(19) österreichisches patentamt

(10) **AT 513461 B1 2014-08-15**

(12) **Patentschrift**

(21) Anmeldenummer: A 523/2013
(22) Anmeldetag: 25.06.2013
(45) Veröffentlicht am: 15.08.2014

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

(56) Entgegenhaltungen:
EP 1752928 A1
US 2011257817 A1
DE 102011011697 A1

(73) Patentinhaber:
EVVA SICHERHEITSTECHNOLOGIE GMBH
1120 WIEN (AT)

(74) Vertreter:
Haffner und Keschmann Patentanwälte GmbH
Wien

(54) **Verfahren zur Zutrittskontrolle**

(57) Bei einem Verfahren zur Zutrittskontrolle insbesondere in Gebäuden (2), bei dem eine bidirektionale Datenübermittlung zwischen einem Zutrittsrechtsdaten speichernden elektronischen Identifikationsmedium (6) und einer Zutrittskontrollvorrichtung (9) stattfindet und in der Zutrittskontrollvorrichtung (9) eine Zutrittsberechtigungsprüfung vorgenommen wird, wobei in Abhängigkeit von der festgestellten Zutrittsberechtigung ein Sperrmittel zum wahlweisen Freigeben oder Sperren des Zutritts angesteuert wird, wobei Zutrittsrechtsdaten in einer zentralen Recheneinheit (1) gespeichert und verwaltet werden und das Identifikationsmedium (6) mit Zutrittsrechtsdaten programmiert wird, wobei die Programmierung des Identifikationsmediums (6) das Senden der Zutrittsrechtsdaten über ein drahtloses Telekommunikationsnetz (4) an ein drahtloses mobiles Telekommunikationsgerät (5) und das Übermitteln der vom mobilen Telekommunikationsgerät (5) empfangenen Zutrittsrechtsdaten an einen Speicher (10) des Identifikationsmediums (6) umfasst, erfolgt die Übermittlung der Zutrittsrechtsdaten vom Telekommunikationsgerät (5) an das Identifikationsmedium (6) drahtlos über Kurzreichweitenfunk und die Zutrittsrechtsdaten werden in einem elektronischen Sicherheitshardwaremodul (10) des Identifikationsmediums (6) gespeichert.

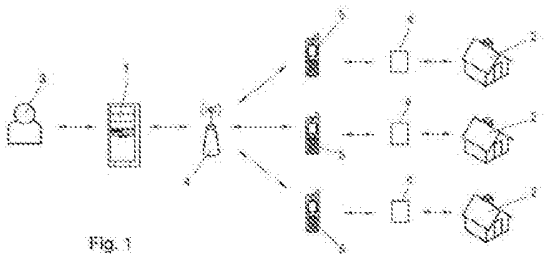

Fig. 1

AT 513461 B1 2014-08-15

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zur Zutrittskontrolle insbesondere in Gebäuden, bei dem eine bidirektionale Datenübermittlung zwischen einem Zutrittsrechtsdaten speichernden elektronischen Identifikationsmedium und einer Zutrittskontrollvorrichtung stattfindet und in der Zutrittskontrollvorrichtung eine Zutrittsberechtigungsprüfung vorgenommen wird, wobei in Abhängigkeit von der festgestellten Zutrittsberechtigung ein Sperrmittel zum wahlweisen Freigeben oder Sperren des Zutritts angesteuert wird, wobei Zutrittsrechtsdaten in einer zentralen Recheneinheit gespeichert und verwaltet werden und das Identifikationsmedium mit Zutrittsrechtsdaten programmiert wird, wobei die Programmierung des Identifikationsmediums das Senden der Zutrittsrechtsdaten über ein drahtloses Telekommunikationsnetz an ein drahtloses mobiles Telekommunikationsgerät und das Übermitteln der vom mobilen Telekommunikationsgerät empfangenen Zutrittsrechtsdaten an einen Speicher des Identifikationsmediums umfasst.

[0002] Die Erfindung betrifft weiters ein Identifikationsmedium zur Verwendung in einem solchen Verfahren.

[0003] Ein Verfahren der eingangs genannten Art ist in der WO 2009/094683 A1 beschrieben. Bei dem dort beschriebenen Verfahren erfolgt die Programmierung der elektronischen Identifikationsmedien mit Zutrittsrechtsdaten über ein drahtloses Telekommunikationsnetz, sodass die Zutrittsrechtsdaten von der zentralen Recheneinheit an ein drahtloses mobiles Telekommunikationsgerät des jeweils gewünschten Benutzers bzw. Schlüsselinhabers gesendet werden. Die vom mobilen Telekommunikationsgerät empfangenen Zutrittsrechtsdaten können einem geeigneten Identifikationsmedium zur Verfügung gestellt werden, welches auf diese Art und Weise eine Schlüsselfunktion erhält. Dadurch wird eine Art „online-Schlüssel" geschaffen, da das Identifikationsmedium über das mobile Telekommunikationsnetz und das entsprechende mobile Endgerät umprogrammiert werden kann, um auf diese Art und Weise die Zutrittsrechtsdaten und damit die Zutrittsberechtigung des Schlüsselinhabers zu ändern.

[0004] Auf Grund der Möglichkeit der entfernten Programmierung von Identifikationsmedien ist es zur Änderung der Zutrittsberechtigungen nicht mehr notwendig, einen Zugriff direkt auf die einzelnen Schließeinheiten bzw. Zutrittskontrollvorrichtungen zu erhalten. Die Zutrittskontrollvorrichtungen können nach der Installation und Initialisierung als autonome Einheiten arbeiten und erfordern insbesondere keine Netzwerkanbindung. Dies ist von besonderem Vorteil, wenn auf Grund der örtlichen Gegebenheiten eine Vernetzung von Schließeinheiten nicht gewünscht ist, beispielsweise, wenn bei kleineren Schließanlagen der Vernetzungsaufwand zu kostenintensiv wäre oder wenn bauliche Eingriffe in der Türe und im Bereich der Türe nicht erwünscht sind.

[0005] Das Dokument EP 1752928 A1 offenbart ein Verfahren zur Zutrittskontrolle, wobei die Zugangscodes für die Schließsysteme von Türen von einer zentralen Rechnereinheit generiert, an ein 1. Mobiltelefon übertragen, dort gegebenenfalls bearbeitet (mit Attributen belegt) und an ein 2. Mobiltelefon mittels NFC-Kommunikation weiterübertragen werden.

[0006] Das Dokument US 2011/0257817 A1 offenbart ein Verfahren zur Zutrittskontrolle, wobei ein tragbares, dem Besitzer zugeordnetes Gerät wie ein Mobiltelefon mit dem Funköffner eines Autos zusammenarbeitet, um u.a. auch die Türschließsysteme des Fahrzeuges anzusteuern.

[0007] Das Dokument DE 102011011697 A1 offenbart ein Verfahren zur Zutrittskontrolle, wobei die Berechtigungsdaten für den Zugang zu einem Fahrzeug zwischen einem Mobiltelefon und einer weiteren mobilen Einheit wie einer Chipkarte drahtlos über NFC-Schnittstellen übertragen werden.

[0008] Wie in der WO 2009/094683 A1 beschrieben, werden die Zutrittsrechtsdaten nach der Übermittlung an das mobile Telekommunikationsgerät unter Verwendung einer gesonderten Schreib-/Leseeinrichtung auf das externe, von dem Telekommunikationsgerät gesonderte Identifikationsmedium geschrieben. Dies erfordert naturgemäß einen zusätzlichen Schreibvorgang und eine entsprechende Schreibeinrichtung, was einen hohen Handhabungsaufwand mit sich bringt. Ein weiteres Problem der genannten Identifikationsmedien ist die Gefahr eines unbe-

rechtigten Auslesens der gespeicherten Zutrittsrechtsdaten, z.B. mittels einer kontaktbehafteten Leseeinrichtung für Chipkarten od. dgl.

[0009] Die vorliegende Erfindung zielt daher darauf ab, die oben genannten Nachteile zu vermeiden.

[0010] Zu Lösung dieser Aufgabe sieht die Erfindung bei einem Verfahren der oben genannten Art im Wesentlichen vor, dass die Übermittlung der Zutrittsrechtsdaten vom Telekommunikationsgerät an das Identifikationsmedium drahtlos über Kurzreichweitenfunk erfolgt und die Zutrittsrechtsdaten in einem elektronischen Sicherheitshardwaremodul des Identifikationsmediums gespeichert werden.

[0011] Dadurch, dass die Zutrittsrechtsdaten vom Telekommunikationsgerät drahtlos und über Kurzreichweitenfunk an das Identifikationsmedium übermittelt werden, können die mit kontaktbehafteten Schreib- bzw. Leseeinrichtungen verbundenen Sicherheitsrisiken vermieden werden. Gleichzeitig wird durch die Verwendung von Kurzreichweitenfunk sichergestellt, dass die Übertragung der sensiblen Zutrittsrechtsdaten nur zu einem sich in unmittelbarer Nähe befindlichen Identifikationsmedium erfolgt. Unter Kurzreichweitenfunk wird hierbei ein drahtloses Datenübertragungsverfahren verstanden, bei dem Signale mit Hilfe elektromagnetischer Wellen übertragen werden. Die maximale Reichweite beträgt bevorzugt 10m, besonders bevorzugt 5m. Zur Erhöhung der Sicherheit kann die Datenübermittlung zwischen dem Telekommunikationsgerät und dem Identifikationsmedium durch kryptographische Authentifizierungsverfahren und/oder durch Verschlüsselungsverfahren gesichert werden.

[0012] Schließlich wird durch die drahtlose Datenübermittlung die Handhabung wesentlich vereinfacht. Die Datenübertragung kann dabei insbesondere automatisch erfolgen, sobald das Telekommunikationsgerät aktualisierte Zutrittsrechtsdaten von der zentralen Recheneinheit erhalten hat. Damit erübrigt sich eine Benutzeraktion vollständig. Der Benutzer muss lediglich ein empfangsbereites Telekommunikationsgerät bei sich tragen und das Identifikationsmedium in der Nähe des Telekommunikationsgeräts, beispielsweise in einer Hosentasche oder einer Handtasche, mitführen, wobei die kommunikationsmäßige Kopplung des Identifikationsmediums mit dem Telekommunikationsgerät bevorzugt selbsttätig erfolgt.

[0013] Die Verwendung des externen Identifikationsmediums an Stelle des Telekommunikationsgeräts als mit der Zutrittskontrollvorrichtung kommunizierendem Träger der Zutrittsrechtsdaten bringt den Vorteil mit sich, dass die für die Zutrittsberechtigungsprüfung erforderliche Datenkommunikation zwischen dem Identifikationsmedium und der Zutrittskontrollvorrichtung über Kommunikationsschnittstellen bzw. -protokolle erfolgen kann, mit welchen übliche Telekommunikationsgeräte, wie z.B. Mobiltelefone, nicht ausgestattet bzw. kompatibel sind. Weiters bietet diese Ausgestaltung den Vorteil, dass Zutrittsrechtsdaten in einem elektronischen Sicherheitshardwaremodul des Identifikationsmediums gespeichert werden können, was bei Telekommunikationsgeräten nicht ohne weiteres möglich ist.

[0014] Das im Rahmen der Erfindung zum Einsatz gelangende Sicherheitshardwaremodul wird in der Fachwelt auch als „Secure Element" bezeichnet, und zeichnet sich dadurch aus, dass der Zugriff auf das Sicherheitshardwaremodul und auf die darin gespeicherten Zutrittsrechtsdaten durch kryptographische Methoden abgesichert ist. Ein Secure Element ist ein vertrauenswürdiges und sicheres Hardwaremodul, das als sicherer Speicher für sicherheitskritische Daten, für kryptographische Operationen und als sichere Umgebung zur Ausführung von Programmcode verwendet werden kann. Meist werden Secure Elements von einem eigenen integrierten Schaltkreis gebildet, sodass eine hardwaremäßige Trennung von anderen, weniger abgesicherten Komponenten sichergestellt ist.

[0015] Das Sicherheitshardwaremodul (Secure Element) kann bevorzugt in das für den Datenaustausch mit der Zutrittskontrollvorrichtung vorgesehene Kommunikationsmodul integriert werden. Die Erfindung ist in diesem Zusammenhang derart weitergebildet, dass die für die Zutrittsberechtigungsprüfung erforderliche Datenkommunikation zwischen dem Identifikationsmedium und der Zutrittskontrollvorrichtung über eine dem Sicherheitshardwaremodul zugeord-

nete erste Sende-/Empfangseinheit des Identifikationsmediums erfolgt, wobei die Datenkommunikation mittels Nahfeldkommunikation, insbesondere nach dem RFID- bzw. NFC-Standard vorgenommen wird. Dadurch, dass die Datenkommunikation bevorzugt nach dem RFID- bzw. NFC-Standard vorgenommen wird, kann auf bewährte Verfahren und Bauteile zurückgegriffen werden. Insbesondere können wegen der Verwendung eines von dem Telekommunikationsgerät gesonderten Identifikationsmediums Kommunikationsschnittstellen, insbesondere RFID und NFC, zum Einsatz gelangen, die bei Telekommunikationsgeräten, wie z.B. Mobiltelefonen üblicherweise weniger verbreitet sind.

[0016] Die Verwendung des RFID oder NFC-Standards ermöglicht eine passive Betriebsweise der ersten Sende-/Empfangseinheit des Identifikationsmediums, sodass eine Abfrage der Zutrittsberechtigung auch ohne Stromversorgung oder bei Ausfall der Stromversorgung des Identifikationsmediums gewährleistet ist. Eine bevorzugte Ausbildung sieht in diesem Zusammenhang vor, dass die Energieversorgung der ersten Sende-/Empfangseinheit des Identifikationsmediums über ein elektromagnetisches, bevorzugt im Wesentlichen magnetisches Wechselfeld der Zutrittskontrollvorrichtung erfolgt.

[0017] Um die Gefahr eines unberechtigten Auslesens oder Abhörens von sensiblen Daten zu verringern, kann bevorzugt vorgesehen sein, dass das Identifikationsmedium in dem Sicherheitshardwaremodul wenigstens ein digitales Zertifikat gespeichert hat, um eine Authentifizierung des elektronischen Identifikationsmediums in der Zutrittskontrollvorrichtung zu ermöglichen. Die Datenübermittlung zwischen dem Identifikationsmedium und der Zutrittskontrollvorrichtung umfasst bevorzugt die Verwendung eines Schlüsselaustausch- oder -ableitungsprotokolls, wodurch dem elektronischen Identifikationsmedium und der Zutrittskontrollvorrichtung wenigstens ein geheimer, gemeinsamer Sitzungsschlüssel zugänglich gemacht wird, worauf der wenigstens eine Sitzungsschlüssel zum Einrichten eines sicheren Übertragungskanals zwischen dem elektronischen Identifikationsmedium und der Zutrittskontrollvorrichtung verwendet wird, und wobei die Zutrittsrechtsdaten über den sicheren Kanal vom elektronischen Identifikationsmedium an die Zutrittskontrollvorrichtung übermittelt werden. Bevorzugt werden die für das Schlüsselaustausch- oder -ableitungsprotokoll im Identifikationsmedium erforderlichen Operationen im Sicherheitshardwaremodul durchgeführt.

[0018] Das wenigstens eine digitale Zertifikat kann hierbei bevorzugt von der zentralen Recheneinheit signiert werden.

[0019] Bevorzugt wird der wenigstens eine Sitzungsschlüssel im Sicherheitshardwaremodul und in der Zutrittskontrollvorrichtung auf Grundlage eines zutrittskontrollvorrichtungsindividuellen Zutrittscodes erzeugt, bevorzugt weiters auf Grundlage einer vom Identifikationsmedium und einer von der Zutrittskontrollvorrichtung erzeugten Zufallszahl und/oder von einer vom Identifikationsmedium und einer von der Zutrittskontrollvorrichtung erzeugten Laufnummer.

[0020] Bevorzugt umfasst das Schlüsselaustausch- oder -ableitungsprotokoll die Generierung eines Kryptogramms unter Verwendung des Sitzungsschlüssels in der Zutrittskontrollvorrichtung und die Übersendung desselben an das Identifikationsmediums, wobei das Kryptogramm im Sicherheitshardwaremodul unter Verwendung des Sitzungsschlüssels verifiziert wird.

[0021] Eine weitere bevorzugte Verfahrensweise sieht vor, dass die Übermittlung der Zutrittsrechtsdaten vom Telekommunikationsgerät an das Identifikationsmedium über eine zweite Sende-/Empfangseinheit des Identifikationsmediums erfolgt, insbesondere über eine Bluetooth-Verbindung. Die Kommunikation des Identifikationsmediums mit der Zutrittskontrollvorrichtung und jene mit dem Telekommunikationsgerät erfolgt somit über unterschiedliche Sende-/Empfangseinheiten, die bevorzugt nach voneinander verschiedenen Übertragungsprotokollen arbeiten. Besonders bevorzugt ist im Falle der zweiten Sende-/Empfangseinheit die Verwendung des Bluetooth- Standard. Insbesondere ist der Bluetooth-Standard 4.0 LE von Vorteil, da dieser einen überaus niedrigen Stromverbrauch aufweist.

[0022] Die zwei Sende-/Empfangseinheiten sind bevorzugt als voneinander gesonderte Hardwareeinheiten ausgebildet.

[0023] Die Kommunikation zwischen dem mobilen Telekommunikationsgerät und dem Identifikationsmedium, um die Zutrittsrechtsdaten des Identifikationsmediums zu aktualisieren, wird beispielsweise durch den Benutzer ausgelöst, indem dieser einen entsprechenden Betätigungsknopf drückt. Dies ermöglicht aber einen Missbrauch dahingehend, dass ein Benutzer bewusst keine Aktualisierung vornimmt, um eine in der zentralen Recheneinheit bereits gelöschte oder geänderte Zutrittsberechtigung weiterzunutzen. Bevorzugt ist daher vorgesehen, dass die Kommunikation zwischen dem mobilen Telekommunikationsgerät und dem Identifikationsmedium in regelmäßigen, voreingestellten Zeitabständen erfolgt.

[0024] Um Missbrauchsmöglichkeiten weiter zu verringern, kann in diesem Zusammenhang bevorzugt vorgesehen sein, dass das Identifikationsmedium in einen Außerbetriebs- oder Sperrmodus wechselt, wenn der Zeitabstand zur letzten Kommunikation zwischen dem mobilen Telekommunikationsgerät und dem Identifikationsmedium einen vorgegebenen Grenzwert überschreitet. Ein solcher Fall kann beispielsweise eintreten, wenn das Identifikationsmedium verloren geht oder entwendet wird. Das Identifikationsmedium befindet sich in einem solchen Fall nicht mehr in der für die Kommunikation mit dem Telekommunikationsgerät erforderlichen Nähe des Telekommunikationsgeräts, sodass ein Verbindungsaufbau mit dem zugehörigen Telekommunikationsgerät nicht gelingt.

[0025] Bevorzugt sind das Telekommunikationsgerät und das Identifikationsmedium elektronisch (z.B. mit Bluetooth) so miteinander gekoppelt, dass eine Datenverbindung nur zwischen den gekoppelten Einheiten möglich ist. Ein entwendetes Identifikationsmedium kann daher nicht mit einem fremden Telekommunikationsgerät gekoppelt werden.

[0026] Grundsätzlich ist die vorliegende Erfindung nicht auf eine bestimmte Ausbildung des Telekommunikationsgeräts beschränkt. Das Telekommunikationsgerät muss lediglich in der Lage sein, eine Datenkommunikation einerseits mit der zentralen Recheneinheit und andererseits mit dem Identifikationsmedium durchzuführen. Das Telekommunikationsgerät weist daher bevorzugt zwei voneinander verschiedene Datenübertragungsschnittstellen auf. Die eine Datenübertragungsschnittstelle ist zum Zwecke der Kommunikation mit der zentralen Recheneinheit bevorzugt für die Kommunikation über ein Telekommunikationsnetzwerk ausgebildet. Die andere Datenübertragungsschnittstelle ist zum Zwecke der Kommunikation mit dem Identifikationsmedium über Kurzreichweitenfunk, z.B. Bluetooth, ausgebildet. Bevorzugt handelt es sich bei dem Telekommunikationsgerät um ein Mobiltelefon, insbesondere ein GSM/UMTS- Mobiltelefon, oder um einen insbesondere tragbaren Personal Computer. Das Telekommunikationsgerät kann aber auch als stationäre Einrichtung ausgebildet sein, z.B. als Bluetooth-Knoten, der die über das Telekommunikationsnetzwerk erhaltenen Daten in das Bluetooth-Protokoll umsetzt.

[0027] Die Datenübermittlung zwischen der zentralen Recheneinheit und dem Telekommunikationsgerät kann über ein mobiles Telekommunikationsnetz, wie z.B. ein GSM, GPRS, UMTS und/oder LTE-Netz, oder über eine drahtlose Internetverbindung, wie z.B. WLAN oder dgl. erfolgen.

[0028] Das Telekommunikationsgerät kann die Funktion einer Relay- oder Proxy-Einheit zwischen der zentralen Recheneinheit und dem Identifikationsmedium übernehmen. In diesem Fall werden die Zutrittsrechtsdaten nicht in dem Telekommunikationsgerät zwischengespeichert, sondern es wird eine End-to-end-Datenverbindung zwischen der zentralen Recheneinheit und dem Identifikationsmedium hergestellt, sodass die Daten lediglich durch das Telekommunikationsgerät durchgeleitet werden. In dem Telekommunikationsgerät erfolgt dann lediglich eine Umsetzung der Daten von dem für die Verbindung zwischen der zentralen Recheneinheit und dem Telekommunikationsgerät verwendeten Übertragungsprotokoll auf das für die Verbindung zwischen dem Telekommunikationsgerät und dem Identifikationsmedium verwendete Übertragungsprotokoll.

[0029] Unter einem Sperrmittel ist im Rahmen der Erfindung z.B. ein mechanisch wirkendes Sperrelement, das zwischen einer Sperr- und einer Freigabestellung bewegt werden kann, ein mechanisches oder magnetisches Kupplungselement, das ein Betätigungselement, wie z.B.

eine Handhabe, mit einem Sperrglied koppelt oder entkoppelt, oder ein elektrisch sperr- und/oder freigebbares Sperrelement, wie z.B. ein elektrischer Türöffner, zu verstehen.

[0030] Zur Lösung der der Erfindung zugrunde liegenden Aufgabe ist gemäß einem weiteren Aspekt der Erfindung ein elektronisches Identifikationsmedium für Zutrittskontrollvorrichtungen vorgesehen, umfassend eine erste Sende-/Empfangseinheit für die Datenkommunikation zwischen dem Identifikationsmedium und der Zutrittskontrollvorrichtung und eine zweite Sende-/Empfangseinheit für die drahtlose Übermittlung von Zutrittsrechtsdaten von einem Telekommunikationsgerät an das Identifikationsmedium mittels Kurzreichweitenfunk, wobei der ersten Sende-/Empfangseinheit ein elektronisches Sicherheitshardwaremodul zum Speichern der Zutrittsrechtsdaten zugeordnet ist.

[0031] Die erste Sende-/Empfangseinheit ist bevorzugt für die drahtlose Datenkommunikation mittels Nahfeldkommunikation, insbesondere nach dem RFID- bzw. NFC-Standard ausgebildet.

[0032] Die zweite Sende-/Empfangseinheit ist bevorzugt zur Datenkommunikation über den Bluetooth-Standard ausgebildet.

[0033] Die erste Sende-/Empfangseinheit ist vorteilhaft als passiv arbeitende RFID- bzw. NFC-Einheit ausgebildet.

[0034] Der Zugriff auf das Sicherheitshardwaremodul und auf die darin gespeicherten Zutrittsrechtsdaten ist bevorzugt durch kryptographische Methoden abgesichert. Die Erfindung wird nachfolgend anhand von in der Zeichnung schematisch dargestellten Ausführungsbeispielen näher erläutert. In dieser zeigt

[0035] Fig. 1 den schematischen Aufbau eines Zutrittskontrollsystems und

[0036] Fig. 2 den Aufbau der einzelnen Komponenten des Systems gemäß Fig. 1.

[0037] In Fig. 1 ist eine zentrale Recheneinheit mit 1 bezeichnet. Die Objekte, zu denen der Zutritt mit Hilfe des Zutrittskontrollsystems kontrolliert werden soll, sind mit 2 bezeichnet und im vorliegenden Fall schematisch als Häuser dargestellt. Die Objekte 2 weisen jeweils eine Tür mit einer auf RFID oder NFC basierenden Schließeinheit auf. Ein Administrator 3 verwaltet die zentrale Recheneinheit 1 und kann Zutrittsberechtigungen vergeben. Die zentrale Recheneinheit 1 ist an eine mobiles, drahtloses Telekommunikationsnetzwerk 4 angeschlossen, wie beispielsweise ein GSM-Handy-Netz und kann über das Telekommunikationsnetzwerk 4 Zutrittsrechtsdaten an mobile Telekommunikationsgeräte 5 senden. Bei den mobilen Telekommunikationsgeräten 5 handelt es sich um Mobiltelefone, die mit einer Softwareapplikation 7 (Fig. 2) ausgestattet sind, welche den Datenaustausch zwischen der zentralen Recheneinheit 1 und einem Identifikationsmedium 6 steuert. Die Softwareapplikation 7 bzw. das Telekommunikationsgerät 5 fungiert als Router, der die von der zentralen Recheneinheit 1 erhaltenen Zutrittsrechtsdaten an das Identifikationsmedium 6 weitergibt. Die zu übertragenden Zutrittsrechtsdaten werden hierbei in der zentralen Recheneinheit 1 verschlüsselt und in dem Identifikationsmedium 6 entschlüsselt. In dem Telekommunikationsgerät 5 erfolgt keine Entschlüsselung der Zutrittsrechtsdaten. Im einfachsten Fall werden die Zutrittsrechtsdaten als Schlosskennung an das mobile Telekommunikationsgerät 5 gesendet. Wenn nun in einem stark vereinfachten Beispiel die Schließeinheiten der in Fig. 1 dargestellten Objekte 2 die Kennung 100, 101 und 102 aufweisen, so bedeutet die Übermittlung der Zutrittsrechtsdaten an ein Telekommunikationsgerät 5 in Form der Kennung 101, dass dies einer Zugangsberechtigung für die Schließeinheit mit der Kennung 101 entspricht. Wenn nun das als Schlüssel verwendete Identifikationsmedium 6 in die Nähe einer Schließeinheit mit der Kennung 101 gebracht wird und im Zuge der Zutrittsberechtigungsprüfung die Zutrittsrechtsdaten, nämlich die Schlosskennung „101" an die Schließeinheit übermittelt wird, so erkennt die Schließeinheit auf Grund eines Vergleichs der vom Schlüssel übermittelten Schlosskennung mit der eigenen Schlosskennung bei Übereinstimmung derselben das Vorhandensein einer Zutrittsberechtigung, worauf das Schloss freigegeben wird.

[0038] Der Aufbau des Identifikationsmediums 6 ist in Fig. 2 näher dargestellt. Das Identifikati-

onsmedium 6 kann in Form einer Chipkarte, als Schlüsselanhänger, nach Art eines RFID- bzw. NFC Transponders oder dgl. ausgebildet sein. Das Identifikationsmedium umfasst ein erstes Sende-/Empfangsmodul 8, welches z.B. für den Datenaustausch 17 mit der Zutrittskontrollvorrichtung 9 nach dem RFID/NFC- Standard ausgebildet ist und eine entsprechende Antenne aufweist. Das erste Sende-/Empfangsmodul 8 ist hierbei als passiv arbeitender RFID/NFC Transponder ausgebildet, dessen Stromversorgung bei Bedarf durch das elektromagnetische, bevorzugt im Wesentlichen magnetische Wechselfeld der Leseeinheit der Zutrittskontrollvorrichtung 9 erfolgt. Der RFID/NFC-Transponder 8 umfasst ein Sicherheitshardwaremodul (Secure Element) 10, in dem die vom Telekommunikationsgerät 5 erhaltenen Zutrittsrechtsdaten gespeichert und gegen unbefugten Zugriff gesichert sind. Die Programmierung des Sicherheitshardwaremoduls 10 erfolgt mittels eines Mikrokontrollers 11, der einerseits mit dem Sicherheitshardwaremodul 10 und andererseits mit dem zweiten Sende-/Empfangsmodul 12 verbunden ist. Das zweite Sende-/Empfangsmodul 12 ist für die Datenkommunikation über Bluetooth 4.0 LE geeignet und kann mit einem entsprechenden Sende-/Empfangsmodul 13 des Telekommunikationsgeräts 5 gekoppelt werden. Der Mikrokontroller 11 ist eingerichtet, um den Aufbau einer drahtlosen Kommunikationsverbindung 15 zwischen dem Identifikationsmedium 6 und dem Telekommunikationsgerät 5 (bzw. über das Telekommunikationsgerät 5 mit der zentralen Recheneinheit 1) zu veranlassen, um einen Datenaustausch zu ermöglichen. Der Verbindungsaufbau kann beispielsweise durch Betätigen eines Tasters 14 am Identifikationsmedium 6 gestartet werden. Alternativ wird der Verbindungsaufbau durch die Softwareapplikation 7 des Telekommunikationsgeräts 5 gesteuert. Bevorzugt erfolgt der Verbindungsaufbau in vorgegebenen Zeitabständen, um die im Identifikationsmedium gespeicherten Zutrittsrechtsdaten regelmäßig zu aktualisieren.

[0039] Die Entschlüsselung der von der zentralen Recheneinheit 1 erhaltenen Zutrittsrechtsdaten erfolgt bevorzugt in dem Sicherheitshardwaremodul 10. Dies bedeutet, dass der Mikrokontroller 11 die über das zweite Sende-/Empfangsmodul 12 erhaltenen Daten unverändert an das Sicherheitshardwaremodul 10 übergibt, wo sie erst entschlüsselt werden. Die Stromversorgung des Identifikationsmediums wird durch einen elektrischen Energiespeicher, wie z.B. eine aufladbare Batterie 16 sichergestellt. Zum Aufladen des Energiespeichers kann das Identifikationsmedium 6 eine geeignete Anschlussbuchse wie z.B. einen MicroUSB Anschluss, aufweisen. Alternativ kann die Aufladung auch kontaktlos, insbesondere induktiv erfolgen.

Patentansprüche

1. Verfahren zur Zutrittskontrolle insbesondere in Gebäuden, bei dem eine bidirektionale Datenübermittlung zwischen einem Zutrittsrechtsdaten speichernden elektronischen Identifikationsmedium und einer Zutrittskontrollvorrichtung stattfindet und in der Zutrittskontrollvorrichtung eine Zutrittsberechtigungsprüfung vorgenommen wird, wobei in Abhängigkeit von der festgestellten Zutrittsberechtigung ein Sperrmittel zum wahlweisen Freigeben oder Sperren des Zutritts angesteuert wird, wobei Zutrittsrechtsdaten in einer zentralen Recheneinheit gespeichert und verwaltet werden und das Identifikationsmedium mit Zutrittsrechtsdaten programmiert wird, wobei die Programmierung des Identifikationsmediums das Senden der Zutrittsrechtsdaten über ein drahtloses Telekommunikationsnetz an ein drahtloses mobiles Telekommunikationsgerät und das Übermitteln der vom mobilen Telekommunikationsgerät empfangenen Zutrittsrechtsdaten an einen Speicher des Identifikationsmediums umfasst, **dadurch gekennzeichnet**, dass die Übermittlung der Zutrittsrechtsdaten vom Telekommunikationsgerät an das Identifikationsmedium drahtlos über Kurzreichenweitenfunk erfolgt und die Zutrittsrechtsdaten in einem elektronischen Sicherheitshardwaremodul des Identifikationsmediums gespeichert werden.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet**, dass die für die Zutrittsberechtigungsprüfung erforderliche Datenkommunikation zwischen dem Identifikationsmedium und der Zutrittskontrollvorrichtung über eine dem Sicherheitshardwaremodul zugeordnete erste Sende- /Empfangseinheit des Identifikationsmediums erfolgt, wobei die Datenkommunikation mittels Nahfeldkommunikation, insbesondere nach dem RFID- bzw. NFC-Standard vorgenommen wird.

3. Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet**, dass die Übermittlung der Zutrittsrechtsdaten vom Telekommunikationsgerät an das Identifikationsmedium über eine zweite Sende-/Empfangseinheit des Identifikationsmediums erfolgt, insbesondere über eine Bluetooth-Verbindung.

4. Verfahren nach Anspruch 2 oder 3, **dadurch gekennzeichnet**, dass die Energieversorgung der ersten Sende-/Empfangseinheit des Identifikationsmediums über ein elektromagnetisches, bevorzugt im Wesentlichen magnetisches Wechselfeld der Zutrittskontrollvorrichtung erfolgt.

5. Verfahren nach einem der Ansprüche 1 bis 4, **dadurch gekennzeichnet**, dass die Kommunikation zwischen dem mobilen Telekommunikationsgerät und dem Identifikationsmedium in regelmäßigen, voreingestellten Zeitabständen erfolgt.

6. Verfahren nach Anspruch 5, **dadurch gekennzeichnet**, dass das Identifikationsmedium in einen Außerbetriebs- oder Sperrmodus wechselt, wenn der Zeitabstand zur letzten Kommunikation zwischen dem mobilen Telekommunikationsgerät und dem Identifikationsmedium einen vorgegebenen Grenzwert überschreitet.

7. Elektronisches Identifikationsmedium (6) für Zutrittskontrollvorrichtungen (9) umfassend eine erste Sende-/Empfangseinheit (8) für die Datenkommunikation (17) zwischen dem Identifikationsmedium (6) und der Zutrittskontrollvorrichtung (9) und eine zweite Sende-/ Empfangseinheit (12) für die drahtlose Übermittlung (15) von Zutrittsrechtsdaten von einem Telekommunikationsgerät (5) an das Identifikationsmedium (6) mittels Kurzreichenweitenfunk, wobei der ersten Sende-/Empfangseinheit (8) ein elektronisches Sicherheitshardwaremodul (10) zum Speichern der Zutrittsrechtsdaten zugeordnet ist.

8. Identifikationsmedium nach Anspruch 7, **dadurch gekennzeichnet**, dass die erste Sende-/ Empfangseinheit (8) für die drahtlose Datenkommunikation (17) mittels Nahfeldkommunikation, insbesondere nach dem RFID- bzw. NFC- Standard ausgebildet ist.

9. Identifikationsmedium nach Anspruch 7 oder 8, **dadurch gekennzeichnet**, dass die zweite Sende-/Empfangseinheit (12) zur Datenkommunikation (15) über den Bluetooth-Standard ausgebildet ist.

10. Identifikationsmedium nach Anspruch 7, 8 oder 9, **dadurch gekennzeichnet**, dass die erste Sende-/Empfangseinheit (8) als passiv arbeitende RFID- bzw. NFC- Einheit ausgebildet ist.

11. Identifikationsmedium nach einem der Ansprüche 7 bis 10, **dadurch gekennzeichnet**, dass der Zugriff auf das Sicherheitshardwaremodul (10) und auf die darin gespeicherten Zutrittsrechtsdaten durch kryptographische Methoden abgesichert ist.

Hierzu 2 Blatt Zeichnungen

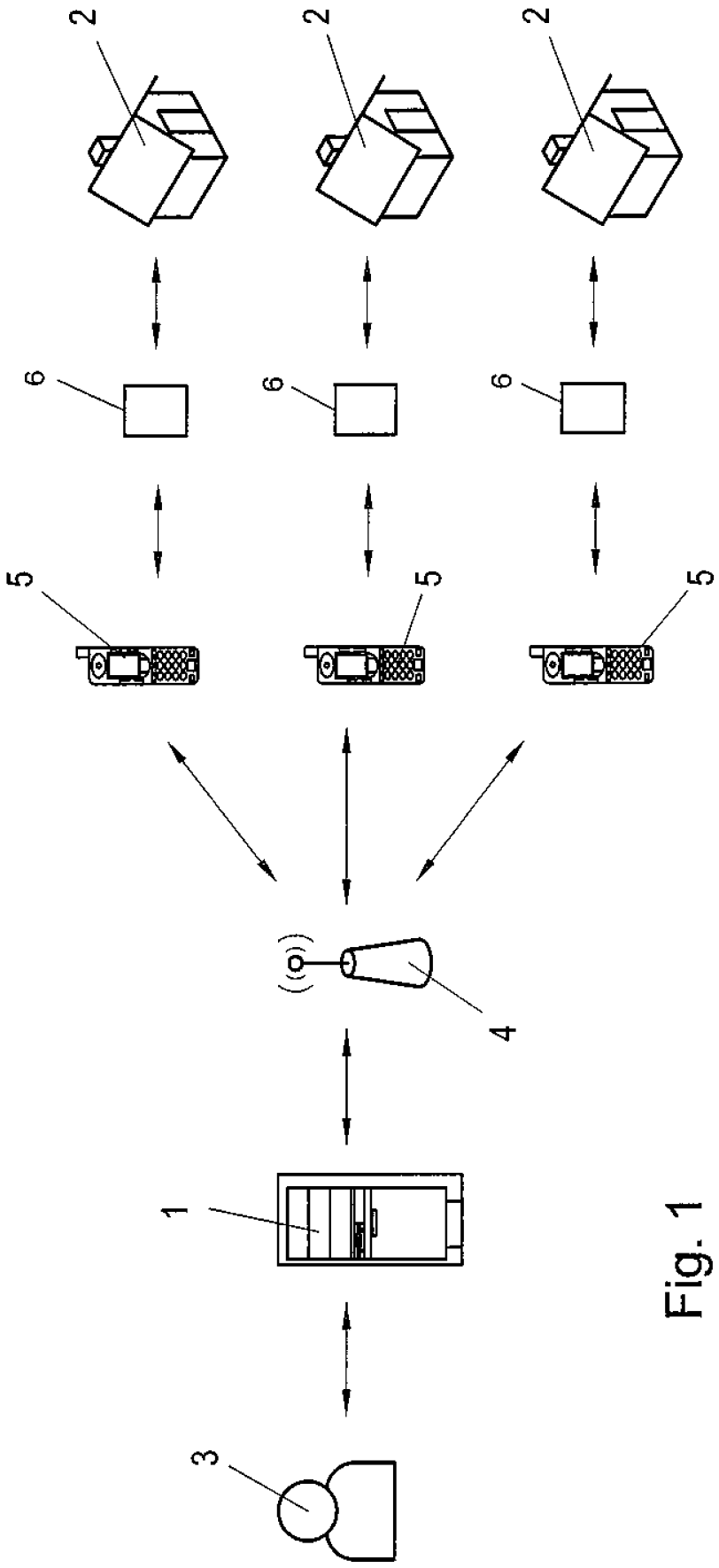

Fig. 1

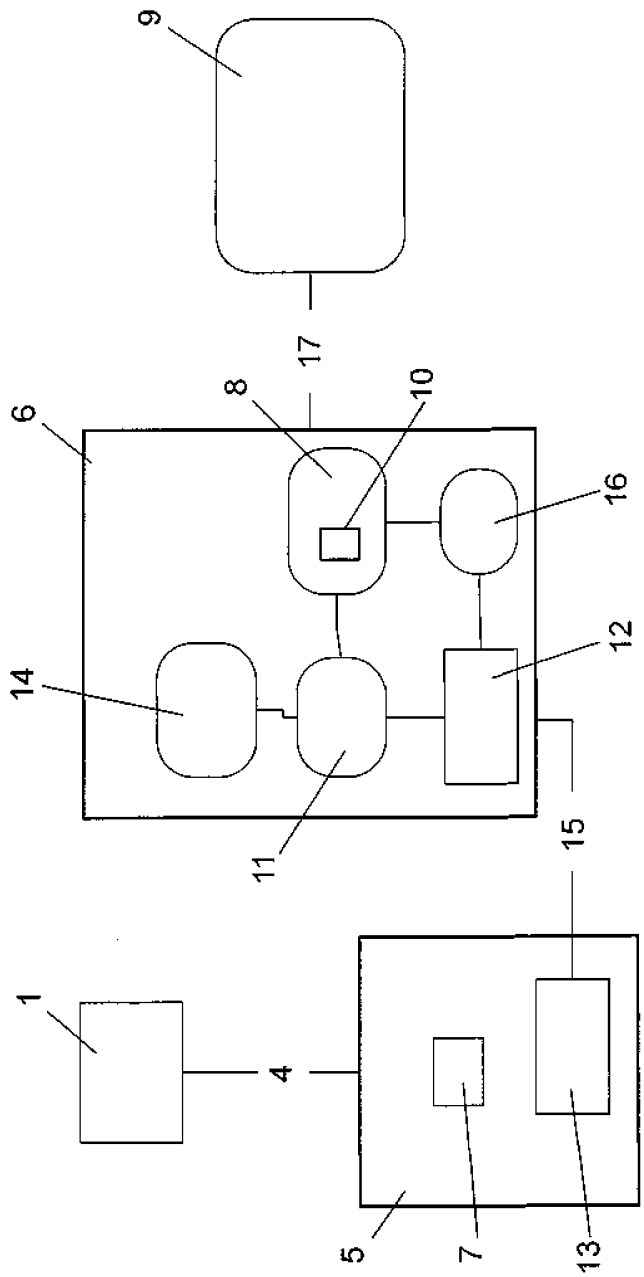

Fig. 2