(19) österreichisches patentamt

(10) **AT 512 419 A1 2013-08-15**

(12) # Österreichische Patentanmeldung

(21) Anmeldenummer: A 132/2012
(22) Anmeldetag: 31.01.2012
(43) Veröffentlicht am: 15.08.2013

(51) Int. Cl. : ***G07C 9/00*** (2006.01)
H04L 9/00 (2006.01)

(56) Entgegenhaltungen:
US 2005060555 A1
WO 199630857 A1
EP 1549020 A2 EP 2063400 A1
WO 2003088564 A1

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

(72) Erfinder:
Ullmann Johannes Dipl.Ing.
Wien (AT)
Groissböck Norbert
Rottenbach (AT)
Zapletal Alexander Dr.
Wien (AT)

(54) **VERFAHREN UND VORRICHTUNG ZUR ZUTRITTSKONTROLLE**

(57) Bei einem Verfahren zur Zutrittskontrolle werden Zutrittsrechtsdaten von einem elektronischen Identifikationsmedium an eine Zutrittskontrollvorrichtung übermittelt, wobei die Zutrittsrechtsdaten in der Zutrittskontrollvorrichtung zur Feststellung der Zutrittsberechtigung ausgewertet werden und in Abhängigkeit von der festgestellten Zutrittsberechtigung ein Sperrmittel zum wahlweisen Freigeben oder Sperren des Zutritts angesteuert wird. Es findet eine Authentifizierung des elektronischen Identifikationsmediums auf Grundlage wenigstens eines digitalen Zertifikats statt. Die Datenübermittlung umfasst 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, wobei die Zutrittsrechtsdaten über den sicheren Kanal vom elektronischen Identifikationsmedium an die Zutrittskontrollvorrichtung übermittelt werden.

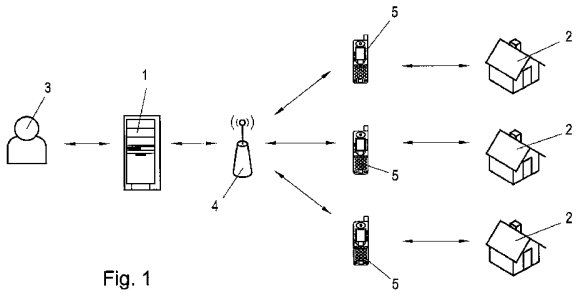


Fig. 1

AT 512 419 A1 2013-08-15

Zusammenfassung:

Bei einem Verfahren zur Zutrittskontrolle werden Zutrittsrechtsdaten von einem elektronischen Identifikationsmedium an eine Zutrittskontrollvorrichtung übermittelt, wobei die Zutrittsrechtsdaten in der Zutrittskontrollvorrichtung zur Feststellung der Zutrittsberechtigung ausgewertet werden und in Abhängigkeit von der festgestellten Zutrittsberechtigung ein Sperrmittel zum wahlweisen Freigeben oder Sperren des Zutritts angesteuert wird. Es findet eine Authentifizierung des elektronischen Identifikationsmediums auf Grundlage wenigstens eines digitalen Zertifikats statt. Die Datenübermittlung umfasst 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, wobei die Zutrittsrechtsdaten über den sicheren Kanal vom elektronischen Identifikationsmedium an die Zutrittskontrollvorrichtung übermittelt werden.

Fig. 1

Die Erfindung betrifft ein Verfahren zur Zutrittskontrolle insbesondere in Gebäuden, bei dem eine bidirektionale Datenübermittlung zwischen einem elektronischen Identifikationsmedium und einer Zutrittskontrollvorrichtung und eine Datenverarbeitung stattfindet, wobei die Datenübermittlung die Übermittlung von Zutrittsrechtsdaten vom elektronischen Identifikationsmedium an die Zutrittskontrollvorrichtung umfasst, wobei die Zutrittsrechtsdaten in der Zutrittskontrollvorrichtung zur Feststellung der Zutrittsberechtigung ausgewertet werden und in Abhängigkeit von der festgestellten Zutrittsberechtigung ein Sperrmittel zum wahlweisen Freigeben oder Sperren des Zutritts angesteuert wird.

Weiters betrifft die Erfindung eine Vorrichtung umfassend eine Zutrittskontrollvorrichtung mit einem Sperrmittel zum wahlweisen Freigeben oder Sperren des Zutritts und einer Sende-/Empfangseinrichtung, um eine bidirektionale Datenübermittlung zwischen einem elektronischen Identifikationsmedium und der Zutrittskontrollvorrichtung zu ermöglichen, wobei die Zutrittskontrollvorrichtung Datenverarbeitungsmittel zur Steuerung der Datenübermittlung und zur Feststellung der Zutrittsberechtigung auf Grund von empfangenen Zutrittsrechtsdaten aufweist und die Datenverarbeitungsmittel mit dem Sperrmittel zum wahlweisen Freigeben oder Sperren des Zutritts zusammenwirken.

Für die elektronische Zutrittskontrolle mit berührungslosen Systemen gibt es mehrere Möglichkeiten. Bisher bekannte RFID-Systeme bestehen aus einem elektronischen Identifikationsmedium, wie z.B. einem elektronischen Schlüssel, auf welchem Zutrittsrechtsdaten, wie z.B. ein Identifikations- bzw. Zugangscode und/oder Zutrittsbedingungen wie z.B. berechtigte Zutrittszeit, berechtigter Zutrittstag, berechtigtes Zu-

trittsdatum eines Benutzers und dgl., elektronisch gespeichert sind und der oft als „Transponder" bezeichnet wird, und einem Lesegerät. Dabei ist der Transponder meist ohne eigene Energiequelle aufgebaut und die benötigte Energie wird aus dem elektromagnetischen Feld des Lesegeräts bezogen. Weiters sind auch Funksysteme bekannt, bei denen das elektronische Identifikationsmedium ein aktiver Sender mit eigener Energiequelle ist (z.B. Fernöffnung der Zentralverriegelung für Kraftfahrzeuge).

Bei größeren Schließsystemen mit einer Mehrzahl von Schließeinheiten und elektronischen Identifikationsmedien bzw. Schlüsseln werden die Zutrittsberechtigungen zur einfacheren Verwaltung meist in einer Zutrittskontrollzentrale gespeichert. Die Zutrittskontrollzentrale weist hierbei üblicherweise eine Datenbank auf, in der die einzelnen Schließeinheiten, die Schlüssel und die jeweiligen Zutrittsberechtigungen verwaltet werden können. Über eine an die Zutrittskontrollzentrale angeschlossene Schreibeinrichtung können die elektronischen Identifikationsmedien entsprechend den jeweils gewünschten Zutrittsberechtigungen mit Zutrittsrechtsdaten programmiert werden.

In der WO 2009/094683 A1 ist in diesem Zusammenhang vorgeschlagen worden, die Programmierung der Schlüssel mit Zutrittsrechtsdaten über ein drahtloses Telekommunikationsnetz vorzunehmen, wobei die Zutrittsrechtsdaten von der Zutrittskontrollzentrale 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. Erfin-

dungsgemäß wird somit eine Art „online-Schlüssel" geschaffen, da der Schlüssel 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.

Auf Grund der Möglichkeit der entfernten Programmierung von Schlüsseln ist es zur Änderungen der Zutrittsberechtigungen nicht mehr notwendig, einen Zugriff direkt auf die einzelnen Schließeinheiten zu erhalten. Die Schließeinheiten können nach der Installation und Initialisierung als autonome Einheiten arbeiten und erfordern insbesondere keine Netzwerkanbindung.

Obwohl die elektronische Überprüfung der Zutrittsberechtigung allgemein eine Reihe von Vorteilen bietet, wie z.B. die Möglichkeit der raschen Änderung von Berechtigungsdaten und eine wesentlich größere Codierungsvielfalt und -komplexität als bei einer mechanischen Berechtigungsabfrage, können elektronisch vorliegende Zutrittsberechtigungsdaten, insbesondere solche, die drahtlos übertragen werden, bei ungenügenden Sicherheitsvorkehrungen leicht und unbemerkt abgefangen oder kopiert und missbräuchlich verwendet werden.

Mit der Übersendung von Zutrittsrechtsdaten von der Zutrittskontrollzentrale an mobile Telekommunikationsgeräte ist beispielsweise das Risiko verbunden, dass die Zutrittsrechtsdaten von unberechtigten Personen manipuliert oder abgefangen werden. Sicherheitskritische Angriffspunkte bietet auch die Datenübertragung zwischen dem Identifikationsmedium und der Zutrittskontrollvorrichtung. Weiters kann die Zutrittskontrollvorrichtung selbst Ziel von Angriffen sein, die beispielsweise auf die Zerstörung der für die Zutrittskontrolle

verantwortlichen elektronischen Bausteine oder Schaltkreise abzielen.

Unter Zutrittskontrollvorrichtungen oder Schließeinheiten sind im Rahmen der Erfindung elektrische, elektronische oder mechatronische Schließeinheiten, insbesondere Schlösser, zu verstehen. Schließeinheiten können hierbei verschiedene Komponenten umfassen, wie z.B. Leseeinrichtungen für Identifikationsmedien, insbesondere elektronische Schlüssel, eine Schließelektronik und dgl. Zutrittskontrollvorrichtungen bzw. Schließeinheiten dienen dabei insbesondere dazu, den Zutritt zu Räumen in Abhängigkeit von der Zutrittsberechtigung zu versperren oder freizugeben und sind dementsprechend zum Einbau in Türen, Fenstern und dgl. vorgesehen. Unter mechanischen Schließeinheiten sind z.B. Zylinderschlösser zu verstehen. Mechatronische Schließeinheiten sind z.B. elektromotorisch angetriebene Sperreinrichtungen, insbesondere E-Zylinder. Elektrische Schließeinheiten sind z.B. elektrische Türöffner.

Unter einem Freigabemittel 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.

Die vorliegende Erfindung zielt daher darauf ab, die Sicherheit von elektronisch arbeitenden Zutrittskontrollsystemen zu erhöhen.

Zur Lösung dieser Aufgabe ist gemäß einem ersten Aspekt der Erfindung bei einem Verfahren der eingangs genannten Art vorgesehen, dass die Datenverarbeitung eine Authentifizierung des elektronischen Identifikationsmediums auf Grundlage wenigstens eines digitalen Zertifikats umfasst und die Datenübermittlung die Verwendung eines Schlüsselaustausch- oder -ableitungsprotokolls umfasst, 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 dass die Zutrittsrechtsdaten über den sicheren Kanal vom elektronischen Identifikationsmedium an die Zutrittskontrollvorrichtung übermittelt werden. Dadurch, dass das elektronische Identifikationsmedium auf Grundlage wenigstens eines digitalen Zertifikats authentifiziert wird, können systemfremde und daher nicht zertifizierte oder ungültig zertifizierte Teilnehmer des Zutrittskontrollsystems erkannt werden. Bevorzugt ist hierbei vorgesehen, dass das wenigstens eine digitale Zertifikat von einer Zutrittskontrollzentrale ausgestellt wird. Bevorzugt ist das wenigstens eine digitale Zertifikat von der Zutrittskontrollzentrale zusätzlich signiert, sodass auch das Zertifikat entsprechend auf Echtheit und Gültigkeit überprüft werden kann. Unter einem digitalen Zertifikat ist hierbei ein digitaler Datensatz zu verstehen, der bestimmte Eigenschaften des Identifikationsmediums bestätigt und dessen Authentizität und Integrität durch kryptographische Verfahren geprüft werden kann. Insbesondere handelt es sich dabei um ein Public-Key-Zertifikat, welches das Identifikationsmedium als Inhaber und weitere Eigenschaften eines öffentlichen kryptographischen Schlüssels bestätigt. Es handelt sich somit um einen

Nachweis, dass der öffentliche Schlüssel eines asymmetrischen Verschlüsselungsverfahrens zu dem Identifikationsmedium gehört. Insbesondere kommt das digitale Zertifikat im Rahmen eines dynamischen asymmetrischen Authentifizierungsverfahrens zum Einsatz.

Erfindungswesentlich ist weiters das Einrichten eines sicheren Übertragungskanals, wobei der hierfür erforderliche Sitzungsschlüssel durch ein Schlüsselaustausch- der -ableitungsprotokoll zugänglich gemacht wird. Unter einem Schlüsselaustausch- oder -ableitungsprotokoll ist hierbei ein Vorgang in der Kryptographie zu verstehen, um zwei oder mehreren Kommunikationspartnern einen gemeinsamen, geheimen Schlüssel zugänglich zu machen, ohne diesen im Klartext zu übertragen. Dies kann geschehen, indem jemand einen Schlüssel an alle beteiligten Partner überträgt oder indem während der Durchführung des Protokolls ein neuer Schlüssel erzeugt oder abgeleitet wird. Das Schlüsselaustausch- der -ableitungsprotokoll legt dabei die genaue Verfahrensweise fest. Der Sitzungsschlüssel wird anschließend verwendet, um die zwischen dem Identifikationsmedium und der Zutrittskontrollvorrichtung übermittelten Daten mittels eines symmetrischen Verschlüsselungsverfahrens zu ver- und entschlüsseln und deren Authentizität zu wahren.

Bevorzugt wird so vorgegangen, dass der wenigstens eine Sitzungsschlüssel im elektronischen Identifikationsmedium und in der Zutrittskontrollvorrichtung auf Grundlage eines zutrittskontrollvorrichtungsindividuellen Zutrittscodes erzeugt oder abgeleitet wird, bevorzugt weiters auf Grundlage einer vom Identifikationsmedium und einer von der Zutrittskontrollvorrichtung erzeugten Zufallszahl und/oder von einer vom Identi-

fikationsmedium und einer von der Zutrittskontrollvorrichtung erzeugten Laufnummer.

Die Übertragungssicherheit kann noch dadurch erhöht werden, dass das Schlüsselaustauschprotokoll die Generierung eines Kryptogramms unter Verwendung des Sitzungsschlüssels in der Zutrittskontrollvorrichtung und die Übersendung desselben an das Identifikationsmedium umfasst, wobei das Kryptogramm im Identifikationsmedium unter Verwendung des Sitzungsschlüssels verifiziert wird. Dieser Vorgang kann zusätzlich auch in der umgekehrten Richtung verwendet werden. In diesem Fall umfasst das Schlüsselaustauschprotokoll die Generierung eines Kryptogramms unter Verwendung des Sitzungsschlüssels im Identifikationsmedium und die Übersendung desselben an die Zutrittskontrollvorrichtung, wobei das Kryptogramm in der Zutrittskontrollvorrichtung unter Verwendung des Sitzungsschlüssels verifiziert wird.

Der Vorteil der erfindungsgemäßen Verfahrensweise ist, dass alle Daten, die nicht dem Aufbau des sicheren Übertragungskanals dienen, in diesem sicheren, sitzungsspezifischen Kanal übertragen werden, wodurch die Integrität, Authentizität und Vertraulichkeit der Daten gewährleistet ist. So werden beispielsweise die Zutrittsrechtsdaten über den sicheren Kanal übermittelt, wobei eine ergänzende Authentifizierung bevorzugt dadurch gelingt, dass die Zutrittsrechtsdaten von einer Zutrittskontrollzentrale signiert und gemeinsam mit der Signatur über den sicheren Kanal vom elektronischen Identifikationsmedium an die Zutrittskontrollvorrichtung übermittelt werden.

Ein weiterer Vorteil der erfindungsgemäßen Verfahrensweise ist, dass die Zutrittskontrollvorrichtung weder an die Zu-

trittskontrollzentrale noch an eine Zertifizierungsstelle drahtlos oder drahtgebunden angebunden sein muss. Vielmehr erfolgt die Ermittlung der Zutrittsberechtigung in der Zutrittskontrollvorrichtung einschließlich der Authentifizierung des elektronischen Identifikationsmediums, der Durchführung des Schlüsselaustausch- bzw. -ableitungsprotokolls und der Einrichtung des sicheren Übertragungskanals ausschließlich auf Grund von zwischen der Zutrittskontrollvorrichtung und dem elektronischen Identifikationsmedium übermittelten oder einmalig und dauerhaft in der Zutrittskontrollvorrichtung abgespeicherten Daten, wie z.B. einer herstellerseitig abgespeicherten Zutrittskontrollvorrichtungsidentifizierung.

Eine weitere Erhöhung der Sicherheit gelingt dadurch, dass die Datenübermittlung rein passiv durch Belastung des elektromagnetischen Feldes zwischen dem elektronischen Identifikationsmedium und der Zutrittskontrollvorrichtung erfolgt. Diese Datenübermittlung funktioniert lediglich über eine sehr begrenzte Reichweite von ca. 10 cm, sodass ein Abhören erschwert wird.

Zur Lösung der der Erfindung zugrundeliegenden Aufgabe ist gemäß einem zweiten Aspekt der Erfindung bei einer Vorrichtung der eingangs genannten Art vorgesehen, dass die Datenverarbeitungsmittel wenigstens einen Mikrokontroller und ein Secure Access Module (SAM) umfassen, wobei das SAM zur Ausführung kryptographischer Funktionen eingerichtet ist, und dass die Sende-/Empfangseinrichtung in einem ersten Bereich der Zutrittskontrollvorrichtung und das SAM in einem zweiten Bereich der Zutrittskontrollvorrichtung angeordnet ist. Es können somit möglichst viele kritische Operationen, wie z.B. der Aufbau eines sicheren Übertragungskanals, kryptographische Operationen, Zutrittsentscheidungen, Logdatei, Black-

lists und dgl., in einem eigens hierfür vorgesehenen Bauteil, nämlich dem Secure Access Module (SAM) gebündelt werden, wobei das SAM in einem von der Sende-/Empfangseinheit gesonderten Bereich der Zutrittskontrollvorrichtung angeordnet werden kann. Bevorzugt ist die Ausbildung hierbei so getroffen, dass der erste Bereich (in dem die Sende-/Empfangseinheit angeordnet ist) ein ungeschützter Bereich und der zweite Bereich (in dem das SAM angeordnet ist) ein baulich geschützter Bereich ist. Dies gewährleistet, dass das SAM gegen Zerstörung oder Manipulation durch Krafteinwirkung oder andere zerstörende Einflüsse, insbesondere gegen physische Angriffe aller Art besser geschützt ist.

Mit Vorteil ist auch der Mikrokontroller im zweiten Bereich angeordnet. Der Mikrokontroller ist bevorzugt so verschaltet, dass er die Sende-/Empfangseinrichtung mit dem SAM verbindet. Der Mikrokontroller ist bevorzugt austauschbar in der Zutrittskontrollvorrichtung angeordnet.

Als geschützter Bereich ist zum Beispiel der Bereich hinter einem Aufbohrschutz oder auch an einer der Zutrittsseite (z.B. der Raumaußenseite) abgewandten Seite (z.B. der Rauminnenseite) zu verstehen. Insbesondere kann vorgesehen sein, dass die Zutrittskontrollvorrichtung zum Einbau in eine Tür ausgebildet ist und mit wenigstens einer ersten Handhabe, wie z.B. einem Knauf oder einem Drücker, versehen ist, wobei der erste Bereich von der ersten Handhabe und der zweite Bereich von einem zur Aufnahme in einer Durchbrechung des Türblattes vorgesehenen Bereich oder einer zweiten, der ersten Handhabe gegenüberliegenden, zweiten Handhabe gebildet ist.

Um die Sicherheit der Berechtigungsabfrage zu erhöhen, umfasst das SAM bevorzugt Authentifizierungsmittel, um das

elektronische Identifikationsmedium auf Grundlage wenigstens eines digitalen Zertifikats zu authentifizieren, und ist mit einem Schlüsselaustauschprotokoll programmiert. Weiters ist das SAM bevorzugt zur Einrichtung eines sicheren Übertragungskanals zwischen dem elektronischen Identifikationsmedium und der Zutrittskontrollvorrichtung ausgebildet oder programmiert. Weiters ist bevorzugt vorgesehen, dass das SAM eine Auswerteschaltung zur Feststellung der Zutrittsberechtigung auf Grund der empfangenen Zutrittsrechtsdaten umfasst. Die Auswerteschaltung kann als Hardwareschaltung ausgebildet oder softwaremäßig realisiert sein.

Das SAM ist besonders bevorzugt als Mikrokontroller in Chipkarten- oder SIM-Karten-Bauform, insbesondere in IC-Bauform ausgebildet. Vorteilhafterweise kann das SAM austauschbar in einer Schnittstelle, insbesondere in einem Steckplatz aufgenommen sein, sodass beispielsweise die Verschlüsselungsart und die Verschlüsselungsstärke in einfacher Weise durch Austausch des SAMs oder Ändern der im SAM laufenden Applikation geändert werden kann.

Bevorzugt ist das Identifikationsmedium in ein mobiles Telekommunikationsgerät, insbesondere ein Mobiltelefon integriert. Die Ausbildung ist in diesem Fall bevorzugt dahingehend weitergebildet, dass die Sende-/Empfangseinrichtung für die drahtlose, bevorzugt induktive Datenübertragung insbesondere nach dem NFC- bzw. RFID-Standard (ISO/IEC 14443) ausgebildet ist.

Die Erfindung wird nachfolgend anhand von in der Zeichnung schematisch dargestellten Ausführungsbeispielen näher erläutert. In dieser zeigt Fig. 1 den schematischen Aufbau eines Zutrittskontrollsystems in einer ersten Ausbildung, Fig. 2

eine weitere Ausbildung eines Zutrittskontrollsystems, Fig. 3 eine abgewandelte Ausbildung eines Zutrittskontrollsystems, Fig. 4 ein Blockschaltbild einer Zutrittskontrollvorrichtung, die in einem Zutrittskontrollsystem gemäß den Fig. 1, 2 oder 3 verwendet werden kann, und Fig. 5 ein Diagramm des vereinfachten Protokollablaufs bei einem Sperrvorgang.

In Fig. 1 ist eine Zutrittskontrollzentrale 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 z.B. auf RFID basierenden Schließeinheit auf. Ein Administrator 3 verwaltet die Zutrittskontrollzentrale 1 und kann Zutrittsberechtigungen vergeben. Die Zutrittskontrollzentrale 1 ist an ein Telekommunikationsnetz 4 angeschlossen, wie beispielsweise ein LAN, WLAN, GSM-, GPRS- oder UMTS-Netz und kann über das Netz 4 Zutrittsrechtsdaten an mobile Telekommunikationseinrichtungen 5 senden. Bei den mobilen Telekommunikationseinrichtungen 5 handelt es sich z.B. um Handys, die mit einer Schlüsselfunktion ausgestattet sind. Die Handys weisen beispielsweise ein NFC- oder RFID-Modul auf, in dessen Speicher die von der Zutrittskontrollzentrale 1 erhaltenen Zutrittsrechtsdaten geschrieben werden können. Wenn nun das als Schlüssel verwendete Telekommunikationsgerät 5 in die Nähe einer Schließeinheit gebracht wird, wird eine bidirektionale Datenübertragung zwischen der entsprechenden NFC- oder RFID-Schnittstelle des Telekommunikationsgerät 5 und einer Sende-/Empfangseinheit der Schließeinheit gestartet, in deren Verlauf die Zutrittsrechtsdaten an die Schließeinheit übermittelt werden. Wenn die Schließeinheit eine Zutrittsberechtigung feststellt, wird das Schloss freigegeben.

Aus der Darstellung in Fig. 2 ergeben sich nun verschiedene Anwendungsmöglichkeiten. Die Zutrittskontrollzentrale ist wiederum mit 1 und der Administrator mit 3 bezeichnet. Die Zutrittskontrollzentrale 1 weist eine Datenbank 6 auf bzw. ist mit einer derartigen Datenbank verbunden, auf welcher die Zutrittsrechtsdaten gespeichert und verwaltet werden. Die Zutrittskontrollzentrale 1 ist weiters mit einer Schreibeinheit 7 verbunden, die beispielsweise als Schreibgerät für RFID-Tags bzw. Transponder ausgebildet ist. Mit 8 ist ein RFID-Transponder dargestellt, der von der Schreibeinheit 7 beschrieben werden kann. Dies entspricht im Prinzip dem herkömmlichen Verfahren, wie RFID-Transponder programmiert werden können.

Eine Datenverbindung zwischen einem mobilen Telekommunikationsgerät 5 und der Zutrittskontrollzentrale 1 kann nun gemäß der Darstellung in Fig. 2 auf verschiedene Art und Weise erfolgen. Beispielsweise kann eine drahtlose Verbindung über verschiedene Verbindungsprotokolle, wie beispielsweise WLAN, GSM oder UMTS mit dem Internet 9 hergestellt werden, wobei auch die Zutrittskontrollzentrale 1 mit dem Internet 9 verbunden ist. Alternativ oder zusätzlich dazu kann ein SMS-Gateway 10 vorgesehen sein, sodass der Datenaustausch zwischen der Zutrittskontrollzentrale 1 und dem mobilen Telekommunikationsgerät 5 über einen Kurzmitteilungsdienst oder einen anderen Push-Dienst erfolgt.

Der Benutzer 11 des mobilen Telekommunikationsgeräts 5 kann hierbei, wie mit der Linie 12 angedeutet, auf die Zutrittskontrollzentrale 1 zugreifen und, wenn er die erforderlichen Zugriffsrechte auf die Zutrittskontrollzentrale 1 aufweist, die Zutrittsberechtigungen verwalten. Wenn es sich bei dem Benutzer 11 nicht um den Administrator handelt, so ist der

ihm auf die Zutrittskontrollzentrale 1 gewährte Zugriff derart gestaltet, dass er lediglich seine eigenen Zutrittsberechtigungen verwalten und gegebenenfalls ändern kann. Der Zugriff auf die Zutrittskontrollzentrale 1 kann beispielsweise über ein Webinterface erfolgen, sodass der Benutzer 11 seine Zutrittsberechtigungen mit Hilfe jedes internetfähigen Computers verwalten kann.

Das in Fig. 2 mit 5 bezeichnete mobile Telekommunikationsgerät kann ein Handy sein, das mit einem NFC-Modul ausgestattet ist. In diesem Fall werden die von der Zutrittskontrollzentrale 1 erhaltenen Zutrittsrechtsdaten dem eingebauten NFC-Modul zur Verfügung gestellt, sodass die Zutrittsrechtsdaten in der Folge über eine NFC-Verbindung an die Schließeinheit 13 übermittelt werden können.

In Fig. 2 ist ein weiteres mobiles Telekommunikationsgerät 14 dargestellt, welches selbst keine Schlüsselfunktion übernimmt. Vielmehr werden die von der Zutrittskontrollzentrale 1 übermittelten Zutrittsrechtsdaten auf einen externen RFID-Transponder 15 überspielt. Der RFID-Transponder 15 kann dann unabhängig von dem mobilen Telekommunikationsgerät 14 verwendet werden, um Schließeinheiten 13 zu sperren.

In Fig. 3 ist ein abgewandeltes Zutrittskontrollsystem dargestellt, bei dem so wie beim System gemäß Fig. 2 eine Zutrittskontrollzentrale 1 über eine beliebige Kommunikationsverbindung, z.B. über das Internet 9, mobile Telekommunikationsvorrichtungen 5 mit Zutrittsrechtsdaten versorgen kann. Dies kann auch über ein SMS-Gateway 10 oder einen anderen Push-Dienst erfolgen. Ein Client-Computer 16 eines Benutzers ist ebenfalls ans Internet 9 angebunden und kann von der Zutrittskontrollzentrale 1 ausgestellte Zutrittsrechtsdaten als

Proxy vermitteln. Der Client-Rechner 16 ist mit einer Schreibeinheit 17 verbunden, die beispielsweise als Schreibgerät für RFID-Tags bzw. Transponder ausgebildet ist. Mit 18 ist ein RFID-Transponder dargestellt, der von der Schreibeinheit 17 beschrieben werden kann.

In Fig. 3 ist nun zusätzlich eine Zertifizierungsstelle 19 in das Zutrittskontrollsystem eingebunden, die mit der Zutrittskontrollzentrale 1 in Verbindung steht. Die Provisionierung der Komponenten im Zutrittskontrollsystem geschieht hierbei wie folgt, wobei dies in der Regel nur einmal erforderlich ist, wenn eine neue Komponente zu dem System hinzugefügt wird. Die Zertifizierungsstelle 19 erstellt ein digitales Zertifikat (entspricht „$cert_{MK}$" in Fig. 5) für das mobile Telekommunikationsgerät 5 bzw. das in diesem angeordnete oder eingebaute Modul, welches die Schlüsselfunktion übernimmt, wie z.B. ein sicheres Element, insbesondere ein Secure Access Module, oder die SIM-Karte des Telekommunikationsgeräts 5. Das Modul wird anhand einer im System eindeutigen ID („ID_{MK}" in Fig. 5) identifiziert. Weiters erstellt die Zertifizierungsstelle 19 ein digitales Zertifikat (entspricht „$cert_L$" in Fig. 5) für ein sicheres Element, insbesondere ein Secure Access Module, der Zutrittskontrollvorrichtung bzw. Schließeinheit 13. Das Modul der Zutrittskontrollvorrichtung 13 wird ebenfalls anhand einer im System eindeutigen ID („ID_L" in Fig. 5) identifiziert.

Das Aufbringen der Zutrittsberechtigungen auf das mobile Telekommunikationsgerät 5 erfolgt wie folgt. Die an das mobile Telekommunikationsgerät 5 zu übertragenden Zutrittsrechtsdaten werden in der Zutrittskontrollzentrale 1 generiert. Die Zutrittsrechtsdaten bestehen z.B. aus einem geheimen zutrittskontrollvorrichtungsindividuellen Schlüssel (entspricht

„LT" in Fig. 5) und einer zeitlichen Berechtigungseinschränkung (entspricht „Calendar" in Fig. 5). Diese zeitliche Berechtigungseinschränkung wird von der Zertifizierungsstelle 19 signiert (siehe „s_c" in Fig. 5), um ihre Authentizität sicherzustellen. Dazu wird die Berechtigungseinschränkung von der Zutrittskontrollzentrale 1 an die Zertifizierungsstelle 19 übertragen, welche dann die signierte Berechtigungseinschränkung an die Zutrittskontrollzentrale 1 zurückliefert. Dort werden dann die individuellen Zutrittsrechtsdaten, die aus dem zutrittskontrollvorrichtungsindividuellen Schlüssel und der von der Zertifizierungsstelle 19 signierten zeitlichen Berechtigungseinschränkung bestehen, zusammengefasst.

Zwischen der Zutrittskontrollzentrale 1 und dem Modul des mobilen Telekommunikationsgeräts 5 wird über das mobile Telekommunikationsgerät 5 eine gesicherte Verbindung mit Hilfe der digitalen Zertifikate, welche bei der Provisionierung aufgebracht wurden, aufgebaut. Das bedeutet, dass das Modul des mobilen Telekommunikationsgeräts 5 und der Zutrittskontrollzentrale 1 gleichsam direkt kommunizieren, das mobile Telekommunikationsgerät 5 dient dabei nur als Vermittler (Proxy).

Über diese gesicherte Verbindung, welche über ein unsicheres Kommunikationsnetzwerk 9 laufen kann, werden die Zutrittskontrolldaten an das mobile Telekommunikationsgerät 5 übertragen und im Modul gesichert abgelegt.

Das Aufbauen der gesicherten Verbindung zwischen der Zutrittskontrollzentrale 1 und dem Modul des mobilen Telekommunikationsgeräts 5 kann auf mehrere Arten erfolgen:

1. SMS: Die Zutrittskontrollzentrale 1 sendet eine SMS über das SMS Gateway 10 an das mobile Telekommunikationsgerät

5, und das mobile Telekommunikationsgerät 5 baut darauf hin die gesicherte Verbindung zur Zutrittskontrollzentrale 1 auf, über welche die Zutrittsrechtsdaten gesichert übertragen werden.

2. Polling: Das mobile Telekommunikationsgerät 5 fragt periodisch die Zutrittskontrollzentrale 1 nach neuen Zutrittsrechtsdaten, die Übertragung erfolgt wie bei 1.
3. Push: Das mobile Telekommunikationsgerät 5 ist an der Zutrittskontrollzentrale 1 dauerhaft registriert (z.B. durch Hinterlegung der IP-Adresse oder Rufnummer) und sendet eine Nachricht an das mobile Telekommunikationsgerät 5, welches daraufhin eine gesicherte Verbindung zur Zutrittskontrollzentrale 1 aufbaut, die Übertragung erfolgt wie bei 1.
4. Der Benutzer startet am mobilen Telekommunikationsgerät 5 eine Applikation, welche die gesicherte Verbindung aufbaut, die Übertragung erfolgt wie bei 1.

In Fig. 4 ist nun der Aufbau der Zutrittskontrollvorrichtung 13 näher erläutert. Die Zutrittskontrollvorrichtung 13 weist einen ungeschützten Bereich 20, z.B. einen Außenbereich, und einen geschützten Bereich 21, z.B. einen Innenbereich, auf. Im ungeschützten Bereich 20 ist die Sende-/Empfangseinheit 22 angeordnet, die z.B. als RFID Lese-/Schreibeinrichtung ausgebildet ist und Daten mit einem in das mobile Telekommunikationsgerät 5 integrierten, passiven RFID Medium oder einer passiven RFID Chipkarte 18 austauschen kann. Die Datenübertragung kann dabei beispielsweise im NFC Card-Emulation-Mode ablaufen. Im geschützten Bereich 21 sind ein Mikrokontroller 23, ein Secure Access Module (SAM) 24, eine Schaltung 25 zum elektromechanischen oder elektrischen Ansteuern eines nicht dargestellten Sperrmittels und eine Hardwareuhr 26 angeordnet. Das Sperrmittel kann hierbei zwischen einer Verriege-

lungsposition und einer Freigabeposition zum wahlweisen Freigeben oder Sperren des Zutritts bewegt werden. Der Mikrokontroller 23 steuert die grundlegenden Funktionen der Zutrittskontrollvorrichtung 13 und verbindet das SAM 24 mit der Sende-/Empfangseinheit 22. Dabei läuft die Kommunikation zwischen dem sicheren Modul des mobilen Telekommunikationsgeräts 5 bzw. der Chipkarte 18 und dem SAM über ISO/IEC 7816-4 Kommandos (APDUs) ab, wobei der Mikrokontroller 23 die Funktion eines APDU-Proxys einnimmt. Unter der Application Protocol Data Unit (APDU) ist hierbei allgemein eine Kommunikationseinheit zwischen einer Chipkarte und einer Chipkartenanwendung (z.B. nach dem ISO/IEC 7816-Standard) zu verstehen. Das SAM 24 enthält die Zutrittskontrolllogik und einen sicheren Speicher, wie dies insbesondere anhand der Beschreibung der Fig. 5 noch nähere erläutert wird. Der Mikrokontroller 23 wirkt mit einem schematisch angedeuteten akustischen und/oder visuellen Signalgeber 27, wie z.B. einem Leuchtring und einem Summer zusammen, um dem Benutzer verschiedene Betriebszustände zu signalisieren.

In Fig. 5 ist nun der grundlegende Ablauf der Kommunikation zwischen dem elektronischen Identifikationsmedium 5, insbesondere dem sicheren Modul des mobilen Telekommunikationsgeräts 5 oder der Chipkarte 18, und dem SAM 24 der Zutrittskontrollvorrichtung 13 dargestellt. Es handelt sich hierbei nicht um das tatsächliche Protokoll, sondern um eine vereinfachte Darstellung der dem Protokoll zugrundeliegenden Prinzipien. Seitens der Zutrittskontrollvorrichtung 13 ist sowohl der Mikrokontroller 23 als auch das SAM in die Kommunikation eingebunden. Auf das sichere Modul des mobilen Telekommunikationsgeräts 5 oder die Chipkarte 18 wird in Fig. 5 mit der Schlüsselbundapplikation 28 Bezug genommen.

Für die vorgesehenen Autorisierungs- und Authentifizierungsfunktionen haben die Zutrittskontrollvorrichtung und das elektronische Identifikationsmedium im Ausgangszustand die folgenden Daten gespeichert:

Identifikationsmedium, nachfolgend auch Mobile Key (MK) genannt:

ID_{MK}: eine eindeutige Identifikation des MK

$cert_{RCA}$: Zertifikat der Zertifizierungsstelle, das den öffentlichen Schlüssel pub_{RCA} der Zertifizierungsstelle enthält

$cert_{MK}$: Zertifikat des MK (enthält unter anderem Identifizierungsdaten des MK und den öffentlichen Schlüssel $pubK_{MK}$ des MK und ist signiert mit dem privaten Schlüssel $priv_{RCA}$ der Zertifizierungsstelle)

$pubK_{MK}$: öffentlicher Schlüssel des MK

$privK_{MK}$: privater Schlüssel des MK

LT: „Lock Token", geheimer zutrittskontrollvorrichtungsindividueller Schlüssel

Calendar: zeitliche Berechtigungseinschränkung

s_C: Signatur der zeitlichen Berechtigungseinschränkung

Ein Datensatz aus LT, Calendar und s_C bildet die Zutrittsrechtsdaten, wobei jeder Datensatz einer Zutrittskontrollvorrichtungsidentifizierung ID_L zugeordnet ist.

Zutrittskontrollvorrichtung, nachfolgend auch Lock (L) genannt:

ID_L: eine eindeutige Identifikation des Lock

$cert_{RCA}$: Zertifikat der Zertifizierungsstelle, das den öffentlichen Schlüssel pub_{RCA} der Zertifizierungsstelle enthält

$cert_L$: Zertifikat des Lock (enthält unter anderem Identifizierungsdaten des Lock und den öffentlichen Schlüssel $pubK_L$ des Lock und ist signiert mit dem privaten Schlüssel $priv_{RCA}$ der Zertifizierungsstelle)

$pubK_L$: öffentlicher Schlüssel des Lock

$privK_L$: privater Schlüssel des Lock

LT: „Lock Token", geheimer zutrittskontrollvorrichtungsindividueller Schlüssel

Das vereinfachte Kommunikationsprotokoll ist nun wie folgt vorgesehen:

Zuerst wird durch die Sende-/Empfangseinheit 22 des Zutrittskontrollvorrichtung ein potentiell im RF-Feld befindlicher, nicht selbst aktiv sendender (passiver) Mobile Key (MK) 28 detektiert, woraufhin die Wake-Up-Sequenz gemäß der verwendeten Norm zur Übertragung (z.B. ISO/IEC 14443-3) durchgeführt wird.

- In Schritt 1 startet die Zutrittskontrollvorrichtung die Kommunikation durch Übermittlung der eindeutigen Zutrittskontrollvorrichtungsidentifizierung ID_L
- In Schritt 2 werden durch die Schlüsselbundapplikation des MK die Zutrittsrechtsdaten bestimmt, welche der im Schritt 1 empfangenen Zutrittskontrollvorrichtungsidentifizierung ID_L zugeordnet sind. Wenn kein ID_L gefunden wird, bedeutet dies, dass der MK nicht berechtigt ist, diese Zutrittskontrollvorrichtung zu betätigen.
- In Schritt 3 wird in der Schlüsselbundapplikation eine Zufallszahl $rand_{MK}$ erzeugt und zwischengespeichert.
- In Schritt 4 werden durch die Schlüsselbundapplikation folgende Daten an das SAM 24 der Zutrittskontrollvorrichtung 13 übermittelt:

- die generierte Zufallszahl $rand_{MK}$
- die eindeutige Identifikation des MK ID_{MK}
- das Zertifikat $cert_{MK}$

• In Schritt 5 wird vom SAM 24 das empfangene Zertifikat $cert_{MK}$ unter Verwendung von pub_{RCA}, welches in $cert_{RCA}$ enthalten ist, überprüft.

• In Schritt 6 werden im SAM 24 der Zutrittskontrollvorrichtung 13 folgende Werte erzeugt:
  - die Zufallszahl $rand_L$
  - die digitale Signatur s_L, die dazu dient, den Besitz des privaten Schlüssels $privK_L$ nachzuweisen: $s_L = sig_{privK_L}(ID_{MK}||rand_{MK}||rand_L)$, wobei die Operation „||" eine Aneinanderreihung von Parametern darstellt.
  - einen aus LT und den Zufallszahlen abgeleiteten Sitzungsschlüssel SK_{ENC}: $SK_{ENC} = deriveEnc_{LT}(rand_{MK}||rand_L)$
  - einen aus LT und den Zufallszahlen abgeleiteten Sitzungsschlüssel SK_{MAC} für ein Message Authentication Codes (MACs): $SK_{MAC} = deriveMac_{LT}(rand_L||rand_{MK})$ (dieser ist von SK_{ENC} verschieden, da die Ableitungsfunktionen (derivation function) Unterscheidungen aufweisen). Die beiden Sitzungsschlüssel dienen der sitzungsspezifischen Absicherung der Kommunikation. Dies umfasst die Integrität, die Authentizität als auch die Vertraulichkeit der nachfolgend übertragenen Daten.
  - ein Kryptogramm c_L wird unter Verwendung des Sitzungsschlüssels SK_{MAC}, ID_L und den Zufallszahlen generiert, welches die Kenntnis des schlossspezifischen Zutrittscodes LT des SAMs 24 der Zutrittskontrollvorrichtung nachweist: $c_L = MACsk_{MAC}(rand_{MK}||rand_L||ID_L)$.

• In Schritt 7 werden durch die Zutrittskontrollvorrichtung 13 folgende Daten an die Schlüsselbundapplikation 28 übermittelt:
  - die generierte Zufallszahl $rand_L$

- das Zertifikat $cert_L$
- die Signatur s_L
- das zutrittskontrollvorrichtungsseitige Kryptogramm c_L

- In Schritt 8 überprüft die Schlüsselbundapplikation 28 das Zertifikat $cert_L$ mit Hilfe von pub_{RCA}, welches im Zertifikat $cert_{RCA}$ enthalten ist.
- In Schritt 9 wird die digitale Signatur s_L mit Hilfe des Zertifikats $cert_L$ überprüft, was deshalb möglich ist, weil die Schlüsselbundapplikation im Besitz von ID_{MK} und der Zufallszahlen ist.
- In Schritt 10 weiß die Schlüsselbundapplikation, dass die Zutrittskontrollvorrichtung im Besitz des Schlüssels $priv_{KL}$ ist, der zum öffentlichen Schlüssel in $cert_L$ gehört, und führt folgende Operationen aus:
  - Erzeugen eines aus LT und den Zufallszahlen abgeleiteten SKENC: SKENC = deriveEncLT (randMK||randL)
  - Erzeugen eines aus LT und den Zufallszahlen abgeleiteten Sitzungsschlüssels SK_{MAC} für einen Message Authentication Code (MAC): SK_{MAC} = $deriveMac_{LT}$ ($rand_L||rand_{MK}$)
  - Überprüfen von c_L durch Erzeugen eines MAC c'_L = $MACsk_{MAC}(rand_{MK}||rand_L||ID_L)$ und Überprüfen, ob $c'_L == c_L$. Wenn die Überprüfung erfolgreich ist, weiß die Schlüsselbundapplikation, dass die Zutrittskontrollvorrichtung LT kennt und dass es unter Verwendung von ID_L kommuniziert.
  - Erzeugen einer digitalen Signatur s_{MK}, die dazu dient, den Besitz des privaten Schlüssels $privK_{MK}$ nachzuweisen: s_{MK} = $sigprivK_{MK}$ ($ID_L||rand_L||rand_{MK}$).
  - Erzeugen eines Kryptogramms c_{MK} unter Verwendung des Sitzungsschlüssels SK_{MAC}, ID_{MK} und der Zufallszahlen: c_{MK} = $MACsk_{MAC}$ ($rand_L||rand_{MK}||ID_{MK}$). Das Kryptogramm c_{MK}

weist der Zutrittskontrollvorrichtung die Kenntnis des schlossspezifischen Zutrittscodes LT nach.

- In Schritt 11 wird nach der Erzeugung von SK_{ENC} und SK_{MAC} auf beiden Seiten ein sicherer Kanal aufgebaut. Die weitere Kommunikation wird mit SK_{ENC} verschlüsselt und mit SK_{MAC} authentifiziert.
- Um den Authentifizierungs- und Autorisierungsvorgang zu beenden, sendet die Schlüsselbundapplikation in Schritt 12 c_{MK}, s_{MK} und das dem ID_L entsprechende Calendar zusammen mit der Signatur S_C zur Zutrittskontrollvorrichtung.
- In Schritt 13 führt die Zutrittskontrollvorrichtung die folgenden Operationen aus:
  - Die Zutrittskontrollvorrichtung überprüft die Signatur s_{MK} mit Hilfe des Zertifikats $cert_{MK}$, das es zuvor erhalten hat, und weiß dann, dass die Schlüsselbundapplikation im Besitz des privaten Schlüssels $privK_{MK}$ ist, der zum öffentlichen Schlüssel $pubK_{MK}$ in $cert_{MK}$ gehört. Mit diesem Schritt hat die Zutrittskontrollvorrichtung die Schlüsselbundapplikation erfolgreich authentifiziert.
  - Die Zutrittskontrollvorrichtung überprüft c_{MK}, indem es einen MAC $c'_{MK} = MACsk_{MAC}(rand_L||rand_{MK}||ID_{MK})$ erzeugt und prüft, ob $c'_{MK} == c_{MK}$. Wenn die Überprüfung erfolgreich ist, weiß die Zutrittskontrollvorrichtung, dass die Schlüsselbundapplikation LT kennt und dass es authentisch mit MK kommuniziert.
  - Die Zutrittskontrollvorrichtung überprüft Calendar mit Hilfe von s_C und dem Zertifikat $cert_{RCA}$ und überprüft, ob die Schlüsselbundapplikation nun autorisiert ist. Wenn die Autorisierung festgestellt wurde, wurde die Schlüsselbundapplikation erfolgreich dahingehend autorisiert, dass sie die Zutrittskontrollvorrichtung betätigen darf.

- Um das Protokoll in Schritt 14 abzuschließen, werden Statusdaten von der Zutrittskontrollvorrichtung an die Schlüsselbundapplikation übermittelt und es werden Blacklist-Einträge für ID_L, sofern vorhanden, an die Zutrittskontrollvorrichtung übermittelt und dort gespeichert.
- Wenn alle Schritte erfolgreich abgeschlossen wurden, kann die Zutrittskontrollvorrichtung in Schritt 15 das Schloss betätigen und die Kommunikation mit der Schlüsselbundapplikation beenden.

Patentansprüche

1. Verfahren zur Zutrittskontrolle insbesondere in Gebäuden, bei dem eine bidirektionale Datenübermittlung zwischen einem elektronischen Identifikationsmedium und einer Zutrittskontrollvorrichtung und eine Datenverarbeitung stattfindet, wobei die Datenübermittlung die Übermittlung von Zutrittsrechtsdaten vom elektronischen Identifikationsmedium an die Zutrittskontrollvorrichtung umfasst, wobei die Zutrittsrechtsdaten in der Zutrittskontrollvorrichtung zur Feststellung der Zutrittsberechtigung ausgewertet werden und in Abhängigkeit von der festgestellten Zutrittsberechtigung ein Sperrmittel zum wahlweisen Freigeben oder Sperren des Zutritts angesteuert wird, dadurch gekennzeichnet, dass die Datenverarbeitung eine Authentifizierung des elektronischen Identifikationsmediums auf Grundlage wenigstens eines digitalen Zertifikats umfasst und die Datenübermittlung die Verwendung eines Schlüsselaustausch- oder -ableitungsprotokolls umfasst, 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 dass die Zutrittsrechtsdaten über den sicheren Kanal vom elektronischen Identifikationsmedium an die Zutrittskontrollvorrichtung übermittelt werden.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass das wenigstens eine digitale Zertifikat von einer Zutrittskontrollzentrale signiert wird.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass der wenigstens eine Sitzungsschlüssel im elektronischen Identifikationsmedium und in der Zutrittskontrollvorrichtung auf Grundlage eines zutrittskontrollvorrichtungsindividuellen Zutrittscodes erzeugt wird, 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.

4. Verfahren nach Anspruch 1, 2 oder 3, dadurch gekennzeichnet, dass das Schlüsselaustausch- der -ableitungsprotokoll die Generierung eines Kryptogramms unter Verwendung des Sitzungsschlüssels in der Zutrittskontrollvorrichtung und die Übersendung desselben an das Identifikationsmediums umfasst, wobei das Kryptogramm im Identifikationsmedium unter Verwendung des Sitzungsschlüssels verifiziert wird.

5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass die Zutrittsrechtsdaten von einer Zutrittskontrollzentrale signiert und gemeinsam mit der Signatur über den sicheren Kanal vom elektronischen Identifikationsmedium an die Zutrittskontrollvorrichtung übermittelt werden.

6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass die Datenübermittlung rein passiv durch Belastung des elektromagnetischen Feldes zwischen dem elektronischen Identifikationsmedium und der Zutrittskontrollvorrichtung erfolgt.

7. Vorrichtung, insbesondere zur Durchführung des Verfahrens nach einem der Ansprüche 1 bis 6, umfassend eine Zutrittskontrollvorrichtung mit einem Sperrmittel zum wahlweisen Freigeben oder Sperren des Zutritts und einer Sende-/Empfangseinrichtung, um eine bidirektionale Datenübermittlung zwischen einem elektronischen Identifikationsmedium und der Zutrittskontrollvorrichtung zu ermöglichen, wobei die Zutrittskontrollvorrichtung Datenverarbeitungsmittel zur Steuerung der Datenübermittlung und zur Feststellung der Zutrittsberechtigung auf Grund von empfangenen Zutrittsrechtsdaten aufweist und die Datenverarbeitungsmittel mit dem Sperrmittel zum wahlweisen Freigeben oder Sperren des Zutritts zusammenwirken, dadurch gekennzeichnet, dass die Datenverarbeitungsmittel wenigstens einen Mikrokontroller und ein Secure Access Module (SAM) umfassen, wobei das SAM zur Ausführung kryptographischer Funktionen eingerichtet ist, und dass die Sende-/Empfangseinrichtung in einem ersten Bereich der Zutrittskontrollvorrichtung und das SAM in einem zweiten Bereich der Zutrittskontrollvorrichtung angeordnet ist.

8. Vorrichtung nach Anspruch 7, dadurch gekennzeichnet, dass der Mikrokontroller im zweiten Bereich angeordnet ist.

9. Vorrichtung nach Anspruch 7 oder 8, dadurch gekennzeichnet, dass der Mikrokontroller die Sende-/Empfangseinrichtung mit dem SAM verbindet.

10. Vorrichtung nach Anspruch 7, 8 oder 9, dadurch gekennzeichnet, dass der erste Bereich ein ungeschützter Bereich und der zweite Bereich ein baulich geschützter Bereich ist.

11. Vorrichtung nach einem der Ansprüche 7 bis 10, dadurch gekennzeichnet, dass die Zutrittskontrollvorrichtung zum Ein-

bau in eine Tür ausgebildet ist und mit wenigstens einer ersten Handhabe, wie z.B. einem Knauf oder einem Drücker, versehen ist, wobei der erste Bereich von der ersten Handhabe und der zweite Bereich von einem zur Aufnahme in einer Durchbrechung des Türblattes vorgesehenen Bereich oder einer zweiten, der ersten Handhabe gegenüberliegenden, zweiten Handhabe gebildet ist.

12. Vorrichtung nach einem der Ansprüche 7 bis 11, dadurch gekennzeichnet, dass das SAM Authentifizierungsmittel umfasst, um das elektronische Identifikationsmedium auf Grundlage wenigstens eines digitalen Zertifikats zu authentifizieren, und mit einem Schlüsselaustausch-
der -ableitungsprotokoll programmiert ist.

13. Vorrichtung nach einem der Ansprüche 7 bis 12, dadurch gekennzeichnet, dass das SAM zur Einrichtung eines sicheren Übertragungskanals zwischen dem elektronischen Identifikationsmedium und der Zutrittskontrollvorrichtung ausgebildet oder programmiert ist.

14. Vorrichtung nach einem der Ansprüche 7 bis 13, dadurch gekennzeichnet, dass das SAM eine Auswerteschaltung zur Feststellung der Zutrittsberechtigung auf Grund der empfangenen Zutrittsrechtsdaten umfasst.

15. Vorrichtung nach einem der Ansprüche 7 bis 14, dadurch gekennzeichnet, dass das SAM als Mikrokontroller in Chipkarten- oder SIM-Karten-Bauform, insbesondere aber in IC-Bauform ausgebildet ist.

16. Vorrichtung nach einem der Ansprüche 7 bis 15, dadurch gekennzeichnet, dass das SAM austauschbar in einer Schnittstelle, insbesondere in einem Steckplatz aufgenommen ist.

17. Vorrichtung nach einem der Ansprüche 7 bis 16, dadurch gekennzeichnet, dass die Sende-/Empfangseinrichtung für die drahtlose, bevorzugt induktive Datenübertragung insbesondere nach dem NFC- bzw. RFID-Standard (ISO/IEC 14443) ausgebildet ist.

Wien, am 31.1.2012

Anmelder
durch:

Haffner und Keschmann
Patentanwälte OG

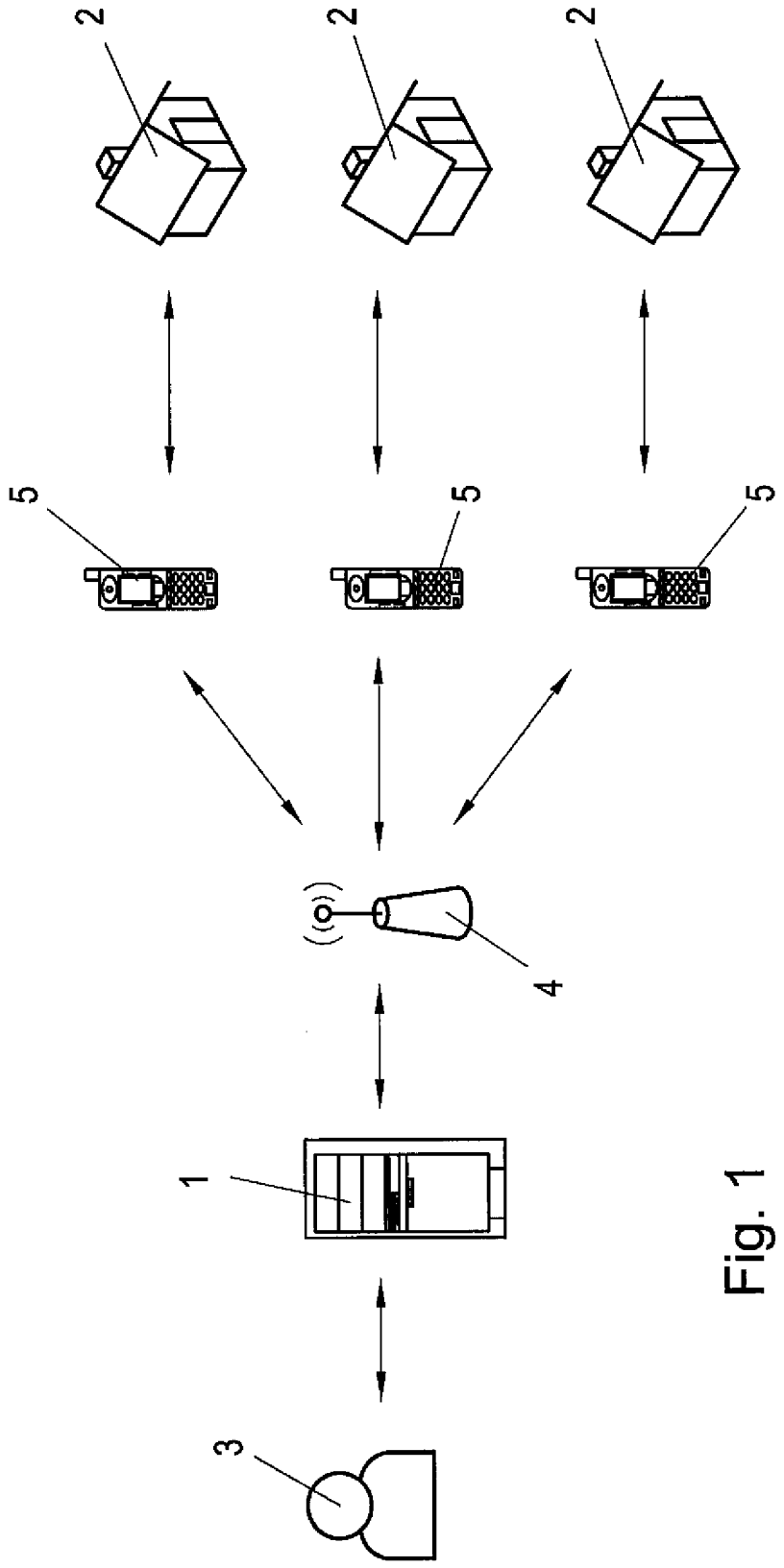
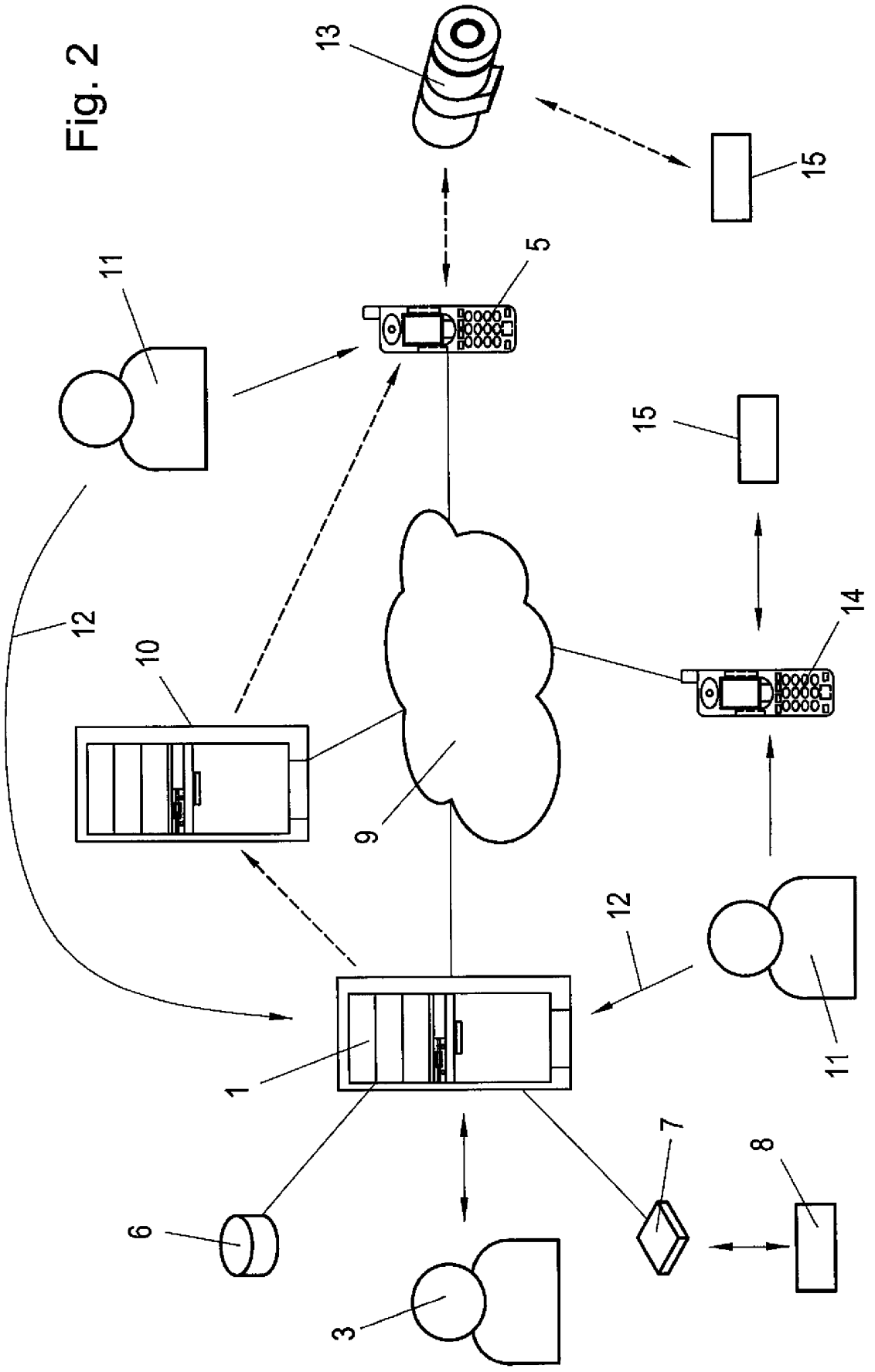


Fig. 1

Fig. 2



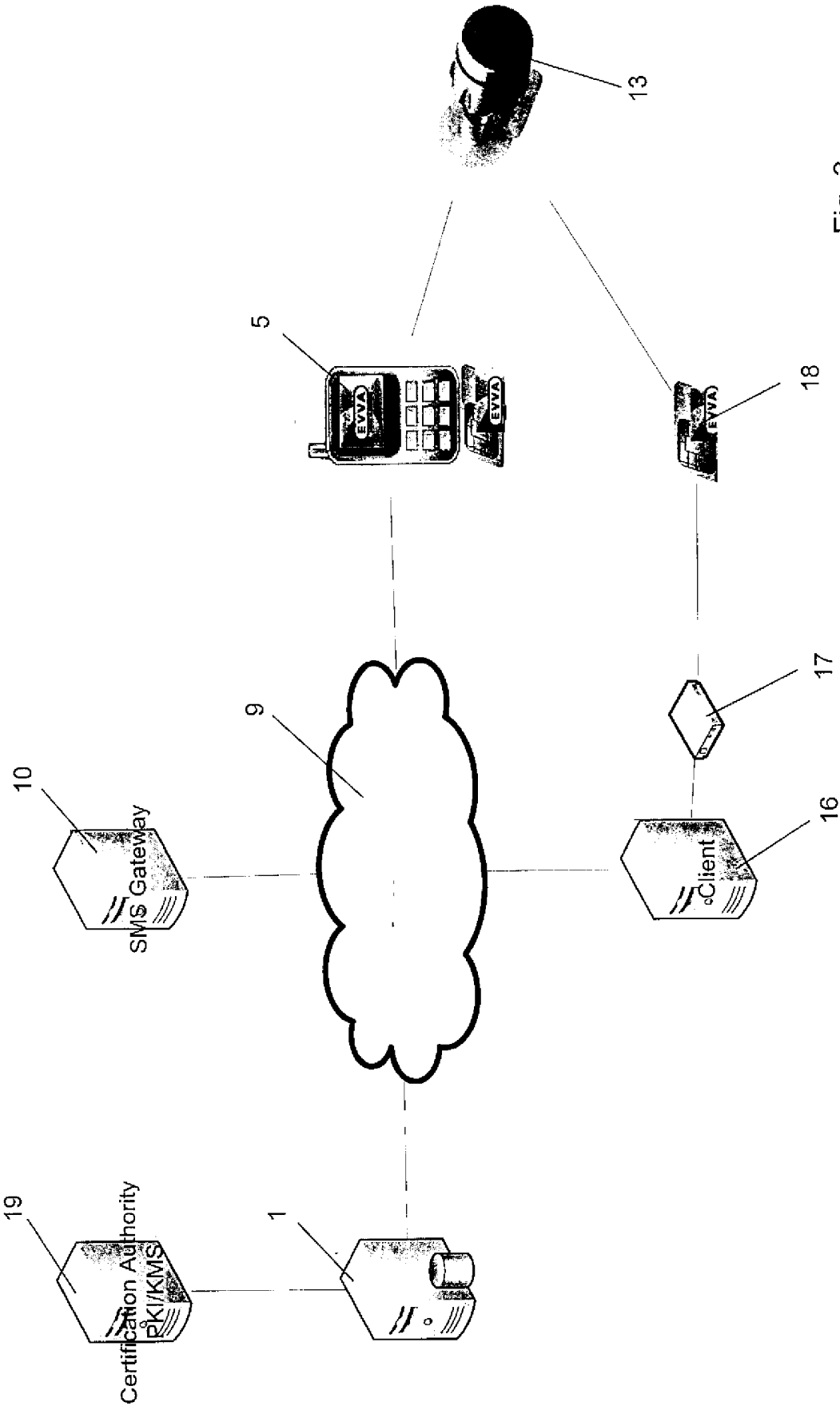

13
5
18
9
17
10
SMS Gateway
Client
16
19
Certification Authority
PKI/KMS
1

Fig. 3

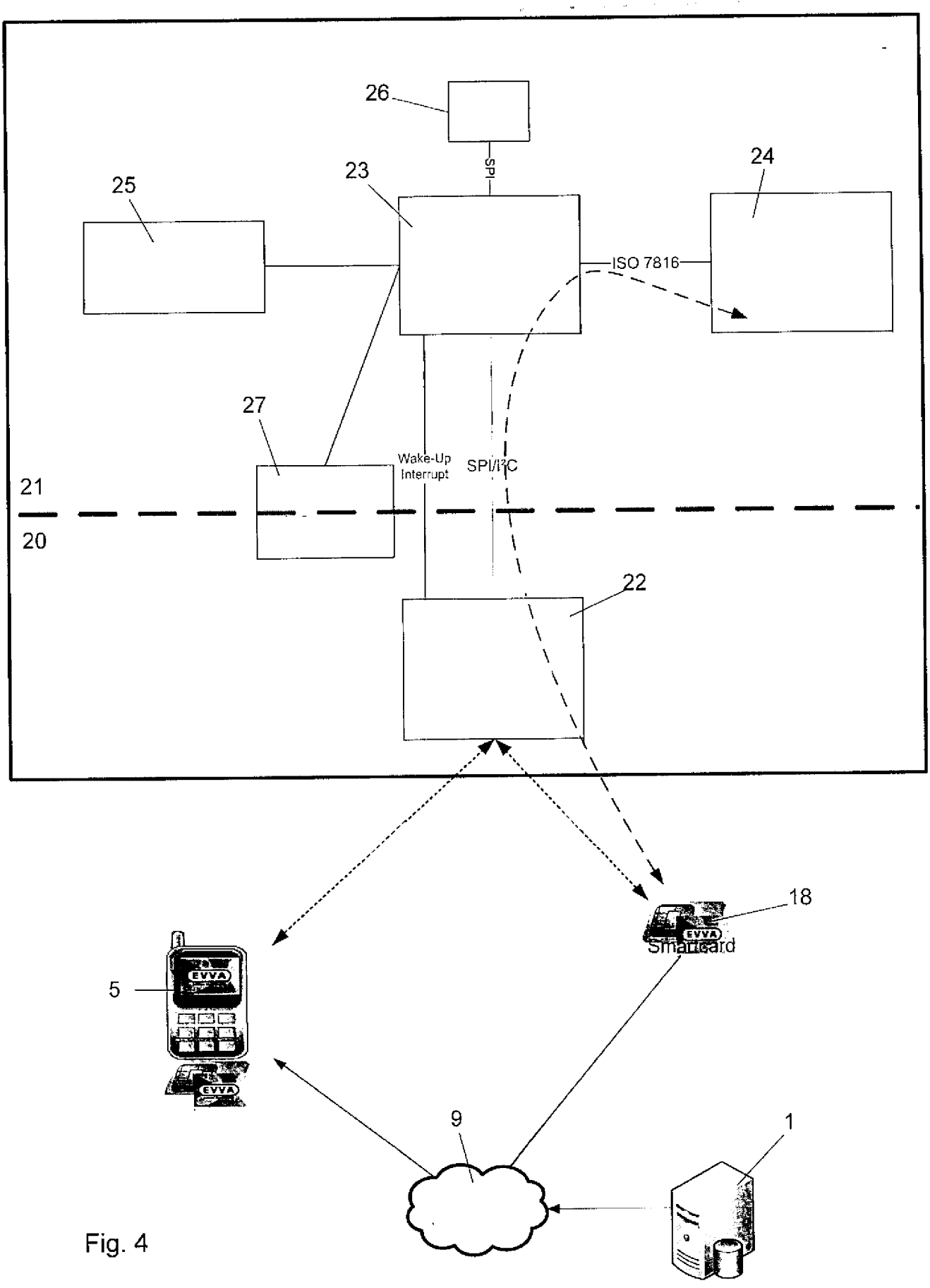

26
SPI
23
24
25
ISO 7816
27
Wake-Up
Interrupt
SPI/I²C
21
20
22
18
EVVA
Smartcard
5
EVVA
EVVA
9
1

Fig. 4

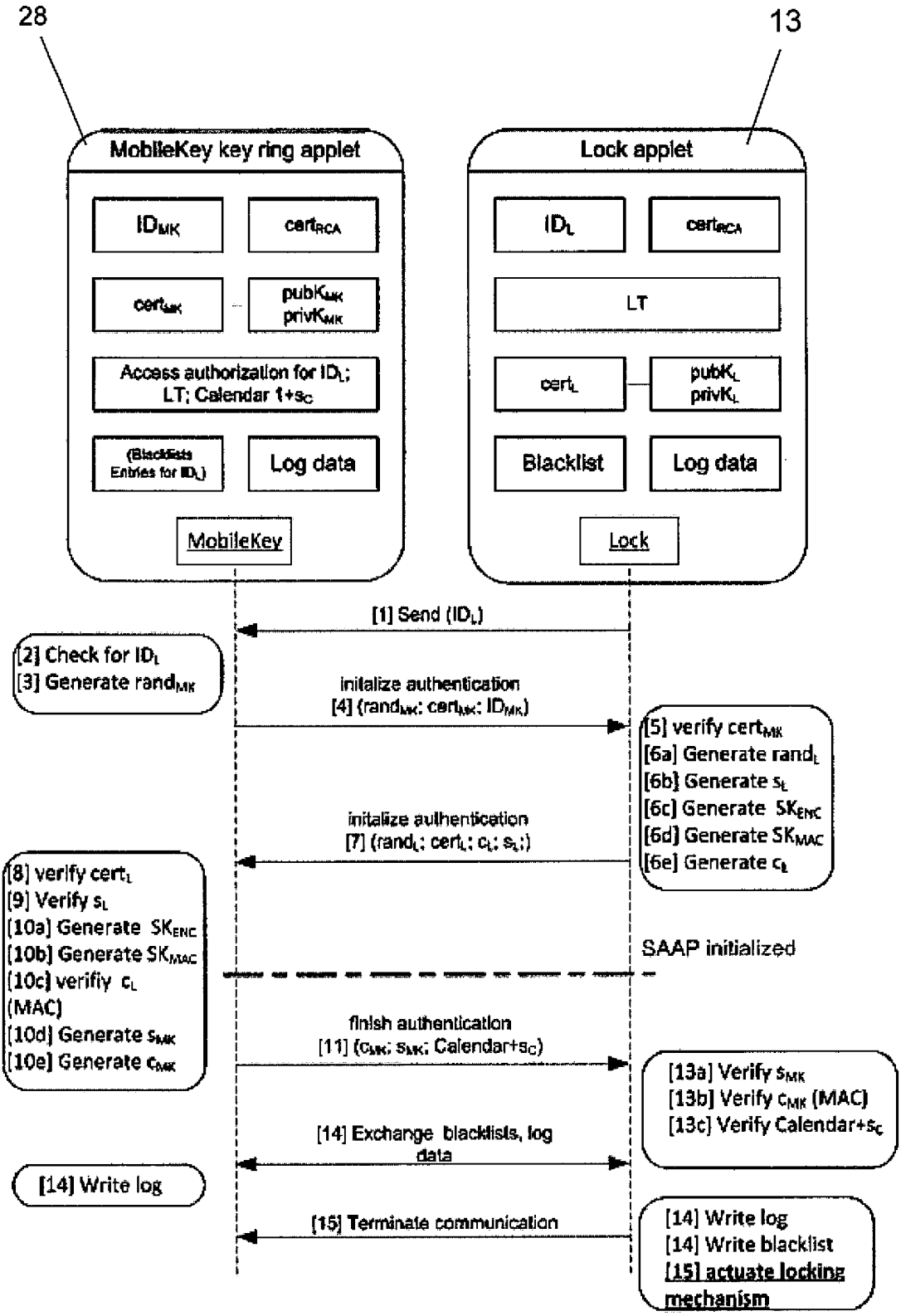

28
13
MobileKey key ring applet
Lock applet
ID_{MK}
$cert_{RCA}$
$cert_{MK}$
$pubK_{MK}$ $privK_{MK}$
Access authorization for ID_L; LT; Calendar $t+s_C$
(Blacklists Entries for ID_L)
Log data
MobileKey
ID_L
$cert_{RCA}$
LT
$cert_L$
$pubK_L$ $privK_L$
Blacklist
Log data
Lock
[1] Send (ID_L)
[2] Check for ID_L
[3] Generate $rand_{MK}$
initalize authentication
[4] ($rand_{MK}$; $cert_{MK}$; ID_{MK})
[5] verify $cert_{MK}$
[6a] Generate $rand_L$
[6b] Generate s_L
[6c] Generate SK_{ENC}
[6d] Generate SK_{MAC}
[6e] Generate c_L
initalize authentication
[7] ($rand_L$; $cert_L$; c_L; s_L;)
[8] verify $cert_L$
[9] Verify s_L
[10a] Generate SK_{ENC}
[10b] Generate SK_{MAC}
[10c] verifiy c_L (MAC)
[10d] Generate s_{MK}
[10e] Generate c_{MK}
SAAP initialized
finish authentication
[11] (c_{MK}; s_{MK}; Calendar+s_C)
[13a] Verify s_{MK}
[13b] Verify c_{MK} (MAC)
[13c] Verify Calendar+s_C
[14] Exchange blacklists, log data
[14] Write log
[15] Terminate communication
[14] Write log
[14] Write blacklist
[15] actuate locking mechanism

Fig. 5

Recherchenbericht zu **A 132/2012**

österreichisches patentamt

Klassifikation des Anmeldungsgegenstands gemäß IPC: ***G07C 9/00*** (2006.01); ***H04L 9/00*** (2006.01)
Klassifikation des Anmeldungsgegenstands gemäß ECLA: G07C 9/00B; H04L 9/00
Recherchierter Prüfstoff (Klassifikation): G07C, H04L
Konsultierte Online-Datenbank: EPODOC, WPI
Dieser Recherchenbericht wurde zu den am 31. Jänner 2012 eingereichten Ansprüchen 1 - 17 erstellt.

Kategorie*)	Bezeichnung der Veröffentlichung: Ländercode, Veröffentlichungsnummer, Dokumentart (Anmelder), Veröffentlichungsdatum, Textstelle oder Figur soweit erforderlich	Betreffend Anspruch
X	US 2005060555 A1 (RAGHUNATH MANDAYAM THONDANUR et al.) 17. März 2005 (17.03.2005) Zusammenfassung; Absätze 8 - 10; Anspruch 1, 4	1 - 6
X	WO 199630857 A1 (CYBERMARK, INC.) 03. Oktober 1996 (03.10.1996) Zusammenfassung; Seite 20, Zeile 14 - 27;	1 - 17
X	EP 1549020 A2 (ACTIVCARD INC.) 29. Juni 2005 (29.06.2005) Zusammenfassung; Absätze 13 - 15, 18	1 - 17
X	EP 2063400 A1 (GEMALTO SA) 27. Mai 2009 (27.05.2009) Zusammenfassung; Absatz 2;	1 - 17
A	WO 2003088564 A1 (SCM MICROSYSTEMS GMBH) 23. Oktober 2003 (23.10.2003) Zusammenfassung; Seite 1, Zeile 10 - Seite 2, Zeile 12	1 - 17

Datum der Beendigung der Recherche:	☐ Fortsetzung siehe Folgeblatt	Prüfer(in):
19. Dezember 2012		ENGLISCH M.

*) **Kategorien** der angeführten Dokumente:

- **X** Veröffentlichung **von besonderer Bedeutung**: der Anmeldungsgegenstand kann allein aufgrund dieser Druckschrift nicht als neu bzw. auf erfinderischer Tätigkeit beruhend betrachtet werden.
- **Y** Veröffentlichung **von Bedeutung**: der Anmeldungsgegenstand kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren weiteren Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese **Verbindung für einen Fachmann naheliegend** ist.
- **A** Veröffentlichung, die den **allgemeinen Stand der Technik** definiert.
- **P** Dokument, das **von Bedeutung** ist (Kategorien **X** oder **Y**), jedoch **nach dem Prioritätstag** der Anmeldung **veröffentlicht** wurde.
- **E** Dokument, das **von besonderer Bedeutung** ist (Kategorie **X**), aus dem ein **älteres Recht** hervorgehen könnte (früheres Anmeldedatum, jedoch nachveröffentlicht, Schutz ist in Österreich möglich, würde Neuheit in Frage stellen).
- **&** Veröffentlichung, die Mitglied der selben **Patentfamilie** ist.