(19) österreichisches patentamt

(10) **AT 500 833 B1 2007-06-15**

(12) # Patentschrift

(21) Anmeldenummer: A 1680/2004

(22) Anmeldetag: 2004-10-08

(43) Veröffentlicht am: 2007-06-15

(51) Int. Cl.[8]: ***H04L 9/32*** (2006.01)

(56) Entgegenhaltungen:
WO 1999/058987A1 US 6286008B1
WO 2001/035685A1

(73) Patentanmelder:
PRIBITZER WOLFGANG ING.
A-1020 WIEN (AT)

(54) **VERFAHREN, TERMINAL UND SYSTEM ZUR FREIGABEKONTROLLE EINER EINRICHTUNG**

(57) Ein Verfahren zur Freigabekontrolle einer Zutrittskontrolleinrichtung, Warenausgabeeinrichtung, etc. umfasst:
- das Aktivieren des Terminals (2) durch einen Benutzer,
- das Erzeugen eines ersten Codes (C1) mittels eines ersten Algorithmus (A1) in dem Terminal (2),
- das Übergeben des ersten Codes (C1) an ein Benutzer- Datenübertragungsgerät (3),
- das Übertragen des ersten Codes (C1) zusammen mit Benutzer-Identitätsdaten (ID) vom Datenübertragungsgerät (3) an einen entfernten Server (1),
- das Überprüfen des ersten Codes (C1) und der Benutzer-Identitätsdaten (ID) im Server (1), und bei Zulässigkeit das Erzeugen eines zweiten Codes (C2) mittels eines zweiten Algorithmus (A2),
- das Übertragen des zweiten Codes (C2) vom Server (1) an das Datenübertragungsgerät (3),
- das Übergeben des zweiten Codes (C2) vom Datenübertragungsgerät (3) an das Terminal (2),
- das Überprüfen der Gültigkeit des zweiten Codes (C2) durch einen dritten Algorithmus (A3) in dem Terminal (2), und bei Gültigkeit
- das Ausgeben eines Freigabesignals (5) an die freizugebende Einrichtung (4).

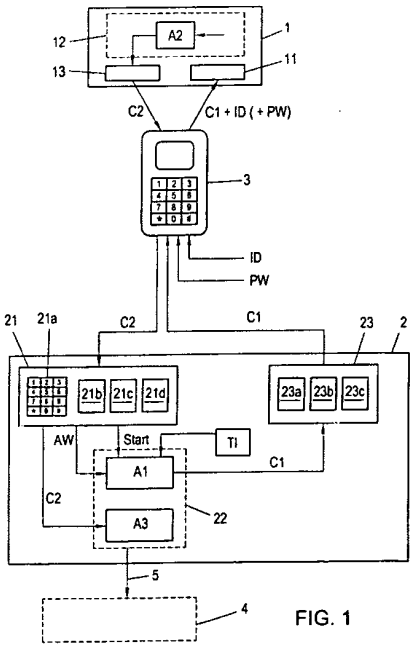

FIG. 1

AT 500 833 B1 2007-06-15

Die Erfindung betrifft ein Verfahren zur durch ein Terminal gesteuerten Freigabekontrolle einer Einrichtung, wie z.B. einer Zutrittskontrolleinrichtung oder einer Warenausgabeeinrichtung.

Die Erfindung betrifft weiters ein Terminal und ein System zur Freigabekontrolle einer Einrichtung, wie z.B. einer Zutrittskontrolleinrichtung oder einer Warenausgabeeinrichtung.

Es sind verschiedenste Systeme bekannt, die die Freigabe von Einrichtungen, wie z.B. Zutrittskontrolleinrichtungen oder Warenausgabeeinrichtungen steuern. Die bekannten Systeme sind dabei entweder als Stand-alone-Geräte ausgebildet, die direkt in die freizugebende Einrichtung integriert sind, wie z.B. Eingangstüren oder Drehkreuze, die durch Tickets o. dergl. geöffnet werden können, oder sind als Server-Client-Systeme ausgebildet, bei denen der Client nur Daten eines Benutzers sammelt, diese an den Server weiterleitet, der eine Überprüfung der Daten vornimmt und gegebenenfalls den Client instruiert, eine Einrichtung freizugeben, eine Ware auszugeben, etc.

Der vorliegenden Erfindung liegt die Aufgabe zugrunde, ein Verfahren, ein Terminal und ein System zur Freigabekontrolle einer Einrichtung bereitzustellen, die nach dem Server-Client-Prinzip funktionieren, bei denen aber aus Sicherheitsgründen und um Kosten zu sparen keine direkte Datenleitung zwischen dem Client und dem Server vorhanden ist.

Das erfindungsgemäße Verfahren zur durch ein Terminal gesteuerten Freigabekontrolle einer Einrichtung, wie z.B. einer Zutrittskontrolleinrichtung oder einer Warenausgabeeinrichtung, weist die folgenden Schritte auf:

- das Aktivieren des Terminals durch einen Benutzer,
- das Erzeugen eines ersten Codes mittels eines ersten Algorithmus in dem Terminal,
- das Übergeben des ersten Codes an ein dem Benutzer zugeordnetes Datenübertragungsgerät,
- das Übertragen des ersten Codes zusammen mit Benutzer-Identitätsdaten von dem Datenübertragungsgerät an einen entfernten Server,
- das Überprüfen des ersten Codes und der Benutzer-Identitätsdaten im Server, und falls der erste Code und der Benutzer zugelassen sind, das Erzeugen eines zweiten Codes mittels eines zweiten Algorithmus in dem Server,
- das Übertragen des zweiten Codes an das dem Benutzer zugeordnete Datenübertragungsgerät,
- das Übergeben des zweiten Codes von dem Datenübertragungsgerät an das Terminal,
- das Überprüfen der Gültigkeit des zweiten Codes durch einen dritten Algorithmus durch das Terminal, und falls der zweite Code gültig ist,
- das Ausgeben eines Freigabesignals an die freizugebende Einrichtung.

Die erfindungsgemäße Aufgabe wird weiters durch Bereitstellen eines Terminals zur Freigabekontrolle einer Einrichtung mit den Merkmalen des Anspruches 9 und durch Bereitstellen eines Systems zur Freigabekontrolle einer Einrichtung mit den Merkmalen des Anspruches 14 gelöst. Vorteilhafte Ausgestaltungen der Erfindung sind in den abhängigen Ansprüchen dargelegt.

Die Erfindung bietet gegenüber dem Stand der Technik folgende Vorteile:

- Das Terminal braucht nur eine Stromversorgung (Stromnetz, Batterien, Akku oder Solarenergie), jedoch keine Datenleitung, Telefonleitung oder Antenne.
- Das Terminal benötigt keine Informationen über das Datum oder die Uhrzeit.
- Es ist eine zentrale Verwaltung einer Vielzahl von Terminals mit nur einem Server möglich, da nur am Server die Regeln für die Freigabe von Einrichtungen hinterlegt werden.

- Eine Änderung der Zugangsregeln für alle oder nur für bestimmte Terminals ist in wenigen Minuten möglich und ab dem Zeitpunkt der Eintragung am Server sofort gültig.

- Die beim Stand der Technik notwendige Herstellung, Verteilung und Verwaltung von Berechtigungskarten kann entfallen.

- Jede denkbare Art von Zutrittskontrolleinrichtung kann damit angesteuert werden (Schranken, Drehkreuz, Tür, Schlüsseltresor...).

- Geringe Anlagenkosten. Die Realisierung des Terminals kann mittels eines Personal Digital Assistant (PDA) und einer Tastatur in einem vandalismussicheren und gegebenenfalls wetterfesten Gehäuse erfolgen. Eine solche Ausführung des Terminals hat sehr geringe Betriebskosten, Strom wird nur für den PDA benötigt.

- Es kann eine perfekte Statistik über die Nutzung des Systems geführt werden (wer war wann dort etc.).

- Das System vermeidet Bargeldtransfer, da entgeltliche Leistungen oder Waren über eine vom Server erstellte Rechnung abgerechnet werden.

In einer vorteilhaften Ausgestaltung der Erfindung wird in den ersten Code eine Terminal-Identifikation eincodiert, die vom Server bei der Überprüfung ausgewertet wird, wobei vorzugsweise der Server seinerseits Information über die Terminal-Identifikation in den von ihm erzeugten zweiten Code eincodiert. Durch diese Ausgestaltung ist die individuelle Einstellung der Zugangsregeln für jedes einzelne Terminal möglich, da jedes Terminal eine andere Terminal-Identifikation hat.

Zur Ansteuerung von Warenausgabeautomaten o. dergl. kann vorgesehen werden, dass in den ersten Code eine Auswahlinformation eincodiert ist, die eine vom Benutzer am Terminal ausgewählte Ware etc. kennzeichnet. Die Auswahlinformation wird vom Server bei der Überprüfung ausgewertet, wobei der Server optional Information über die Auswahlinformation in den von ihm erzeugten zweiten Code eincodiert. Bei der Auswertung des zweiten Codes durch das Terminal kann das Terminal aus der in den zweiten Code eincodierten Information über die Auswahlinformation erkennen, ob der Benutzer überhaupt zur Auswahl einer bestimmten Ware berechtigt ist. Auf diese Weise können Zugangsbeschränkungen an bestimmten Warenausgabeautomaten (Zigaretten, Alkohol) realisiert werden. Solche Zugangsbeschränkungen können beispielsweise auch die Kontrolle des Alters des Benutzers umfassen, sofern dieses bei einer vorherigen Anmeldung des Kunden abgefragt und diese Daten dann am Server gespeichert wurden.

Da es sein könnte, dass ein Benutzer den erhaltenen zweiten Code aus irgendwelchen Gründen doch nicht zum Warenkauf verwendet, indem er ihn einfach nicht an das Terminal übergibt, wird im Terminal jeder empfangene zweite Code in einem Speichermedium abgespeichert. Das Speichermedium wird beim Befüllen des Warenautomaten ausgetauscht und die gespeicherten zweiten Codes werden mit den am Server gespeicherten zweiten Codes verglichen. Eine Belastung des Kundenkontos erfolgt nur, wenn ein vom Server ausgesendeter zweiter Code auch wirklich am Terminal verwendet wurde, d.h. sich auf dem Speichermedium befindet.

In einer bevorzugten Ausführungsform der Erfindung ist das dem Benutzer zugeordnete Datenübertragungsgerät als Mobiltelefon ausgebildet und erfolgt das Übertragen des ersten Codes vom Mobiltelefon an den Server bzw. das Übertragen des zweiten Codes vom Server an das Mobiltelefon per SMS oder MMS. Durch den flächendeckenden Ausbau der Mobilfunksysteme ist ein solches System überall anwendbar. Es bietet weiters den Vorteil, dass Bargeldtransfer vermieden wird, indem entgeltliche Leistungen oder Waren über die Telefonrechnung des Benutzers bei seinem Mobilfunkbetreiber abgerechnet werden können. Dabei ist es zweckmäßig, wenn bei dieser Ausgestaltung der Erfindung als die durch den Server zu überprüfenden

Benutzer-Identitätsdaten eine eindeutige Mobiltelefonkennung, insbesondere die Mobiltelefonnummer, herangezogen wird.

Für das Übergeben des ersten Codes vom Terminal an das Datenübertragungsgerät bzw. das Übergeben des zweiten Codes vom Datenübertragungsgerät an das Terminal sind verschiedene erfindungsgemäße Varianten vorgesehen:

In einer ersten Variante sind das Ausgangsinterface und/oder das Eingangsinterface des Terminals als Funkinterface ausgebildet, das beispielsweise nach Bluetooth- oder WLAN-Standard arbeitet oder als NFC (Near Field Communication) Device ausgebildet ist.

In einer zweiten Variante sind das Ausgangsinterface und/oder das Eingangsinterface des Terminals als optisches Datenübertragungsinterface ausgebildet, das z.B. als IrDA (Infrared Data Association) Device gestaltet ist.

In wiederum einer anderen Variante ist das Ausgangsinterface des Terminals als Display zur Klartextanzeige des ersten Codes oder zur Anzeige des durch die Recheneinheit des Terminals als visuelle Information, z.B. Strichcode, aufbereiteten ersten Codes ausgestaltet. Im ersten Fall kann der Benutzer den angezeigten Klartext des ersten Codes vom Display ablesen und in sein Datenübertragungsgerät eintippen (insbesondere bei Benutzung eines Mobiltelefons) und als SMS an den Server versenden. Im zweiten Fall kann der Benutzer beispielsweise den visuell aufbereiteten Code durch eine in sein Mobiltelefon eingebaute Kamera aufnehmen und als MMS an den Server versenden.

Das Eingangsinterface des Terminals kann weiters optische Scannmittel zum Scannen visueller Information umfassen, wobei es sich bei der visuellen Information um den vom Server visuell, z.B. als Strichcode, aufbereiteten zweiten Code handelt, der in einem solchen Fall zweckmäßig vom Server per MMS an das als Mobiltelefon ausgebildete Datenübertragungsgerät des Benutzers gesendet wurde und von der Anzeige des Mobiltelefons scannbar ist.

Das Eingangsinterface des Terminals kann weiters eine Tastatur zur manuellen Eingabe des zweiten Codes aufweisen, wenn dieser beispielsweise per SMS an das als Mobiltelefon ausgebildete Datenübertragungsgerät des Benutzers gesendet wurde.

Zur Erhöhung der Sicherheit wird vorzugsweise beim Übertragen des ersten Codes vom Datenübertragungsgerät an den entfernten Server ein vom Benutzer zuvor in das Datenübertragungsgerät oder das Terminal einzugebendes Passwort mit übertragen, das vom Server ausgewertet wird.

Vorteilhaft werden aus Sicherheitsgründen und Abrechnungsgründen im Server einer oder mehrere Datensätze bestehend aus Benutzer-Identifikation, Terminal-Identifikation, Auswahlinformation, Datum, Zeit und Inhalt der eingehenden ersten Codes und ausgehenden zweiten Codes protokolliert und gegebenenfalls für die Durchführung einer Abrechnung verwendet.

Die Erfindung wird nun unter Bezugnahme auf die einzige Zeichnung, Fig. 1, anhand eines Ausführungsbeispiels beschrieben, auf das die Erfindung aber nicht eingeschränkt ist.

Auf Fig. 1 Bezug nehmend ist darin schematisch in einem Blockschaltbild ein erfindungsgemäßes System zur Freigabekontrolle einer Einrichtung 4, wie z.B. einer Zutrittskontrolleinrichtung oder einer Warenausgabeeinrichtung, dargestellt. Das erfindungsgemäße System zur Freigabekontrolle umfasst einen Server 1 und eine Vielzahl an gleichartigen Terminals 2, von denen in Fig. 1 nur eines dargestellt ist.

Das Terminal 2 kann vorteilhaft als PDA ausgestaltet sein, der in einem vandalensicheren Gehäuse untergebracht ist. Dem Terminal ist eine eindeutige Terminal-Identifikation TI zuge-

ordnet, die es von anderen Terminals unterscheidbar macht. Die Terminal-Identifikation TI ist vorzugsweise in einem nicht-flüchtigen Speicher im Terminal abgespeichert. Das Terminal 2 umfasst ein Eingangsinterface 21, das eine Tastatur 21a aufweist. Indem ein Benutzer eine Taste der Tastatur 21a drückt, wird das Terminal 2 aktiviert (START), worauf eine im Terminal 2 ausgebildete Recheneinheit 22 einen ersten Code C1 mittels eines ersten Algorithmus A1 erzeugt. Es sei erwähnt, dass die Tastatur 21a auch als berührungsempfindliche Oberfläche des Display 23a ausgebildet sein könnte.

Der Algorithmus A1 kann beispielsweise die folgenden Schritte aufweisen, wobei für dieses Beispiel der Terminal-Identifikation TI die Nummer *4578* zugeordnet ist. Zunächst wird eine Zufallszahl (0 bis 9), *hier 5* erzeugt, - dann werden an die erzeugte Zufallszahl die ersten beiden Ziffern der Terminal-Identifikation TI angehängt, *hier 545* - anschließend wird eine weitere Zufallszahl (0 bis 9) erzeugt, *hier 8* - diese weitere Zufallszahl wird an die vorhandene Zahl angehängt, *hier 5458* - anschließend werden die letzten beiden Ziffern der Terminal-Identifikation TI an die vorhandene Zahl angehängt, *hier 545878* -die so ermittelte Zahl wird modulo 3 dividiert, *hier 1* -das Ergebnis wird an die vorhandene Zahl angehängt, *hier 5458781* - und abschließend die Zahl in eine Hexadezimalzahl umgewandelt, *hier 534B5D*, die den ersten Code C1 darstellt.

Der erste Code C1 wird von der Recheneinheit 22 an ein Ausgangsinterface 23 des Terminals 2 weitergeleitet, was dem Ausgangsinterface 23 das Übergeben des ersten Codes C1 an ein dem Benutzer zugeordnetes Datenübertragungsgerät 3 ermöglicht. Für die Zwecke der Beschreibung dieses Ausführungsbeispieles der Erfindung sei angenommen, dass das Datenübertragungsgerät 3 als Mobiltelefon ausgebildet ist. Das Ausgangsinterface 23 des Terminals 2 kann verschiedene Module beinhalten, um mit dem Datenübertragungsgerät 3 kommunizieren zu können. So ist im Ausgangsinterface 23 ein Funkinterface 23a ausgebildet, das beispielsweise nach Bluetooth- oder WLAN-Standard arbeitet oder als NFC (Near Field Communication) Device ausgebildet ist, um den ersten Code C1 an das Datenübertragungsgerät 3 zu übertragen. Weiters ist in dem Ausgangsinterface 23 des Terminals 2 ein optisches Datenübertragungsinterface 23b ausgebildet, das z.B. als IrDA (Infrared Data Association) Device gestaltet ist. Weiters umfasst das Ausgangsinterface 23 des Terminals 2 ein Display 23c zur Klartextanzeige des ersten Codes C1 oder zur Anzeige des durch die Recheneinheit 22 als visuelle Information, z.B. Strichcode, aufbereiteten ersten Codes C1. Im Fall der Klartextanzeige kann der Benutzer den angezeigten Klartext des ersten Codes C1 vom Display 23c ablesen und in sein Datenübertragungsgerät 3 eintippen und als SMS an den Server 1 versenden. Im Fall der visuellen Aufbereitung des ersten Codes C1 kann der Benutzer beispielsweise diesen visuell aufbereiteten ersten Code C1 durch eine in sein Datenübertragungsgerät 3 eingebaute Kamera aufnehmen und als MMS an den Server 1 versenden. Zusammen mit dem ersten Code werden an den Server Benutzer-Identitätsdaten ID gesandt, bei denen es sich um eine dem Benutzer bei der Anmeldung von einem Betreiber des Systems zugeteilte Benutzerkennnummer oder vorteilhaft auch um die Telefonnummer des als Mobiltelefon ausgebildeten Datenübertragungsgerätes 3 handelt. Optional wird vom Datenübertragungsgerät 3 zusammen mit dem ersten Code C1 ein Passwort PW an den Server mitgesendet, das der Benutzer zuvor eingegeben hat.

Der Server 1 weist ein Eingangsinterface 11 zum Empfangen des ersten Codes C1, der Benutzer-Identitätsdaten ID und optional des Passwortes PW auf, sowie eine Recheneinheit 12 zum Überprüfen des ersten Codes C1 und der Benutzer-Identitätsdaten ID. Falls der erste Code C1 und die Benutzer-Identitätsdaten ID sowie gegebenenfalls das Passwort PW zugelassen sind, erzeugt die Recheneinheit einen zweiten Code C2 gemäß einem zweiten Algorithmus A2 und leitet diesen zweiten Code C2 an ein Ausgangsinterface 13 des Servers 1 weiter, das für das Übertragen an das dem Benutzer zugeordnete Datenübertragungsgerät 3 sorgt.

Unter Bezugnahme auf das obige Beispiel für den Algorithmus A1 kann der Algorithmus A2 beispielsweise die folgenden Schritte aufweisen: Einlesen des ersten Codes C1 (nach Überprüfung der Berechtigungen), *hier 534B5D* - Umwandeln der Zeichenfolge des Codes C1 in eine Dezimalzahl, *hier 5458781* - Abschneiden der letzten Ziffer, *hier 1* - Dividieren der verbleiben-

den Zahl modulo 3 und Vergleichen, ob das Ergebnis mit der abgeschnittenen Zahl übereinstimmt, *hier o.k.* - Abschneiden der ersten und der letzten Ziffer der verbliebenen Zahl, *hier 5 und 8* - Verwenden der verbliebenen Zahl, *hier 4587* - Multiplizieren dieser Zahl mit 2, *hier 9174* - erzeugen einer Zufallszahl (0 bis 9), *hier 4* - Anhängen der Zufallszahl an die vorhandene Zahl, *hier 91744* - die den zweiten Code C2 darstellt. Dieser Code C2 wird an das Datenübertragungsgerät zurückgesendet, das den ersten Code C1 gesendet hat. In einer bevorzugten Ausgestaltung ist das Eingangsinterface 11 des Servers 1 zum Empfang von SMS und/oder MMS ausgebildet, und ist das Ausgangsinterface 13 des Servers 1 zum Senden des zweiten Codes C2 als SMS und/oder MMS ausgebildet.

Die Recheneinheit 12 des Servers kann weitere Überprüfungen und Protokollierungen vornehmen, die nachfolgend näher erklärt werden, wobei insbesondere auf die Ausbildung des dem Benutzer zugeordneten Datenübertragungsgerätes 3 als Mobiltelefon Bezug genommen wird.

- Überprüfung, ob der als SMS oder MMS angekommene erste Code C1 korrekt ist (zum System passt)
- Überprüfung ob die Mobiltelefonnummer ausgelesen werden kann
- Ist diese Mobiltelefonnummer gesperrt ?
- Ist diese Mobiltelefonnummer für das System registriert ?
- Ist das Mobiltelefon mit dieser Nummer als gestohlen oder verloren gemeldet ?
- Ist das Passwort PW korrekt? (wenn Passwort verwendet wird)
- Ist die örtliche Berechtigung des Benutzers gegeben ?
- Ist die zeitliche Berechtigung des Benutzers gegeben ?
- Hat der Kunde das erforderliche Alter? (nur bei Alterskontrolle)

Das Datenübertragungsgerät 3 empfängt den vom Server 1 gesendeten zweiten Code C2, beispielsweise entweder als Klartextanzeige in ein SMS gepackt, oder als visuell aufbereitete Information (Strichcode), beispielsweise in ein MMS gepackt. Nun hat der Benutzer die Möglichkeit, den zweiten Code C2 an das Terminal 2 zu übergeben, wofür neben der manuellen Eingabe über die Tastatur 21a des Eingangsinterface 21 des Terminals 2 das Eingangsinterface 21 auch ein Funkinterface 21b, das beispielsweise nach Bluetooth- oder WLAN-Standard arbeitet oder als NFC (Near Field Communication) Device ausgebildet ist, und/oder ein optisches Datenübertragungsinterface 21c, das z.B. als IrDA (Infrared Data Association) Device gestaltet ist, und/oder optische Scannmittel 21d, z.B. einen Strichcodeleser, aufweist.

Der über das Eingangsinterface 21 vom Terminal 2 empfangene zweite Code C2 wird von der Recheneinheit 22 des Terminals 2 auf seine Gültigkeit gemäß einem dritten Algorithmus A3 überprüft. Bei festgestellter Gültigkeit gibt die Recheneinheit 22 ein Freigabesignal 5 an die freizugebende Einrichtung 4 ab.

Der dritte Algorithmus A3 kann beispielsweise die folgenden Schritte umfassen (wenn der obige Algorithmus A2 verwendet wurde): Nimm den zweiten Code C2, *hier 91744* - Abschneiden der letzten Ziffer, *hier 4* - ergibt Vergleichszahl, *hier 9174* - Hole den zuletzt ausgegebenen ersten Code C1 aus einem Speicher im Terminal, in dem der jeweils zuletzt erzeugte erste Code C1 protokolliert wurde, *hier 545878* - Abschneiden der ersten und der letzten Ziffer, *hier 5 und 8* - Verwenden der verbliebenen Zahl, *hier 4587* - Multipliziere sie mit 2, *hier 9174* - vergleiche diese Zahl mit der vorher erzeugten Vergleichszahl, *hier 9174* => alles o.k. - Das Freigabesignal 5 wird abgegeben.

Die Verwendungsmöglichkeiten der Erfindung sind vielfältig. Lediglich als Beispiele seien die Folgenden angeführt:

- als Eintrittskarte,
- zur Kontrolle des Zugangs zu öffentlichen Einrichtungen (z.B. Parkhäuser, Lagerplätze, WC-Anlagen ...),

- zur Kontrolle des Zugangs zu nicht ständig besetzten Schihütten und Berghütten,
- zum Einschalten von Strom oder Wasser auf Campingplätzen (Abgabe einer bestimmten Menge oder für eine bestimmte Zeitdauer),
- zum Zugang für Rauchfangkehrer, Stromableser, Gasableser in unbewohnten Gebäuden (an Zweitwohnsitzen),
- zur Ausgabe von Waren bei Warenausgabeautomaten (inkl. Alterskontrolle wenn nötig),
- zum Einschalten von Spielautomaten/Glücksspielautomaten (inkl. Alterskontrolle wenn nötig).

Ein besonderer Vorteil der Erfindung liegt in ihrer hohen Sicherheit gegen Missbrauch. Dies wird im Folgenden anhand verschiedener Angriffsszenarien näher erläutert:

Szenario 1:

Rechtmäßiger Besitzer eines am System teilnehmenden Mobiltelefons möchte seine Identität verbergen um die Ware oder die Dienstleistung nicht bezahlen zu müssen. Dies wird bei der Überprüfung der in der SMS-Nachricht enthaltenen Mobiltelefonnummer, mit welcher SMS der erste Code C1 an den Server übertragen wurde, durch den Server bemerkt => ANGRIFF VEREITELT

Szenario 2:

Jemand versucht mit einem Mobiltelefon, das nicht am System teilnimmt, eine Ware oder Dienstleistung zu erhalten. Dies wird bei der Überprüfung der in der SMS-Nachricht enthaltenen Mobiltelefonnummer, mit welcher SMS der erste Code C1 an den Server übertragen wurde, durch den Server bemerkt => ANGRIFF VEREITELT

Szenario 3:

Der unrechtmäßige Besitzer eines Mobiltelefons (nach Verlust oder Diebstahl) versucht eine Ware oder Dienstleistung zu erhalten. Wenn der Verlust/Diebstahl des Mobiltelefons bereits gemeldet und im System vermerkt wurde, wird das bei der Überprüfung der Mobiltelefonnummer der SMS-Nachricht durch den Server bemerkt => ANGRIFF VEREITELT

Wenn der Verlust/Diebstahl des Mobiltelefons noch nicht gemeldet oder noch nicht im System vermerkt wurde, dann ist der MISSBRAUCH MÖGLICH, sofern kein Passwort verwendet wird.

Szenario 4:

Jemand versucht mit Hilfe eines Computers anhand der Zeichenfolge am Display des Terminals die Zeichenfolge die vom SMS-Server zurückgesendet würde zu errechnen und so die Ware oder Dienstleistung kostenlos zu bekommen.

4a) Dem Angreifer ist keiner der verwendeten Algorithmen bekannt:
Durch die Verwendung von Zufallszahlen in den Algorithmen => MISSBRAUCH praktisch UNMÖGLICH
4b) Dem Angreifer ist nur der Serveralgorithmus (A2) bekannt => MISSBRAUCH MÖGLICH
4c) Dem Angreifer ist nur der Terminalalgorithmus (A1) bekannt => MISSBRAUCH UNMÖGLICH
4d) Dem Angreifer ist nur der Terminalalgorithmus (A3) bekannt => MISSBRAUCH MÖGLICH

Daraus ergibt sich die Schlussfolgerung, dass der Serveralgorithmus (A2) unbedingt geheim gehalten werden muss. Umsetzung zum Beispiel durch Hardwarecodierung des Algorithmus A2 in einem ASIC möglich. Der Algorithmus A2 muss (für hohe Sicherheitsanforderungen) vom Algorithmus A3 verschieden sein (was technisch durchaus möglich ist). Die Verwendung eines

Passworts ist empfehlenswert.

Patentansprüche:

1. Verfahren zur durch ein Terminal gesteuerten Freigabekontrolle einer Einrichtung, wie z.B. einer Zutrittskontrolleinrichtung oder einer Warenausgabeeinrichtung, *gekennzeichnet durch*:
   - das Aktivieren des Terminals (2) durch einen Benutzer,
   - das Erzeugen eines ersten Codes (C1) mittels eines ersten Algorithmus (A1) in dem Terminal (2),
   - das Übergeben des ersten Codes (C1) an ein dem Benutzer zugeordnetes Datenübertragungsgerät (3),
   - das Übertragen des ersten Codes (C1) zusammen mit Benutzer-Identitätsdaten (ID) von dem Datenübertragungsgerät (3) an einen entfernten Server (1),
   - das Überprüfen des ersten Codes (C1) und der Benutzer-Identitätsdaten (ID) im Server (1), und falls der erste Code (C1) und der Benutzer zugelassen sind, das Erzeugen eines zweiten Codes (C2) mittels eines zweiten Algorithmus (A2) in dem Server (1),
   - das Übertragen des zweiten Codes (C2) an das dem Benutzer zugeordnete Datenübertragungsgerät (3),
   - das Übergeben des zweiten Codes (C2) von dem Datenübertragungsgerät (3) an das Terminal (2),
   - das Überprüfen der Gültigkeit des zweiten Codes (C2) durch einen dritten Algorithmus (A3) in dem Terminal (2), und falls der zweite Code (C2) gültig ist,
   - das Ausgeben eines Freigabesignals (5) an die freizugebende Einrichtung (4).

2. Verfahren nach Anspruch 1, *dadurch gekennzeichnet*, dass in den ersten Code (C1) eine Terminal-Identifikation (TI) eincodiert ist, die vom Server (1) bei der Überprüfung ausgewertet wird, wobei der Server (1) vorzugsweise Information über die Terminal-Identifikation (TI) in den von ihm erzeugten zweiten Code (C2) eincodiert.

3. Verfahren nach Anspruch 1 oder 2, *dadurch gekennzeichnet*, dass in den ersten Code (C1) eine Auswahlinformation (AW) eincodiert ist, die vom Server (1) bei der Überprüfung ausgewertet wird, wobei der Server (1) optional Information über die Auswahlinformation (AW) in den von ihm erzeugten zweiten Code (C2) eincodiert.

4. Verfahren nach einem der vorhergehenden Ansprüche, *dadurch gekennzeichnet*, dass das dem Benutzer zugeordnete Datenübertragungsgerät (3) als Mobiltelefon ausgebildet ist und das Übertragen des ersten Codes (C1) vom Mobiltelefon an den Server (1) bzw. das Übertragen des zweiten Codes (C2) vom Server (1) an das Mobiltelefon per SMS oder MMS erfolgt.

5. Verfahren nach Anspruch 4, *dadurch gekennzeichnet*, dass die durch den Server (1) zu überprüfenden Benutzer-Identitätsdaten (ID) eine eindeutige Mobiltelefonkennung umfassen.

6. Verfahren nach einem der vorhergehenden Ansprüche, *dadurch gekennzeichnet*, dass das Übergeben des ersten Codes (C1) vom Terminal (2) an das Datenübertragungsgerät (3) bzw. das Übergeben des zweiten Codes (C2) vom Datenübertragungsgerät (3) an das Terminal (2) durch Datenfunkübertragung, optische Datenübertragung, manuelle Eingabe über ein Eingabe-Interface, und/oder Aufbereitung der Codes als visuelle Information, z.B. Strichcode, und Übergeben der aufbereiteten visuellen Information erfolgt.

7. Verfahren nach einem der vorhergehenden Ansprüche, *dadurch gekennzeichnet*, dass beim Übertragen des ersten Codes (C1) vom Datenübertragungsgerät (3) an den entfern-

ten Server (1) ein vom Benutzer zuvor in das Datenübertragungsgerät (3) oder das Terminal (1) einzugebendes Passwort (PW) mit übertragen wird.

8. Verfahren nach einem der vorhergehenden Ansprüche, *dadurch gekennzeichnet*, dass im Server (1) eines oder mehrere aus Benutzer-Identifikation (ID), Terminal-Identifikation (TI), Auswahlinformation (AW), Datum und Zeit der eingehenden ersten Codes (C1) und ausgehenden zweiten Codes (C2) protokolliert und gegebenenfalls für die Durchführung einer Abrechnung verwendet werden.

9. Verfahren nach einem der vorhergehenden Ansprüche, *dadurch gekennzeichnet*, dass im Server (1) einer oder mehrere Datensätze aus Benutzer-Identifikation (ID), Terminal-Identifikation (TI), Auswahlinformation (AW), Datum, Zeit und Inhalt der eingehenden ersten Codes (C1) und ausgehenden zweiten Codes (C2) protokolliert und gegebenenfalls für die Durchführung einer Abrechnung verwendet werden.

10. Terminal zur Freigabekontrolle einer Einrichtung, wie z.B. einer Zutrittskontrolleinrichtung oder einer Warenausgabeeinrichtung, wobei das Terminal durch einen Benutzer aktivierbar ist, *dadurch gekennzeichnet*, dass das Terminal (2) eine Recheneinheit (22) zur Erzeugung eines ersten Codes (C1) mittels eines ersten Algorithmus (A1), ein Ausgangsinterface (23), das das Übergeben des ersten Codes (C1) an ein dem Benutzer zugeordnetes Datenübertragungsgerät (3) ermöglicht, und ein Eingangsinterface (21) zum Empfangen eines zweiten Codes (C2) aufweist, wobei die Recheneinheit (22) weiters dazu ausgebildet ist, die Gültigkeit des zweiten Codes (C2) gemäß einem dritten Algorithmus (A3) zu überprüfen, und bei festgestellter Gültigkeit ein Freigabesignal (5) an die freizugebende Einrichtung (4) abzugeben.

11. Terminal nach Anspruch 9, *dadurch gekennzeichnet*, dass die Recheneinheit (22) dazu ausgebildet ist in den ersten Code (C1) eine Terminal-Identifikation (TI) einzucodieren, wobei vorzugsweise die Recheneinheit (22) auch dazu ausgebildet ist, bei der Überprüfung eines empfangenen zweiten Codes (C2) zu ermitteln, ob in den zweiten Code (C2) eine mit der Terminal-Identifikation (TI) korrespondierende Information eincodiert ist.

12. Terminal nach Anspruch 9 oder 10, *dadurch gekennzeichnet*, dass ein Eingabe-Interface (21) vorgesehen ist, über das der Benutzer eine Auswahl treffen kann und dass die Recheneinheit (22) dazu ausgebildet ist, der getroffenen Auswahl entsprechende Auswahlinformation (AW) in den ersten Code (C1) einzucodieren, wobei vorzugsweise die Recheneinheit (22) auch dazu ausgebildet ist, bei der Überprüfung eines empfangenen zweiten Codes (C2) auszuwerten, ob in den zweiten Code (C2) eine zur Auswahlinformation (AW) korrespondierende Information eincodiert ist.

13. Terminal nach einem der Ansprüche 9 bis 11, *dadurch gekennzeichnet*, dass das Ausgangsinterface (23) ein Funkinterface (23a) und/oder ein optisches Datenübertragungsinterface (23b) und/oder ein Display (23c) zur Klartextanzeige des ersten Codes oder zur Anzeige des durch die Recheneinheit (22) als visuelle Information, z.B. Strichcode, aufbereiteten ersten Codes (C1) aufweist.

14. Terminal nach einem der Ansprüche 9 bis 12, *dadurch gekennzeichnet*, dass das Eingangsinterface (21) ein Funkinterface (21b) und/oder ein optisches Datenempfangsinterface (21c) und/oder optische Scannmittel (21d) zum Scannen visueller Information, z.B. einen Strichcodeleser, und/oder eine Tastatur (21a) zur manuellen Eingabe des zweiten Codes (C2) aufweist.

15. System zur Freigabekontrolle einer Einrichtung, wie z.B. einer Zutrittskontrolleinrichtung oder einer Warenausgabeeinrichtung, *gekennzeichnet durch*:
ein durch einen Benutzer aktivierbares Terminal (2) gemäß einem der Ansprüche 9 bis 13,

und durch einen Server (1), wobei der Server (1) ein Eingangsinterface (11) zum Empfangen des ersten Codes (C1) und von Benutzer-Identitätsdaten (ID), eine Recheneinheit (12) zum Überprüfen des ersten Codes (C1) und der Benutzer-Identitätsdaten (ID), und falls der erste Code (C1) und der Benutzer zugelassen sind, zum Erzeugen eines zweiten Codes (C2) gemäß einem zweiten Algorithmus (A2), und ein Ausgangsinterface (13) zum Übertragen des zweiten Codes (C2) an das dem Benutzer zugeordnete Datenübertragungsgerät (3) aufweist.

16. System nach Anspruch 14, *dadurch gekennzeichnet*, dass die Recheneinheit (12) des Servers (1) dazu ausgebildet ist, eine in den ersten Code (C1) eincodierte Terminal-Identifikation (TI) auszuwerten, und vorzugsweise die Recheneinheit (12) weiters ausgebildet ist, Information über die ausgewertete Terminal-Identifikation (TI) in den zweiten Code einzucodieren.

17. System nach Anspruch 14 oder 15, *dadurch gekennzeichnet*, dass die Recheneinheit (12) des Servers (1) dazu ausgebildet ist, eine in den ersten Code (C1) eincodierte Auswahlinformation (AW) auszuwerten, und vorzugsweise die Recheneinheit (12) weiters ausgebildet ist, Information über die ausgewertete Auswahlinformation (AW) in den zweiten Code (C2) einzucodieren.

18. System nach einem der Ansprüche 14 bis 16, *dadurch gekennzeichnet*, dass das Eingangsinterface (11) des Servers (1) zum Empfang von SMS oder MMS ausgebildet ist, die den ersten Code (C1) in Klartext oder visuell aufbereiteter Form enthalten.

19. System nach einem der Ansprüche 14 bis 17, *dadurch gekennzeichnet*, dass das Ausgangsinterface (13) des Servers (1) zum Senden von SMS oder MMS ausgebildet ist, die den zweiten Code (C2) in Klartext oder visuell aufbereiteter Form enthalten.

20. System nach einem der Ansprüche 14 bis 18, *dadurch gekennzeichnet*, dass die Recheneinheit (12) des Servers (1) dazu ausgebildet ist, ein zusammen mit dem ersten Code (C1) empfangenes Passwort (PW) des Benutzers auszuwerten.

21. System nach einem der Ansprüche 14 bis 19, *dadurch gekennzeichnet*, dass die Recheneinheit (12) des Servers (1) dazu ausgebildet ist, einen oder mehrere Datensätze aus Benutzer-Identifikation (ID), Terminal-Identifikation (TI), Auswahlinformation (AW), Datum, Zeit und Inhalt der eingehenden ersten Codes (C1) und ausgehenden zweiten Codes (C2) zu protokollieren und gegebenenfalls für die Durchführung einer Abrechnung zu verwenden.

Hiezu 1 Blatt Zeichnungen

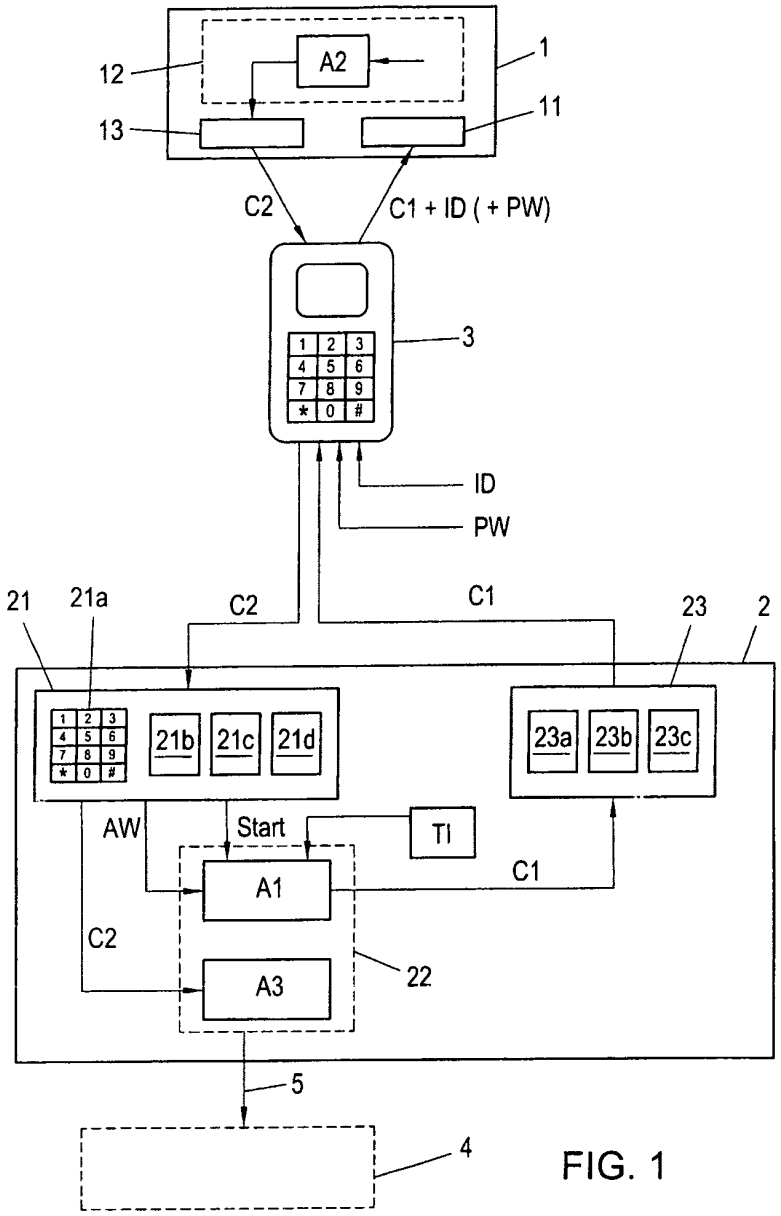
A2
1
12
11
13
C2
C1 + ID (+ PW)
3
ID
PW
21
21a
C2
C1
23
2
21b
21c
21d
23a
23b
23c
AW
Start
TI
C1
A1
C2
A3
22
5
4

FIG. 1