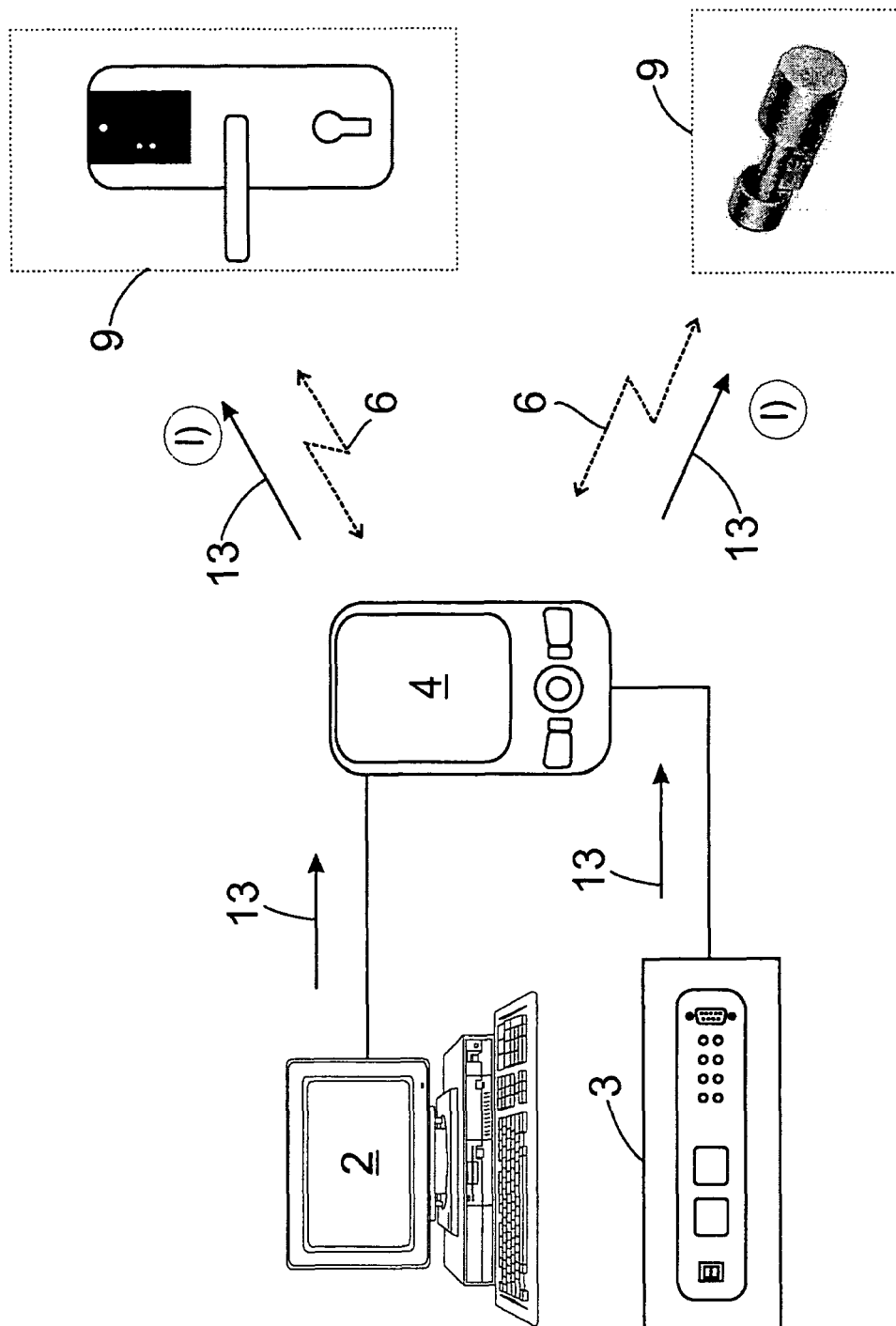


Fig. 2

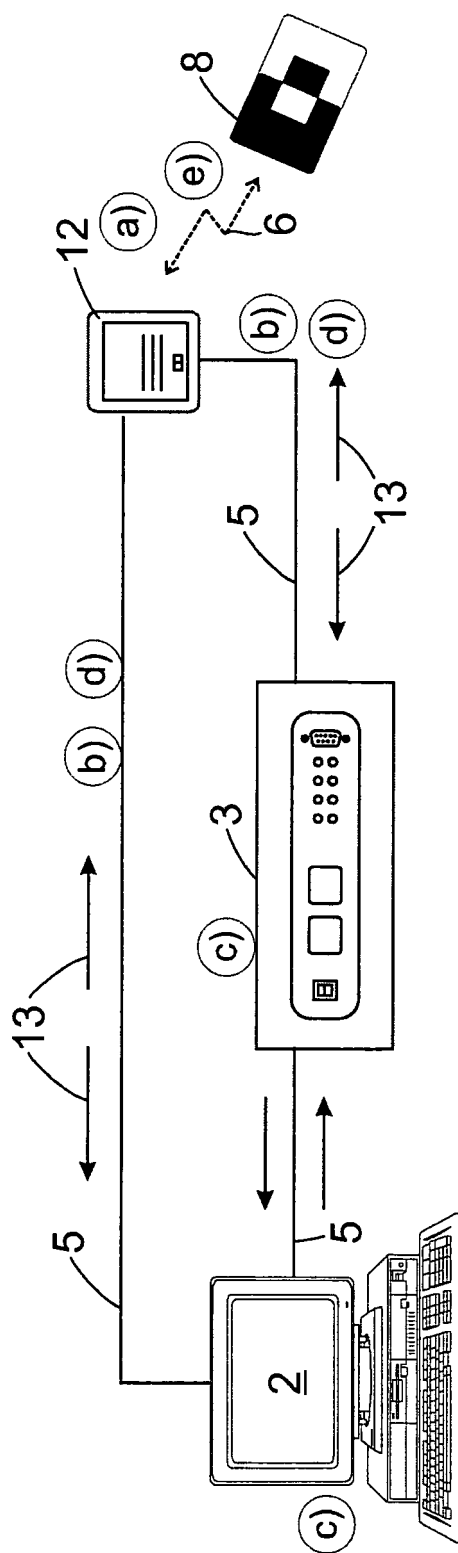


Fig. 3

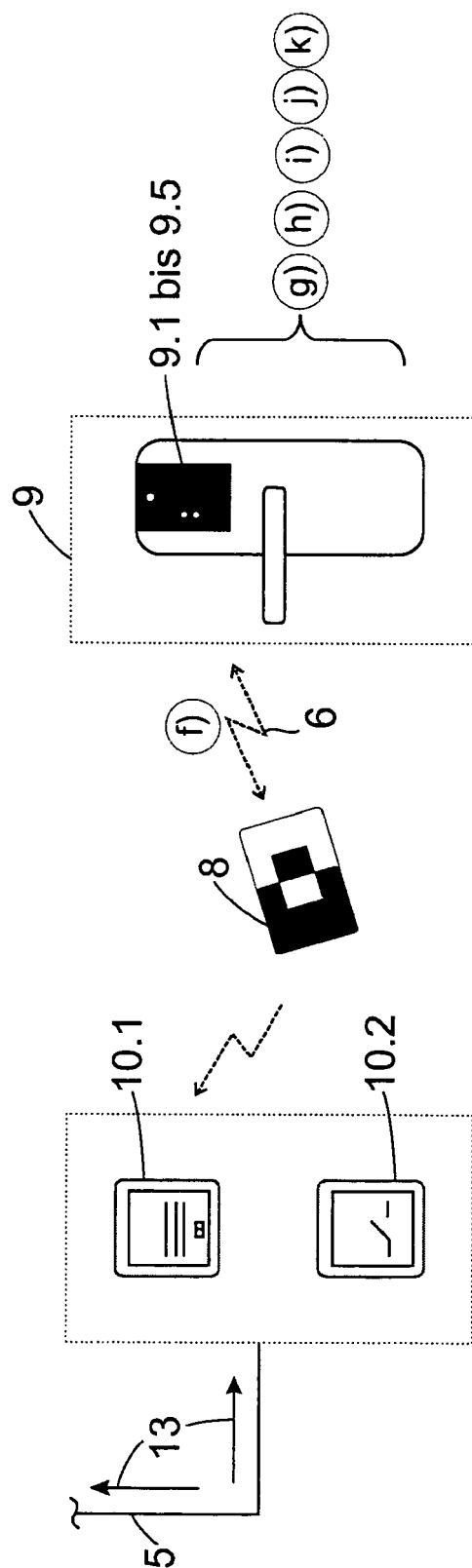


Fig. 4

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 10246664 A1 [0004]
- WO 2006056085 A1 [0005]