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

(11) **EP 2 387 007 A1**

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
16.11.2011 Patentblatt 2011/46

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

(21) Anmeldenummer: **10075200.5**

(22) Anmeldetag: **14.05.2010**

(84) Benannte Vertragsstaaten:
AL 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 SM TR
Benannte Erstreckungsstaaten:
BA ME RS

(71) Anmelder: **Deutsche Telekom AG**
53113 Bonn (DE)

(72) Erfinder:
- **Ren, Zhiyun**
  DE-12357 Berlin (DE)
- **Heuer, Jörg**
  DE-14163 Berlin (DE)
- **Yin, Ming**
  DE-12203 Berlin (DE)
- **Kulbach, Moritz**
  DE-10551 Berlin (DE)
- **Steffens, Ernst-Joachim**
  DE-13089 Berlin (DE)
- **Hofmann, Klaus-Peter**
  DE-12205 Berlin (DE)

(74) Vertreter: **Drosch, Ulrich**
Patentanwalt
Behringstrasse 43
14482 Potsdam (DE)

(54) Verfahren und System zur Zugangskontrolle

(57) Gemäß der vorgeschlagenen Lösung für eine Zugangskontrolle wird zur Authentifizierung einer Zugang zu einem zugangskontrollierten Bereich (1) begehrenden Person (3) ein von der betreffenden Person (3) mitgeführtes Mobilfunkgerät (5) verwendet. Das Mobilfunkgerät (5) überträgt einen in ihm, vorzugsweise auf einer UICC in Form seiner SIM-Karte gehaltenen personalisierten Zugangscode zusammen mit einer den zugangskontrollierten Bereich (1) identifizierenden ID (Bereichs-ID), welche zuvor von einem passiven, an dem Bereich (1) angeordneten Tag (6), vorzugsweise durch funkgestützte Nahbereichsübertragung, ausgelesen und in das Mobilfunkgerät (5) übernommen wurde, an einen über mindestens ein öffentliches Netz (8), vorzugsweise ein Mobilfunknetz, zugänglichen Server (7) einer Zugangskontrolleinrichtung (2). Hier, demnach entfernter Stelle, erfolgt die Überprüfung der Authentifizierungsdaten der Person (3) und ihrer Berechtigung für einen Zugang zu dem durch die Bereichs-ID gekennzeichneten Bereich (1). Ist eine solche Berechtigung gegeben, wird von der Zugangskontrolleinrichtung (2) durch Fernbetätigung eines entsprechenden Aktors eine den zugangskontrollierten Bereich (1) verschließende Sicherheitseinrichtung (4) entsperrt.

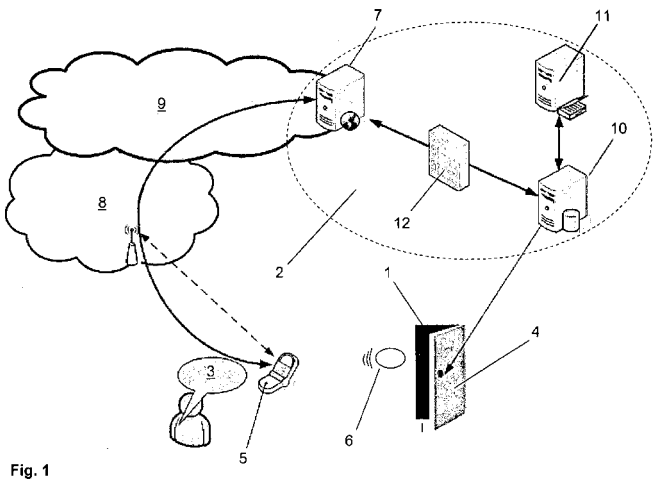

Fig. 1

EP 2 387 007 A1

Beschreibung

[0001] Die Erfindung betrifft eine Lösung zur Kontrolle des Zugangs zu einem durch eine Sicherungseinrichtung verschlossenen Bereich. Sie bezieht sich auf ein entsprechendes Verfahren und ein zur Durchführung des Verfahrens ausgebildetes Zugangskontrollsystem.

[0002] Bei dem hinsichtlich des Zugangs kontrollierten beziehungsweise zu kontrollierenden Bereich handelt es sich entsprechend einer bevorzugten Ausbildung der Erfindung um einen Raum, beispielsweise in einem Gebäude, welcher durch eine die Sicherungseinrichtung ausbildende Tür verschlossen ist. Auch wenn sich die nachfolgenden Darstellungen im Allgemeinen auf eine solche Ausbildungsform beziehen, ist jedoch die Erfindung hierauf nicht beschränkt. Vielmehr kommt die Anwendung des erfindungsgemäßen Prinzips, beispielsweise auch für die Zugangskontrolle bei entsprechend gesicherten Schließfächern oder anderen vergleichbaren Einrichtungen, in Betracht. Insoweit ist der Begriff des Zugangs gemäß dem allgemeinen Prinzip der vorgestellten Lösung nicht ausschließlich im Sinne des Betretens eines Raumes zu verstehen, sondern bezieht sich grundsätzlich auf die Möglichkeit, dass eine hierzu berechtigte Person mindestens einen Körperteil oder, im Falle des Raumes, ihren gesamten Körper in einen dafür zunächst freizugebenden Bereich hineinbewegen kann.

[0003] In modernen Bürogebäuden, beispielsweise von Entwicklungs- und/oder Forschungseinrichtungen, ist es vielfach üblich, den Zugang zu besonders sensiblen Bereichen beziehungsweise zu bestimmten Räumen zu kontrollieren. Dabei ist es durchaus üblich, dass nicht alle Mitarbeiter einer entsprechenden Firma Zugang zu derartig sensiblen Bereichen haben. Darüber hinaus ist selbstverständlich insbesondere betriebsfremden Personen der Zugang zu diesen Bereichen verwehrt. Die hierzu berechtigen Personen müssen sich zum Erhalt des Zugangs gegenüber einem Zugangskontrollsystem authentifizieren und ihre Berechtigung für den Zugang nachweisen. Hierfür sind unterschiedliche Lösungen gebräuchlich.

[0004] Einfache Lösungen basieren darauf, dass beispielsweise ein entsprechender Raum durch eine Tür mit einem elektronischen Schloss gesichert ist, an welcher eine Tastatur zur Eingabe eines den Zutritt ermöglichenden Zugangscodes angebracht ist. Derartige Lösungen weisen jedoch mehrere Nachteile auf. Zum einen können außenstehende, nicht berechtigte Personen aus Gebrauchsspuren, welche an den zur Eingabe des korrekten Codes zu betätigenden Tasten entstehen, möglicherweise auf den Zugangscode schließen. Andererseits muss im Falle dessen, dass einer Person die Berechtigung für den Zugang entzogen wird oder sie das Unternehmen verlässt, gegebenenfalls der Zugangscode verändert werden, um zu verhindern, dass der betreffenden Person weiterhin der Zugang zu dem entsprechenden Bereich möglich ist.

[0005] Insoweit günstiger und sicherer ist die Zugangskontrolle unter Verwendung spezieller Zugangskarten. Hierbei müssen zum Zugang berechtigte Personen, sofern sie Zugang zu dem entsprechenden Bereich begehren, beispielsweise eine mit einem Magnetstreifen ausgestattete Zugangskarte als Token mit sich führen. Zum Erhalt des Zugangs ist die entsprechende Karte durch einen im Bereich der Tür angeordneten Kartenleser zu ziehen. Ergibt sich aus den auf dem Magnetstreifen der Karte gespeicherten Daten, dass die betreffende Person für den Zugang zu dem Bereich berechtigt ist, wird die diesen verschließende Sicherungseinrichtung nach dem Auslesen der Kartendaten und deren Überprüfung durch einen dementsprechend angesteuerten Aktor eines elektronischen Türschlosses freigegeben.

[0006] Noch günstiger und ebenfalls gebräuchlich sind kontaktlose Chipkarten. Zum Erhalt des Zugangs ist die entsprechende Chipkarte von einer sie mitführenden Person in den Nahbereich eines vorzugsweise ebenfalls in der Nähe oder an der Tür angeordneten Lesegeräts zu halten. Der Datenaustausch zwischen diesem Lesegerät und der kontaktlosen Chipkarte erfolgt hierbei über Funk unter Einsatz der so genannten Nahbereichskommunikation beziehungsweise Near-Field-Communication (NFC). Das Lesegerät an der Tür des zugangskontrollierten Bereichs und die kontaktlose Chipkarte sind dazu mit entsprechenden NFC-Schnittstellen, also Funksende- und Empfangseinheiten ausgestattet. Über die entsprechende Schnittstelle wird durch die Chipkarte ein personalisierter Zugangscode zu dem Lesegerät am zugangskontrollierten Bereich übertragen. Durch eine dem Lesegerät nachgeschaltete Auswerteelektronik wird der von diesem empfangene Zugangscode überprüft und im Wege des Vergleichs mit entsprechenden Datenbankeinträgen festgestellt, ob für die betreffende, sich mit diesem Zugangscode authentifizierende Person eine Berechtigung für den Zugang zu dem entsprechenden Bereich vorliegt. Ist dies gegeben, wird die den Bereich verschließende Sicherungseinrichtung, also beispielsweise eine Tür mit elektronischem Türschloss, freigegeben und damit der betreffenden Person der Zugang ermöglicht. Als Nachteil dieser Lösungen ist es anzusehen, dass sie einen zumeist nicht unbeträchtlichen Hardware-Aufwand erfordern. Dies gilt insbesondere dann, wenn beispielsweise innerhalb eines Bürokomplexes mehrere verschiedene Räume unter Einsatz einer entsprechenden- Lösung bezüglich des Zugangs kontrolliert werden sollen. Selbst wenn beispielsweise die Auswertung der Zugangsdaten von Personen, welche Zugang zu einem der entsprechenden Räume begehren, an zentraler Stelle erfolgt, so ist es doch zumindest erforderlich, an jedem zugangskontrollierten Raum ein entsprechendes Lesegerät mit einer NFC-Schnittstelle vorzusehen. Aus Sicherheitsgründen erfordern entsprechende Systeme zudem häufig noch die Eingabe eines weiteren Sicherheitsbeziehungsweise Authentisierungsmerkmals. Soweit dabei eine Zugang begehrende Person, wie in der Praxis gebräuchlich, ein solches Merkmal, beispielsweise in Form einer PIN, über einen Touchscreen eingeben

muss, erhöht sich dementsprechend der Hardware-Aufwand noch weiter. Als nachteilig kann es außerdem angesehen werden, dass jede den Zugang zu einem zugangskontrollierten Bereich begehrende Person gemäß der zuvor dargestellten Lösung stets ein gesondertes Token in Form der genannten Chipkarte mit sich führen muss.

[0007] Der letztgenannte Nachteil hat im Hinblick darauf, dass sich der Grad der Penetration der Bevölkerung mit Mobilfunkgeräten in den letzten Jahren sehr stark erhöht hat und heutzutage fast jeder ein entsprechendes Gerät nahezu ständig bei sich trägt, zu der Überlegung geführt, als Token für die Authentifizierung gegenüber Zugangskontrolleinrichtungen Mobilfunkgeräte beziehungsweise in diesen angeordnete Smartkarten zu verwenden. Bei den bekannt gewordenen Lösungen dieser Art verhält sich die als Token in dem Mobilfunkgerät angeordnete Smartkarte wie eine passive Zugangskarte. Über eine in dem Mobilfunkgerät ausgebildete NFC-Schnittstelle wird ein auf dieser passiven Zugangskarte gespeicherter Code zu einer ebenfalls mit einer NFC-Schnittstelle ausgestatteten Einheit an den zugangskontrollierten Bereich übermittelt und von einer nachgeschaltete Elektronik überprüft. Demnach müssen zur Einführung einer derartigen Zugangskontrolle beispielsweise die Türen entsprechend kontrollierter Räume mit einem solchen Lesegerät oder NFCfähigen Türschildern ausgestattet werden. Dies führt wiederum zu vergleichsweise hohen Investitionskosten.

[0008] Aufgabe der Erfindung ist es, eine alternative Lösung für die Zugangskontrolle bereitzustellen, durch welche gegenüber dem Stand der Technik geringere Investitionskosten entstehen und welche darüber hinaus zu einer erhöhten Flexibilität bei der Einrichtung von unter Einsatz der entsprechenden Lösung bezüglich des Zugangs zu kontrollierenden Bereichen führt. Hierzu sind ein Verfahren und ein zur Durchführung des Verfahrens geeignetes Zugangskontrollsystem anzugeben.

[0009] Die Aufgabe wird durch ein Verfahren mit den Merkmalen des Patentanspruchs 1 gelöst. Ein die Aufgabe lösendes Zugangskontrollsystem ist durch den ersten Sachanspruch charakterisiert. Vorteilhafte Aus- und Weiterbildungen der Erfindung sind durch die Unteransprüche gegeben.

Der grundsätzliche, dem zur Lösung der Aufgabe vorgeschlagenen Verfahren zugrunde liegende Ablauf ist im Wesentlichen bekannt. Danach authentifiziert sich eine den Zugang zu einem durch eine Sicherungseinrichtung verschlossenen Bereich begehrende Person zunächst gegenüber einer Zugangskontrolleinrichtung. Nach erfolgreicher Authentifizierung wird durch die vorgenannte Zugangskontrolleinrichtung das Bestehen einer Zugangsberechtigung für den genannten Bereich für die den Zugang begehrende Person geprüft. Im Falle des Bestehens einer solchen Zugangsberechtigung wird die den zugangskontrollierten Bereich verschließende Sicherungseinrichtung von der Zugangskontrolleinrichtung durch Betätigung eines Aktors entsperrt und damit der als berechtigt erkannten Person der Zugang zu dem betreffenden Bereich ermöglicht. Entsprechend dem vorgeschlagenen Verfahren verwendet die den Zugang zu dem zugangskontrollierten Bereich begehrende Person zur Authentifizierung gegenüber der Zugangskontrolleinrichtung ein von ihr mitgeführtes Mobilfunkgerät, in welchem, vorzugsweise auf einer entsprechenden, von dem Mobilfunkgerät aufgenommenen Smartkarte, ein personalisierter Zugangscode abgelegt ist.

Erfindungsgemäß wird jedoch der vorgenannte personalisierte Zugangscode zur Authentifizierung der Person nicht, wie aus dem Stand der Technik bekannt, an eine Leseeinrichtung des zugangskontrollierten Bereichs übertragen und dort von einer nachgeordneten Einheit ausgewertet. Der entsprechende Zugangscode wird vielmehr zusammen mit einer die Prüfung der Zugangsberechtigung ermöglichenden, den bezüglich des Zugangs kontrollierten Bereich identifizierenden ID von dem Mobilfunkgerät zur Prüfung über ein öffentliches Netz, vorzugsweise über ein Mobilfunknetz an einen Server der Zugangskontrolleinrichtung übermittelt. Die Entgegennahme des die den Zugang begehrende Person authentifizierenden Zugangscodes erfolgt demnach an zentraler Stelle durch einen über ein öffentliches Netz zugänglichen Server der Zugangskontrolleinrichtung. Die mit dem personalisierten Zugangscode zusammen übertragene ID des zugangskontrollierten Bereichs wird zuvor von einem an dem betreffenden Bereich angeordneten, ihn kennzeichnenden Tag ausgelesen und in das diese ID (im Weiteren auch Bereichs-ID) zusammen mit dem personalisierten Zugangscode an den vorgenannten Server übertragende Mobilfunkgerät übernommen. Dieser an dem zugangskontrollierten Bereich angeordnete Tag ist dabei, anders als die Leseeinrichtungen nach dem Stand der Technik, lediglich ein passives, von dem dazu ausgebildeten Mobilfunkgerät auszulesendes Element. Andererseits stellt das von der den Zugang wünschenden Person als Token verwendete Mobilfunkgerät beziehungsweise die dafür von diesem vorzugsweise aufgenommene Smartkarte abweichend von den Lösungen des Standes der Technik nicht nur ein passives Authentifizierungsmerkmal dar, sondern steuert aktiv den Prozess der Authentifizierung und der Überprüfung des Bestehens einer Zugangsberechtigung der betreffenden Person. Wie bereits ausgeführt, wird, sofern die Prüfung die Berechtigung einer den Zugang zu dem zugangskontrollierten Bereich begehrenden Person bestätigt, die Sicherungseinrichtung des betreffenden Bereichs mittels eines Aktors entsperrt. Der betreffende Aktor wird dabei erfindungsgemäß durch die Zugangskontrolleinrichtung fernbetätigt.

Bei einer besonders praxisrelevanten Ausbildung der Erfindung wird nach dem zuvor beschriebenen Verfahren der Zugang zu einem Raum kontrolliert, welcher durch eine mit einem elektronischen Schloss versehene, als Sicherungseinrichtung fungierende Tür verschlossen ist. Dabei ist der den Raum als zugangskontrollierten Bereich kennzeichnende Tag vorzugsweise an der Tür oder

im Bereich der Tür an einer Außenseite einer Wand des betreffenden Raumes angebracht.

Der zur Authentifizierung einer den Zugang zu einem zugangskontrollierten Bereich wünschenden Person dienende personalisierte Zugangscode wird vorzugsweise auf einer von dem zur Authentifizierung verwendeten Mobilfunkgerät aufgenommenen Smartcard abgelegt. Entsprechend einer besonders bevorzugten Ausbildung der Erfindung handelt es sich hierbei um eine UICC (Universal Integrated Circuit Card = universelle Karte mit integriertem Schaltkreis), nämlich insbesondere um die den Zugang zu mindestens einem Mobilfunknetz ermöglichende SIM-karte des betreffenden Mobilfunkgerätes. Die Verwendung einer solchen UICC bietet dabei die Möglichkeit, nicht nur den personalisierten Zugangscode auf dieser Karte zu hinterlegen, sondern mit ihm zusammen eine spezielle, die durch das Mobilfunkgerät auszuführenden Teile des Verfahrens steuernde und dabei diesen Zugangscode verwendende Applikation beziehungsweise Client-Anwendung auf der Karte zu speichern. Gegebenfalls kann dabei die betreffende Applikation zu ihrer Bereitstellung für eine zu ihrer Nutzung berechtigte Person sogar im Wege der Übertragung über ein Mobilfunknetz auf die UICC beziehungsweise SIM-Karte gebracht werden. Der personalisierte Zugangscode und die Bereichs-ID werden entsprechend dem Grundgedanken der Erfindung mittels des zur Authentifizierung der den Zugang begehrenden Person dienenden Mobilfunkgeräts über ein öffentliches Netz zur Überprüfung an einen entfernten Server übertragen. Vorzugweise geschieht dies über ein Mobilfunknetz, wobei hierdurch, aufgrund der im Mobilfunk ohnehin erfolgenden verschlüsselten Datenübertragung, auch im Zusammenhang mit der vorzugsweise den Zugangscode und gegebenenfalls eine Applikation zur Steuerung dieser Vorgänge aufnehmenden UICC ein hohes Maß an Sicherheit gegeben ist. Gegebenfalls, aber nicht zwingend, kann im Zuge dessen auch noch die für die Mobilfunkübertragung relevante MSISDN als ein zusätzliches Authentifizierungsmerkmal verwendet werden. Neben einer Übertragung von Zugangscode oder Bereichs-ID über ein Mobilfunknetz kommt aber auch eine Übertragung dieser Daten über ein WLAN an einen in das Internet eingebundenen Accesspoint in Betracht, wobei in diesem Falle das entsprechende Mobilfunkgerät selbstverständlich WLAN-fähig sein muss und der Zugangscode sowie die Bereichs-ID dem sie überprüfenden Server über das Internet zugeleitet werden. Eine solche Variante ist insbesondere in Gebäuden mit eventuell eingeschränkter Mobilfunkabdeckung vorteilhaft. Gegebenfalls sind bei entsprechender Ausbildung des Zugangskontrollsystems sogar beide Übertragungswege möglich, wobei dann zum Beispiel in Abhängigkeit von der jeweils gegebenen Mobilfunkabdeckung einer der beiden Wege für die Übertragung der Daten zum entfernten Server gewählt wird.

Wie bereits ausgeführt, wird die den zugangskontrollierten Bereich identifizierende ID von einem an diesem Bereich - im Falle eines zugangskontrollierten Raumes beispielsweise an dessen Tür - angeordneten Tag ausgelesen und in das diese ID zusammen mit den personalisierten Zugangscode an den entfernten Server übertragende Mobilfunkgerät übernommen. Im einfachen Fall kann dies dadurch geschehen, dass eine den Zugang wünschende Person die in diesem Falle in Klarschrift wiedergegebene ID abliest und in das Mobilfunkgerät eintippt. Vorzugsweise nimmt jedoch der an dem jeweiligen zugangskontrollierten Bereich angeordnete Tag diese ID in Form eines maschinenlesbaren Codes auf, welcher von der den Zugang zu diesem Bereich wünschenden Person unmittelbar mit Hilfe des dafür entsprechend ausgebildeten Mobilfunkgeräts ausgelesen, das heißt in das Mobilfunkgerät eingelesen wird. Denkbar ist hierbei zum Beispiel, dass die Bereichs-ID in Form eines zweidimensionalen oder dreidimensionalen Barcodes auf dem Tag verschlüsselt ist, welcher mittels einer Kamera des Mobilfunkgeräts in dieses eingelesen wird. Entsprechend einer besonders bevorzugten Ausbildungsform wird jedoch die in dem Tag verschlüsselte ID des zugangskontrollierten Bereichs im Wege der Nahbereichskommunikation über Funk von dem Tag zu dem die ID auslesenden Mobilfunkgerät einer den Zugang zu dem betreffenden Bereich begehrenden Person übertragen. Darüber hinaus ist das Verfahren vorzugsweise so gestaltet, dass unabhängig davon, auf welchem Wege die Bereichs-ID in das Mobilfunkgerät übernommen wird, mit erfolgter Übernahme der ID gewissermaßen selbsttätig eine Applikation angestoßen wird, welche die Übertragung dieser ID und des personalisierten Zugangscodes an den entfernten Server veranlasst.

Das Verfahren kann noch dadurch weitergebildet sein, dass die den Zugang wünschende Person nach der Übertragung des personalisierten Zugangscodes zu dem entfernten Server der Zugangskontrolleinrichtung von Letzterem zur Eingabe eines zusätzlichen, ihrer Authentifizierung dienenden Merkmals aufgefordert wird. Hierbei kann es sich beispielsweise um eine über die Tastatur des Mobilfunkgeräts einzugebende PIN handeln. Vorzugsweise wird dabei jedoch als zusätzliches Merkmal für die Authentifizierung der Person ein biometrisches Merkmal der betreffenden Person verwendet. Als biometrisches Merkmal kann beispielsweise eine Stimmprobe der betreffenden Person dienen. Eine andere Möglichkeit besteht in der Verwendung eines mittels des der Authentifizierung dienenden Mobilfunkgeräts eingescannten Fingerabdrucks der betreffenden Person. Vorzugsweise wird das Ergebnis der Überprüfung der Berechtigung einer den Zugang zu dem entsprechend gesicherten Bereich wünschenden Person zusätzlich auf das von ihr zur Authentifizierung benutzte Mobilfunkgerät übertragen und von diesem als akustisches Signal ausgegeben und/oder auf einem Display visualisiert.

Ein die Aufgabe lösendes Zugangskontrollsystem besteht aus mindestens einem hinsichtlich des Zugangs zu kontrollierenden, durch eine Sicherungseinrichtung ver-

schlossenen Bereich, aus einer Zugangskontrolleinrichtung und aus einem von einer Zugang zu dem mindestens einen zugangskontrollierten Bereich begehrenden Person mitzuführenden Token. Auf dem Token ist, wie bereits zum Verfahren erläutert, ein der Authentifizierung der betreffenden Person gegenüber der Zugangskontrolleinrichtung dienender personalisierter Zugangscode gespeichert. Bei dem genannten Token handelt es sich um eine von einem Mobilfunkgerät aufgenommene Smartkarte. Die Prüfung der Identität und der Berechtigung von Personen, welche den Zugang zu dem mindestens einen zugangskontrollierten Bereich wünschen, erfolgt durch die bereits genannte Zugangskontrolleinrichtung, durch welche im Falle des Vorliegens einer solchen Berechtigung auch die Freigabe des Zugangs erfolgt. Hierzu wird von der genannten Zugangskontrolleinrichtung ein Aktor der den zugangskontrollierten Bereich verschließenden Sicherungseinrichtung entsprechend betätigt. Erfindungsgemäß ist bei dem vorgeschlagenen Zugangskontrollsystem an dem mindestens einen zugangskontrollierten Bereich ein passiver Tag angeordnet, auf welchem eine diesen Bereich identifizierende ID (Bereichs-ID) abgespeichert ist. Das die Smartkarte mit dem personalisierten Zugangscode aufnehmende Mobilfunkgerät ist ferner erfindungsgemäß mit einer Einheit zum Auslesen einer für einen zugangskontrollierten Bereich auf einem entsprechenden Tag gespeicherten ID ausgestattet. Die Zugangskontrolleinrichtung umfasst erfindungsgemäß mindestens einen über ein öffentliches Netz zugänglichen Server, der zum Empfang von Daten ausgebildet ist, welche von einem ein Token in Form einer Smartkarte aufnehmenden Mobilfunkgerät an den betreffenden Server gesendet werden. Dabei umfassen die betreffenden, über das öffentliche Netz übertragenen Daten mindestens den auf dem Token gespeicherten personalisierten Zugangscode und eine einen zugangskontrollierten Bereich identifizierende ID. Ferner verfügt die Zugangskontrolleinrichtung erfindungsgemäß über Mittel zur Fernbetätigung des Aktors der den zugangskontrollierten Bereich verschließenden Sicherungseinrichtung.

Vorzugsweise handelt es sich bei der das Token ausbildenden Smartkarte, welche von dem der Authentifizierung dienenden Mobilfunkgerät aufgenommen wird, um eine auch der Authentifizierung in einem Mobilfunknetz dienende UICC in Form einer SIM-Karte, wobei der personalisierte Zugangscode und die Bereichs-ID vorzugsweise unter Nutzung eines Mobilfunknetzes an den sie überprüfenden Server übertragen werden. Denkbar ist es aber auch, dass der personalisierte Zugangscode auf einer separaten, von dem Mobilfunkgerät aufgenommenen Smartkarte gespeichert ist. Das erfindungsgemäße Zugangskontrollsystem ist vorteilhaft dadurch ausgestaltet, dass es sich bei dem Tag um einen Aufkleber mit einem RFID-Chip handelt und die in dem das Token aufnehmende Mobilfunkgerät angeordnete Einheit zum Auflesen der auf diesem RFID-Chip gespeicherten ID eines zugangskontrollierten Bereichs eine NFC-Schnittstelle zur funkgestützten Nahbereichskommunikation umfasst. Entsprechend einer besonders bevorzugten Weiterbildung wird auf dem von dem Mobilfunkgerät in Form der Smartkarte aufgenommenen Token mindestens eine Client-Anwendung gehalten, welche nach dem Auslesen eines Tags mit einer einen zugangskontrollierten Bereich identifizierenden ID automatisch gestartet wird. Diese Client-Anwendung, bei welcher es sich um Programmanweisungen und zugehörige Daten handelt, sendet nach ihrem automatischen Starten den auf dem Token gehaltenen personalisierten Zugangscode sowie die ausgelesene ID des zugangskontrollierten Bereichs an den dafür ausgebildeten Server der Zugangskontrolleinrichtung.

Eine weitere vorteilhafte Ausgestaltung der Erfindung ist dadurch gegeben, dass die Zugangskontrolleinrichtung Einheiten, vorzugsweise zur Infrastruktur eines Mobilfunknetzbetreibers gehörende Einheiten, umfasst, mittels welcher ein einer Person aufgrund einer entsprechenden Anmeldung bei dem Zugangskontrollsystem zugeteilter personalisierter Zugangscode und gegebenenfalls eine zugehörige Client-Anwendung auf das als Bestandteil des erfindungsgemäßen Zugangskontrollsystems ausgebildete Mobilfunkgerät übertragbar sind. Entsprechend dem bevorzugten Anwendungsgebiet der Erfindung handelt es sich bei dem zugangskontrollierten Bereich um einen Raum und bei der diesen Raum verschließenden Sicherungseinrichtung um eine Tür mit einem elektronischen Türschloss. Dabei ist Bestandteil des vorgenannten elektronischen Türschlosses ein mittels der Zugangskontrolleinrichtung fernzubetätigender Aktor. Der Tag mit der den entsprechenden zugangskontrollierten Raum identifizierenden ID ist gemäß dieser Ausbildungsform an der vorgenannten Tür oder im Bereich dieser Tür an der Außenseite einer Wand des Raumes angeordnet.

[0010] Anhand der Fig. 1 soll ein mögliches Ausführungsbeispiel der Erfindung erläutert werden. Die Figur zeigt ein entsprechendes Zugangskontrollsystem in einer schematischen Darstellung. Wesentliche Elemente dieses Zugangskontrollsystems sind der zugangskontrollierte Bereich 1, in diesem Falle ein entsprechend gesicherter Raum in einem Gebäude, welcher durch eine Sicherungseinrichtung 4, vorliegend einer Tür mit einem elektronischen Türschloss, verschlossen ist, die Zugangskontrolleinrichtung 2 und das von einer Zugang zu dem zugangskontrollierten Bereich 1 wünschenden Person 3 mitgeführte, hier nicht im Detail gezeigte Token, welches in Form einer Smartkarte in einem Mobilfunkgerät 5 der betreffenden Person 3 angeordnet ist. Ferner gehören zum System ein Tag 6, auf welchem eine den zugangskontrollierten Bereich 1 beziehungsweise Raum identifizierende ID gespeichert ist, und mindestens ein öffentliches Netz 8, über welches der in dem Token gespeicherte personalisierte Zugangscode und die zuvor mittels des Mobilfunkgeräts 5 ausgelesene ID des zugangskontrollierten Bereichs 1 durch das Mobilfunkgerät 5 übertragen werden. Vorliegend sind in die Übertragung

dieser Daten zwei öffentliche Netze 8, 9 einbezogen, nämlich ein Mobilfunknetz 8, in welches das Mobilfunkgerät 5 eingebucht ist, und das Internet 9, in welches ein Server 7 der Zugangskontrolleinrichtung 2 zum Empfang der vorgenannten Daten eingebunden ist. Der Übergang zwischen den Netzen 8, 9 erfolgt über ein hier nicht dargestelltes Gateway. Die zur Überprüfung der Zugangsberechtigung an die Zugangskontrolleinrichtung 2 übermittelten Daten (der auf der Smartkarte beziehungsweise der UICC des Mobilfunkgeräts gespeicherte personalisierte Zugangscode und die mittels des Mobilfunkgeräts 5 von dem Tag 6 ausgelesene, den zugangskontrollierten Bereich 1 identifizierende ID) werden durch den in das Internet eingebundenen Server 7 empfangen. Nach erfolgreicher Authentifizierung der den Zugang zu dem Bereich begehrenden Person 3 wird deren Berechtigung zum Zugang durch einen weiteren Server 10 der Zugangskontrolleinrichtung 2 anhand entsprechender Einträge in einer Datenbank überprüft. Im Falle eines positiven Ergebnisses wird die Tür des Raumes, zu welchem die betreffende Person 3 Zugang begehrt, von der Zugangskontrolleinrichtung 2 durch Fernbetätigung eines Aktors (Teil des hier nicht gezeigten elektronischen Türschlosses) entsperrt. In dem dargestellten Beispiel umfasst die Zugangskontrolleinrichtung 2 auch Mittel beziehungsweise einen Server 11 zur Auswertung eines zusätzlichen, der Authentifizierung der den Zugang wünschenden Person 3 dienenden Merkmals, nämlich einer Sprachprobe. Zur Sicherheitsarchitektur der Zugangskontrolleinrichtung 2 gehört außerdem eine Firewall 12. Unter Verwendung des dargestellten Zugangskontrollsystems vollzieht sich, bevor die betreffende Person 3 den Raum beziehungsweise den zugangskontrollierten Bereich 1 betreten kann, folgender grundsätzlicher Ablauf:

a.) Die den Zugang zu dem zugangskontrollierten Bereich 1 beziehungsweise Raum wünschende Person 3 hält das von ihr zur Authentifizierung mitgeführte Mobilfunkgerät 5 beziehungsweise Mobiltelefon in die Nähe des neben der Tür des Raumes angebrachten NFC Tags 6, so dass das Mobilfunkgerät im Wege der Nahbereichskommunikation (NFC) die ID des Raumes aus dem NFC Tag 6 auslesen kann.
b.) Nach dem Auslesen der den Raum identifizierenden ID wird selbsttätig eine Client-Anwendung auf dem Mobilfunkgerät 5 gestartet, die dann aus der UICC oder einer separaten Smartkarte (Sicherheitstoken) des Mobilfunkgeräts 5 den eineindeutigen personalisierten Zugangscode der betreffenden Person 3 beziehungsweise des Nutzers ausliest.
c.) Das Mobiltelefon baut über das Netz 8 unter Nutzung von UMTS, GPRS oder WLAN eine IP-Datenverbindung zu dem externen Server 7 der Zugangskontrolleinrichtung 2 auf. Über diese Datenverbindung ruft das Mobiltelefon 5 einen Webservice auf, der von diesem externen Server 7 angeboten wird und übergibt den personalisierten Zugangscode der den Zugang begehrenden Person 3 (Nutzer) und die den Raum identifizierende ID innerhalb eines "openDoor-Request". Der Aufruf des betreffenden Webservice erfolgt über eine gesicherte Datenverbindung.
d.) Der externe Server 7 überprüft den personalisierten Zugangscode des Nutzers und die Raum-ID und leitet, wenn die Überprüfung positiv war, die Raum-ID und den personalisierten Zugangscode des Nutzers zu einem internen Server 10 weiter.
e.) Der interne Server 10 überprüft anhand seiner Datenbank, ob für den Nutzer beziehungsweise die Person 3 mit dem übermittelten personalisierten Zugangscode eine Zugangsberechtigung für den zugangskontrollierten Bereich 1 beziehungsweise für den Raum mit der übermittelten Bereichs-ID vorliegt.
f.) Wenn die Überprüfung positiv ist, wird die Sicherungseinrichtung 4, also die Tür, von der Zugangskontrolleinrichtung 2 durch Fernbetätigung eines entsprechenden Aktors im Türschloss beziehungsweise eines Türöffners geöffnet und ein "Response" über den externen Server 7 zum Mobilfunkgerät 5 gesendet.
g.) Das Mobilfunkgerät 5 zeigt dem Nutzer das Ergebnis an, zum Beispiel im Falle einer positiven Antwort: "Willkommen" oder im negativen Fall: "Zum Zutritt nicht berechtigt".

[0011] Das in der Fig. 1 gezeigte Beispiel, geht davon aus, dass sich eine den Zugang zu dem zugangskontrollierten Bereich 1 wünschende Person 3 gegenüber der Zugangskontrolleinrichtung 2 zum Erhalt des Zugangs noch durch ein zusätzliches biometrisches Merkmal, nämlich eine Stimmprobe, authentifizieren muss. Demgemäß ist der vorstehend dargestellte grundsätzliche Ablauf im Punkt e) noch wie folgt untersetzt:

e1.) Der externe Server 7 stellt auf Grund festgelegter Regeln fest, dass für die Zugangsberechtigung noch eine weitergehende Authentisierung der den Zugang begehrenden Person 3 erforderlich ist. Er sendet eine Response mit dem Wert "Auth required" an deren Mobilfunkgerät 5 zurück.

e2.) Das Mobilfunkgerät 5 fordert daraufhin die betreffende Person 3 auf, zur Abgabe einer Stimmenprobe in das Mikrofon des Mobilfunkgeräts 5 zu sprechen.

e3.) Die Client-Anwendung auf dem Mobilfunkgerät 5 übermittelt dann die Stimmprobe an den externen Server 7 der Zugangskontrolleinrichtung 2, innerhalb welcher die Stimmprobe an einen Voice-Ident-Server 11 weitergeleitet wird.

e4.) Der Server 11 vergleicht die Stimmprobe mit den Informationen in seiner Datenbank.

e5.) Ist die Authentifizierung gemäß e4.) erfolgreich, überprüft der interne Server 10 anhand seiner Datenbank, ob für die Person 3 mit dem übermittelten personalisierten Zugangscode eine Zugangsberechtigung für den Bereich 1 beziehungsweise für den Raum mit der übermittelten Raum-ID vorliegt.

Liste der Bezugszeichen

[0012]

1	zugangskontrollierter Bereich
2	Zugangskontrolleinrichtung
3	Person
4	Sicherungseinrichtung
5	Mobilfunkgerät
6	Tag
7	Server
8	öffentliches Netz
9	Netz
10	Server
11	Server
12	Firewall

Patentansprüche

1. Verfahren zur Kontrolle des Zugangs zu einem durch eine Sicherungseinrichtung (4) verschlossenen Bereich (1), wonach eine Zugang zu dem betreffenden Bereich (1) begehrende Person (3) sich gegenüber einer Zugangskontrolleinrichtung (2) authentifizieren muss und nach erfolgreicher Authentifizierung durch die Zugangskontrolleinrichtung (2) das Bestehen einer Zugangsberechtigung zu dem genannten Bereich (1) für die den Zugang begehrende Person (3) geprüft sowie im Falle des Bestehens einer solchen Zugangsberechtigung von der Zugangskontrolleinrichtung (2) durch Betätigung eines Aktors die Sicherungseinrichtung (4) entsperrt und der als berechtigt erkannten Person (3) der Zugang zu dem Bereich (1) ermöglicht wird, wobei sich die den Zugang zu dem Bereich (1) begehrende Person (3) gegenüber der Zugangskontrolleinrichtung (2) mittels eines von ihr mitgeführten Mobilfunkgerätes (5) authentifiziert, **dadurch gekennzeichnet, dass** ein zum Zweck der Authentifizierung in dem Mobilfunkgerät (5) abgelegter personalisierter Zugangscode zusammen mit einer die Prüfung der Zugangsberechtigung ermöglichenden, den bezüglich des Zugangs kontrollierten Bereich (1) identifizierenden ID von dem Mobilfunkgerät (5) zur Prüfung über mindestens ein öffentliches Netz (8) an einen Server (7) der Zugangskontrolleinrichtung (2) übermittelt wird, wobei die ID des zugangskontrollierten Bereiches (1) zuvor von einem an diesem Bereich angeordneten, ihn kennzeichnenden Tag (6) ausgelesen und in das Mobilfunkgerät (5) übernommen wird und wobei der die Sicherungseinrichtung (4) entsperrende Aktor durch die Zugangskontrolleinrichtung (2) fernbetätigt wird.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, dass** der personalisierte Zugangscode und die den zugangskontrollierten Bereich (1) identifizierende ID mittels des Mobilfunkgerätes (5) über ein Mobilfunknetz (8) an den Server (7) übertragen werden.

3. Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet, dass** der personalisierte Zugangscode auf einer UICC, nämlich auf der den Zugang zu mindestens einem Mobilfunknetz ermöglichenden SIM-Karte des Mobilfunkgeräts abgelegt wird.

4. Verfahren nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet, dass** die in dem Tag (6) verschlüsselte ID durch die den Zugang begehrende Person (3) mittels des Mobilfunkgerätes (5) ausgelesen wird.

5. Verfahren nach Anspruch 4, **dadurch gekennzeichnet, dass** die in dem Tag (6) verschlüsselte ID des zugangskontrollierten Bereichs (1) im Wege der Nahbereichskommunikation über Funk von dem Tag (6) zu dem Mobilfunkgerät (5) der den Zugang zu dem Bereich begehrenden Person (3) übertragen wird.

6. Verfahren nach Anspruch 4, **dadurch gekennzeichnet, dass** die den zugangskontrollierten Bereich (1) identifizierende ID mittels einer Kamera des Mobilfunkgerätes (5) von einem die ID in Form eines zweidimensionalen oder dreidimensionalen Barcodes verschlüsselnden Tag (6) ausgelesen wird.

7. Verfahren nach einem der Ansprüche 1 bis 6, **dadurch gekennzeichnet, dass** die den Zugang zu dem zugangskontrollierten Bereich (1) begehrende Person (3) nach der Übertragung des personalisierten Zugangscodes von dem diesen Zugangscode empfangenden Server (7) zur Eingabe eines zusätzlichen, ihrer Authentifizierung dienenden Merkmals aufgefordert wird.

8. Verfahren nach Anspruch 7, **dadurch gekennzeichnet, dass** als zusätzliches Merkmal zur Authentifizierung der Person (3) eine von dieser an dem Mobilfunkgerät (5) einzugebende PIN verwendet wird.

9. Verfahren nach Anspruch 7, **dadurch gekennzeichnet, dass** als zusätzliches Merkmal zur Authentifizierung der Person (3) ein biometrisches Merkmal der betreffenden Person (3) verwendet wird.

10. Verfahren nach Anspruch 9, **dadurch gekennzeichnet, dass** als zusätzliches biometrisches Merkmal eine Stimmprobe der betreffenden Person (3) dient.

11. Verfahren nach Anspruch 9, **dadurch gekennzeichnet, dass** als zusätzliches biometrisches Merkmal ein mittels des zur Authentifizierung verwendeten Mobilfunkgeräts (5) eingescannter Fingerabdruck der betreffenden Person (3) verwendet wird.

12. Verfahren nach einem der Ansprüche 1 bis 11, **dadurch gekennzeichnet, dass** nach erfolgter Überprüfung der Zugangsberechtigung einer Zugang zu einem zugangskontrollierten Bereich (1) begehrenden Person (3) durch die Zugangskontrolleinrichtung (2) das Ergebnis der entsprechenden Überprüfung auf das Mobilfunkgerät (5) der betreffenden Person (3) übertragen und von dem Mobilfunkgerät (5) als akustisches Signal ausgegeben und/oder auf einem Display visualisiert wird.

13. Zugangskontrollsystem mit mindestens einem hinsichtlich des Zugangs zu kontrollierenden, durch eine Sicherungseinrichtung (4) verschlossenen Bereich (1), mit einer Zugangskontrolleinrichtung (2) zur Prüfung der Identität und der Berechtigung von Zugang zu dem mindestens einen zugangskontrollierten Bereich (1) begehrenden Personen (3) sowie zur Freigabe des Zugangs ausschließlich für berechtigte Personen durch Betätigung eines Aktors der den betreffenden Bereich (1) verschließenden Sicherungseinrichtung (4) und mit einem von einer Zugang zu dem mindestens einen zugangskontrollierten Bereich (1) begehrenden Person (3) mitzuführen Token, auf welchem ein der Authentifizierung dieser Person (3) gegenüber der Zugangskontrolleinrichtung (2) dienender, personalisierter Zugangscode gespeichert ist, wobei das Token als eine von einem Mobilfunkgerät (5) aufgenommene Smartkarte ausgebildet ist, **dadurch gekennzeichnet, dass**

a.) an dem mindestens einen zugangskontrollierten Bereich (1) ein Tag (6) angeordnet ist, auf welchem eine diesen Bereich (1) identifizierende ID abgespeichert ist,

b.) das, die Smartkarte mit dem personalisierten Zugangscode aufnehmende Mobilfunkgerät (5) mit einer Einheit zum Auslesen einer für einen zugangskontrollierten Bereich (1) auf einem Tag (6) gespeicherten ID ausgestattet ist,

c.) die Zugangskontrolleinrichtung (2) mindestens einen über ein öffentliches Netz (8) zugänglichen Server (7) umfasst, an welchen Daten zur Überprüfung der Zugangsberechtigung einer den Zugang zu dem mindestens einen zugangskontrollierten Bereich (1) begehrenden Person (3), nämlich mindestens der auf der Smartkarte in dem von der betreffenden Person (3) mitgeführten Mobilfunkgerät (5) gespeicherte personalisierte Zugangscode und die mittels dieses Mobilfunkgeräts (5) ausgelesene, den betreffenden Bereich (1) identifizierende ID übertragen werden,

d.) die Zugangskontrolleinrichtung (2) Mittel zur Fernbetätigung des Aktors der den zugangkontrollierten Bereich (1) verschließenden Sicherungseinrichtung (4) umfasst.

14. Zugangskontrollsystem nach Anspruch 13, **dadurch gekennzeichnet, dass** es sich bei der das Token ausbildenden Smartkarte um eine auch der Authentifizierung in einem Mobilfunknetz (8) dienende UICC in Form einer SIM-Karte des Mobilfunkgeräts (5) handelt.

15. Zugangskontrollsystem nach Anspruch 13 oder 14 **dadurch gekennzeichnet, dass** es sich bei dem Tag (6) um einen Aufkleber mit einem RFID-Chip handelt und die in dem das Token aufnehmende Mobilfunkgerät (5) angeordnete Einheit zum Auslesen der in dem RFID-Chip gespeicherten ID eines zugangskontrollierten Bereiches (1) eine NFC-Schnittstelle zur funkgestützten Nahbereichskommunikation umfasst.

16. Zugangskontrollsystem nach einem der Ansprüche 13 bis 15, **dadurch gekennzeichnet, dass** auf dem von dem Mobilfunkgerät (5) in Form der Smartkarte aufgenommenen Token mindestens eine Client-Anwendung, in Form von Programmanweisungen mit zugehörigen Daten, gespeichert ist, welche nach dem Auslesen eines Tags (6) mit einer einen zugangskontrollierten Bereich (1) identifizierenden ID automatisch gestartet wird und den auf dem Token gehaltenen personalisierten Zugangscode sowie die ausgelesene ID des betreffenden zugangskontrollierten Bereichs (1) an den dafür ausgebildeten Server (7) der Zugangskontrolleinrichtung (2) sendet.

17. Zugangskontrollsystem nach einem der Ansprüche 13 bis 16, **dadurch gekennzeichnet, dass** die Zugangskontrolleinrichtung (2) Einheiten umfasst, mit-

tels welcher ein einer Person (3) aufgrund einer Anmeldung bei dem Zugangskontrollsystem zugeteilter personalisierter Zugangscode und gegebenenfalls eine zugehörige Client-Anwendung auf ein als Bestandteil des Zugangskontrollsystems ausgebildetes Mobilfunkgerät (5) der betreffenden Person (3) übertragbar sind.

18. Zugangskontrollsystem nach einem der Ansprüche 13 bis 17, **dadurch gekennzeichnet, dass** es sich bei dem mindestens einen zugangskontrollierten Bereich (1) um einen Raum und bei der diesen verschließenden Sicherungseinrichtung (4) um eine Tür mit einem elektronischen Türschloss handelt, wobei Bestandteil des elektronischen Türschlosses ein mittels der Zugangskontrolleinrichtung (2) fernzubetätigender Aktor ist und wobei der Tag (6) mit der diesen Raum (1) identifizierenden ID an der Tür oder im Bereich der Tür an der Außenseite einer Wand des Raumes angeordnet ist.

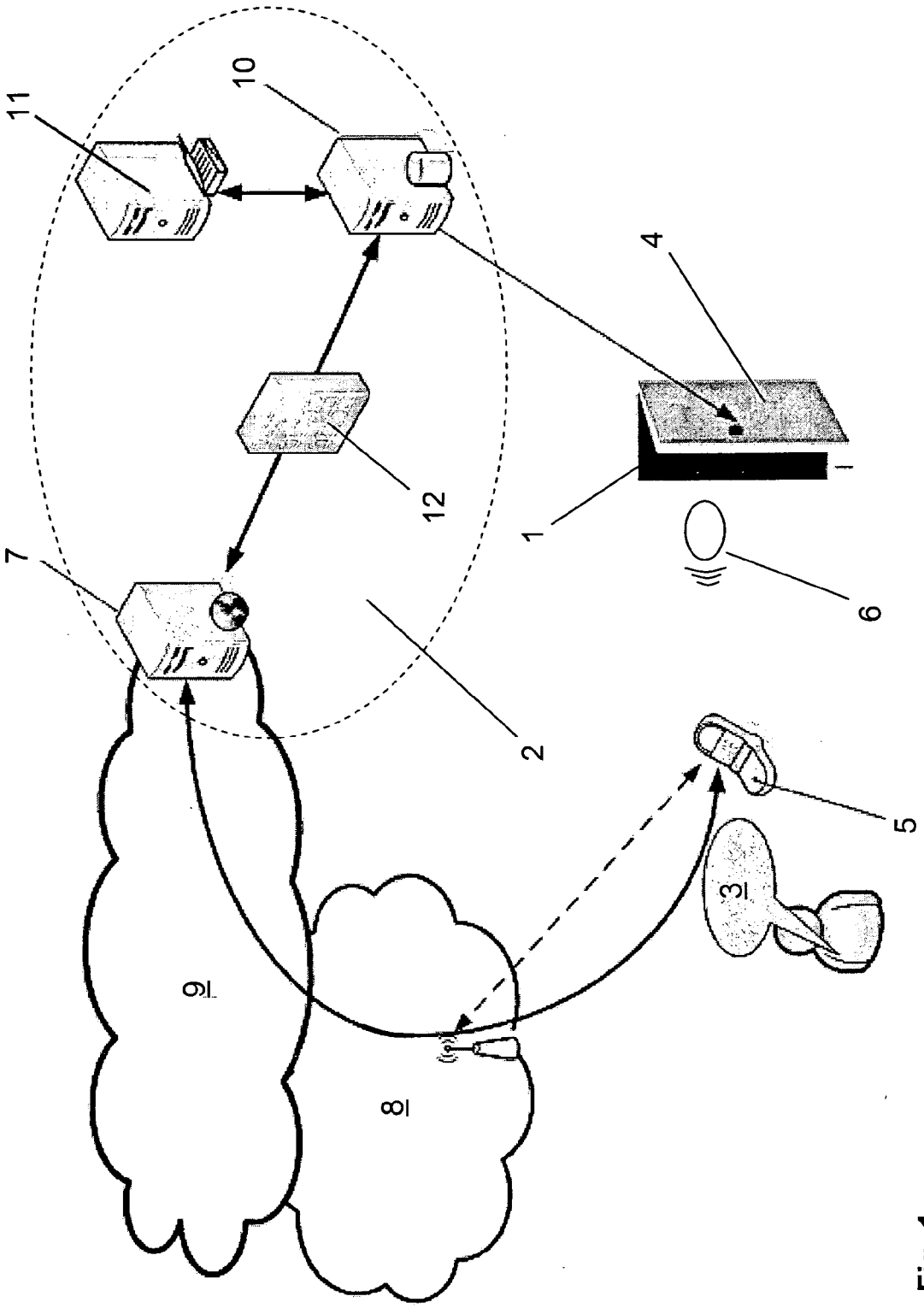

Fig. 1

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 10 07 5200

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (IPC)
X Y	WO 2005/066908 A2 (KABA AG [CH]; STUDERUS PAUL [CH]) 21. Juli 2005 (2005-07-21) * Zusammenfassung * * Seite 2, Zeile 27 - Seite 10, Zeile 18 * * Seite 12, Zeile 4 - Zeile 14 * * Seite 16, Zeile 5 - Seite 18, Zeile 1 * -----	1-5,7-18 6	INV. G07C9/00
Y	EP 1 669 941 A2 (SKIDATA AG [AT]) 14. Juni 2006 (2006-06-14) * Zusammenfassung * * Absatz [0021] - Absatz [0022] * -----	6	
A	DE 10 2006 038438 A1 (KEPPLER BERNHARD [US]) 21. Februar 2008 (2008-02-21) * Zusammenfassung * * Absatz [0007] - Absatz [0012] * * Ansprüche 1,2,6,7 * -----	10,11	

RECHERCHIERTE SACHGEBIETE (IPC)

G07C

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
Den Haag	29. September 2010	Teutloff, Ivo

KATEGORIE DER GENANNTEN DOKUMENTE

X : von besonderer Bedeutung allein betrachtet
Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie
A : technologischer Hintergrund
O : nichtschriftliche Offenbarung
P : Zwischenliteratur

T : der Erfindung zugrunde liegende Theorien oder Grundsätze
E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist
D : in der Anmeldung angeführtes Dokument
L : aus anderen Gründen angeführtes Dokument

& : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument

1

EPO FORM 1503 03.82 (P04C03)

ANHANG ZUM EUROPÄISCHEN RECHERCHENBERICHT ÜBER DIE EUROPÄISCHE PATENTANMELDUNG NR. EP 10 07 5200

In diesem Anhang sind die Mitglieder der Patentfamilien der im obengenannten europäischen Recherchenbericht angeführten Patentdokumente angegeben.
Die Angaben über die Familienmitglieder entsprechen dem Stand der Datei des Europäischen Patentamts am
Diese Angaben dienen nur zur Unterrichtung und erfolgen ohne Gewähr.

29-09-2010

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
WO 2005066908 A2	21-07-2005	AT 477561 T	15-08-2010
		EP 1702306 A2	20-09-2006
		US 2007200665 A1	30-08-2007
EP 1669941 A2	14-06-2006	DE 102004059608 A1	14-06-2006
		US 2006124734 A1	15-06-2006
DE 102006038438 A1	21-02-2008	EP 2054840 A1	06-05-2009
		WO 2008019800 A1	21-02-2008
		US 2008045806 A1	21-02-2008

EPO FORM P0461

Für nähere Einzelheiten zu diesem Anhang : siehe Amtsblatt des Europäischen Patentamts, Nr.12/82