(19) Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 10 2004 045 978 A1** 2006.03.30

(12) **Offenlegungsschrift**

(21) Aktenzeichen: **10 2004 045 978.9**
(22) Anmeldetag: **22.09.2004**
(43) Offenlegungstag: **30.03.2006**

(51) Int Cl.[8]: ***G07C 9/00*** (2006.01)
G06F 12/14 (2006.01)

(71) Anmelder:
Siemens AG, 80333 München, DE

(72) Erfinder:
Schaub, Peter, 81379 München, DE

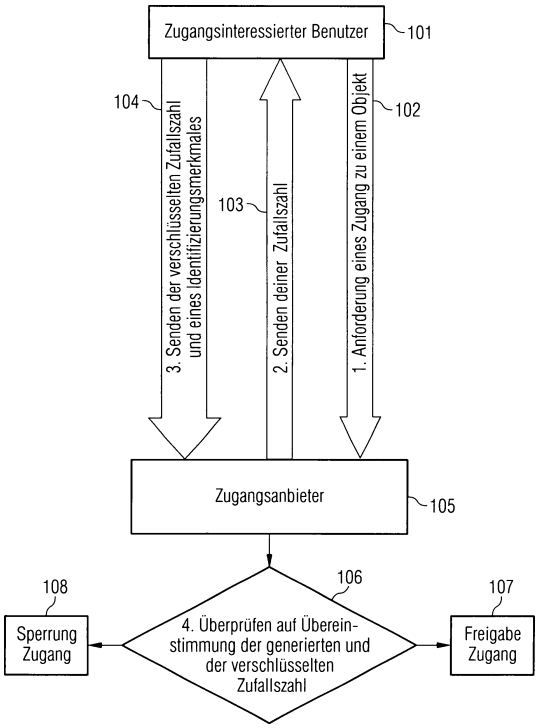
(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:
DE 41 38 816 A1
FR 28 26 394 A1
FR 27 17 286 A1
KÖNIGS, H.-P.: Cryptographic identification methods for smart cards in the process of standardization. In: IEEE Communications Magazine ISSN 0163-6804, 1991, Vol. 29, Issue 6, S. 42-48;

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gemäß § 44 PatG ist gestellt.

(54) Bezeichnung: **Verfahren und System zur Überprüfung und Einräumung einer Zugangsberechtigung für einen Benutzer**

(57) Zusammenfassung: Für die Steuerung des Zugangs zu einem abgeschlossenen Areal, wie beispielsweise einem Firmengelände oder einer Tiefgarage, wird üblicherweise eine Funkfernbedienung benutzt. Über die Funkfernbedienung können dabei mit einer Frequenz von 433 MHz die Steuerungsbefehle zum Öffnen und Schließen des jeweiligen Tores gegeben werden. Nachteilig bei diesen Verfahren ist, dass bei großen Anlagen mit mehreren zugangsberechtigten Benutzern eine Vielzahl von Funkfernbedienungen von den Zugangsanbietern verwaltet werden müssen und hierbei Sicherheitsprobleme entstehen. Aufgabe der vorliegenden Erfindung ist es, ein Verfahren anzugeben, mit dem eine einfache administrative Steuerung der Zugangsberechtigungen durch den Zugangsanbieter ermöglicht wird. Dies wird entsprechend der Erfindung dadurch erreicht, dass die Zugangsberechtigung über einen Datenaustausch zwischen einem Benutzer und einer Authentifizierungseinrichtung festgestellt wird. Zugang zu der Anlage hat somit nicht mehr derjenige, der eine Funkfernbedienung für die Anlage besitzt, sondern derjenige, dessen Identifizierungsmerkmal zudem durch Eintragung bzw. Löschung durch den Zugangsanbieter der Authentifizierungseinrichtung bekannt gemacht wurde.



Beschreibung

[0001] Die vorliegende Erfindung betrifft ein System zur Überprüfung und Einräumung einer Zugangsberechtigung für einen Benutzer, ein Verfahren zur Überprüfung und Einräumung einer Zugangsberechtigung für einen Benutzer und ein Programm für eine Programmsteuerungseinrichtung.

Stand der Technik

[0002] Für die Steuerung des Zugangs zu einem abgeschlossenen Areal, wie beispielsweise einem Firmengelände oder einer Tiefgarage, wird üblicherweise eine Funkfernbedienung benutzt. Über die Funkfernbedienung können dabei mit einer Frequenz von 433 MHz die Steuerungsbefehle zum Öffnen und Schließen des jeweiligen Tores gegeben werden. Hierbei wird ein sogenanntes Hopping-Code Verfahren angewendet, bei dem die Sicherheitscodierung zur Übertragung der Steuerungsbefehle nach jeder Betätigung der Funkfernbedienung geändert wird. So wird ein zufälliges Auslösen durch eine fremde Fernbedienung nahezu ausgeschlossen.

[0003] Nachteilig bei diesen Verfahren ist, dass bei großen Anlagen mit mehreren zugangsberechtigten Benutzern eine Vielzahl von Funkfernbedienungen von den Zugangsanbietern verwaltet werden müssen und hierbei Sicherheitsprobleme entstehen. In einer großen Wohnanlage mit mehreren Parteien beispielsweise kauft sich ein Mieter üblicherweise eine Funkfernbedienung, um bequem seinen Tiefgaragenplatz zu erreichen. Bei einem späteren Umzug des Mieters wird die Funkfernbedienung nicht zurückgegeben, da sie Eigentum des Mieters ist. Somit entsteht ein unnötiges Sicherheitsrisiko für die Nutzer der Wohnanlage. Werden die Funkfernbedienungen durch die Wohnanlagenverwaltung oder eine Mieter-Interessengruppe gegen Kaution vermietet, stellen sich dieselben Sicherheitsprobleme. Wenn eine Funkfernbedienung gestohlen wird oder verloren geht bzw. nach einem Auszug des Mieters nicht zurückgegeben wird, besteht für Unbefugte die Möglichkeit, sich Zutritt zu der Tiefgarage zu beschaffen.

[0004] Ein weiterer Nachteil entsteht, wenn ein Benutzer Zugangsberechtigungen für mehrere Anlagen besitzt, wie beispielsweise zu Tiefgaragen in der Firma, im Mietshaus oder im Fitnesscenter. Der Nutzer hat somit eine Vielzahl von Funkfernbedienungen mit sich zu führen und zu bedienen, wodurch die Verkehrssicherheit beeinträchtigt wird.

[0005] Ein zusätzlicher Nachteil besteht darin, dass nicht protokollierbar ist, welcher Nutzer zu welchem Zeitpunkt ein abgeschlossenes Areal betreten oder verlassen hat.

Aufgabenstellung

[0006] Der vorliegenden Erfindung liegt die Aufgabe zugrunde, ein Verfahren zur Überprüfung und Einräumung einer Zugangsberechtigung für einen Benutzer zu schaffen, mit dem eine einfache administrative Steuerung der Zugangsberechtigung durch den Zugangsanbieter ermöglicht wird und somit die beschriebenen Sicherheitsrisiken und Komforteinbußen behoben werden können. Außerdem ist es Teil der Aufgabe ein zur Durchführung des Verfahrens geeignetes System und ein Programm für die Programmsteuerungseinrichtung anzugeben.

[0007] Diese Aufgabe wird erfindungsgemäß durch ein System mit den in Anspruch 1 angegebenen Merkmalen, ein Verfahren mit den in Anspruch 5 angegebenen Merkmalen und ein Programm mit den in Anspruch 8 angegebenen Merkmalen gelöst. Vorteilhafte Weiterbildungen der Erfindung sind in den abhängigen Ansprüchen angegeben.

[0008] Entsprechend dem erfindungsgemäßen System weist die Vorrichtung zur Überprüfung einer Zugangsberechtigung eines Benutzers eine Chipkarte auf, auf der zumindest ein Identifizierungsmerkmal einer Authentifizierungseinrichtung und zumindest ein Identifizierungsmerkmal eines Benutzers gespeichert ist. Des weiteren umfasst das System eine Leseeinrichtung, die auf der Chipkarte gespeicherte Daten ausliest, eine Verschlüsselungseinrichtung, die auf der Chipkarte gespeicherte Daten verschlüsselt und eine Authentifizierungseinrichtung, die auf der Chipkarte gespeicherte Daten und in der Authentifizierungseinrichtung hinterlegte Daten auf Übereinstimmung überprüft. Außerdem umfasst das System eine Datenübertragungseinrichtung, die auf der Chipkarte gespeicherte Daten an die Authentifizierungseinrichtung überträgt und eine mit der Authentifizierungseinrichtung verbindbare Programmsteuerungseinrichtung, die einen Zugang zu einem Objekt für den Benutzer bereitstellt abhängig von einer Übereinstimmung der auf der Chipkarte gespeicherten Daten und den in der Authentifizierungseinrichtung hinterlegten Daten.

[0009] Entsprechend einer vorteilhaften Weiterbildung der vorliegenden Erfindung weist das System zusätzlich eine Eingabeeinrichtung auf, auf der von einem Systemadministrator das Identifizierungsmerkmal eines zugangsberechtigten Benutzers und/oder das Identifizierungsmerkmal eines nicht zugangsberechtigten Benutzers eingebbar sind. Zudem umfasst das System eine Datenübertragungseinrichtung zur Übermittlung von durch den Systemadministrator eingegebenen Daten an die Authentifizierungseinrichtung. Dies hat den Vorteil, dass in einfacher Weise durch den Zugangsanbieter der Zugang für das Identifizierungsmerkmal eines Benutzers mit einer verlorenen oder gestohlenen Chipkarte gesperrt

werden kann oder der Zugang für das Identifizierungsmerkmal eines Benutzers mit einer neuen Chipkarte freigegeben werden kann.

[0010] Entsprechend dem erfindungsgemäßen Verfahren wird zur Überprüfung einer Zugangsberechtigung eines Benutzers eine von einer Authentifizierungseinrichtung erhaltene Zufallszahl mit einem auf einer Chipkarte eines Benutzers gespeicherten privaten Schlüssel verschlüsselt. Diese verschlüsselte Zufallszahl wird zusammen mit einem Identifizierungsmerkmal des Benutzers zurück an die Authentifizierungseinrichtung übermittelt. Die Authentifizierungseinrichtung überprüft die von ihr erzeugte Zufallszahl und die an sie zurück übermittelte und anhand des Identifizierungsmerkmales entschlüsselte Zufallszahl auf Übereinstimmung. Abhängig von einer Übereinstimmung der von der Authentifizierungseinrichtung erzeugten und der an die Authentifizierungseinrichtung zurück übermittelten Zufallszahl wird durch eine Programmsteuerungseinrichtung ein Zugang zu einem Objekt für den Benutzer bereitgestellt.

[0011] In vorteilhafter Weise sendet der Benutzer in einem ersten Schritt eine Liste mit Identifizierungsmerkmalen von zumindest einer Authentifizierungseinrichtung, zu der er eine Zugangsberechtigung hat, an die Authentifizierungseinrichtung. Die Authentifizierungseinrichtung sendet bei Übereinstimmung zumindest eines Identifizierungsmerkmales aus der Liste mit zumindest einem eigenen Identifizierungsmerkmal die Zufallszahl an den Benutzer. Dies macht für einen Benutzer mit Zugangsberechtigungen für mehrere Objekte nur eine Chipkarte erforderlich und gewährleistet somit eine größere Bedienerfreundlichkeit und einen höheren Komfort für den Benutzer.

[0012] Bei der Ausführung des erfindungsgemäßen Steuerungsprogramms wird durch die Programmsteuerungseinrichtung abhängig von einer Übereinstimmung einer von einer Authentifizierungseinrichtung erzeugten Zufallszahl und einer an die Authentifizierungseinrichtung zurück übermittelten und anhand eines Identifizierungsmerkmales entschlüsselten Zufallszahl ein Zugang zu einem Objekt für den Benutzer bereitgestellt.

Ausführungsbeispiel

[0013] Die vorliegende Erfindung wird nachfolgend an einem Ausführungsbeispiel anhand der Zeichnung näher erläutert. Es zeigt die

[0014] Figur ein Ablaufdiagramm für ein Verfahren zur Überprüfung und Einrichtung einer Zugangsberechtigung für einen Benutzer.

[0015] An dem in der Figur dargestellten Verfahrensablauf sind ein zugangsinteressierter Benutzer **101** und ein Zugangsanbieter **105** beteiligt. Im vorliegenden Ausführungsbeispiel ist der zugangsinteressierte Benutzer **101** ein Auto fahrender Bewohner einer Wohnanlage, nachfolgend als Autofahrer bezeichnet. Der Autofahrer **101** verfügt über eine Fernbedienung, die eine Chipkarte, eine Leseeinrichtung für die Chipkarte, eine Verschlüsselungseinrichtung und eine Datenübertragungseinrichtung umfasst. Die Fernbedienung ist beispielsweise als Funk- oder Infrarotfernbedienung ausführbar. Dem Zugangsanbieter **105** ist eine Authentifizierungseinrichtung einer Tiefgarage der Wohnanlage zugeordnet, wobei die Authentifizierungseinrichtung eine Datenübertragungseinrichtung, eine Eingabeeinrichtung und eine Programmsteuerungseinrichtung umfasst.

[0016] Möchte der Autofahrer **101** nun Zugang zu der Tiefgarage erhalten, sendet er in einem ersten Schritt **102** über die Fernbedienung eine Zugangsanforderung an die Authentifizierungseinrichtung des Zugangsanbieters. Die Zugangsanforderung umfasst ein Identifizierungsmerkmal der Authentifizierungseinrichtung.

[0017] Stimmt das gesendete Identifizierungsmerkmal mit dem Identifizierungsmerkmal der Authentifizierungseinrichtung überein, generiert die Authentifizierungseinrichtung in einem zweiten Schritt **103** eine Zufallszahl und sendet diese zusammen mit ihrem Identifizierungsmerkmal an die Fernbedienung des Autofahrers **101**.

[0018] In einem dritten Schritt **104** wird von der Verschlüsselungseinrichtung der Fernbedienung die empfangene Zufallszahl anhand eines auf der Chipkarte gespeicherten privaten Schlüssels verschlüsselt. Anschließend sendet die Fernbedienung die verschlüsselte Zufallszahl zusammen mit einem Identifizierungsmerkmal des Autofahrers **101** an die Authentifizierungseinrichtung.

[0019] Die Authentifizierungseinrichtung entschlüsselt in einem letzten Schritt **106** die verschlüsselte Zufallszahl, wobei sie anhand des Identifizierungsmerkmales des Autofahrers **101** den öffentlichen Schlüssel für die Entschlüsselung erkannt hat. Bei einer Übereinstimmung der generierten Zufallszahl und der zurück erhaltenen und entschlüsselten Zufallszahl, gibt die Authentifizierungseinrichtung den Zugang frei (Schritt **107**) und öffnet das Garagentor. Stimmen die generierte Zufallszahl und die zurück erhaltene und entschlüsselte Zufallszahl nicht überein, sperrt die Authentifizierungseinrichtung den Zugang (Schritt **108**).

[0020] Ein Verwalter der Wohnanlage kann gemäß einer vorteilhaften Ausgestaltung der vorliegenden Erfindung über die Eingabeeinrichtung der Authentifizierungseinrichtung ein Identifizierungsmerkmal eines Autofahrers **101** löschen und ihm somit den Zugang zur Tiefgarage verwehren. In gleicher Weise

kann der Verwalter ein Identifizierungsmerkmal eines Autofahrers **101** hinzufügen und ihm somit den Zugang zur Tiefgarage gewähren. Es ist dem Verwalter folglich in einfacher Weise möglich den Zugang zur Tiefgarage der Wohnanlage zu kontrollieren.

[0021] Außerdem kann durch die Authentifizierungseinrichtung anhand der Identifizierungsmerkmale protokolliert werden, welcher Nutzer zu welchem Zeitpunkt die Wohnanlage betreten oder verlassen hat. Dies kann in Einzelfällen bei Anlagen mit besonders hohen Sicherheitsanforderungen wünschenswert sein.

[0022] Bei einer weiteren vorteilhaften Ausgestaltung der vorliegenden Erfindung besitzt der Autofahrer **101** Zugangsberechtigungen für mehrere Tiefgaragen. Die Identifizierungsmerkmale der verschiedenen Tiefgaragen sind auf der Chipkarte des Autofahrers **101** gespeichert. Bei einer Zugangsanforderung **102** sendet der Autofahrer über seine Fernbedienung alle Identifizierungsmerkmale der Authentifizierungseinrichtungen der Tiefgaragen für die er eine Zugangsberechtigung hat. Stimmt ein gesendetes Identifizierungsmerkmal mit dem Identifizierungsmerkmal der jeweiligen Authentifizierungseinrichtung überein, generiert die Authentifizierungseinrichtung einer der Tiefgaragen in einem zweiten Schritt **103** eine Zufallszahl und sendet diese zusammen mit ihrem Identifizierungsmerkmal an die Fernbedienung des Autofahrers **101**. Durch dieses Verfahren benötigt der Autofahrer **101** nur noch eine Fernbedienung, anstatt für jede Tiefgarage, zu der er eine Zugangsberechtigung hat, eine gesonderte Fernbedienung mit sich führen zu müssen.

Patentansprüche

1. System zur Überprüfung einer Zugangsberechtigung eines Benutzers mit
– einer Chipkarte, auf der zumindest ein Identifizierungsmerkmal einer Authentifizierungseinrichtung und zumindest ein Identifizierungsmerkmal eines Benutzers gespeichert ist,
– einer Leseeinrichtung zum Auslesen von auf der Chipkarte gespeicherten Daten,
– einer Verschlüsselungseinrichtung zum Verschlüsseln der auf der Chipkarte gespeicherten Daten,
– einer Authentifizierungseinrichtung zur Überprüfung der auf der Chipkarte gespeicherten Daten und von in der Authentifizierungseinrichtung hinterlegten Daten auf Übereinstimmung,
– einer Datenübertragungseinrichtung zur Übermittlung der auf der Chipkarte gespeicherten Daten an die Authentifizierungseinrichtung,
– einer mit der Authentifizierungseinrichtung verbindbaren Programmsteuerungseinrichtung zur Bereitstellung eines Zugangs zu einem Objekt für den Benutzer abhängig von einer Übereinstimmung der auf der Chipkarte gespeicherten Daten und den in der Authentifizierungseinrichtung hinterlegten Daten.

2. System nach Anspruch 1,
mit
– einer Eingabeeinrichtung, auf der von einem Systemadministrator das Identifizierungsmerkmal eines zugangsberechtigten Benutzers und/oder das Identifizierungsmerkmal eines nicht zugangsberechtigten Benutzers eingebbar sind,
– einer Datenübertragungseinrichtung zur Übermittlung von durch den Systemadministrator auf der Eingabeeinrichtung eingegebenen Daten an die Authentifizierungseinrichtung.

3. System nach mindestens einem der Ansprüche 1 und 2, bei dem die Verschlüsselungseinrichtung in die Chipkarte integriert ist.

4. System nach mindestens einem der Ansprüche 1-3, bei dem die Chipkarte als Smart-Card ausgebildet ist.

5. Verfahren zur Überprüfung einer Zugangsberechtigung eines Benutzers, bei dem
– eine von einer Authentifizierungseinrichtung erhaltene Zufallszahl mit einem auf einer Chipkarte eines Benutzers gespeicherten privaten Schlüssel verschlüsselt wird und diese verschlüsselte Zufallszahl zusammen mit einem Identifizierungsmerkmal des Benutzers zurück an die Authentifizierungseinrichtung übermittelt wird,
– die Authentifizierungseinrichtung die von der Authentifizierungseinrichtung erzeugte Zufallszahl und die an die Authentifizierungseinrichtung zurück übermittelte und anhand des Identifizierungsmerkmales entschlüsselte Zufallszahl auf Übereinstimmung überprüft,
– abhängig von einer Übereinstimmung der von der Authentifizierungseinrichtung erzeugten und der an die Authentifizierungseinrichtung zurück übermittelten Zufallszahl durch eine Programmsteuereinrichtung ein Zugang zu einem Objekt für den Benutzer bereitgestellt wird.

6. Verfahren nach Anspruch 5,
bei dem
– der Benutzer eine Liste mit Identifizierungsmerkmalen von zumindest einer Authentifizierungseinrichtung, zu der er eine Zugangsberechtigung hat, an die Authentifizierungseinrichtung sendet,
– die Authentifizierungseinrichtung bei Übereinstimmung zumindest eines Identifizierungsmerkmales aus der Liste mit zumindest einen eigenen Identifizierungsmerkmal die Zufallszahl an den Benutzer sendet.

7. Verfahren nach mindestens einem der Ansprüche 5 und 6, bei dem die Authentifizierungseinrichtung zusätzlich zu der Zufallszahl ihr zumindest eines eigenes Identifizierungsmerkmal an den Benutzer

sendet.

8. Programm für eine Programmsteuerungseinrichtung, das in einen Arbeitsspeicher einer Programmsteuerungseinrichtung ladbar ist und zumindest einen Codeabschnitt aufweist, bei dessen Ausführung
– durch die Programmsteuerungseinrichtung abhängig von einer Übereinstimmung einer von einer Authentifizierungseinrichtung erzeugten Zufallszahl und einer an die Authentifizierungseinrichtung zurück übermittelten und anhand eines Identifizierungsmerkmales entschlüsselten Zufallszahl ein Zugriff auf ein Objekt für den Benutzer bereitgestellt wird, wenn das Programm auf der Programmsteuerungseinrichtung abläuft.

Es folgt ein Blatt Zeichnungen

Anhängende Zeichnungen