(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

PCT

(43) Internationales Veröffentlichungsdatum
6. August 2009 (06.08.2009)

(10) Internationale Veröffentlichungsnummer
WO 2009/094683 A1

(51) Internationale Patentklassifikation:
G07C 9/00 (2006.01)

(21) Internationales Aktenzeichen: PCT/AT2009/000033

(22) Internationales Anmeldedatum:
30. Januar 2009 (30.01.2009)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
A 145/2008 30. Januar 2008 (30.01.2008) AT

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **EVVA-WERK SPEZIALERZEUGUNG VON ZYLINDER- UND SICHERHEITSSCHLÖSSERN GESSELLSCHAFT M.B.H. & CO. KG** [AT/AT]; Wienerbergstrasse 59-65, A-1120 Wien (AT).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **ULLMANN, Johannes** [AT/AT]; Oswaldgasse 33a/2/1.02, A-1120 Wien (AT).

(74) Anwalt: **HAFFNER UND KESCHMANN Patentanwälte OG**; Schottengasse 30, A-1014 Wien (AT).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG,

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD AND DEVICE FOR REGULATING ACCESS CONTROL

(54) Bezeichnung: VERFAHREN UND VORRICHTUNG ZUR STEUERUNG DER ZUTRITTSKONTROLLE

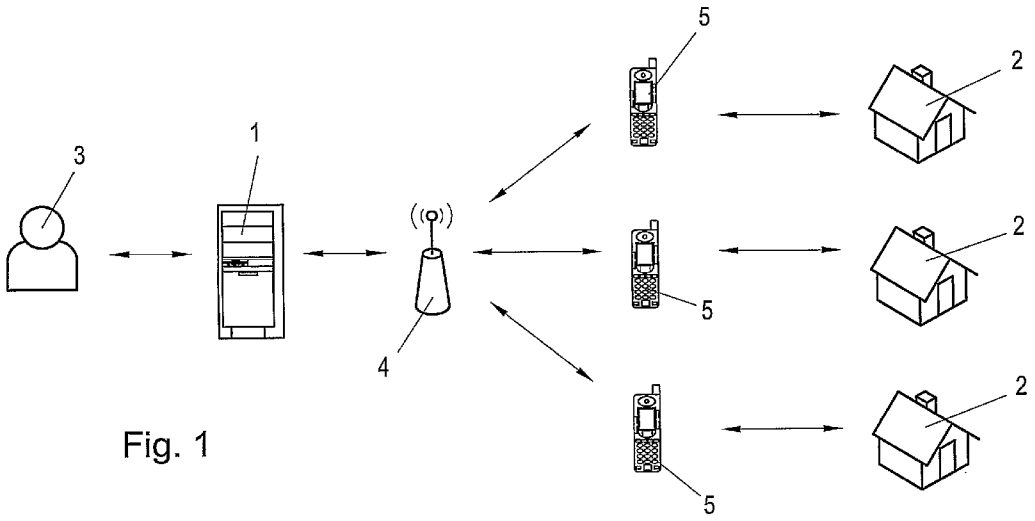


Fig. 1

(57) **Abstract:** In a method for regulating access control with a locking unit, particularly locks, and electronic keys, wherein access authorizations are stored and managed in a central processor, the keys are programmed in keeping with the respective access authorization with authorization information for a predetermined selection of locking units, in the event of an access request the authorization information is wirelessly sent from a key to a locking unit, and in the locking unit the access authorization is determined as a function of the authorization information received, the programming of a key comprises the sending of the authorization information via a wireless telecommunication network to a wireless mobile telecommunication device and the transmission of the authorization information received from the mobile telecommunication device to a memory of the key.

(57) **Zusammenfassung:** Bei einem Verfahren zur Steuerung der Zutrittskontrolle mit Schließeinheit, insbesondere Schlössern, und elektronischen Schlüsseln, bei welchem Zutrittsberechtigungen in einer zentralen Recheneinheit gespeichert und verwaltet werden, die Schlüssel entsprechend der jeweiligen Zutrittsberechtigung mit Berechtigungsinformationen für eine vorgegebenen Auswahl an Schließeinheiten programmiert werden, die Berechtigungsinformationen im Falle eines Zutrittswunsches drahtlos

[Fortsetzung auf der nächsten Seite]

WO 2009/094683 A1

PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— *mit internationalem Recherchenbericht*

von einem Schlüssel an eine Schließeinheit gesendet werden und in der Schließeinheit in Abhängigkeit von den empfangenen Berechtigungsinformationen die Zutrittsberechtigung ermittelt wird, umfasst die Programmierung eines Schlüssels das Senden der Berechtigungsinformationen über ein drahtloses Telekommunikationsnetz an ein drahtloses mobiles Telekommunikationsgerät und das Übermitteln der vom mobilen Telekommunikationsgerät empfangenen Berechtigungsinformationen an einen Speicher des Schlüssels.

Verfahren und Vorrichtung zur Steuerung der Zutrittskontrolle

Die Erfindung betrifft ein Verfahren zur Steuerung der Zutrittskontrolle mit Schließeinheiten, insbesondere Schlössern, und elektronischen Schlüsseln, bei welchem Zutrittsberechtigungen in einer zentralen Recheneinheit gespeichert und verwaltet werden, die Schlüssel entsprechend der jeweiligen Zutrittsberechtigung mit Berechtigungsinformationen für eine vorgegebene Auswahl an Schließeinheiten programmiert werden, die Berechtigungsinformationen im Falle eines Zutrittswunsches drahtlos von einem Schlüssel an eine Schließeinheit gesendet werden und in der Schließeinheit in Abhängigkeit von den empfangenen Berechtigungsinformationen die Zutrittsberechtigung ermittelt wird.

Die Erfindung betrifft weiters eine Vorrichtung zur Zutrittskontrolle umfassend eine Mehrzahl von Schließeinheiten, insbesondere Schlössern, und elektronischen Schlüsseln zum berührungslosen Sperren und Entsperren der Schließeinheiten,

- eine zentrale Recheneinheit zum Speichern und Verwalten von Zutrittsberechtigungen,
- Mittel, um die Schlüssel entsprechend der jeweiligen Zutrittsberechtigung mit Berechtigungsinformationen für eine vorgegebene Auswahl an Schließeinheiten zu programmieren,
- Mittel zum drahtlosen Übermitteln der Berechtigungsinformationen vom Schlüssel an die Schließeinheit,

wobei die Schließeinheit jeweils eine Auswerteschaltung aufweist, um die Zutrittsberechtigung auf Grund der erhaltenen Berechtigungsinformationen zu ermitteln.

Unter dem Begriff „Schließeinheiten" sind im Rahmen der Erfindung elektrische, elektronische oder mechatronische Schließeinheiten, insbesondere Schlösser, zu verstehen. Schließ-

einheiten können hierbei verschiedene Komponenten umfassen, wie z.B. Leseeinrichtungen für Identifikationsmedien, insbesondere elektronische Schlüssel, eine Schließelektronik und dgl.

Für die elektronische Zutrittskontrolle mit berührungslosen Systemen gibt es mehrere Möglichkeiten. Bisher bekannte RFID-Systeme bestehen aus einem elektronischen Schlüssel, auf welchem ein Identifikations- bzw. Zugangscode elektronisch gespeichert ist 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 der Schlüssel ein aktiver Sender mit eigener Energiequelle ist (z.B. Fernöffnung der Zentralverriegelung für Kraftfahrzeuge).

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

Bei anderen Systemen kann die Zutrittsberechtigung ausschließlich in der jeweiligen Schließeinheit gespeichert werden, was den Vorteil aufweist, dass die Schlüssel selbst nicht notwendigerweise programmiert werden müssen, jedoch den Nachteil mit sich bringt, dass bei jeder Änderung der Zutrittsberechtigung

die Schließeinheit mit entsprechenden Informationen versorgt werden muss, was oftmals einen direkten Zugang zur Schließeinheit erfordert.

Bisher bekannt ist weiters, dass die Komponenten an der Türe, wie beispielsweise das Lesegerät vernetzt sind, womit eine Änderung der Zutrittsberechtigung von einer Zentrale aus möglich ist, ohne dass ein von der Änderung der Zutrittsberechtigung betroffener Schlüssel zu einem bestimmten Punkt, wie zum Beispiel zu einer Programmierstation gebracht werden muss. Für den Fall hingegen, dass die Türen bzw. Schließeinheiten nicht vernetzbar sind, besteht nun das Problem darin, dass bei einer Änderung der Zutrittsberechtigung entweder die betroffenen Schlüssel vorhanden sein müssen oder die geänderten Informationen auf anderem Wege als über ein Netzwerk zur Tür gebracht werden müssen, zum Beispiel mit Hilfe eines Programmiergerätes.

Die vorliegende Erfindung zielt nun darauf ab, ein Verfahren und eine Vorrichtung zur Steuerung der Zutrittskontrolle dahingehend zu verbessern, dass Zutrittsberechtigungen in einfacher Weise vergeben und geändert werden können, ohne dass die jeweils betroffenen Schlüssel zu einer Programmierstation gebracht werden müssen und gleichzeitig auch ohne dass es einer Vernetzung der Schließeinheiten bedarf. Es soll somit von einer zentralen Kontrollstation aus jederzeit möglich sein, Zutrittsberechtigungen zu vergeben und zu verändern, ohne dass ein direkter Zugriff auf die Schließeinheiten vorhanden ist.

Zur Lösung dieser Aufgabe zeichnet sich das erfindungsgemäße Verfahren im Wesentlichen dadurch aus, dass die Programmierung eines Schlüssels das Senden der Berechtigungsinformationen über ein drahtloses Telekommunikationsnetz an ein drahtloses mobiles Telekommunikationsgerät und das Übermitteln der vom

mobilen Telekommunikationsgerät empfangenen Berechtigungsinformationen an einen Speicher des Schlüssels umfasst.

Zur Lösung dieser Aufgabe ist weiters die Vorrichtung der eingangs genannten Art erfindungsgemäß derart weitergebildet, dass die Vorrichtung weiters wenigstens ein drahtloses mobiles Telekommunikationsgerät umfasst, dass die Mittel zum Programmieren der Schlüssel Mittel zum Senden der Berechtigungsinformationen über ein drahtloses Telekommunikationsnetz an eine erste Kommunikationsschnittstelle des mobilen Telekommunikationsgeräts umfassen und dass Mittel zum Übermitteln der vom mobilen Telekommunikationsgerät empfangenen Berechtigungsinformationen an einen Speicher des Schlüssels vorgesehen sind.

Dadurch, dass nun die Programmierung der Schlüssel mit Berechtigungsinformationen über ein drahtloses Telekommunikationsnetz erfolgt, können die Berechtigungsinformationen von der zentralen Recheneinheit an ein drahtloses mobiles Telekommunikationsgerät des jeweils gewünschten Benutzers bzw. Schlüsselinhabers gesendet werden, sofern das mobile Telekommunikationsgerät im jeweiligen Telekommunikationsnetz registriert ist. Die vom mobilen Telekommunikationsgerät empfangenen Berechtigungsinformationen können einem geeigneten Identifikationsmedium zur Verfügung gestellt werden, welches auf diese Art und Weise eine Schlüsselfunktion erhält. Erfindungsgemäß 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 Berechtigungsinformationen 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. Dies ist von besonderem Vorteil, wenn auf Grund der örtlichen Gegebenheiten eine Vernetzung von Schließeinheiten nicht gewünscht ist, beispielsweise, wenn bei kleineren Schließanlagen der Vernetzungsaufwand zu kostenintensiv wäre oder wenn bauliche Eingriffe in der Türe und im Bereich der Türe nicht erwünscht sind.

Wie bereits erwähnt müssen im Rahmen der vorliegenden Erfindung die von dem Kommunikationsgerät empfangenen Berechtigungsinformationen an ein Identifikationsmedium übermittelt werden, damit dieses eine Schlüsselfunktion erhält oder um die auf diesem gespeicherten Berechtigungsinformationen zu aktualisieren. Hierzu sind mehrere Möglichkeiten denkbar. Gemäß einer bevorzugten Weiterbildung der Erfindung wird derart vorgegangen, dass das mobile Telekommunikationsgerät selbst als Schlüssel verwendet wird und das Übermitteln der vom mobilen Telekommunikationsgerät empfangenen Berechtigungsinformationen an einen Speicher des Schlüssels das Schreiben der Berechtigungsinformationen in einen einer Kommunikationsschnittstelle des mobilen Telekommunikationsgeräts zum drahtlosen Senden der Berechtigungsinformationen an die Schließeinheit zugeordneten Speicher umfasst. Die erfindungsgemäße Vorrichtung ist in diesem Fall derart weitergebildet, dass der Schlüssel im Telekommunikationsgerät ausgebildet ist und der Speicher als mit einer zweiten Kommunikationsschnittstelle des mobilen Telekommunikationsgeräts verbundener Speicher des Telekommunikationsgeräts ausgebildet ist, welche zweite Kommunikationsschnittstelle von der ersten Kommunikationsschnittstelle verschieden und zum drahtlosen Übermitteln der Berechtigungsinformationen vom Schlüssel an die Schließeinheit ausgebildet ist. Bei einer derartigen Weiterbildung erübrigt sich das Übermitteln der vom

mobilen Telekommunikationsgerät empfangenen Berechtigungsinformationen an ein externes Medium. Vielmehr werden die Berechtigungsinformationen unmittelbar an ein in das Telekommunikationsgerät integriertes Schlüsselmodul und insbesondere an einen Speicher dieses Schlüsselmoduls übermittelt und dort abgelegt. Es muss sich hierbei nicht um einen dezidierten Speicher des Schlüsselmoduls handeln, sondern es kann sich um den Hauptspeicher des Telekommunikationsgerätes handeln. Die Berechtigungsinformationen werden hierbei derart gespeichert, dass sie einer Telekommunikationsschnittstelle des mobilen Telekommunikationsgeräts zur Verfügung stehen, damit die Berechtigungsinformationen über diese Kommunikationsschnittstelle drahtlos an die Schließeinheit gesendet werden können. Bevorzugt handelt es sich hierbei um eine gesonderte Kommunikationsschnittstelle des Telekommunikationsgerätes, welche von derjenigen Kommunikationsschnittstelle verschieden ist, über welche die Berechtigungsinformationen von der zentralen Recheneinheit erhalten werden. Während es sich bei derjenigen Kommunikationsschnittstelle, über welche die Berechtigungsinformationen von der zentralen Recheneinheit erhalten werden, bevorzugt um eine übliche Kommunikationsschnittstelle eines Telekommunikationsnetzwerks, wie beispielsweise eine GSM- oder UMTS-Schnittstelle handelt, ist die Kommunikationsschnittstelle zum drahtlosen Senden von Berechtigungsinformationen an die Schließeinheit bevorzugt für die lokale Kommunikation mit entsprechend geringerer Übertragungsreichweite ausgebildet. Bevorzugt erfolgt das Übermitteln der Berechtigungsinformationen vom Schlüssel an die Schließeinheit hierbei unter Verwendung von RFID. Gemäß einer anderen bevorzugten Weiterbildung erfolgt das Übermitteln der Berechtigungsinformationen vom Schlüssel an die Schließeinheit unter Verwendung von Nahfeldkommunikation, beispielsweise nach dem NFC-Standard. In bevorzugter Weise findet die Übertragung in einem lizenzfreien Band, bzw. dem ISM-Band, statt.

Eine andere Möglichkeit zur Übermittlung der Berechtigungsinformationen vom mobilen Telekommunikationsgerät an den Schlüssel besteht bevorzugt darin, dass das Übermitteln der vom mobilen Telekommunikationsgerät empfangenen Berechtigungsinformationen an einen Speicher des Schlüssels die Verwendung einer Schreib-/Leseeinrichtung für Identifikationsmedien oder dgl. umfasst. Die erfindungsgemäße Vorrichtung ist in diesem Zusammenhang derart weitergebildet, dass die Mittel zum Übermitteln der vom mobilen Telekommunikationsgerät empfangenen Berechtigungsinformationen an einen Speicher des Schlüssels eine Schreib-/Leseeinrichtung für Identifikationsmedien oder dgl. umfasst. In einem derartigen Fall wird als Schlüssel ein externes Identifikationsmedium verwendet, das mit Hilfe einer Schreibeinrichtung programmiert wird, das heißt mit den jeweiligen Berechtigungsinformationen beschrieben wird. Dies erfordert naturgemäß einen zusätzlichen Schreibvorgang und eine entsprechende Schreibeinrichtung, jedoch ist der Schlüssel bei dieser Erfindungsvariante vom mobilen Telekommunikationsgerät unabhängig, sodass die Einsatzmöglichkeiten vergrößert werden. Außerdem benötigen derartige externe Identifikationsmedien in der Regel keine eigene Stromversorgung, sodass die Schlüsselfunktion auch ohne Stromversorgung aufrecht bleibt, wohingegen bei der Verwendung des mobilen Telekommunikationsgeräts selbst als Schlüssel immer für eine ausreichende Stromversorgung Sorge zu tragen ist.

Bevorzugt ist die Erfindung derart weitergebildet, dass die Berechtigungsinformation wenigstens eine Schlosskennung enthält. Das Vorliegen einer bestimmten Schlosskennung im Schlüssel bedeutet dann beispielsweise, dass eine Zugangsberechtigung für die Schließeinheit mit der entsprechenden Schlosskennung vorhanden ist.

In diesem Zusammenhang wird erfindungsgemäß bevorzugt derart vorgegangen, dass die Ermittlung der Zutrittsberechtigung in der Schließeinheit den Vergleich der empfangenen Berechtigungsinformationen mit der in der Schließeinheit gespeicherten eigenen Schlosskennung umfasst. Die erfindungsgemäße Vorrichtung ist in diesem Fall derart weitergebildet, dass die Auswerteschaltung der Schließeinheit eine Vergleichsschaltung zum Vergleichen der empfangenen Berechtigungsinformationen mit der eigenen Schlosskennung umfasst. Die Ermittlung der Zutrittsberechtigung erfolgt hierbei somit unter Verwendung der in der Schließeinheit gespeicherten eigenen Schlosskennung, welche bevorzugt eine innerhalb des Schließsystems eindeutige Schlosskennung ist und welche der Schließeinheit bei deren Initialisierung zugeteilt und in die Schließeinheit einprogrammiert wurde.

Um das unautorisierte Auslesen einer Berechtigungsinformation, insbesondere einer Schlosskennung aus dem Schlüssel und das Anfertigen von Schlüsselkopien zu verhindern, wird bevorzugt derart vorgegangen, dass die Berechtigungsinformationen im Schlüssel verschlüsselt vorliegen. Die erfindungsgemäße Vorrichtung ist dann derart weitergebildet, dass die Auswerteschaltung der Schließeinheit eine Entschlüsselungseinrichtung umfasst.

Im einfachsten Falle wird dabei bevorzugt so vorgegangen, dass alle Berechtigungsinformationen mit einem allgemeinen Systemschlüssel verschlüsselt vorliegen. Dadurch kann von eventuell ausgelesenen Schlüsseln ohne das Wissen des allgemeinen Systemschlüssels keine Information über die tatsächlichen Schließberechtigungen erhalten werden. Ein allgemeiner Systemschlüssel, der in jedem Schlüssel und jeder Schließeinheit fest gespeichert ist und nicht ausgelesen werden kann, verhin-

dert somit auch in einfacher Weise, dass Schließberechtigungen eines Schlüssels nachträglich verändert werden können.

Die Verschlüsselung kann hierbei in verschiedener Art und Weise erfolgen. Gemäß einer bevorzugten Verfahrensweise ist vorgesehen, dass den Schließeinheiten jeweils ein schlossindividueller Verschlüsselungsschlüssel zugeordnet wird, dass die Berechtigungsinformationen für eine Schließeinheit in der zentralen Recheneinheit mit dem jeweils zugeordneten schlossindividuellen Verschlüsselungsschlüssel verschlüsselt und als schloss-individuell verschlüsselte Berechtigungsinformationen an das Telekommunikationsgerät bzw. den Schlüssel gesendet und dort gespeichert werden und dass die schloss-individuell verschlüsselten Berechtigungsinformationen in der Schließeinheit unter Verwendung des dort gespeicherten, zugeordneten schlossindividuellen Verschlüsselungsschlüssels entschlüsselt werden. Die zentrale Recheneinheit verschlüsselt die Berechtigungsinformationen, also etwa die Schlosskennung, in diesem Fall daher derart, dass nur die Schließeinheit mit der entsprechenden Schlosskennung, für welche die Berechtigung vorliegt, auf Grund des dort vorliegenden schloss-individuellen Verschlüsselungsschlüssels die Berechtigungsinformationen entschlüsseln und in der Folge an Hand der entschlüsselten Information die Zutrittsberechtigung ermitteln kann. Das unauthorisierte Auslesen der Berechtigungsinformationen aus der zentralen Recheneinheit oder dem Schlüssel ist daher im Sinne der Umgebung der Zutrittskontrolle nicht zielführend, solange der jeweils verwendete schloss-individuelle Verschlüsselungsschlüssel nicht bekannt ist.

Zur weiteren Erhöhung der Sicherheit wird bevorzugt derart vorgegangen, dass den Schlüsseln jeweils ein schlüsselindividueller Verschlüsselungsschlüssel zugeordnet wird, dass die Berechtigungsinformationen für einen Schlüssel in der

zentralen Recheneinheit mit dem jeweils zugeordneten schlüssel-individuellen Verschlüsselungsschlüssel verschlüsselt und als schlüssel-individuell verschlüsselte Berechtigungsinformationen an das Telekommunikationsgerät bzw. den Schlüssel gesendet und dort gespeichert werden und dass die schlüssel-individuell verschlüsselten Berechtigungsinformationen im Schlüssel unter Verwendung des dort gespeicherten, zugeordneten schlüssel-individuellen Verschlüsselungsschlüssels entschlüsselt werden. Bei dieser Vorgehensweise werden die Berechtigungsinformationen nicht schloss-individuell, sondern schlüssel-individuell verschlüsselt. Die an einen bestimmten Schlüssel gesendeten Berechtigungsinformationen werden hierbei mit dem diesem Schlüssel zugeordneten Verschlüsselungsschlüssel, z.B. mit einer Schlüssel-ID, verschlüsselt, sodass nur dieser Schlüssel die Berechtigungsinformationen entschlüsseln und verwenden kann. Das unauthorisierte Auslesen der verschlüsselten Berechtigungsinformationen vom Schlüssel ist daher insofern im Sinne der Umgebung der Zutrittskontrolle nicht zielführend als ein Entschlüsseln und Verwenden der Berechtigungsinformationen dann nicht mehr möglich ist. Zur weiteren Erhöhung der Sicherheit kann der schlüssel-individuelle Schlüssel in einfacher Weise mit dem allgemeinen Systemschlüssel gekoppelt werden (z.B. von diesem verschlüsselt werden).

Eine weitere Erhöhung der Sicherheit ist dann möglich, wenn die Berechtigungsinformationen sowohl mit einem schloss-individuellen Verschlüsselungsschlüssel als auch mit einem schlüssel-individuellen Verschlüsselungsschlüssel verschlüsselt werden. Das Verfahren wird in diesem Fall bevorzugt derart durchgeführt, dass die Berechtigungsinformationen in der zentralen Recheneinheit zuerst jeweils mit dem schloss-individuellen Verschlüsselungsschlüssel verschlüsselt werden, dass die schloss-individuell verschlüsselten Berechtigungsinformationen danach mit dem schlüssel-individuellen Verschlüs-

selungsschlüssel verschlüsselt werden, dass die schloss- und schlüssel-individuell verschlüsselten Berechtigungsinformationen an das Telekommunikationsgerät bzw. den Schlüssel gesendet und dort gespeichert werden, dass die schloss- und schlüssel-individuell verschlüsselten Berechtigungsinformationen im Schlüssel unter Verwendung des im Schlüssel gespeicherten schlüssel-individuellen Verschlüsselungsschlüssels entschlüsselt werden, dass die (teil-)entschlüsselten Berechtigungsinformationen an die Schließeinheit übermittelt und in der Schließeinheit unter Verwendung des dort gespeicherten schloss-individuellen Verschlüsselungsschlüssels entschlüsselt werden. Die Berechtigungsinformationen werden somit doppelt verschlüsselt, wobei die Entschlüsselung zweistufig erfolgt. Zunächst kann nur derjenige Schlüssel, für welchen die Berechtigungsinformationen beabsichtigt sind, die schlüssel-individuelle Verschlüsselung entschlüsseln. Es verbleibt im Schlüssel dann ein oder mehrere schloss-individuell verschlüsselte(s) Datenpaket(e) für eine oder mehrere Schließeinheiten. Nach Übertragung dieser Daten an eine Schließeinheit kann diese die Daten endgültig entschlüsseln und die entsprechende Aktion (z.B. Berechtigungsprüfung) vornehmen. Mit dieser Vorgehensweise könnten Kopierattacken entlang des Informationsweges verhindert werden. Des Weiteren müssen nicht die gesamten Informationswege gesichert sein, denn die Daten sind ohnehin nur von den jeweils berechtigten Empfängern entschlüsselbar.

Zur weiteren Erhöhung der Sicherheit gegen unautorisierte Handlungen wird bevorzugt derart vorgegangen, dass das übermitteln der Berechtigungsinformationen vom Schlüssel an die Schließeinheit über eine gesicherte Verbindung erfolgt. Die erfindungsgemäße Vorrichtung ist hierbei bevorzugt derart weitergebildet, dass Mittel zum Herstellen einer gesicherten Verbindung für das Übermitteln der Berechtigungsinformationen vom Schlüssel an die Schließeinheit vorgesehen sind. Bei einer

derartigen Ausbildung wird verhindert, dass die Berechtigungsinformationen während der drahtlosen Übertragung vom Schlüssel an die Schließeinheit „abgehört" werden.

Weiters kann bevorzugt auch vorgesehen sein, dass das Senden der Berechtigungsinformationen von der zentralen Recheneinheit an das mobile Telekommunikationsgerät bzw. den Schlüssel über eine gesicherte Verbindung erfolgt.

Die Zutrittsberechtigung muss im Rahmen der Erfindung nicht notwendiger Weise anhand einer Schlosskennung erfolgen. Denkbar ist es auch, dass die Berechtigungsinformationen eine Schlüsselkennung enthält. Die Überprüfung der Zutrittsberechtigung in der Schließeinheit kann in einem solchen Fall naturgemäß nicht auf einem einfachen Vergleich mit der in der Schließeinheit gespeicherten Schlosskennung beruhen. Vielmehr könnte die Schließeinheit die Zutrittsberechtigung aus der jeweiligen Schlüsselkennung unter Anwendung eines Rechenalgorithmus ermitteln. Dieser Rechenalgorithmus müsste auch bei der Erstellung des Schlüssels in der zentralen Recheneinheit berücksichtigt werden. Die Berechtigungsinformationen können aber beides, eine Schlosskennung und die jeweilige Schlüsselkennung, enthalten. Dies ist bei einer bevorzugten Verfahrensweise von Vorteil, bei welcher die Ermittlung der Zutrittsberechtigung in der Schließeinheit zusätzlich den Vergleich einer vom Schlüssel empfangenen Schlüsselkennung mit einer in der Schließeinheit gespeicherten Schlüsselkennungsliste umfasst, wobei bei Übereinstimmung der empfangenen Schlüsselkennung mit einer Schlüsselkennung aus der Schlüsselkennungsliste der Zutritt verwehrt wird. Die erfindungsgemäße Vorrichtung ist hierbei bevorzugt derart weitergebildet, dass die Schließeinheit einen Speicher für eine Schlüsselkennungsliste aufweist, der mit der Auswerteschaltung in der Schließeinheit den Vergleich einer vom Schlüssel empfangenen Schlüsselkennung mit

einer in der Schließeinheit gespeicherten Schlüsselkennungsliste umfasst, wobei bei Übereinstimmung der empfangenen Schlüsselkennung mit einer Schlüsselkennung aus der Schlüsselkennungsliste der Zutritt verwehrt wird.

Die in der Schließeinheit gespeicherte Schlüsselkennungsliste bildet daher eine so genannte „black list", enthaltend diejenigen Schlüsselkennungen, für die, unabhängig davon, ob sich auf Grund der vom Schlüssel übermittelten Schlosskennung eine Zutrittsberechtigung ergeben würde oder nicht, jedenfalls kein Zutritt gewährt werden soll. Dies ist zum Beispiel dann von besonderem Nutzen, wenn einzelnen Benutzer des Systems die Zutrittsberechtigung entzogen werden soll und das mobile Telekommunikationsgerät der betroffenen Benutzer von der zentralen Recheneinheit nicht erreichbar ist, um die Berechtigungsinformationen über diesen Weg entsprechend verändern zu können.

Gemäß einer bevorzugten Vorgangsweise wird hierbei derart vorgegangen, dass die Schlüsselkennungsliste in der zentralen Recheneinheit gespeichert und verwaltet wird, über das drahtlose Telekommunikationsnetz an mobile Telekommunikationsgeräte übermittelt, drahtlos von einem Schlüssel an die Schließeinheit gesendet und in der Schließeinheit gespeichert wird. Die Vorrichtung ist in diesem Zusammenhang bevorzugt derart weitergebildet, dass die zentrale Recheneinheit einen Speicher für die Schlüsselkennungsliste aufweist und Mittel zum Übermitteln der Schlüsselkennungsliste über das drahtlose Telekommunikationsnetz an mobile Telekommunikationsgeräte und zum drahtlosen Senden der Schlüsselkennungsliste von einem Schlüssel an die Schließeinheit vorgesehen sind. Bei einer derartigen Ausbildung kann die Schlüsselkennungsliste, die bevorzugt in allen Schließeinheiten eines Systems bereit gehalten wird, in einfacher Weise und innerhalb kürzester Zeit aktualisiert werden, um zusätzliche Schlüsselkennungen in die Liste einzu-

fügen oder um Schlüsselkennungen aus der Liste zu streichen. Die Schlüsselkennungsliste einer bestimmten Schließeinheit wird hierbei aktualisiert, sobald der erste Benutzer, dessen mobiles Telekommunikationsgerät bzw. dessen Schlüssel von der zentralen Recheneinheit hinsichtlich der Schlüsselkennungsliste aktualisiert wurde, sich an die betreffende Schließeinheit annähert und einen Öffnungs- oder Schließvorgang initiiert. Wenn nun nach einem derartigen Aktualisierungsvorgang der in der Schließeinheit gespeicherten Schlüsselkennungsliste ein Benutzer einen Öffnungs- oder Schließvorgang initiieren möchte, dessen Schlüsselkennung zwischenzeitlich in die Schlüsselkennungsliste aufgenommen wurde, dessen mobiles Telekommunikationsgerät sich aber außerhalb der Reichweite des Telekommunikationsnetzwerks befand bzw. von der zentrale Recheneinheit nicht erreicht werden konnte, so wird diesem der Zugang dennoch verwehrt.

Um die Datenübertragung zwischen der zentralen Recheneinheit und den mobilen Telekommunikationsgeräten zu vereinfachen, wird bevorzugt derart vorgegangen, dass die Berechtigungsinformationen und/oder die Schlüsselkennungsliste als Kurztextmitteilung über das drahtlose Telekommunikationsnetz an das mobiles Telekommunikationsgerät übermittelt werden. Die erfindungsgemäße Vorrichtung ist in diesem Zusammenhang bevorzugt derart weitergebildet, dass ein Kurztextmitteilungsdienst vorgesehen ist zum Übermitteln der Berechtigungsinformationen und/oder der Schlüsselkennungsliste als Kurztextmitteilung über das drahtlose Telekommunikationsnetz an das mobiles Telekommunikationsgerät. Das Übersenden einer Kurztextmitteilung an das mobile Telekommunikationsgerät hat den Vorteil, dass der Empfang ohne Einwirkungsmöglichkeit bzw. ohne Mitwirkung des Benutzers erfolgt, sodass der Bedienungsaufwand minimiert wird. Zur erfolgreichen Datenübermittlung reicht es aus, dass das mobile Telekommunikationsgerät sich innerhalb des Sendebe-

reichs des Telekommunikationsnetzes befindet und dass das Gerät angeschaltet ist. Es bedarf nicht notwendigerweise einer benutzerseitigen Anforderung an die zentrale Recheneinheit, um die Übermittlung von Berechtigungsinformationen, von Statusinformationen und dergleichen auszulösen.

Wenn nun aber jemand beispielsweise eine Zugangsberechtigung zu einer bestimmten Schließeinheit erhalten möchte, für die er bisher keine Zugangsberechtigung hat, so sollte es möglich sein, dass der Benutzer eine diesbezügliche Anfrage an die zentrale Recheneinheit sendet. Zu diesem Zweck wird das Verfahren bevorzugt derart durchgeführt, dass das Senden der Berechtigungsinformationen von der zentralen Recheneinheit an das mobile Telekommunikationsgerät als Antwort auf eine vom Benutzer vom mobilen Telekommunikationsgerät an die zentrale Recheneinheit gesendete Anfrage erfolgt.

Um die Verwaltung von größeren Schließanlagen mit einer Vielzahl von Schließeinheiten und Schlüsseln zu vereinfachen, ist es von Vorteil, wenn in der zentralen Recheneinheit eine Übersicht über den Status der einzelnen Schließeinheiten abgefragt werden kann. Zu diesem Zweck bedarf es einer Übertragung von Statusinformationen von den Schließeinheiten zur zentralen Recheneinheit. Das erfindungsgemäße Verfahren ist in diesem Zusammenhang bevorzugt derart weitergebildet, dass Statusinformationen der Schließeinheit, wie z.B. Batterieladezustand, Log-Daten oder dgl., drahtlos an den Schlüssel bzw. das mobile Telekommunikationsgerät übertragen und vom mobilen Telekommunikationsgerät über das drahtlose Telekommunikationsnetz an die zentrale Recheneinheit versendet werden. Die erfindungsgemäße Vorrichtung ist in diesem Zusammenhang derart weitergebildet, dass die Schließeinheit einen Speicher für Statusinformationen der Schließeinheit, wie z.B. Batterieladezustand, Log-Daten oder dgl. und Mittel zum drahtlosen Übertragen der

Statusinformationen an den Schlüssel bzw. das mobile Telekommunikationsgerät aufweist. Wenn bei jedem Öffnungs- oder Schließvorgang der Schließeinheiten jeweils Statusinformationen übertragen werden, so ist es möglich, in der zentralen Recheneinheit Informationen zu jedem einzelnen Schließ- und Öffnungsvorgang abzurufen, sowohl jede Schließeinheit als auch jeden Schlüssel betreffend.

Es ist aber auch möglich, eine Datenübertragung in umgekehrter Richtung, von der zentralen Recheneinheit an einzelne Schließeinheiten, durchzuführen, abgesehen von der Übertragung von Berechtigungsinformationen. Eine derartige Datenübertragung kann beispielsweise der Programmierung von Schließeinheiten dienen, z.B. im Zusammenhang mit einer Erstinbetriebnahme, bei welcher jede Schließeinheit mit einer Schlosskennung und ggf. eines schloss-individuellen Verschlüsselungsschlüssels versehen wird. Hierbei dient das mobile Telekommunikationsgerät, über welches die Datenübertragung vorgenommen wird, als Programmiergerät für die Schließeinheiten.

Insgesamt wird mit der Erfindung die Steuerung der Zutrittskontrolle wesentlich vereinfacht, wobei eine Netzanbindung der Schließeinheiten nicht erforderlich ist. Die Ermittlung der Zutrittsberechtigung in der Schließeinheit erfolgt mit Vorteil daher lediglich auf Grund der vom Schlüssel erhaltenen und der gegebenenfalls in der Schließeinheit bereits gespeicherten Daten. Für die Ermittlung der Zutrittsberechtigung ist es daher nicht notwendig, dass die Schließeinheit zusätzlich zu den jeweils vom Schlüssel erhaltenen Daten für eine oder während einer Zutrittskontrolle weitere Daten von gesonderten Kontroll- oder Authentifizierungsstellen oder von der zentralen Recheneinheit erhält. Vielmehr ist hierbei vorgesehen, dass die Schließeinheiten als autonome Einheiten ohne Netzwerkanbindung ausgebildet sind.

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 und Fig. 2 eine weitere Ausbildung eines Zutrittskontrollsystems.

In Fig. 1 ist eine zentrale Recheneinheit mit 1 bezeichnet. Die Objekte, zu denen der Zutritt mit Hilfe des Zutrittskontrollsystems kontrolliert werden soll, sind mit 2 bezeichnet und im vorliegenden Fall schematisch als Häuser dargestellt. Die Objekte 2 weisen jeweils eine Tür mit einer auf RFID basierenden Schließeinheit auf. Ein Administrator 3 verwaltet die zentrale Recheneinheit 1 und kann Zutrittsberechtigungen vergeben. Die zentrale Recheneinheit 1 ist an eine mobiles, drahtloses Telekommunikationsnetzwerk 4 angeschlossen, wie beispielsweise ein GSM-Handy-Netz und kann über das GSM-Netz 4 Berechtigungsinformationen an mobile Telekommunikationseinrichtungen 5 senden. Bei den mobilen Telekommunikationseinrichtungen 5 handelt es sich um Handys, die mit einer Schlüsselfunktion ausgestattet sind. Die Handys weisen beispielsweise ein RFID-Modul auf, in dessen Speicher die von der zentralen Recheneinheit 1 erhaltenen Berechtigungsinformationen geschrieben werden können. Im einfachsten Fall wird die Berechtigungsinformation als Schlosskennung an das mobile Telekommunikationsgerät 5 gesendet. Wenn nun in einem stark vereinfachten Beispiel die Schließeinheiten der in Fig. 1 dargestellten Objekte die Kennung 100, 101 und 102 aufweisen, so bedeutet die Übermittlung der Berechtigungsinformation an ein Telekommunikationsgerät 5 in Form der Kennung 101, dass dies einer Zugangsberechtigung für die Schließeinheit mit der Kennung 101 entspricht. Wenn nun das als Schlüssel verwendete Telekommunikationsgerät 5 in die Nähe einer Schließeinheit mit der Kennung 101 gebracht wird und im Zuge der Zutrittsberechtigungs-

prüfung die Berechtigungsinformation, nämlich die Schlosskennung „101" an die Schließeinheit übermittelt wird, so erkennt die Schließeinheit auf Grund eines Vergleichs der vom Schlüssel übermittelten Schlosskennung mit der eigenen Schlosskennung bei Übereinstimmung derselben das Vorhandensein einer Zutrittsberechtigung, worauf das Schloss freigegeben wird.

Aus der Darstellung in Fig. 2 ergeben sich nun verschiedene Anwendungsmöglichkeiten. Die zentrale Recheneinheit ist wiederum mit 1 und der Administrator mit 3 bezeichnet. Die zentrale Recheneinheit 1 weist eine Datenbank 6 auf bzw. ist mit einer derartigen Datenbank verbunden, auf welcher die Zutrittsberechtigungen gespeichert und verwaltet werden. Die zentrale Recheneinheit 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 zentralen Recheneinheit 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 W-LAN, GSM oder UMTS mit dem Internet 9 hergestellt werden, wobei auch die zentrale Recheneinheit 1 mit dem Internet 9 verbunden ist. Alternativ oder zusätzlich dazu kann ein SMS-Gateway 10 vorgesehen sein, sodass der Datenaustausch zwischen der zentralen Recheneinheit 1 und dem mobilen Telekommunikationsgerät 5 über einen Kurzmitteilungsdienst erfolgt.

Der Benutzer 11 des mobilen Telekommunikationsgeräts 5 kann hierbei, wie mit der Linie 12 angedeutet, auf die zentrale Recheneinheit 1 zugreifen und, wenn er die erforderlichen Zugriffsrechte auf die zentrale Recheneinheit 1 aufweist, die Zugangsberechtigungen verwalten. Wenn es sich bei dem Benutzer 11 nicht um den Administrator handelt, so ist der ihm auf die zentrale Recheneinheit 1 gewährte Zugriff derart gestaltet, dass er lediglich seine eigenen Zutrittsberechtigungen verwalten und gegebenenfalls ändern kann. Der Zugriff auf die zentrale Recheneinheit 1 kann beispielsweise über ein WEB-Interface 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 zentralen Recheneinheit 1 erhaltenen Berechtigungsinformationen dem eingebauten NFC-Modul zur Verfügung gestellt, sodass die Berechtigungsinformationen 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 zentralen Recheneinheit 1 übermittelten Berechtigungsinformationen 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.

Patentansprüche:

1. Verfahren zur Steuerung der Zutrittskontrolle mit Schließeinheiten, insbesondere Schlössern, und elektronischen Schlüsseln, bei welchem Zutrittsberechtigungen in einer zentralen Recheneinheit gespeichert und verwaltet werden, die Schlüssel entsprechend der jeweiligen Zutrittsberechtigung mit Berechtigungsinformationen für eine vorgegebene Auswahl an Schließeinheiten programmiert werden, die Berechtigungsinformationen im Falle eines Zutrittswunsches drahtlos von einem Schlüssel an eine Schließeinheit gesendet werden und in der Schließeinheit in Abhängigkeit von den empfangenen Berechtigungsinformationen die Zutrittsberechtigung ermittelt wird, dadurch gekennzeichnet, dass die Programmierung eines Schlüssels das Senden der Berechtigungsinformationen über ein drahtloses Telekommunikationsnetz an ein drahtloses mobiles Telekommunikationsgerät und das Übermitteln der vom mobilen Telekommunikationsgerät empfangenen Berechtigungsinformationen an einen Speicher des Schlüssels umfasst.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass das mobile Telekommunikationsgerät als Schlüssel verwendet wird und das Übermitteln der vom mobilen Telekommunikationsgerät empfangenen Berechtigungsinformationen an einen Speicher des Schlüssels das Schreiben der Berechtigungsinformationen in einen einer Kommunikationsschnittstelle des mobilen Telekommunikationsgeräts zum drahtlosen Senden der Berechtigungsinformationen an die Schließeinheit zugeordneten Speicher umfasst.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass das Übermitteln der vom mobilen Telekommunikationsgerät empfangenen Berechtigungsinformationen an einen Speicher des Schlüssels die Verwendung einer Schreib-/Leseeinrichtung für Identifikationsmedien oder dgl. umfasst.

4. Verfahren nach Anspruch 1, 2 oder 3, dadurch gekennzeichnet, dass die Berechtigungsinformation wenigstens eine Schlosskennung enthält.

5. Verfahren nach Anspruch 4, dadurch gekennzeichnet, dass die Ermittlung der Zutrittsberechtigung in der Schließeinheit den Vergleich der empfangenen Berechtigungsinformationen mit der in der Schließeinheit gespeicherten eigenen Schlosskennung umfasst.

6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass die Berechtigungsinformationen im Schlüssel verschlüsselt vorliegen.

7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, dass alle Berechtigungsinformationen mit einem allgemeinen Systemschlüssel verschlüsselt vorliegen.

8. Verfahren nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass den Schließeinheiten jeweils ein schloss-individueller Verschlüsselungsschlüssel zugeordnet wird, dass die Berechtigungsinformationen für eine Schließeinheit in der zentralen Recheneinheit mit dem jeweils zugeordneten schloss-individuellen Verschlüsselungsschlüssel verschlüsselt und als schloss-individuell verschlüsselte Berechtigungsinformationen an das Telekommunikationsgerät bzw. den Schlüssel gesendet und dort gespeichert werden und dass die schloss-individuell verschlüsselten Berechtigungsinformationen in der Schließeinheit unter Verwendung des dort gespeicherten, zugeordneten schloss-individuellen Verschlüsselungsschlüssels entschlüsselt werden.

9. Verfahren nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, dass den Schlüsseln jeweils ein schlüssel-

individueller Verschlüsselungsschlüssel zugeordnet wird, dass die Berechtigungsinformationen für einen Schlüssel in der zentralen Recheneinheit mit dem jeweils zugeordneten schlüssel-individuellen Verschlüsselungsschlüssel verschlüsselt und als schlüssel-individuell verschlüsselte Berechtigungsinformationen an das Telekommunikationsgerät bzw. den Schlüssel gesendet und dort gespeichert werden und dass die schlüssel-individuell verschlüsselten Berechtigungsinformationen im Schlüssel unter Verwendung des dort gespeicherten, zugeordneten schlüssel-individuellen Verschlüsselungsschlüssels entschlüsselt werden.

10. Verfahren nach Anspruch 8 und 9, dadurch gekennzeichnet, dass die Berechtigungsinformationen in der zentralen Recheneinheit zuerst jeweils mit dem schloss-individuellen Verschlüsselungsschlüssel verschlüsselt werden, dass die schloss-individuell verschlüsselten Berechtigungsinformationen danach mit dem schlüssel-individuellen Verschlüsselungsschlüssel verschlüsselt werden, dass die schloss- und schlüssel-individuell verschlüsselten Berechtigungsinformationen an das Telekommunikationsgerät bzw. den Schlüssel gesendet und dort gespeichert werden, dass die schloss- und schlüssel-individuell verschlüsselten Berechtigungsinformationen im Schlüssel unter Verwendung des im Schlüssel gespeicherten schlüssel-individuellen Verschlüsselungsschlüssels entschlüsselt werden, dass die (teil-)entschlüsselten Berechtigungsinformationen an die Schließeinheit übermittelt und in der Schließeinheit unter Verwendung des dort gespeicherten schloss-individuellen Verschlüsselungsschlüssels entschlüsselt werden.

11. Verfahren nach einem der Ansprüche 1 bis 10, dadurch gekennzeichnet, dass das Übermitteln der Berechtigungsinformationen vom Schlüssel an die Schließeinheit über eine gesicherte Verbindung erfolgt.

12. Verfahren nach einem der Ansprüche 1 bis 11, dadurch gekennzeichnet, dass das Senden der Berechtigungsinformationen von der zentralen Recheneinheit an das mobile Telekommunikationsgerät bzw. den Schlüssel über eine gesicherte Verbindung erfolgt.

13. Verfahren nach einem der Ansprüche 1 bis 12, dadurch gekennzeichnet, dass das Übermitteln der Berechtigungsinformationen vom Schlüssel an die Schließeinheit unter Verwendung von RFID erfolgt.

14. Verfahren nach einem der Ansprüche 1 bis 13, dadurch gekennzeichnet, dass das Übermitteln der Berechtigungsinformationen vom Schlüssel an die Schließeinheit unter Verwendung von Nahfeldkommunikation, beispielsweise nach dem NFC-Standard, erfolgt.

15. Verfahren nach einem der Ansprüche 1 bis 14, dadurch gekennzeichnet, dass die Ermittlung der Zutrittsberechtigung in der Schließeinheit zusätzlich den Vergleich einer vom Schlüssel empfangenen Schlüsselkennung mit einer in der Schließeinheit gespeicherten Schlüsselkennungsliste umfasst, wobei bei Übereinstimmung der empfangenen Schlüsselkennung mit einer Schlüsselkennung aus der Schlüsselkennungsliste der Zutritt verwehrt wird.

16. Verfahren nach Anspruch 15, dadurch gekennzeichnet, dass die Schlüsselkennungsliste in der zentralen Recheneinheit gespeichert und verwaltet wird, über das drahtlose Telekommunikationsnetz an mobile Telekommunikationsgeräte übermittelt, drahtlos von einem Schlüssel an die Schließeinheit gesendet und in der Schließeinheit gespeichert wird.

17. Verfahren nach einem der Ansprüche 1 bis 16, dadurch gekennzeichnet, dass die Berechtigungsinformationen und/oder die Schlüsselkennungsliste als Kurztextmitteilung über das drahtlose Telekommunikationsnetz an das mobiles Telekommunikationsgerät übermittelt werden.

18. Verfahren nach einem der Ansprüche 1 bis 17, dadurch gekennzeichnet, dass die Ermittlung der Zutrittsberechtigung in der Schließeinheit lediglich auf Grund der vom Schlüssel erhaltenen Daten erfolgt.

19. Verfahren nach einem der Ansprüche 1 bis 18, dadurch gekennzeichnet, dass das Senden der Berechtigungsinformationen von der zentralen Recheneinheit an das mobile Telekommunikationsgerät als Antwort auf eine vom Benutzer vom mobilen Telekommunikationsgerät an die zentrale Recheneinheit gesendete Anfrage erfolgt.

20. Verfahren nach einem der Ansprüche 1 bis 19, dadurch gekennzeichnet, dass Statusinformationen der Schließeinheit, wie z.B. Batterieladezustand, Log-Daten, Schließzustand oder dgl., drahtlos an den Schlüssel bzw. das mobile Telekommunikationsgerät übertragen und vom mobilen Telekommunikationsgerät über das drahtlose Telekommunikationsnetz an die zentrale Recheneinheit versendet werden.

21. Vorrichtung zur Zutrittskontrolle, insbesondere zur Durchführung des Verfahrens nach einem der Ansprüche 1 bis 20, umfassend

- eine Mehrzahl von Schließeinheiten, insbesondere Schlössern, und Schlüsseln zum berührungslosen Sperren und Entsperren der Schließeinheiten,
- eine zentrale Recheneinheit zum Speichern und Verwalten von Zutrittsberechtigungen,

- Mittel, um die Schlüssel entsprechend der jeweiligen Zutrittsberechtigung mit Berechtigungsinformationen für eine vorgegebene Auswahl an Schließeinheiten zu programmieren,
- Mittel zum drahtlosen Übermitteln der Berechtigungsinformationen vom Schlüssel an die Schließeinheit,

wobei die Schließeinheit jeweils eine Auswerteschaltung aufweist, um die Zutrittsberechtigung auf Grund der erhaltenen Berechtigungsinformationen zu ermitteln, dadurch gekennzeichnet, dass die Vorrichtung weiters wenigstens ein drahtloses mobiles Telekommunikationsgerät umfasst, dass die Mittel zum Programmieren der Schlüssel Mittel zum Senden der Berechtigungsinformationen über ein drahtloses Telekommunikationsnetz an eine erste Kommunikationsschnittstelle des mobilen Telekommunikationsgeräts umfassen und dass Mittel zum Übermitteln der vom mobilen Telekommunikationsgerät empfangenen Berechtigungsinformationen an einen Speicher des Schlüssels vorgesehen sind.

22. Vorrichtung nach Anspruch 21, dadurch gekennzeichnet, dass der Schlüssel im Telekommunikationsgerät ausgebildet ist und der Speicher als mit einer zweiten Kommunikationsschnittstelle des mobilen Telekommunikationsgeräts verbundener Speicher des Telekommunikationsgeräts ausgebildet ist, welche zweite Kommunikationsschnittstelle von der ersten Kommunikationsschnittstelle verschieden und zum drahtlosen Übermitteln der Berechtigungsinformationen vom Schlüssel an die Schließeinheit ausgebildet ist.

23. Vorrichtung nach Anspruch 21, dadurch gekennzeichnet, dass die Mittel zum Übermitteln der vom mobilen Telekommunikationsgerät empfangenen Berechtigungsinformationen an einen

Speicher des Schlüssels eine Schreib-/Leseeinrichtung für Identifikationsmedien oder dgl. umfasst.

24. Vorrichtung nach Anspruch 21, 22 oder 23, dadurch gekennzeichnet, dass die Berechtigungsinformation wenigstens eine Schlosskennung enthält.

25. Vorrichtung nach einem der Ansprüche 21 bis 24, dadurch gekennzeichnet, dass die Auswerteschaltung der Schließeinheit eine Vergleichsschaltung zum Vergleichen der empfangenen Berechtigungsinformationen mit der eigenen Schlosskennung umfasst.

26. Vorrichtung nach einem der Ansprüche 21 bis 25, dadurch gekennzeichnet, dass die Berechtigungsinformationen im Schlüssel verschlüsselt vorliegen.

27. Vorrichtung nach einem der Ansprüche 21 bis 26, dadurch gekennzeichnet, dass alle Berechtigungsinformationen mit einem allgemeinen Systemschlüssel verschlüsselt vorliegen.

28. Vorrichtung nach einem der Ansprüche 21 bis 27, dadurch gekennzeichnet, dass die Berechtigungsinformationen schlossindividuell verschlüsselt vorliegen und dass die Auswerteschaltung eine Entschlüsselungseinrichtung umfasst.

29. Vorrichtung nach einem der Ansprüche 21 bis 28, dadurch gekennzeichnet, dass die Berechtigungsinformationen im Schlüssel schlüssel-individuell verschlüsselt vorliegen und dass der Schlüssel eine Entschlüsselungseinrichtung umfasst.

30. Vorrichtung nach einem der Ansprüche 21 bis 29, dadurch gekennzeichnet, dass Mittel zum Herstellen einer gesicherten

Verbindung für das Übermitteln der Berechtigungsinformationen vom Schlüssel an die Schließeinheit vorgesehen sind.

31. Vorrichtung nach einem der Ansprüche 21 bis 30, dadurch gekennzeichnet, dass Mittel zum Herstellen einer gesicherten Verbindung für das Senden der Berechtigungsinformationen von der zentralen Recheneinheit an das mobile Telekommunikationsgerät bzw. den Schlüssel vorgesehen sind

32. Vorrichtung nach einem der Ansprüche 21 bis 31, dadurch gekennzeichnet, dass der Schlüssel als RFID-Datenträger ausgebildet ist.

33. Vorrichtung nach einem der Ansprüche 21 bis 32, dadurch gekennzeichnet, dass die Mittel zum drahtlosen Übermitteln der Berechtigungsinformationen vom Schlüssel an die Schließeinheit für die Nahfeldkommunikation, beispielsweise nach dem NFC-Standard, ausgebildet sind.

34. Vorrichtung nach einem der Ansprüche 21 bis 33, dadurch gekennzeichnet, dass die Schließeinheit einen Speicher für eine Schlüsselkennungsliste aufweist, der mit der Auswerteschaltung derart zusammenwirkt, dass die Ermittlung der Zutrittsberechtigung in der Schließeinheit den Vergleich einer vom Schlüssel empfangenen Schlüsselkennung mit einer in der Schließeinheit gespeicherten Schlüsselkennungsliste umfasst, wobei bei Übereinstimmung der empfangenen Schlüsselkennung mit einer Schlüsselkennung aus der Schlüsselkennungsliste der Zutritt verwehrt wird.

35. Vorrichtung nach Anspruch 34, dadurch gekennzeichnet dass die zentrale Recheneinheit einen Speicher für die Schlüsselkennungsliste aufweist und Mittel zum Übermitteln der Schlüsselkennungsliste über das drahtlose Telekommunikationsnetz an

mobile Telekommunikationsgeräte und zum drahtlosen Senden der Schlüsselkennungsliste von einem Schlüssel an die Schließeinheit vorgesehen sind.

36. Vorrichtung nach einem der Ansprüche 21 bis 35, dadurch gekennzeichnet, dass ein Kurztextmitteilungsdienst vorgesehen ist zum Übermitteln der Berechtigungsinformationen und/oder der Schlüsselkennungsliste als Kurztextmitteilung über das drahtlose Telekommunikationsnetz an das mobiles Telekommunikationsgerät.

37. Vorrichtung nach einem der Ansprüche 21 bis 36, dadurch gekennzeichnet, dass die Schließeinheiten als autonome Einheiten ohne Netzwerkanbindung ausgebildet sind, wobei die Ermittlung der Zutrittsberechtigung in der Schließeinheit lediglich auf Grund der vom Schlüssel erhaltenen Daten erfolgt.

38. Vorrichtung nach einem der Ansprüche 21 bis 37, dadurch gekennzeichnet, dass die Schließeinheit einen Speicher für Statusinformationen der Schließeinheit, wie z.B. Batterieladezustand, Log-Daten, Schließzustand oder dgl., aufweist und Mittel zum drahtlosen Übertragen der Statusinformationen an den Schlüssel bzw. das mobile Telekommunikationsgerät.

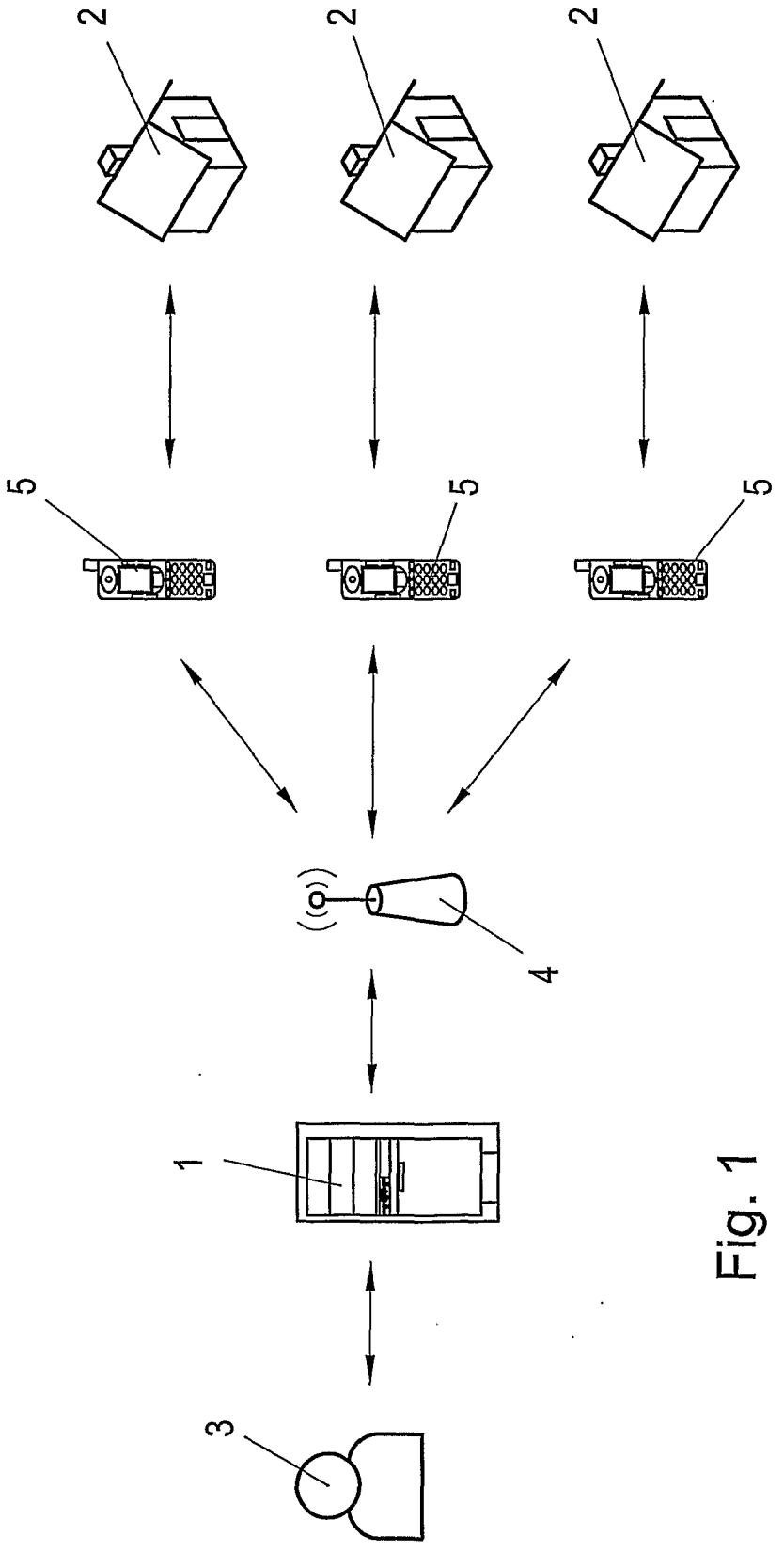
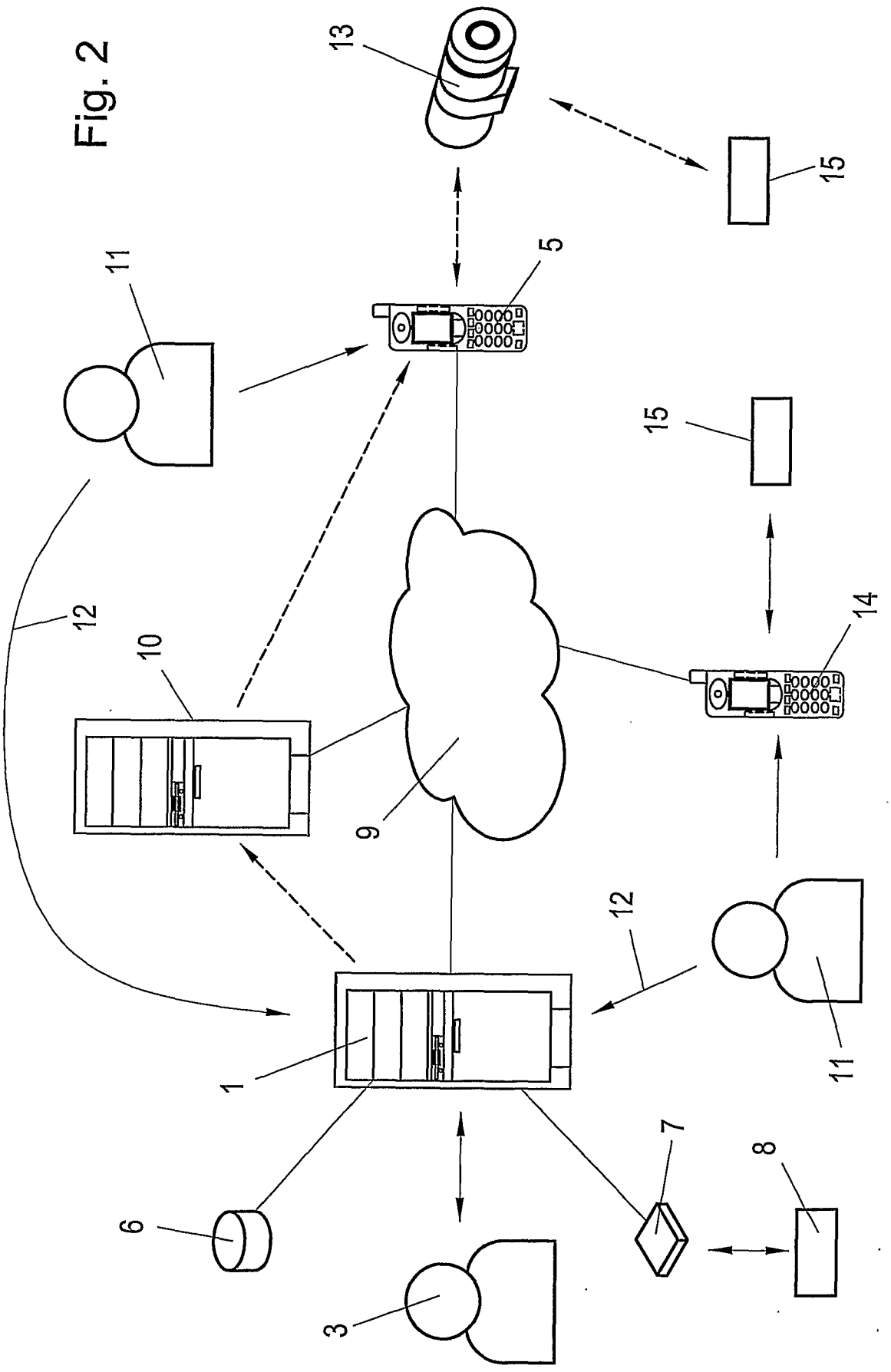


Fig. 1

Fig. 2



INTERNATIONAL SEARCH REPORT

International application No
PCT/AT2009/000033

A. CLASSIFICATION OF SUBJECT MATTER
INV. G07C9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G07C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 336 937 A (SWISSCOM AG [CH]) 20 August 2003 (2003-08-20) abstract; figures paragraphs [0015] - [0025] -----	1-38
X	US 2005/242921 A1 (ZIMMERMAN TIMOTHY M [US] ET AL ZIMMERMAN TIMOTHY M [US] ET AL) 3 November 2005 (2005-11-03) abstract; figure 2 paragraphs [0005], [0012] - [0014] paragraphs [0044] - [0055] claims 1,2,6,7 ----- -/--	1-8, 11-14, 18,19, 21-28, 31-33

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 April 2009	21/04/2009

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Fax: (+31–70) 340–3016	Buron, Emmanuel

INTERNATIONAL SEARCH REPORT

International application No
PCT/AT2009/000033

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2007/126375 A (SICS SWEDISH INST OF COMP SCIE [SE]; SADIGHI BABAK [SE]; CAO LING [SE]) 8 November 2007 (2007-11-08) figures 6,7 page 4, line 15 - page 7, line 2 page 22, line 11 - page 23, last line	1-14,18, 19, 21-33,37
X	US 6 072 402 A (KNIFFIN JOHN M [US] ET AL) 6 June 2000 (2000-06-06) abstract; figure 2 column 2, lines 1-5 column 2, lines 31-35 column 5, line 65 - column 8, line 2 column 10, lines 16-19	1-7, 11-16, 19-27, 31-35, 37,38

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/AT2009/000033

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1336937 A	20-08-2003	AT 268926 T	15-06-2004
		DE 50200512 D1	15-07-2004
		DK 1336937 T3	27-09-2004
		ES 2223033 T3	16-02-2005
		PT 1336937 E	29-10-2004
		US 2003151493 A1	14-08-2003
US 2005242921 A1	03-11-2005	NONE	
WO 2007126375 A	08-11-2007	EP 2016566 A1	21-01-2009
		SE 529849 C2	11-12-2007
		SE 0600959 A	29-10-2007
US 6072402 A	06-06-2000	NONE	

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/AT2009/000033

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. G07C9/00

Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
G07C

Recherchierte, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	EP 1 336 937 A (SWISSCOM AG [CH]) 20. August 2003 (2003-08-20) Zusammenfassung; Abbildungen Absätze [0015] - [0025] -----	1-38
X	US 2005/242921 A1 (ZIMMERMAN TIMOTHY M [US] ET AL ZIMMERMAN TIMOTHY M [US] ET AL) 3. November 2005 (2005-11-03) Zusammenfassung; Abbildung 2 Absätze [0005], [0012] - [0014] Absätze [0044] - [0055] Ansprüche 1,2,6,7 ----- -/--	1-8, 11-14, 18,19, 21-28, 31-33

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen [X] Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
14. April 2009	21/04/2009

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Fax: (+31–70) 340–3016	Buron, Emmanuel

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/AT2009/000033

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	WO 2007/126375 A (SICS SWEDISH INST OF COMP SCIE [SE]; SADIGHI BABAK [SE]; CAO LING [SE]) 8. November 2007 (2007-11-08) Abbildungen 6,7 Seite 4, Zeile 15 - Seite 7, Zeile 2 Seite 22, Zeile 11 - Seite 23, letzte Zeile	1-14,18, 19, 21-33,37
X	US 6 072 402 A (KNIFFIN JOHN M [US] ET AL) 6. Juni 2000 (2000-06-06) Zusammenfassung; Abbildung 2 Spalte 2, Zeilen 1-5 Spalte 2, Zeilen 31-35 Spalte 5, Zeile 65 - Spalte 8, Zeile 2 Spalte 10, Zeilen 16-19	1-7, 11-16, 19-27, 31-35, 37,38

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/AT2009/000033

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 1336937 A	20-08-2003	AT 268926 T	15-06-2004
		DE 50200512 D1	15-07-2004
		DK 1336937 T3	27-09-2004
		ES 2223033 T3	16-02-2005
		PT 1336937 E	29-10-2004
		US 2003151493 A1	14-08-2003
US 2005242921 A1	03-11-2005	KEINE	
WO 2007126375 A	08-11-2007	EP 2016566 A1	21-01-2009
		SE 529849 C2	11-12-2007
		SE 0600959 A	29-10-2007
US 6072402 A	06-06-2000	KEINE	