(19) Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 197 44 106 B4** 2007.11.29

(12) **Patentschrift**

(21) Aktenzeichen: **197 44 106.8**
(22) Anmeldetag: **06.10.1997**
(43) Offenlegungstag: **09.04.1998**
(45) Veröffentlichungstag der Patenterteilung: **29.11.2007**

(51) Int Cl.[8]: ***G06K 19/073*** (2006.01)
G07C 11/00 (2006.01)
G07F 19/00 (2006.01)
H04L 9/32 (2006.01)

(30) Unionspriorität:
96-44125 05.10.1996 KR

(73) Patentinhaber:
Samsung Electronics Co., Ltd., Suwon, Kyonggi, KR

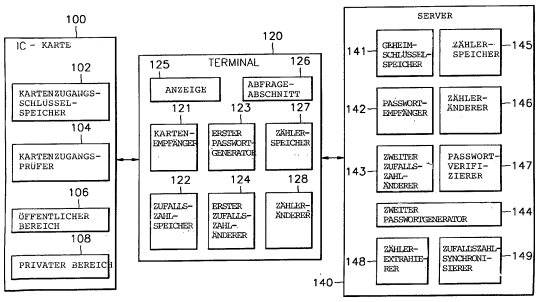
(74) Vertreter:
Wilhelms, Kilian & Partner, 81541 München

(72) Erfinder:
Yu, Ju-Yeol, Seoul, KR; Chung, Ho-Suk, Seoul, KR; Moon, Soon-Il, Seoul, KR

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:
US 54 42 342 A
US 53 47 580 A

(54) Bezeichnung: **System zur Authentizierung eines Benutzers und Verfahren hierzu**

(57) Hauptanspruch: System zur Authentizierung eines Benutzers, welches aufweist:
eine IC-Karte (100) zur Speicherung eines Geheimschlüssels zur Generierung eines Einzeit-Passworts und bestimmter Zufallszahlen,
ein Terminal (120) zur Generierung eines Einmal-Passworts unter Verwendung der IC-Karte als Eingabe, und
einen Server (140) zur Authentizierung des mit dem Terminal generierten Einmal-Passworts,
wobei das Terminal (120) aufweist:
einen Kartenempfänger (121) für den Empfang der IC-Karte und als Schnittstelle zu dieser, wobei der Kartenempfänger bestimmt, ob die IC-Karte das erste Mal eingegeben wird,
einen Zufallszahlspeicher (122) zum Lesen und Speichern und nachfolgenden Löschen der Zufallszahlen aus der IC-Karte, wenn die IC-Karte das erste Mal in den Kartenempfänger eingeführt wird,
einen ersten Passwortgenerator (123) zur Generierung eines Einmal-Passworts durch Lesen des Geheimschlüssels der IC-Karte und der in dem Zufallszahlspeicher gespeicherten Zufallszahl,
einen ersten Zufallszahländerer (124) zum Ändern der in dem Zufallszahlspeicher gespeicherten Zufallszahl auf einen bestimmten Wert und Speichern des...



Beschreibung

[0001] Die Erfindung bezieht sich auf eine Benutzerauthentizierungseinrichtung und im besonderen auf eine Vorrichtung zur Authentizierung eines ein tragbares Terminal und eine IC-Karte verwendenden Benutzers, die auf einen Kontostand und Aufzeichnungsunterlagen von elektronischem Geld Bezug nehmen und ein Einzeit- bzw. kurzlebiges Passwort erzeugen kann, sowie ein Verfahren hierzu.

[0002] Die Entwicklung von Computern und Telekommunikation, die Verbreitung von Computer-Netzwerken sowie die Entwicklung der IC-Kartentechnologie mit Speicher- und Rechenfähigkeit haben viele neue Anwendungsgebiete hervorgebracht und Annehmlichkeiten geschaffen. Elektronisches Geld, welches eines der Anwendungsgebiete der IC-Karte ist, sollte auch in der Lage sein, auf einen Kontostand und Transaktionsaufzeichnungen in einer elektronischen Geldbörse Bezug nehmen zu können.

[0003] So kann ein Benutzer Geld auf seinem Konto verwalten, ohne eine Bank aufzusuchen, und ohne Schwierigkeiten viele Dinge über einen Fernanschluss unter Verwendung eines Computers von zuhause erledigen. Ein Dienstleistungsanbieter, wie etwa eine Bank, und ein Netzwerk-Server müssen feststellen, ob eine Person, die einen bestimmten Dienstleistung haben möchte, ein autorisierter Benutzer ist. Falls ein Versuch einer Person, die vorgibt, der autorisierte Benutzer zu sein, infolge eines schwachen Benutzerauthentizierungssystems erfolgreich ist, sind ein Eindringen in die Privatsphäre und immaterielle und materielle Schäden möglich. Insbesondere wenn ein Benutzer eine Dienstleistung aus der Entfernung möchte, benötigt der Dienstleistungsanbieter ein Verfahren zur Feststellung der Identität des Benutzers, ohne den Benutzer persönlich zu treffen.

[0004] Zur Authentizierung der Identität des Benutzers kann etwas, das nur der Benutzer kennt, das nur der Benutzer weiß, sowie körperliche Merkmale und Eigenheiten des Benutzers verwendet werden. Die grundlegendste und allgemeinste Methode, die zur Authentizierung der Benutzeridentität verwendet wird, besteht im Verwenden eines Passworts. Beim Passwortverfahren wird die Benutzeridentität authentiziert, indem etwas festgestellt bzw. bestätigt wird, was nur der Benutzer weiß. Das heißt, der Benutzer, der eine Dienstleistung wünscht, wählt ein Passwort aus, das nur er kennt, und registriert es beim Dienstleistungsanbieter (dem Server). Der Benutzer verwendet als Passwort im Allgemeinen eine Folge aus mehreren Zahlen oder Buchstaben. Wenn der Benutzer, der seine Identitätsauthentizierung wünscht, das Passwort an den Server sendet, vergleicht der Server in einem Anfangsstadium das gesendete Passwort mit dem registerten Passwort und authentiziert den Benutzer.

[0005] Für eine sicherere Benutzerauthentizierung ist es vorzuziehen, ein Einmal-Passwort zu verwenden, bei welchem sich das Passwort jedes Mal ändert, wenn der Benutzer authentiziert zu werden wünscht. Bei dieser Methode kann ein unautorisierter Zutrittsucher ein Passwort, das er herausgefunden hat, nicht noch einmal verwenden, da ein Passwort jedes Mal geändert wird, wenn der Benutzer authentiziert zu werden wünscht. Zur Authentizierung der Identität unter Verwendung des Einmal-Passworts ist eine Vorrichtung zur Generierung des Einmal-Passworts erforderlich. Wenn dabei jeder Benutzer ein eigenes Terminal zur Generierung des Einmal-Passworts verwendet, ist es möglich, die Sicherheit zu verbessern, da es möglich ist, gleichzeitig etwas zu bestätigen, was nur der Benutzer weiß und was nur der Benutzer besitzt, um den Benutzer zu authentizieren.

[0006] Beim Einmal-Passwort sind Variable, die sich jedes Mal ändern, erforderlich, um Passwörter zu erzeugen, die sich jedes Mal ändern, anders als dies bei einem herkömmlichen Passwort der Fall ist. Hierzu wird ein Verfahren der Verwendung eines Echtzeittakts (EZT) sowie ein Herausforderungs/Reaktions-Verfahren der Verwendung von Zufallszahlen verwendet.

[0007] Bei dem Benutzerauthentizierungsverfahren, bei welchem der EZT als Variable verwendet wird, sind das Terminal, das ein Benutzer besitzt, und der Server eines Dienstanbieters synchronisiert. Das heißt, der Benutzer wird authentiziert, indem das Einmal-Passwort, das entsprechend der Zeit, zu der der Benutzer authentiziert zu werden wünscht, im Terminal erzeugt wird, mit dem vom Server zur gleichen Zeit erzeugten Passwort verglichen wird.

[0008] Bei dem Herausforderungs/Reaktions-Verfahren der Benutzung von Zufallszahlen werden unter Verwendung eines Zufallszahlengenerators erzeugte Zufallszahlen zur Bestimmung des Einmal-Passworts verwendet. Wenn die Benutzerauthentizierung beginnt, erzeugt der Server Zufallszahlen und überträgt diese an den Benutzer. Das Terminal verschlüsselt die Zufallszahlen mit einer mit dem Server gemeinsamen Geheimzahl, erzeugt das Einmal-Passwort und überträgt es an den Server. Der Server authentiziert den Benutzer, indem er ein Passwort unter Verwendung der gleichen Geheimzahl, die er mit dem Terminal gemeinsam hat, und der gleichen übertragenen Zufallszahlen erzeugt und es mit dem vom Terminal erzeugten Passwort vergleicht.

[0009] Die oben erwähnten Benutzerauthentizierungsverfahren mit Passwort, die gegenwärtig am häufigsten benutzt werden, weisen jedoch viele Probleme auf. Das Passwort, das aus mehreren Zahlen

und Buchstaben, beruhend auf persönlicher Information, wie etwa Telefonnummer, Geburtstag und einer Bürger-ID-Zahl, erzeugt wird, kann unter Umständen leicht durch andere herausgefunden werden. Wenn der Benutzer das Passwort irgendwo aufschreibt, um es nicht zu vergessen, kann es für andere sichtbar sein. In Fällen, wo der Benutzer, der eine Ferndienstleistung wünscht, sein Passwort dem Server über eine Telefonleitung oder ein Netzwerk übermittelt, um authentiziert zu werden, kann das Passwort durch eine Leitungsanzapfung leicht anderen zugänglich werden.

[0010] Beim Benutzerauthentizierungsverfahren, bei welchem der EZT verwendet wird, ist die Zeit im Terminal des Benutzers mit der Zeit im Server des Dienstleistungsanbieters zur Erzeugung des Einmal-Passworts und der Benutzerauthentizierung synchronisiert. Wenn das Terminal mit der Zeit die Synchronisierung mit dem Server verliert, wird selbst ein autorisierter Benutzer nicht authentiziert, da das vom Terminal erzeugte Passwort nicht mit dem vom Server erzeugten Passwort zusammenfällt. Eine spezielle Vorrichtung ist erforderlich, um das Terminal mit dem Server zu synchronisieren. Wenn daher das Einmal-Passwort zur Stärkung der Benutzerauthentizierung einer herkömmlichen angewandten Dienstleistung verwendet wird, ist ein spezieller Server für die Synchronisierung der Zeit im Terminal mit der Zeit im Server erforderlich, was hohe Kosten für den Dienstleistungsanbieter zur Folge hat. Auch kann ein Terminal Einmal-Passwörter nur für eine einzige Dienstleistung erzeugen, da die im Terminal zur Erzeugung des Passworts unter Verwendung des Echtzeittakts verwendeten Variablen die Echtzeittakte sind. Wenn der Benutzer verschiedene angewandte Dienste möchte, ist ein separates Terminal für jeden Dienst erforderlich.

[0011] Bei dem oben erwähnten Herausforderungs/Reaktions-Verfahren, bei dem Zufallszahlen verwendet werden, müssen die vom Server gesendeten Zufallszahlen in das Terminal eingegeben werden, um das Einmal-Passwort zu erzeugen. Hierzu muss das Terminal eine Eingabevorrichtung enthalten. Da ferner ein Prozess erforderlich ist, bei welchem der Server die Zufallszahlen an den Benutzer überträgt und der Benutzer die Zufallszahlen ins Terminal eingibt, braucht dies lange Zeit und ist für den Benutzer unbequem. Auch kann, wenn der Server nicht in der Lage ist, die Zufallszahlen an den Benutzer zu übertragen, dieses Verfahren nicht verwendet werden.

[0012] Aus US 5 347 580 A ist ein kartenbasiertes Authentizierungssystem der vorliegenden Art bekannt, bei dem eine Smartcard verwendet wird, welche die auf ihr angezeigte Uhrzeit mit einem geheimen, kryptografisch starken Schlüssel verschlüsselt. Der Rechner erhält als Eingabe einige Werte, die den Benutzer definieren, die Karte und einen speziellen aus der Uhrzeit berechneten Wert und schickt diese Werte zum Server, der anhand der empfangenen Werte den Benutzer authentizieren kann.

[0013] Gemäß US 5 442 342 werden Benutzer-Passwörter von einem Rechner generiert und auf einer Karte verschlüsselt gespeichert. Um auf den Rechner zugreifen zu können, wird der Benutzer aufgefordert, korrekt auf eine Reihe von Authentizierungsherausforderungen zu antworten. Zusätzlich wird der Benutzer während der Sitzung zu zufällig ausgewählten Zeitpunkten aufgefordert, auf ausgewählte Authentizierungsherausforderungen zu antworten.

[0014] Es ist eine Aufgabe der Erfindung, eine System zur Authentizierung des Benutzers zu schaffen, bei welchem ein tragbares Terminal und eine IC-Karte, die auf einen Kontostand und Transaktionsaufzeichnungen von elektronischem Geld Bezug nehmen und ein Einmal-Passwort erzeugen können, benutzt werden, um den Benutzer billig und sicher zu authentizieren.

[0015] Zur Lösung dieser Aufgabe wird eine System zur Authentizierung eines Benutzers vorgesehen, das eine IC-Karte zur Speicherung eines Geheimschlüssels zur Erzeugung eines Einmal-Passworts und bestimmter Zufallszahlen, ein Terminal zur Erzeugung eines Einmal-Passworts unter Verwendung der IC-Karte als Eingabe sowie einen Server zur Authentizierung des mit dem Terminal erzeugten Einmal-Passworts aufweist. Das Terminal enthält einen Kartenempfänger zur Aufnahme der IC-Karte und als Schnittstelle mit dieser und zur Bestimmung, ob die IC-Karte das erste Mal eingegeben wird, einen Zufallszahlspeicher zum Lesen und Speichern und dann Löschen der Zufallszahlen der IC-Karte, wenn die IC-Karte das erste Mal in den Kartenempfänger eingeführt wird, einen ersten Passwortgenerator zur Erzeugung eines Einmal-Passworts durch Lesen des Geheimschlüssels der IC-Karte und der im Zufallszahlspeicher gespeicherten Zufallszahl, einen ersten Zufallszahländerer zur Änderung der im Zufallszahlspeicher gespeicherten Zufallszahl auf einen bestimmten Wert und Speicherung des geänderten Werts im Zufallszahlspeicher, wenn ein Einmal-Passwort im ersten Passwortgenerator erzeugt wird, sowie eine Anzeige zur Anzeige der verarbeiteten Ergebnisse des Terminals und des Servers. Der Server enthält einen Geheimschlüsselspeicher zur Speicherung eines Geheimschlüssels und einer bestimmten Zufallszahl, die mit dem Geheimschlüssel und einer bestimmten zu Anfang in der IC-Karte gespeicherten Zufallszahl identisch sind, einen zweiten Passwortgenerator zum Lesen des Geheimschlüssels und der Zufallszahl, die im Geheimschlüsselspeicher gespeichert sind, und zur Erzeugung eines Einmal-Passworts nach dem gleichen Verfahren, wie es im Termi-

nal verwendet wird, einen zweiten Zufallszahländerer zur Änderung des Zufallszahlwerts des Geheimschlüsselspeichers auf einen mit dem Zufallszahländerer des Terminals identischen Wert und Speichern des geänderten Werts im Geheimschlüsselspeicher, wenn ein Einmal-Passwort mit dem zweiten Passwortgenerator erzeugt wird, einen Passwortempfänger für den Empfang des im Terminal erzeugten Einmal-Passworts über eine Telefonleitung oder ein Netzwerk, und einen Passwortverifizierer zur Verifizierung, ob das empfangene Passwort mit dem erzeugten Passwort identisch ist.

[0016] Die IC-Karte enthält ferner einen Kartenzugangsschlüsselspeicher mit einem öffentlichen Bereich, auf welchen ein Zugriff bedingungslos erlaubt ist, und einem privaten Bereich, für welchen ein Kartenzugangsschlüssel erforderlich ist, damit Zugriff von außen gestattet wird, zur sicheren Speicherung eines Kartenzugangsschlüssels, der für die Gestattung des Zugriffs auf den Geheimbereich erforderlich ist, und einen Kartenzugriffsprüfer zur Bestimmung, ob ein Zugriff auf interne Information zugelassen werden sollte, durch Vergleichen des von außen eingegebenen Kartenzugangsschlüssels mit dem im Kartenzugangsschlüsselspeicher gespeicherten Kartenzugangsschlüssel. Der Zufallszahlspeicher des Terminals liest die Zufallszahl sowie den Kartenzugriffsschlüssel der IC-Karte und speichert sie und löscht die Zufallszahl und den Kartenzugriffsschlüssel aus dem öffentlichen Bereich der IC-Karte, wenn die IC-Karte das erste Mal in den Kartenempfänger eingeführt wird.

[0017] Der erste Passwortgenerierungsabschnitt des Terminals enthält einen Symmetrischschlüssel-Verschlüsselungsabschnitt zum Lesen des Geheimschlüssels der IC-Karte und der Zufallszahl des Zufallszahlspeichers und Erzeugen einer Verschlüsselung unter Verwendung eines Symmetrischschlüssel-Verschlüsselungsalgorithmus, einen Hash-Funktionsabschnitt zur Umwandlung der in dem Symmetrischschlüssel-Verschlüsselungsabschnitt erzeugten Verschlüsselung unter Verwendung einer Einrichtungs-Hash-Funktion zur Verhinderung einer inversen Verfolgung des Geheimschlüssels, sowie einen Formatumwandler zur Umwandlung der vom Hash-Funktionsabschnitt ausgegebenen Verschlüsselung in ein bestimmtes Format. Der zweite Passwortgenerierungsabschnitt des Servers umfasst einen Symmetrischschlüssel-Verschlüsselungsabschnitt zum Lesen des Geheimschlüssels und der Zufallszahl, die im Geheimschlüsselspeicherungsabschnitt gespeichert sind und zur Erzeugung einer Verschlüsselung unter Verwendung eines Symmetrischschlüssel-Verschlüsselungsalgorithmus, einen Hash-Funktionsabschnitt zur Verhinderung einer inversen Verfolgung der im Symmetrischschlüssel-Verschlüsselungsabschnitt erzeugten Verschlüsselung, unter Verwendung einer Einrichtungs-Hash-Funktion, sowie einen Formatumwandler zur Umwandlung der vom Hash-Funktionsabschnitt ausgegebenen Verschlüsselung in ein bestimmtes Format.

[0018] Zur Lösung obiger Aufgabe wird erfindungsgemäß ein Verfahren zur Authentizierung eines Benutzers unter Verwendung einer Benutzerauthentizierungsvorrichtung mit einer IC-Karte zur Speicherung einer bestimmten Zufallszahl und eines Geheimschlüssels zur Erzeugung eines Einmal-Passworts, einem Terminal zur Erzeugung eines Einmal-Passworts unter Verwendung der IC-Karte als Eingabe und einem Server zur Speicherung des Geheimschlüssels und einer Zufallszahl, die mit denjenigen der IC-Karte identisch sind, und zur Authentizierung des im Terminal erzeugten Einmal-Passworts, vorgesehen, wobei das Verfahren die Schritte des Einführens der IC-Karte in das Terminal, Bestimmens, ob die IC-Karte das erste Mal in das Terminal eingeführt wird, Initialisierens einer bestimmten Dienstleistung und Erzeugens eines Einmal-Passworts, wenn die IC-Karte das erste Mal eingeführt wird, und Erzeugens eines Einmal-Passworts, wenn die IC-Karte ein späteres Mal eingeführt wird, und Empfangens eines in dem Terminal erzeugten Einmal-Passworts über ein bestimmtes Kommunikationsmedium, und Verifizierens des Einmal-Passworts aufweist. Der Schritt der Initialisierung einer Dienstleistung im Passworterzeugungsschritt umfasst die Schritte des Lesens der Zufallszahl der IC-Karte und Speicherns derselben im Terminal sowie Löschens der Zufallszahl in der IC-Karte. Der Schritt der Erzeugung des Einmal-Passworts im Passworterzeugungsschritt umfasst die Schritte des Lesens des Geheimschlüssels der IC-Karte und der im Terminal gespeicherten Zufallszahl, des Ausführens eines Symmetrischschlüssel-Verschlüsselungsalgorithmus unter Verwendung des Geheimschlüssels und der Zufallszahl als Eingabe, Durchführens einer Einrichtungs-Hash-Funktion auf dem vom Symmetrischschlüssel-Verschlüsselungsalgorithmus ausgegebenen Wert, Änderns der Zufallszahl auf einen bestimmten Wert und Speicherns derselben in dem Terminal, sowie Umwandelns der Ausgabe der Einrichtungs-Hash-Funktion in ein bestimmtes Format. Der Verifizierungsschritt umfasst die Schritte des Empfangens des im Terminal erzeugten Einmal-Passworts über ein bestimmtes Kommunikationsmedium, Lesens des Geheimschlüssels und der Zufallszahl, die im Server gespeichert sind, Durchführens eines Symmetrisch-Verschlüsselungsalgorithmus unter Verwendung des Geheimschlüssels und der Zufallszahl als Eingabe, Durchführens einer Einrichtungs-Hash-Funktion auf dem vom Symmetrischschlüssel-Verschlüsselungsalgorithmus ausgegebenen Wert, Änderns der Zufallszahl auf einen bestimmten Wert und Speicherns derselben im Terminal sowie Umwandelns der Ausgabe der Einrichtungs-Hash-Funktion in ein bestimmtes Format und Authentizierens eines Benutzers, wenn das bestimm-

te Format das gleiche wie das empfangene Einmal-Passwort ist, und Nicht-Authentizierens des Benutzers, wenn es nicht das gleiche ist.

[0019] Wenn die IC-Karte einen privaten Bereich und einen öffentlichen Bereich eines Speichers aufweist und ferner einen für den Zugriff auf einen geheimen Bereich erforderlichen Kartenzugangsschlüssel aufweist, umfasst das Initialisieren einer Dienstleistung im Passworterzeugungsschritt die Schritte des Lesens der Zufallszahl und eines Kartenzugangschlüssels, zur Ermöglichung des Zugriffs auf die Zufallszahl und den privaten Bereich, aus dem öffentlichen Bereich der IC-Karte und Speicherns derselben in dem Terminal, sowie Löschens der Zufallszahl und des Kartenzugangsschlüssels aus dem öffentlichen Bereich der IC-Karte. Der Schritt des Lesens des Geheimschlüssels der IC-Karte im Passworterzeugungsschritt umfasst die Schritte des Eingebens des im Terminal gespeicherten Kartenzugangsschlüssels in die IC-Karte, Prüfens, ob der in die IC-Karte eingegebene Kartenzugangsschlüssel der gleiche wie der Kartenzugangsschlüssel des IC-Karten-Privatbereichs ist, und, wenn sie dies der Fall ist, Gestattens des Zugangs zur Karte, sowie Lesens des Geheimschlüssels der IC-Karte, wenn der Zugang im Schritt des Prüfens des Kartenzugangsschlüssels erlaubt wird.

[0020] Wenn das Terminal und der Server jeweils einen Zähler zur Synchronisierung des Terminals mit dem Server aufweisen, umfasst der Schritt des Erzeugens eines Einmal-Passworts im Passworterzeugungsschritt den Schritt des Änderns der Zufallszahl und des Zählwerts in bestimmte Werte und Speicherns derselben in dem Terminal. Der Schritt des Erzeugens eines Einmal-Passworts im Passworterzeugungsschritt umfasst die Schritte des Einfügens des Zählwerts in einen Passwort-Bitstrom, der durch den Schritt der Durchführung einer Einrichtungs-Hash-Funktion auf dem über den Symmetrischschlüssel-Verschlüsselungsalgorithmus ausgegebenen Wert erzeugt ist, und Umwandelns des Passwort-Bitstroms, in den der Zählwert eingefügt ist, in ein bestimmtes Format. Der Empfangsschritt im Verifizierungsschritt umfasst ferner die Schritte des Herausziehens eines Zählwerts aus dem empfangenen Einmal-Passwort, des Vergleichens des im Herausziehschritt herausgezogenen Zählwerts mit dem Zählwert des Servers sowie Gleichmachens der Zählwerte der Zähler und Änderns der Zufallszahl in eine Zufallszahl, die dem Zählwert entspricht, falls im Vergleichsschritt die Zählwerte nicht gleich sind. Der Schritt des Änderns der Zufallszahl im Verifizierungsschritts dient der Änderung der Zufallszahl auf einen bestimmten Wert und dem Speichern derselben im Terminal. Der Umwandlungsschritt im Verifizierungsschritts umfasst die Schritte des Durchführens der Einrichtungs-Hash-Funktion und Einfügens des Zählwerts in den ausgegebenen Passwort-Bitstrom und Umwandelns des Passwortwerts, in den der Zählwert eingefügt ist, in ein bestimmtes Format.

[0021] Im Folgenden werden bevorzugte Ausführungsformen der Erfindung anhand der beigefügten Zeichnungen beschrieben, auf welchen

[0022] Fig. 1 ein Blockschaltbild des Aufbaus einer Vorrichtung zur Authentizierung eines Benutzers gemäß der Erfindung ist,

[0023] Fig. 2 ein Blockschaltbild des detaillierten Aufbaus eines ersten Passwortgenerators ist,

[0024] Fig. 3 ein Blockschaltbild des detaillierten Aufbaus eines zweiten Passwortgenerators ist,

[0025] Fig. 4 ein Flussdiagramm der Gesamtarbeitsweise der Vorrichtung zur Authentizierung eines Benutzers gemäß der Erfindung ist,

[0026] Fig. 5 ein Flussdiagramm eines Dienstleistungsinitialisierungsprozesses ist,

[0027] Fig. 6 ein Flussdiagramm des detaillierten Prozesses des Schritts der Erzeugung eines Einmal-Passworts aus Fig. 4 ist, und

[0028] Fig. 7 ein Flussdiagramm eines Prozesses zur Verifizierung des von einem Benutzer auf den Server eines Dienstleistungsanbieters übertragenen Passworts ist.

[0029] Nachfolgend wird die Erfindung unter Bezugnahme auf die beigefügten Zeichnungen beschrieben. Gemäß Fig. 1 enthält eine Vorrichtung zur Authentizierung eines Benutzers eine IC-Karte **100** für ein sicheres Aufbewahren und Tragen von persönlicher Geheiminformation, ein Terminal **120**, welches subminiaturisiert ist, so dass es leicht tragbar ist, zur Erzeugung eines Einmal-Passworts für die Bestätigung der Identität einer Person und für die Bezugnahme auf einen Kontostand von elektronischem Geld, sowie einen Server **140** zur Authentizierung des im Terminal **120** erzeugten Einmal-Passworts und zur Lieferung eines Dienstes.

[0030] Die IC-Karte **100** speichert einen Geheimschlüssel und eine bestimmte Zufallszahl zur Erzeugung eines Einmal-Passworts. Die IC-Karte **100** enthält einen öffentlichen Bereich **106**, auf den ein Zugriff von außen zugelassen ist, einen privaten Bereich **108**, für welchen ein Kartenzugangsschlüssel für einen Zugang von außen erforderlich ist, einen Kartenzugangsschlüsselspeicher **102** zur Speicherung des für einen Zugang zum privaten Bereich **108** erforderlichen Kartenzugangsschlüssels und einen Kartenzugangsüberprüfer **104** zum Vergleichen des von außen eingegebenen Kartenzugangsschlüssels mit dem Kartenzugangsschlüssel, der im Kartenzu-

gangsschlüsselspeicher **102** gespeichert ist (gesetzt als privater Bereich) und zur Bestimmung, ob Zugang zu innerer Information zugelassen wird. Die IC-Karte **100** kann als Identitätskarte oder elektronisches Geld verwendet werden und kann eine Menge an Information enthalten, die ein Benutzer sich nicht merken kann, da die Speicherkapazität der IC-Karte **100** viel größer als diejenige einer herkömmlichen Magnetkarte ist. Da ferner der Kartenzugangsschlüssel der IC-Karte **100** benötigt wird, um die in der IC-Karte gespeicherten Daten zu lesen, können Dritte nicht ohne weiteres an die persönliche Information eines Benutzers gelangen, auch wenn dieser die IC-Karte verlegt.

[0031] Das Terminal **120** dient der Aufnahme der IC-Karte **102** und der Erzeugung eines Einmal-Passworts. Das Terminal **120** enthält einen Kartenempfänger **121**, einen Zufallszahlspeicher **122**, einen ersten Passwortgenerator **123**, einen ersten Zufallszahländerer **124**, eine Anzeige **125**, einen Abfrageabschnitt **126**, einen Zählerspeicher **127** und einen Zähleränderer **128**.

[0032] Der Kartenempfänger **121** weist einen Schlitz zur Aufnahme der IC-Karte **100** auf und bildet die Schnittstelle zur IC-Karte **100**. Der Zufallszahlspeicher **120** liest die in der IC-Karte **100** gespeicherte Zufallszahl, wenn die IC-Karte **100** am Anfang in den Kartenempfänger **121** eingegeben wird, speichert die Zufallszahl und löscht die in der IC-Karte gespeicherte Zufallszahl.

[0033] Der erste Passwortgenerator **123** dient dem Lesen des Geheimschlüssels der IC-Karte **100** und der im Zufallszahlspeicherabschnitt **122** gespeicherten Zufallszahl und der Erzeugung des Einmal-Passworts nach einer bestimmten Methode. Wie in Fig. 2 gezeigt, enthält der erste Passwortgenerator **123** einen Symmetrischschlüssel-Verschlüsselungsabschnitt **200**, einen Hash-Funktionsabschnitt **210** und einen ersten Formatumwandlungsabschnitt **220**. Der Symmetrischschlüssel-Verschlüsselungsabschnitt **200** liest den Geheimschlüssel der IC-Karte **100** und die Zufallszahl des Zufallszahlspeichers **122** und erzeugt einen Schlüssel unter Verwendung eines Symmetrischschlüssel-Verschlüsselungsalgorithmus.
Der Hash-Funktionsabschnitt **210** verhindert, indem er den im Symmetrischschlüssel-Verschlüsselungsabschnitt **200** erzeugten Schlüssel unter Verwendung einer Einrichtungs-Hash-Funktion umwandelt, dass eine unautorisierte Person den Geheimschlüssel und die Zufallszahl rückwärts verfolgt. Der erste Formatumwandlungsabschnitt **220** dient zur Umwandlung des Passwort-Bitstroms, den der Hash-Funktionsabschnitt **210** ausgibt, in ein bestimmtes Format, das vom Benutzer leicht gelesen werden kann. Der erste Formatumwandlungsabschnitt **220** enthält einen Zählereinfüger **222** zum Einfügen des Zählwerts des Zählerspeichers **127** in den Passwort-Bitstrom und einen Formatumwandler **224** zum Umwandlen des vom Zählereinfüger **222** ausgegebenen Passwort-Bitstroms in ein bestimmtes Format, das vom Benutzer leicht gelesen werden kann. Ein Protokolltypselektions-(PTS-)Bit, das sich auf das Protokoll eines Algorithmus zur Erzeugung von mehr als einem Einmal-Passwort bezieht, kann zusätzlich durch den Zählereinfüger **222** eingefügt werden. Der Formatumwandler **224** wandelt einen binären Passwort-Bitstrom vorzugsweise in eine Dezimalzahl um, die vom Benutzer leicht gelesen werden kann.

[0034] Der erste Zufallszahländerer **124** ändert die im Zufallszahlspeicher **122** gespeicherte Zufallszahl auf einen bestimmten Wert und speichert die geänderte Zufallszahl im Zufallszahlspeicher **122**, nachdem das Einmal-Passwort durch den ersten Passwortgenerator **123** erzeugt worden ist. Die Anzeige **125** dient der Anzeige des im ersten Passwortgenerator **123** erzeugten Passworts. Eine Flüssigkristallanzeige (LCD) wird vorzugsweise als Anzeige **125** verwendet.

[0035] Der Abfrageabschnitt **126** nimmt auf Kontostände und Transaktionsaufzeichnungen der IC-Karte Bezug. Der Zählerspeicher **127** speichert einen Zählwert zur Synchronisierung des Terminals **120** mit dem Server **140**. Der Zähländerer **128** ändert den Zählwert auf einen bestimmten Wert, jedes Mal wenn ein Einmal-Passwort erzeugt wird, und speichert den Wert im Zählerspeicher **127**.

[0036] Der Server **140** dient zur Authentizierung eines im Terminal **120** erzeugten Einmal-Passworts. Der Server **140** enthält einen Geheimschlüsselspeicher **141**, einen zweiten Passwortgenerator **144**, einen zweiten Zufallszahländerer **143**, einen Passwortempfänger **142**, einen Passwortverifizierer **147**, einen Zählerspeicher **145**, einen Zähleränderer **146**, einen Zählerextraktor **148** und einen Zufallszahlsynchronisierer **149**.

[0037] Der Geheimschlüsselspeicher **141** speichert einen Geheimschlüssel und eine Zufallszahl, die identisch mit dem anfänglich in der IC-Karte gespeicherten Geheimschlüssel bzw. einer bestimmten Zufallszahl sind.

[0038] Der zweite Passwortgenerator **144** dient zum Lesen des Geheimschlüssels und der Zufallszahl, die im Geheimschlüsselspeicher **141** gespeichert sind, und zur Erzeugung des Einmal-Passworts nach der gleichen Methode, wie es die im Terminal **120** verwendete bestimmte Methode ist. Wie in Fig. 3 gezeigt, enthält der zweite Passwortgenerator **144** einen Symmetrischschlüssel-Verschlüsselungsabschnitt **300**, einen Hash-Funktionsabschnitt **310** und einen zweiten Formatumwandlungsabschnitt **320**. Der Symmetrischschlüssel-Verschlüsselungsabschnitt **300** liest den Geheimschlüssel und die Zu-

fallszahl, die im Geheimschlüsselspeicher **141** gespeichert sind, und erzeugt einen Schlüssel unter Verwendung eines Symmetrischschlüssel-Verschlüsselungsalgorithmus. Der Hash-Funktionsabschnitt **310** verhindert, indem er den im Symmetrischschlüssel-Verschlüsselungsabschnitt **300** erzeugten Schlüssel unter Verwendung einer Einrichtungs-Hash-Funktion umwandelt, dass eine unautorisierte Person den Geheimschlüssel und die Zufallszahl rückwärts verfolgt. Der zweite Formatumwandlungsabschnitt **320** dient der Umwandlung des vom Hash-Funktionsabschnitt **310** ausgegebenen Passwort-Bitstroms in ein bestimmtes Format. Der zweite Formatumwandlungsabschnitt **320** enthält einen Zählereinfüger **322** zum Einfügen des Zählwerts des Zählerspeichers **145** in den Passwort-Bitstrom und einen Formatumwandler **324** zum Umwandeln des vom Zählereinfüger **322** ausgegebenen Passwort-Bitstroms in ein bestimmtes Format, das vom Benutzer einfach gelesen werden kann. Der Formatumwandler **324** wandelt den binären Passwort-Bitstrom vorzugsweise in eine Dezimalzahl um, die vom Benutzer einfach gelesen werden kann.

[0039] Der zweite Zufallszahländerer **143** macht den Zufallszahlwert des Geheimschlüsselspeichers **141** identisch mit demjenigen des ersten Zufallszahländerers **124** des Terminals **120** und speichert den geänderten Wert im Geheimschlüsselspeicher **141**, nachdem das Einmal-Passwort durch den zweiten Passwortgenerator **144** erzeugt worden ist. Der Passwortempfänger **142** empfängt das Einmal-Passwort wie auf der Anzeige **125** des Terminals **120** angezeigt durch eine Telefonleitung oder ein bestimmtes Netzwerk.

[0040] Der Passwortverifizierer **147** prüft, ob das empfangene Passwort identisch mit dem erzeugten Passwort ist, und verifiziert das Einmal-Passwort. Der Zählerspeicher **145** speichert einen Zählwert zur Synchronisierung des Terminals **120** mit dem Server **140**. Der Zähleränderer **146** ändert den Zählwert auf einen bestimmten Wert und speichert ihn im Zählerspeicher **145**, jedes Mal wenn ein Einmal-Passwort erzeugt wird.

[0041] Der Zählextraktor **148** extrahiert den Zählwert aus dem mit dem Passwortempfänger **142** empfangenen Einmal-Passwort und extrahiert das PTS, wenn das PTS mit dem Zählereinfüger **222** des Terminals **120** eingefügt ist. Der Zufallszahlsynchronisierer **149** prüft, ob der vom Zählerextraktor **148** herausgezogene Zählwert mit dem Zählwert des Servers **140** übereinstimmt. Wenn nicht, erzeugt der Zufallszahlsynchronisierer **149** eine Zufallszahl, die dem extrahierten Zählwert entspricht, und gibt die Zufallszahl dem Symmetrischschlüssel-Verschüsselungsabschnitt **300** des Servers **140** ein.

[0042] Die Arbeitsweise der Vorrichtung zur Authentizierung eines Benutzers, und ein Verfahren hierzu, gemäß der Erfindung wird im Folgenden beschrieben. Bei der vorliegenden Erfindung wird ein Einmal-Passwort verwendet, das jedes Mal geändert wird, wenn der Benutzer authentiziert wird. Ein Geheimschlüssel, eine Zufallszahl und ein Zählwert werden als Variable zur Erzeugung des Einmal-Passworts verwendet. Der Geheimschlüssel für einen Symmetrischschlüssel-Verschlüsselungsalgorithmus wird als Geheimwert zur Verschlüsselung verwendet und in der IC-Karte **100** für jeden Benutzer gespeichert. Die Zufallszahl zur Erzeugung eines jedes Mal anderen Passworts liegt in der IC-Karte **100** vor und wird in einem Prozess zur Initialisierung der Dienstleistung auf das tragbare Terminal **120** übertragen und dort gespeichert und wird in der IC-Karte gelöscht. Der Zähler zur Synchronisierung des Terminals **120** mit dem Server **140** ist im Terminal **120** untergebracht. Das Einmal-Passwort wird unter Verwendung der Zufallszahl und des im Terminal **120** gespeicherten Zählwerts erzeugt. Wenn der Benutzer wünscht, von verschiedenen Servern authentiziert zu werden, sind IC-Karten für jeden Dienst, aber nur ein Terminal erforderlich.

[0043] Es ist möglich, das Terminal **120** mit dem Server **140** zu synchronisieren, indem der Zählwert in das Passwort während eines Prozesses zur Erzeugung des Einmal-Passworts eingefügt wird. Der Server **140** zieht den Zählwert aus dem vom Benutzer empfangenen Passwort heraus, synchronisiert mit dem Terminal, erzeugt das Passwort unter Verwendung des Geheimschlüssels und des Zufallszahlwerts, die mit dem Terminal gemeinsam sind, und prüft, ob das erzeugte Passwort mit dem vom Benutzer empfangenen Passwort zusammenfällt. Es ist möglich, das Terminal leicht mit dem Server zu synchronisieren, obwohl nur der Zähler des Terminals geändert wird und der Zähler des Servers nicht geändert wird, so dass der Benutzer zufällig den Zählwert ändert. Auch kann die IC-Karte **100** verlangen, dass der Kartenzugangsschlüssel unterbreitet wird, damit die Information, die im privaten Bereich **108** der Karte gespeichert ist, gelesen werden kann. Es ist möglich, die private Information des Benutzers sicher aufzubewahren, da nur ein autorisierter Benutzer die private Information lesen kann, indem er den Kartenzugangsschlüssel liefert.

[0044] Die Arbeitweise der vorliegenden Erfindung wird nun in größeren Einzelheiten beschrieben. Die Benutzerauthentizierungsvorrichtung gemäß der vorliegenden Erfindung hat Funktionen der Abfrage des Kontostands und von Handelsdetails, der Initialisierung des Dienstes zur Erzeugung eines Einmal-Passworts, Erzeugung des Einmal-Passworts und Verifizierens des Einmal-Passworts im Server.

[0045] Bei der vorliegenden Erfindung wird gemäß Fig. 4 die Authentizierung eines Benutzers unter Ver-

wendung des Einzeit-Passworts in drei Schritten durchgeführt: Initialisieren des Dienstes, wenn ein Benutzer die IC-Karte an das Terminal einführt, um die Dienstleistung zu erhalten (Schritt **470**), Erzeugen des Einmal-Passworts im Terminal (Schritt **430**) und Verifizieren des Passworts des Benutzers im Server (Schritt **450**).

[0046] Der Benutzer führt die IC-Karte **100** für den Dienst, den er wünscht, in den Kartenempfänger **121** des Terminal **120** ein (Schritt **400**). Wenn der Benutzer die IC-Karte einführt, bestimmt der Kartenempfänger **121** des Anschlusses **120** die Art der IC-Karte und prüft, ob die IC-Karte **100** das erste Mal eingeführt wird oder in der Vergangenheit bereits einmal eingeführt und initialisiert worden war (Schritt **410**). Falls die IC-Karte das erste Mal eingeführt wird, wird der Initialisierungsvorgang (Schritt **470**) durchgeführt. Wenn eine schon vorher initialisierte IC-Karte eingeführt wird, wird bestimmt, ob das Einmal-Passwort zu erzeugen ist (Schritt **420**). Üblicherweise wird der Vorgang abgeschlossen, nachdem nur der Kontostand abgefragt worden ist (Schritt **460**). Ein Benutzer, der authentiziert zu werden wünscht, generiert das Einmal-Passwort unter Verwendung der Bedienungsvorrichtung des Terminals (Schritt **430**). Das Terminal **120** bietet den während des Initialisierungsprozesses empfangenen Kartenzugangsschlüssel der IC-Karte **100** an, liest die Geheimwerte (einen Geheimschlüssel für einen symmetrischen Verschlüsselungsalgorithmus) der Karte und erzeugt das Einmal-Passwort (Schritt **430**). Wenn der Benutzer dieses Ergebnis auf den Server **140** überträgt (Schritt **440**), verifiziert es der Server **140** (Schritt **450**).

[0047] Fig. 5 zeigt den Dienstinitialisierungsprozess (Schritt **470**) in größeren Einzelheiten. Der Dienstinitialisierungsprozess (Schritt **470**) dient zur Übertragung des Kartenzugangsschlüssels, zum Lesen der Zufallszahl, die für die Benutzerauthentizierung kritisch und im öffentlichen Bereich der IC-Karte gespeichert ist, und des Geheimschlüssels, der im privaten Bereich der IC-Karte des Benutzers gespeichert ist, auf das Terminal und zum Löschen der Zufallszahl und des Kartenzugangsschlüssels aus dem öffentlichen Bereich, nachdem der Benutzer die IC-Karte **100** das erste Mal in das Terminal **120** eingesetzt hat (Schritt **400** der Fig. 4). Das Terminal **120** fühlt dabei ab, dass die IC-Karte **100** das erste Mal eingeführt ist, und führt den Initialisierungsprozess durch. Das Terminal **120** liest die Zufallszahl und den Kartenzugangsschlüssel, die im öffentlichen Bereich der IC-Karte **100** gespeichert sind (Schritt **510**), speichert sie im Zufallszahlspeicher **122** des Terminals **120** (Schritt **520**) und löscht die Zufallszahl und den Kartenzugangsschlüssel aus dem öffentlichen Bereich der IC-Karte **100** (Schritt **530**). Daher verbleibt nur der Geheimschlüssel im sicheren privaten Bereich der initialisierten IC-Karte.

[0048] Die Information der IC-Karte zur Bezugnahme auf den Kontostand ist offen für jedermann. Der Datenzugangsschlüssel wird zum Lesen des Geheimschlüssels für die Benutzerauthentizierung, der im Geheimbereich gespeichert ist, benötigt. Nach Durchführung des Dienstinitialisierungsprozesses kann der Geheimschlüssel in der IC-Karte nur durch das Terminal gelesen werden, das den Initialisierungsprozess durchgeführt hat. Der Benutzer kann ein Einmal-Passwort für verschiedene Dienste mit einem einzigen Terminal generieren. Getrennte Speicherräume sind im Terminal den einzelnen Dienstleistungen zugeordnet. Die Information, die für die Authentizierung des Benutzers der einzelnen Dienstleistungen benötigt wird, wird in den Speicherräumen gehalten.

[0049] Fig. 6 ist ein Flussdiagramm, welches das Arbeiten im Schritt **430** (Fig. 4) zur Erzeugung des Einmal-Passworts in größeren Einzelheiten zeigt. Das Einmal-Passwort wird unter Verwendung des Geheimschlüssels (Geheimschlüssel für den Symmetrischschlüssel-Verschlüsselungsalgorithmus), den sich IC-Karte **100** und Server **140** teilen, und eines Zufallszahlwerts, den sich Terminal **120** und Server **140** teilen, erzeugt. Wenn der Benutzer die IC-Karte in das Terminal einführt (Schritt **400** der Fig. 4) und das Terminal anweist, ein Einmal-Passwort zu erzeugen, liest der Symmetrischschlüssel-Verschlüsselungsabschnitt **200** des ersten Passwortgenerators **123** des Terminals **120** den Geheimschlüssel aus der IC-Karte **100** sowie die Zufallszahl und den Zählwert aus dem Zufallszahlspeicher **122** aus (Schritt **610**), erzeugt einen Schlüssel aus den gelesenen Werten unter Verwendung des Symmetrischschlüssel-Verschlüsselungsalgorithmus (Schritt **620**) und berechnet den sich ergebenden Binärwert unter Verwendung einer Einrichtungs-Hash-Funktion im Hash-Funktionsabschnitt **210** (Schritt **630**). Die Einrichtungs-Hash-Funktion wird verwendet, um zu verhindern, dass eine Person, die einen unautorisierten Zugangsversuch macht, Information zum Geheimwert unter Verwendung des Ergebnisses des Einmal-Passworts herausfinden kann.

[0050] Der sich ergebende Wert der Einrichtungs-Hash-Funktion durchläuft einen Umwandlungsalgorithmusprozess, da er nicht direkt als Einmal-Passwort verwendet werden kann (Schritt **680**). Zunächst wird der sich ergebende Binärwert, mit dem der Benutzer nicht vertraut ist, in eine Dezimalzahl umgewandelt, mit der der Benutzer leicht umgehen kann. Das Einmal-Passwort, umgewandelt in Dezimalform, wird auf der Anzeige **125** angezeigt (Schritt **690**). Da die Binärzahl, die durch die Einrichtungs-Hash-Funktion ausgegeben wird, sehr groß ist (beispielsweise eine Binärzahl von mehr als 64 Bit), muss sie in eine Zahl innerhalb einer gewissen Größe (beispielsweise eine Binärzahl von ungefähr 26 Bit im Falle der Verwendung einer Dezimalzahl von 8

Stellen als Einmal-Passwort) umgewandelt werden, die auf der Anzeige **125** des Terminal angezeigt werden kann.

[0051] Beim Umwandlungsalgorithmus (Schritt **680**) werden der resultierende Wert der Einrichtungs-Hash-Funktion, der Zählwert und die Protokolltypselektion (PTS) verwendet. Die PTS und der Zählwert N werden dabei durch den Zählwerteinfüger **222** in den Bitstrom des Einmal-Passworts eingefügt, um das Terminal **120** mit dem Server **140** zu synchronisieren. Beispielsweise wird ein Passwort von 26 Bits in einem Bereich, der durch den resultierenden Wert der Einrichtungs-Hash-Funktion besetzt ist, und einen Bereich, der durch den Zählwert N und die BTS besetzt ist, unterteilt. Die PTS ist erforderlich, wenn der Server verschiedene Algorithmen zur Erzeugung des Einmal-Passworts kategorisiert.

[0052] Der Zählwert N wird jedes Mal um eins reduziert, wenn ein Passwort erzeugt wird (Schritt **650**). Es wird geprüft, ob der verminderte Wert 0 ist (Schritt **650**). Wenn der Wert 0 wird, kehrt der Prozess zur Ausgangsstufe zurück. Die Zufallszahl wird üblicherweise um eins erhöht und initialisiert, wenn N zu 0 wird. Im Prozess der Initialisierung des Dienstes wird die in der IC-Karte gelesene und verwendete Zufallszahl nur zur Erzeugung des Anfangspaßworts verwendet, und nach dem anfänglichen wird die Zufallszahl um eins erhöht, wenn jedes Passwort erzeugt wird (Schritt **650**). Wenn der Zählwert N zu 0 wird, wird eine Zufallszahl, die bei der Generierung des Passwortes generiert wird (beispielsweise der sich ergebende Wert des Symmetrischschlüssel-Verschlüsselungsalgorithmus) als Zufallszahlinitialisierungswert gesetzt. Das Passwort wird generiert, indem die Zufallszahl um eins erhöht wird (Schritt **650**). Eine neue Zufallszahl wird eingestellt, wenn der Zählwert N zu 0 wird (Schritt **660**). Nach Erzeugung eines Passworts werden der Zählwert N und die Zufallszahl RN im Zufallszahlspeicher **122** aufgezeichnet (Schritt **670**).

[0053] Fig. 7 ist ein Flussdiagramm eines Prozesses zur Verifizierung des Passwortes, das vom Benutzer auf den Server des Dienstanbieters übertragen worden ist. Der Server **140** empfängt das vom Benutzer übertragene Einmal-Passwort über den Passwortempfänger **142** (Schritt **700**). Der Server zieht dann aus dem erhaltenen Datenbitstrom mit dem Zählwertextraktor **148** den Zählwert heraus (Schritt **710**) und synchronisiert mit dem Terminal **120**. Der Server **140** erzeugt ein Einmal-Passwort nach dem gleichen Verfahren wie im Terminal unter Verwendung der synchronisierten Zufallszahl und Geheimzahl (Schritt **720**). Da der Prozess zur Erzeugung des Einmal-Passworts der gleiche wie im Terminal ist, wird auf eine Erläuterung derselben verzichtet. Dann wird das generierte Einmal-Passwort mit dem vom Benutzer generierten verglichen (Schritt **730**). Wenn die beiden Passwörter identisch sind, wird die Identität des Benutzers authentiziert (Schritt **770**).

[0054] Wenn das durch den Benutzer übertragene Passwort nicht mit dem im Server **140** erzeugten zusammenfällt, bedeutet dies, dass eine unautorisierte Person die Karte zu benützen versucht oder dass das Terminal **120** des Benutzers nicht mit dem Server **140** synchronisiert ist.

[0055] Falls das vom autorisierten Benutzer übertragene Einmal-Passwort nicht mit dem im Server **140** generierten Passwort zusammenfällt, bedeutet dies, dass der Benutzer einen Fehler gemacht hat oder der Zählwert des Terminals **120** nicht mit demjenigen des Servers **140** zusammenfällt. Es kann nämlich sein, dass trotz der Gleichheit des Zählwerts des Terminals **120** und des Zählwerts des Servers **140** die Passwörter wegen des Unterschieds in der Zufallszahl, wenn die Perioden N der beiden Zähler verschieden sind, nicht die gleichen sind. Der Server **140** erhöht den Zählwert und die Zufallszahl, berechnet das Passwort und vergleicht das Passwort mit dem vom Benutzer übertragenen Passwort in Einheiten der Periode des Zählers, um dies zu kompensieren. Es ist nicht notwendig, dass der Server **140** alle Passwörter von N-Malen berechnet, um die Passwörter nach der Periode N-mal zu berechnen. Da eine zusätzliche Berechnung zum Einstellen einer neuen Zufallszahl nur notwendig ist, wenn N zu 0 wird, ist eine große Rechenmenge nicht erforderlich (Schritt **760**). Falls die Passwörter nach dem N-ten Passwort nicht mit dem vom Benutzer übertragenen Passwort zusammenfallen, müssen die Passwörter nach dem N-ten Passwort erneut berechnet werden. Es ist möglich zu bestimmen, wie oft ein solcher Prozess wiederholt werden soll, wenn nötig (Schritt **740**). Wenn das vom Benutzer übertragene Passwort nicht mit dem Passwort des Servers innerhalb einer bezeichneten Zeit übereinstimmt, wird bestimmt, dass es sich um den Versuch einer unautorisierten Person handelt, und der Dienst wird zurückgewiesen (Schritt **750**).

[0056] Wie oben erwähnt, ist es möglich, das Sicherheitsniveau zu verbessern, indem zusätzlich das vom Benutzer erinnerte Passwort für die Benutzerauthentizierung verwendet wird, bei welcher nur die IC-Karte **100** und das tragbare Terminal **120** des Benutzers verwendet werden. Wenn der Benutzer die IC-Karte **100** und das Terminal **120** verlegt, könnte eine Person, die die persönliche Information über den Benutzer kennt, durch Erlangung derselben authentiziert werden. Wenn der Prozess zur Bestätigung des nur vom Benutzer erinnerten Passworts dem Benutzerauthentizierungsprozess des gegenständlichen Authentizierungssystems hinzugefügt wird, steht eine sicherere Benutzerauthentizierung zur Verfügung. Das heißt, der Benutzer sollte das nur vom Be-

nutzer erinnerte Passwort, die nur vom Benutzer besessene IC-Karte und das tragbare Terminal zur Generierung des Einmal-Passworts besitzen, um als autorisierter Benutzer authentiziert zu werden.

[0057] Wie oben erwähnt, benutzt der Benutzer das Terminal zur Erzeugung des Einmal-Passworts. Ein besonderer Geheimschlüssel zur Erzeugung eines anderen Einmal-Passworts für jeden Benutzer liegt im Terminal vor. Der Geheimschlüssel sollte im Server enthalten sein, um das vom Benutzer übertragene Einmal-Passwort zu verifizieren. Der Geheimschlüssel kann dabei in der Fabrik bei der Herstellung in das Terminal eingeführt werden. Vorzugsweise wird der Geheimschlüssel jedoch in das Terminal eingeführt, wenn ein Dienstanbieter eine Benutzerregistrierung des Terminals durchführt. Der Dienstanbieter erzeugt einen Geheimschlüssel für das Terminal, führt ihn in das Terminal über die IC-Karte ein und registriert ihn auf dem Server.

[0058] Dadurch, dass dies geschieht, ist ein zusätzlicher Prozess für die Einführung des Geheimschlüssels nicht erforderlich, wenn das Terminal hergestellt wird. Dementsprechend ist es möglich, die Produktivität zu verbessern, wenn das Terminal in der Fabrik massenhergestellt wird. Auch ist der Geheimschlüssel für die Benutzerauthentizierung, der nur dem Dienstanbieter bekannt ist, sicher und hinsichtlich einer Offenlegung ungefährdet. Der Terminal-Hersteller oder der Dienstanbieter müssen dann das Terminal nicht vorkonfigurieren, bevor es einem Benutzer zur Verfügung gestellt wird.

[0059] Bei der vorliegenden Erfindung ist das Sicherheitsniveau durch die Verwendung eines Einmal-Passworts, bei welchem sich das Passwort jedes Mal ändert, wenn ein Benutzer authentiziert wird, erhöht.

[0060] Bei der vorliegenden Erfindung ist das Sicherheitsniveau viel höher als bei einer herkömmlichen Benutzerauthentizierungsmethode, da ein korrektes Einmal-Passwort nur dann erzeugt wird, wenn die vom Benutzer besessene IC-Karte **100** mit dem vom Benutzer besessenen Terminal **120** zusammenfällt, so dass eine unautorisierte Person auch dann ein korrektes Passwort nicht erzeugen kann, wenn sie in den Besitz des Terminals oder der IC-Karte eines autorisierten Benutzers gelangt. Auch sind das Passwort, die IC-Karte und das Terminal zur Generierung des Passworts des Benutzers wesentlich für die Authentizierung als autorisierten Benutzer, da ein Prozess der Bestätigung des nur vom Benutzer erinnerten Passworts während des Prozesses zur Authentizierung des Benutzers hinzugefügt wird.

[0061] Bei der vorliegenden Erfindung ist die Offenlegung der privaten Information verhindert, und das Einmal-Passwort für verschiedene Dienste wird durch ein einziges Terminal generiert, da der Benutzer seine eigene IC-Karte und sein eigenes tragbares Terminal zur Generierung des Einmal-Passworts verwendet und einen Kartenzugangsschlüssel zum Lesen der Information in der IC-Karte zur Speicherung der privaten Information des Benutzers setzt.

[0062] Die vorliegende Erfindung lässt sich einfach als Software in einem herkömmlichen System zur Authentizierung des Benutzers implementieren, wobei die Zufallszahl zur Erzeugung des Einmal-Passworts und der Zähler zur Synchronisierung des Terminals des Benutzers mit dem Server des Dienstanbieters verwendet wird. Dementsprechend ist es möglich, kosteneffektiv die Benutzerauthentizierung ohne zusätzliche Kosten für den Dienstanbieter zu verbessern.

[0063] Die Vorrichtung zur Authentizierung des Benutzers und das zugehörige Verfahren der vorliegenden Erfindung können überall angewandt werden, wo eine Benutzerauthentizierung erforderlich ist, wie etwa beim Tele-Banking, Home-Shopping und Banking unter Verwendung eines PC, einer bezahlten PC-Kommunikation und einem Netzwerkdienst. Insbesondere braucht der Benutzer nicht direkt zum Dienstanbieter für eine Dienstleistungsregistrierung gehen. Der Benutzer bestellt einen Dienst, erhält eine IC-Karte mit der Post von einem Dienstanbieter, bezieht ein Terminal aus einem Geschäft und wird sicher authentiziert. Dies ist sehr bequem in einer Situation, in der es für den Benutzer schwierig ist, den Dienstanbieter aufzusuchen. Auch muss der Dienstanbieter nicht Benutzern für massengelieferte Dienstleistungen gegenübertreten.

[0064] Das gemäß der Erfindung verwendete Terminal kann ein Einmal-Passwort generieren und nimmt auf den Kontostand und Transaktionsaufzeichnungen des elektronischen Gelds einer allgemeinen IC-Karte Bezug. Das Terminal der vorliegenden Erfindung ist sehr nützlich, wenn man bedenkt, dass die Benutzung elektronischen Gelds rasch Verbreitung gewinnen wird.

Patentansprüche

1. System zur Authentizierung eines Benutzers, welches aufweist:
eine IC-Karte (**100**) zur Speicherung eines Geheimschlüssels zur Generierung eines Einzeit-Passworts und bestimmter Zufallszahlen,
ein Terminal (**120**) zur Generierung eines Einmal-Passworts unter Verwendung der IC-Karte als Eingabe, und
einen Server (**140**) zur Authentizierung des mit dem Terminal generierten Einmal-Passworts,
wobei das Terminal (**120**) aufweist:
einen Kartenempfänger (**121**) für den Empfang der IC-Karte und als Schnittstelle zu dieser, wobei der

Kartenempfänger bestimmt, ob die IC-Karte das erste Mal eingegeben wird,
einen Zufallszahlspeicher (**122**) zum Lesen und Speichern und nachfolgenden Löschen der Zufallszahlen aus der IC-Karte, wenn die IC-Karte das erste Mal in den Kartenempfänger eingeführt wird,
einen ersten Passwortgenerator (**123**) zur Generierung eines Einmal-Passworts durch Lesen des Geheimschlüssels der IC-Karte und der in dem Zufallszahlspeicher gespeicherten Zufallszahl,
einen ersten Zufallszahländerer (**124**) zum Ändern der in dem Zufallszahlspeicher gespeicherten Zufallszahl auf einen bestimmten Wert und Speichern des geänderten Werts in dem Zufallszahlspeicher, wenn ein Einmal-Passwort in dem ersten Passwortgenerator generiert wird, und
eine Anzeige (**125**) zur Anzeige der verarbeiteten Ergebnisse des Terminals und des Servers, und
wobei der Server (**140**) aufweist:
einen Geheimschlüsselspeicher (**141**) zur Speicherung eines Geheimschlüssels und einer bestimmten Zufallszahl, die mit dem Geheimschlüssel und einer bestimmten Zufallszahl, die anfänglich in der IC-Karte gespeichert worden sind, identisch sind,
einen zweiten Passwortgenerator (**144**) zum Lesen des Geheimschlüssels und der Zufallszahl, die in dem Geheimschlüsselspeicher gespeichert sind und zur Generierung eines Einmal-Passworts nach der gleichen Methode, wie sie im Terminal verwendet wird,
einem zweiten Zufallszahländerer (**143**) zum Ändern des Zufallszahlwerts des Geheimschlüsselspeichers in einen Wert, der mit dem des Zufallzahländerers des Terminals identisch ist, und Speichern des geänderten Werts im Geheimschlüsselspeicher, wenn ein Einmal-Passwort durch den zweiten Passwortgenerator erzeugt wird,
einen Passwortempfänger (**142**) für den Empfang des im Terminal generierten Einmal-Passworts über eine Telefonleitung oder ein Netzwerk, und
einen Passwortverifizierer (**147**) zur Verifizierung, ob das empfangene Passwort mit dem generierten Passwort identisch ist.

2. System nach Anspruch 1, wobei die IC-Karte (**100**) sowohl als Identitätskarte als auch für elektronisches Geld verwendet wird und einen Geheimwert für die Authentizierung eines Benutzers sicher speichert.

3. System nach Anspruch 1, wobei der Geheimschlüssel des Terminals (**120**) anfänglich in das Terminal durch einen Dienstanbieter während eines Benutzerregistrationsprozesses eingeführt wird.

4. System nach Anspruch 1, wobei die IC-Karte ferner aufweist:
einen Kartenzugriffsschlüsselspeicher (**102**) mit einem öffentlichen Bereich, zu dem Zugang unbedingt zugelassen wird, und einem privaten Bereich, für welchen ein Kartenzugangsschlüssel erforderlich ist, um Zugang von außerhalb zuzulassen, für die sichere Speicherung eines Kartenzugangsschlüssels, der für die Gestattung von Zugang zu dem Geheimbereich erforderlich ist, aufweist, und
einen Kartenzugangsüberprüfer (**104**) zur Bestimmung, ob Zugang zu interner Information gestattet werden sollte, durch Vergleichen des von außen eingegebenen Kartenzugangsschlüssels mit dem in dem Kartenzugangsschlüsselspeicher gespeicherten Kartenzugangsschlüssel,
wobei der Zufallszahlspeicher (**122**) des Terminals (**120**) die Zufallszahl und den Kartenzugangsschlüssel der IC-Karte liest und diese speichert und die Zufallszahl und den Kartenzugangsschlüssel aus dem öffentlichen Bereich der IC-Karte löscht, wenn die IC-Karte in den Kartenempfänger das erste Mal eingeführt wird.

5. System nach Anspruch 1, wobei das Terminal ferner einen Abfrageabschnitt zur Abfrage der Kontostände und von Transaktionsaufzeichnungen der IC-Karte aufweist.

6. System zur Authentizierung eines Benutzers nach Anspruch 4, wobei der erste Passwortgenerierungsabschnitt (**123**) des Terminals (**120**) aufweist:
einen Symmetrischschlüssel-Verschlüsselungsabschnitt (**200**) zum Lesen des Geheimschlüssels der IC-Karte und der Zufallszahl des Zufallszahlenspeichers (**122**) und Generierung eines Schlüssels unter Verwendung eines Symmetrischschlüssel-Verschlüsselungsalgorithmus,
einen Hash-Funktionsabschnitt (**210**) zur Umwandlung der in dem Symmetrischschlüssel-Verschlüsselungsabschnitt generierten Verschlüsselung unter Verwendung einer Einrichtungs-Hash-Funktion, um eine Rückwärtsverfolgung des Geheimschlüssels zu verhindern, und
einen Formatumwandler (**224**) zur Umwandlung der von dem Hash-Funktionsabschnitt ausgegebenen Verschlüsselung in ein bestimmtes Format, und
wobei der zweite Passwortgenerierungsabschnitt (**144**) des Servers aufweist:
einen Symmetrischschlüssel-Verschlüsselungsabschnitt (**300**) zum Lesen des Geheimschlüssels und der Zufallszahl, die in dem Geheimschlüsselspeicherabschnitt (**141**) gespeichert sind, und zur Generierung eines Schlüssels unter Verwendung eines Symmetrischschlüssel-Verschlüsselungsalgorithmus,
einen Hash-Funktionsabschnitt (**310**) zur Verhinderung einer Rückwärtsverfolgung der in dem Symmetrischschlüssel-Verschlüsselungsabschnitt generierten Verschlüsselung unter Verwendung einer Einrichtungs-Hash-Funktion, und
einen Formatumwandler (**324**) zur Umwandlung der von dem Hash-Funktionsabschnitt ausgegebenen Verschlüsselung in ein bestimmtes Format.

7. System nach Anspruch 6, wobei das Terminal (**120**) und der Server (**140**) ferner aufweisen:
einen Zählerspeicher (**127**, **145**) zur Speicherung eines Zählwerts für die Synchronisierung des Terminals mit dem Server, und
einen Zähleränderer (**128**, **146**) zur Änderung des Zählwerts auf einen bestimmten Wert, jedes Mal wenn ein Einmal-Passwort erzeugt wird, und Speichern des neuen Werts in dem Zählerspeicher,
wobei der Formatumwandler (**224**) des ersten Passwortgenerators (**123**) und der Formatumwandler (**324**) des zweiten Passwortgenerators (**144**) jeweils ferner einen Zählwerteinfüger (**222**, **322**) zur Einfügung des Zählwerts des Zählerspeichers in einen von dem Hash-Funktionsabschnitt (**210**, **310**) ausgegebenen Passwortbitstrom aufweisen, und
wobei der Server (**140**) ferner aufweist:
einen Zählwertextraktor (**148**) zum Extrahieren eines Zählwerts aus dem vom Passwortempfänger empfangenen Einmal-Passwort, und
einem Zufallszahlsynchronisierer (**149**) zur Erzeugung einer Zufallszahl entsprechend dem extrahierten Zählwert und Eingeben desselben in den Symmetrischschlüssel-Verschlüsselungsabschnitt (**300**) des Servers, falls der mit dem Zählwertextraktor extrahierte Zählwert nicht mit dem Zählwert des Servers übereinstimmt.

8. System nach Anspruch 7, wobei der Formatumwandler (**224**, **324**) eine Binärzahl in eine Dezimalzahl umwandelt.

9. System nach Anspruch 7, wobei sowohl der Zählwert- einfüger (**222**) des Terminals (**120**) als auch der Zählwerteinfüger (**322**) des Servers (**140**) zusätzlich ein PTS-Bit einfügt, welches auf das Protokoll eines Algorithmus zur Erzeugung von mehr als einem Einmal-Passwort Bezug nimmt, wobei der Zählwertextraktor (**148**) des Servers ferner das PTS-Bit extrahiert und der erste und der zweite Passwortgenerator (**123**, **144**) ein Einmal-Passwort unter Verwendung eines Algorithmus zur Generierung eines Einmal-Passworts gemäß der PTS-Information generieren.

10. Verfahren zur Authentizierung eines Benutzers unter Verwen- dung einer Benutzerauthentizierungsvorrichtung mit einer IC-Karte (**100**) zur Speicherung einer bestimmten Zufallszahl und eines Geheimschlüssels zur Generierung eines Einmal-Passworts, eines Terminals (**120**) zur Generierung eines Einmal-Passworts unter Verwendung der IC-Karte als Eingabe und eines Servers (**140**) zur Speicherung des Geheimschlüssels und einer Zufallszahl, die mit denjenigen der IC-Karte identisch sind, und zur Authentizierung des in dem Terminal erzeugten Einmal-Passworts, wobei das Benutzerauthentizierungsverfahren die Schritte des
Einführens der IC-Karte in das Terminal,
Bestimmens, ob die IC-Karte in das Terminal das erste Mal eingegeben wird,
Initialisierens eines bestimmten Diensts und Generierens eines Einmal-Passworts, wenn die IC-Karte das erste Mal eingegeben wird, und
Generierens eines Einmal-Passworts, wenn die IC-Karte ein späteres Mal eingegeben wird, und
Empfangens eines in dem Terminal generierten Einmal-Passworts über ein bestimmtes Kommunikationsmedium und Verifizierens des Einmal-Passworts aufweist,
wobei der Initialisierungsschritt eines Dienstes beim Passwortgenerierungsschritt die Schritte des
Lesens der Zufallszahl der IC-Karte und Speicherns derselben in dem Terminal, und
Löschens der Zufallszahl aus der IC-Karte aufweist,
wobei der Generierungsschritt des Einmal-Passworts beim Schritt der Generierung eines Passworts die Schritte des
(a) Lesens des Geheimschlüssels der IC-Karte und der in dem Terminal gespeicherten Zufallszahl,
(b) Ausführens eines Symmetrischschlüssel-Verschlüsselungsalgorithmus unter Verwendung des Geheimschlüssels und der Zufallszahl als Eingabe,
(c) Durchführens einer Einrichtungs-Hash-Funktion auf dem von dem Symmetrischschlüssel-Verschlüsselungsalgorithmus ausgegebenen Wert,
(d) Änderns der Zufallszahl auf einen bestimmten Wert und Speicherns desselben in dem Terminal, und
(e) Umwandelns der Ausgabe der Einrichtungs-Hash-Funktion in ein bestimmtes Format aufweist, und
wobei der Verifizierungsschritt die Schritte des
Empfangens des in dem Terminal generierten Einmal-Passworts über ein bestimmtes Kommunikationsmedium,
Lesens des Geheimschlüssels und der Zufallszahl, die in dem Server gespeichert sind,
Durchführens eines Symmetrischschlüssel-Verschlüsselungsalgorithmus unter Verwendung des Geheimschlüssels und der Zufallszahl als Eingabe,
Durchführens einer Einrichtungs-Hash-Funktion auf dem von dem Symmetrischschlüssel-Verschlüsselungsalgorithmus ausgegebenen Wert,
Änderns der Zufallszahl auf einen bestimmten Wert und Speicherns desselben in dem Terminal, und
Umwandelns der Ausgabe der Einrichtungs-Hash-Funktion in ein bestimmtes Format, und
Authentizierens eines Benutzers, wenn das bestimmte Format das gleiche wie das empfangene Einmal-Passwort ist, und Nicht-Authentizierens des Benutzers, wenn es nicht das gleiche ist, aufweist.

11. Verfahren nach Anspruch 10, wobei die IC-Karte (**100**) ferner einen Kartenzugangsschlüssel, der für einen Zugang zu einem Geheimbereich erforderlich ist, aufweist, wobei die Initialisierung eines Dienstes beim Passwortgenerierungsschritt die Schritte des
Auslesens der Zufallszahl und eines Kartenzugangsschlüssels, zur Gestattung von Zugang zur Zufalls-

zahl und zum privaten Bereich (**108**), aus dem öffentlichen Bereich (**106**) der IC-Karte und Speicherns desselben im Terminal (**120**), und
Löschens der Zufallszahl und des Kartenzugangsschlüssels im öffentlichen Bereich der IC-Karte aufweist, und
wobei der Schritt (a) des Lesens des Geheimschlüssels der IC-Karte beim Passwortgenerierungsschritt die Schritte des
Eingebens des in dem Terminal gespeicherten Kartenzugangsschlüssels in die IC-Karte,
Prüfens, ob der in die IC-Karte eingegebene Kartenzugangsschlüssel der gleiche wie der Kartenzugangsschlüssel des IC-Kartenprivatbereichs ist, und, wenn Übereinstimmung vorliegt, des Gestattens von Zugang zur Karte und
Lesens des Geheimschlüssels der IC-Karte, wenn der Zugang gestattet wird, beim Schritt des Prüfens des Kartenzugangsschlüssels aufweist.

12. Verfahren nach Anspruch 11, wobei das Terminal (**120**) und der Server (**140**) jeweils einen Zähler zur Synchronisierung des Terminals mit dem Server aufweisen, wobei der Schritt (d) der Generierung des Einmal-Passworts beim Schritt der Generierung eines Passworts den Schritt des Änderns der Zufallszahl und des Zählwerts auf bestimmte Werte und des Speicherns derselben im Terminal aufweist,
wobei der Schritt (e) aus der Generierung eines Einmal-Passworts die Schritte des
Einfügens des Zählwerts in einen Passwortbitstrom, der mit dem Schritt (c) der Durchführung einer Einrichtungs-Hash-Funktion auf dem über den Symmetrischschlüssel-Verschlüsselungsalgorithmus ausgegebenen Wert erzeugt wird, und
Umwandelns des Passwort-Bitstroms, in welchen der Zählwert eingefügt ist, in ein bestimmtes Format aufweist,
wobei der Empfangsschritt des Verifizierungsschritts ferner die Schritte des
Extrahierens eines Zählwerts aus dem empfangenen Einmal-Passwort,
Vergleichens des im Extraktionsschritt extrahierten Zählwerts mit dem Zählwert des Servers, und
Gleichmachens der Zählwerte des Zählers und Änderns der Zufallszahl auf eine Zufallszahl, die dem Zählwert entspricht, falls im Vergleichsschritt die Zählwerte nicht gleich sind, aufweist,
wobei der Schritt der Änderung der Zufallszahl des Verifizierungsschritts der Änderung der Zufallszahl auf einen bestimmten Wert und Speicherung desselben in dem Terminal dient, und
der Umwandlungsschritt des Verifizierungsschritts die Schritte des Durchführens der Einrichtungs-Hash-Funktion und Einfügens des Zählwerts in den ausgegebenen Passwort-Bitstrom, und Umwandelns des Passwortwerts, in welchen der Zählwert eingefügt ist, in ein bestimmtes Format aufweist.

Es folgen 6 Blatt Zeichnungen

Anhängende Zeichnungen

FIG. 1

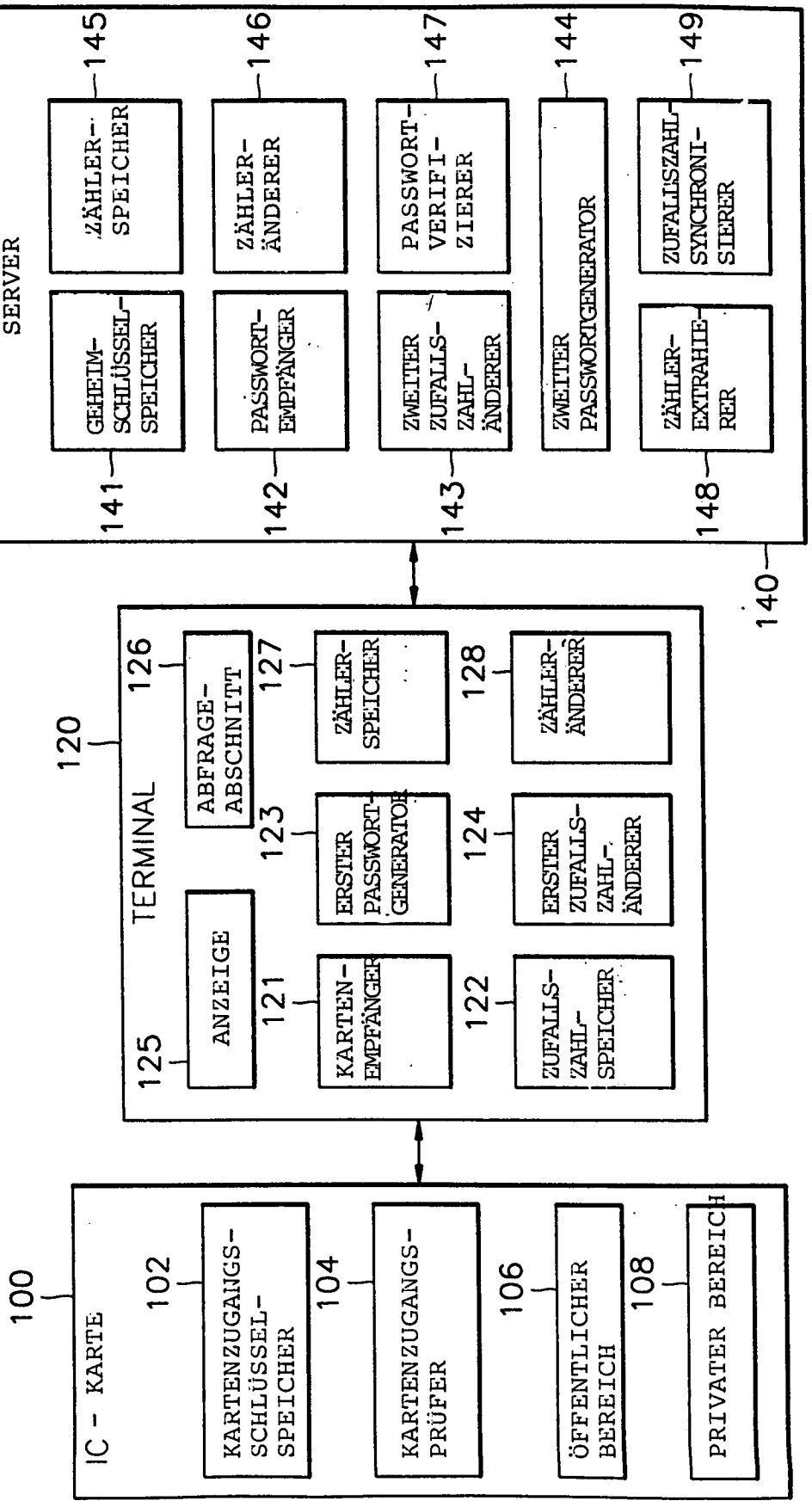


FIG. 2

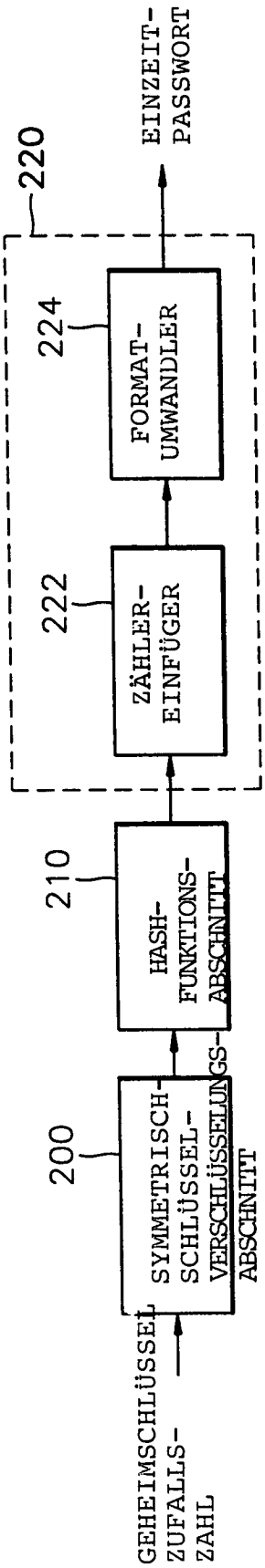

GEHEIMSCHLÜSSEL-
ZUFALLS-
ZAHL
200
SYMMETRISCH-
SCHLÜSSEL-
VERSCHLÜSSELUNGS-
ABSCHNITT
210
HASH-
FUNKTIONS-
ABSCHNITT
220
222
ZÄHLER-
EINFÜGER
224
FORMAT-
UMWANDLER
EINZEIT-
PASSWORT

FIG. 3

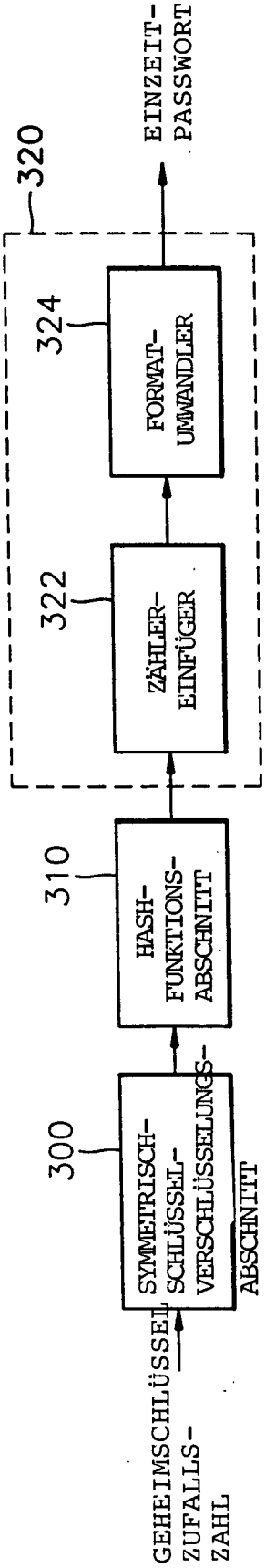

GEHEIMSCHLÜSSEL-
ZUFALLS-
ZAHL
300
SYMMETRISCH-
SCHLÜSSEL-
VERSCHLÜSSELUNGS-
ABSCHNITT
310
HASH-
FUNKTIONS-
ABSCHNITT
320
322
ZÄHLER-
EINFÜGER
324
FORMAT-
UMWANDLER
EINZEIT-
PASSWORT

FIG. 4

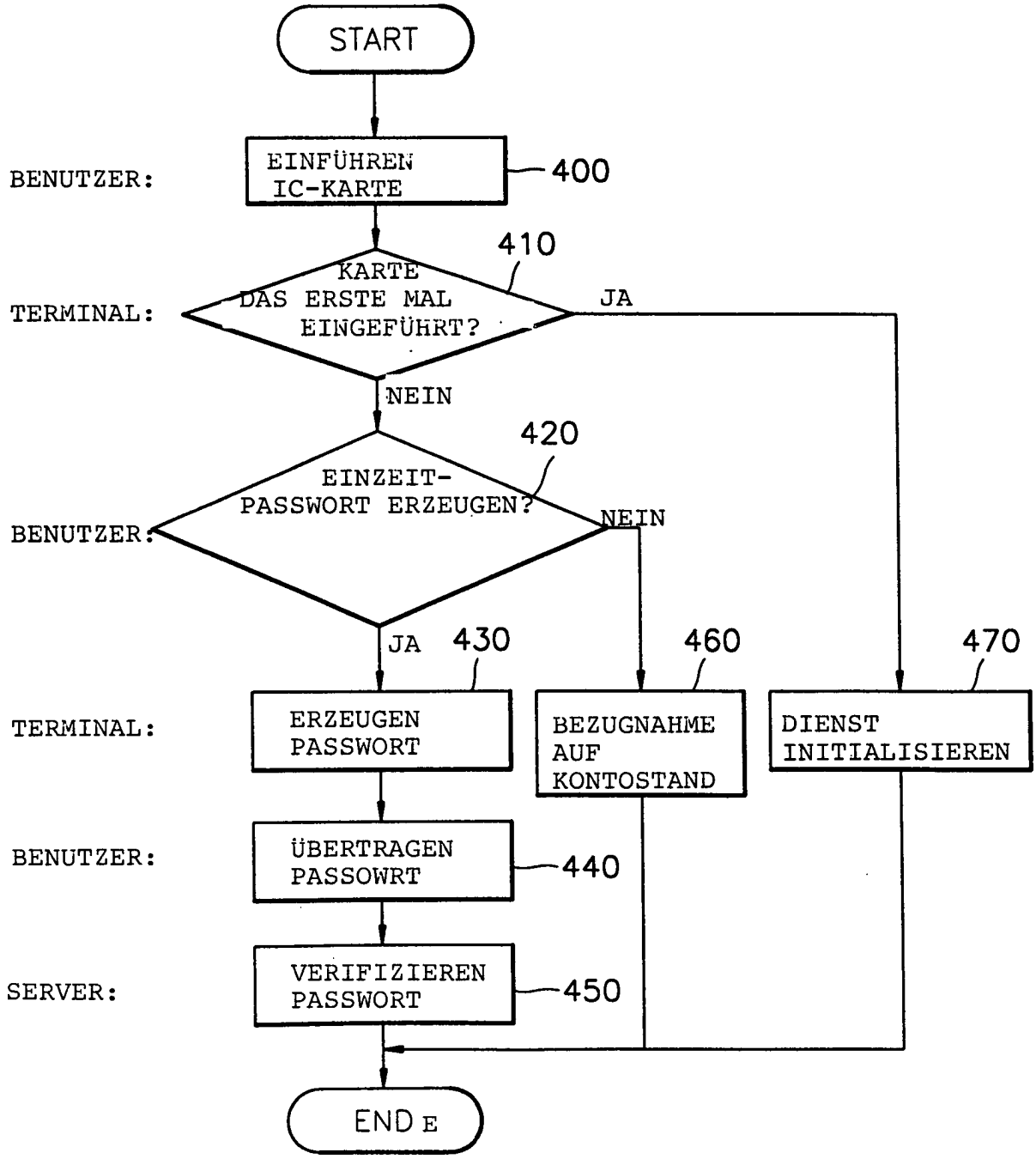

START
BENUTZER:
EINFÜHREN IC-KARTE
400
410
TERMINAL:
KARTE DAS ERSTE MAL EINGEFÜHRT?
JA
NEIN
420
BENUTZER:
EINZEIT-PASSWORT ERZEUGEN?
NEIN
JA
430
460
470
TERMINAL:
ERZEUGEN PASSWORT
BEZUGNAHME AUF KONTOSTAND
DIENST INITIALISIEREN
BENUTZER:
ÜBERTRAGEN PASSOWRT
440
SERVER:
VERIFIZIEREN PASSWORT
450
END E

FIG. 5

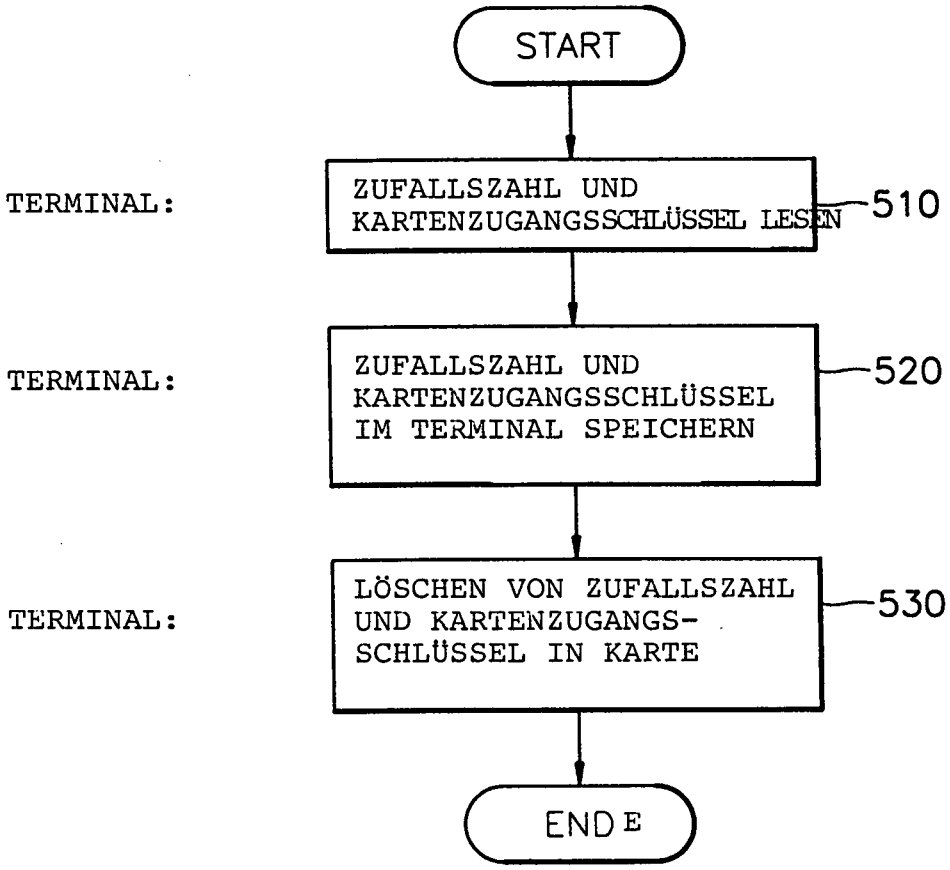

START
TERMINAL:
ZUFALLSZAHL UND KARTENZUGANGSSCHLÜSSEL LESEN
510
TERMINAL:
ZUFALLSZAHL UND KARTENZUGANGSSCHLÜSSEL IM TERMINAL SPEICHERN
520
TERMINAL:
LÖSCHEN VON ZUFALLSZAHL UND KARTENZUGANGS-SCHLÜSSEL IN KARTE
530
ENDE

FIG. 6

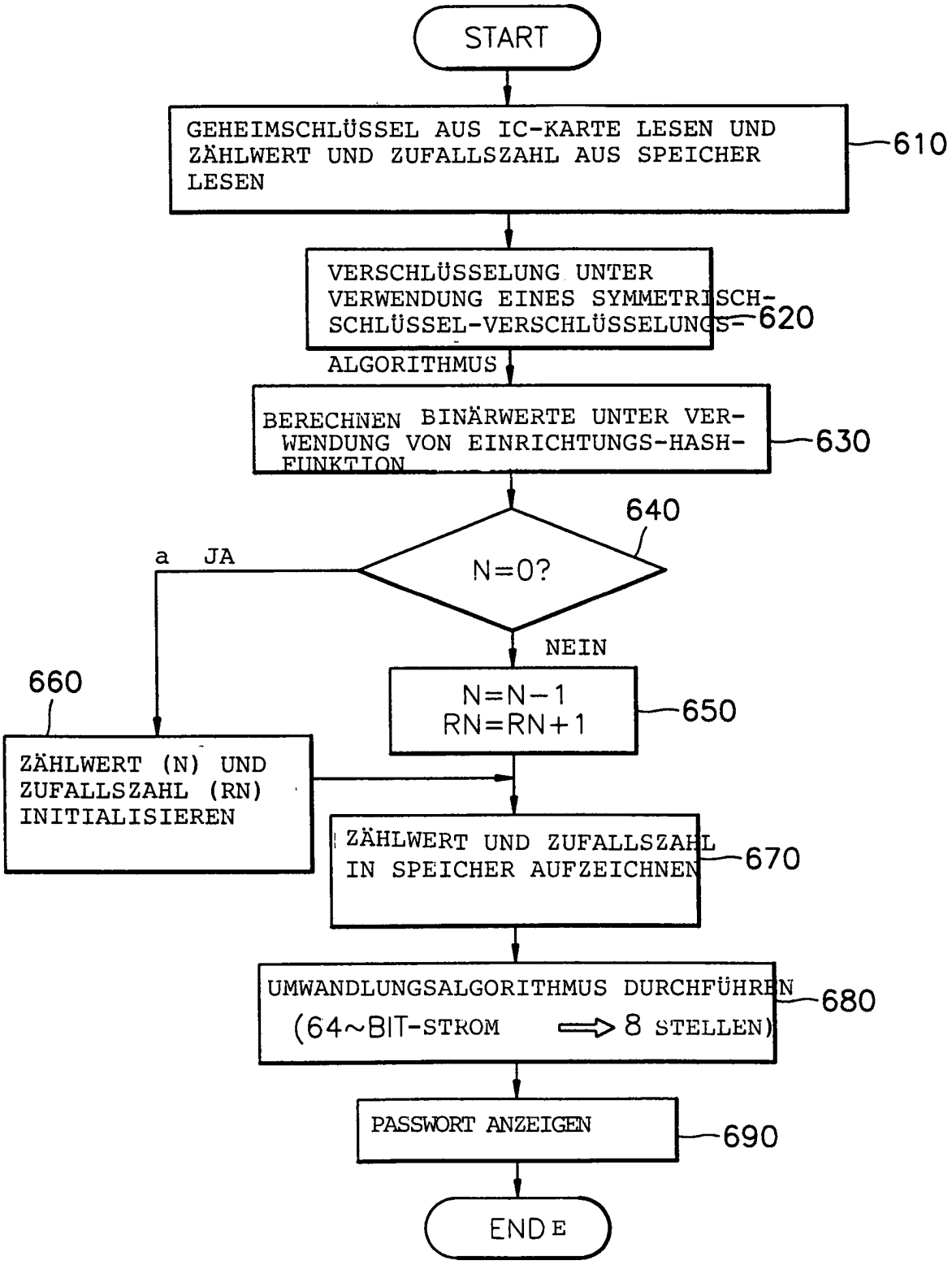
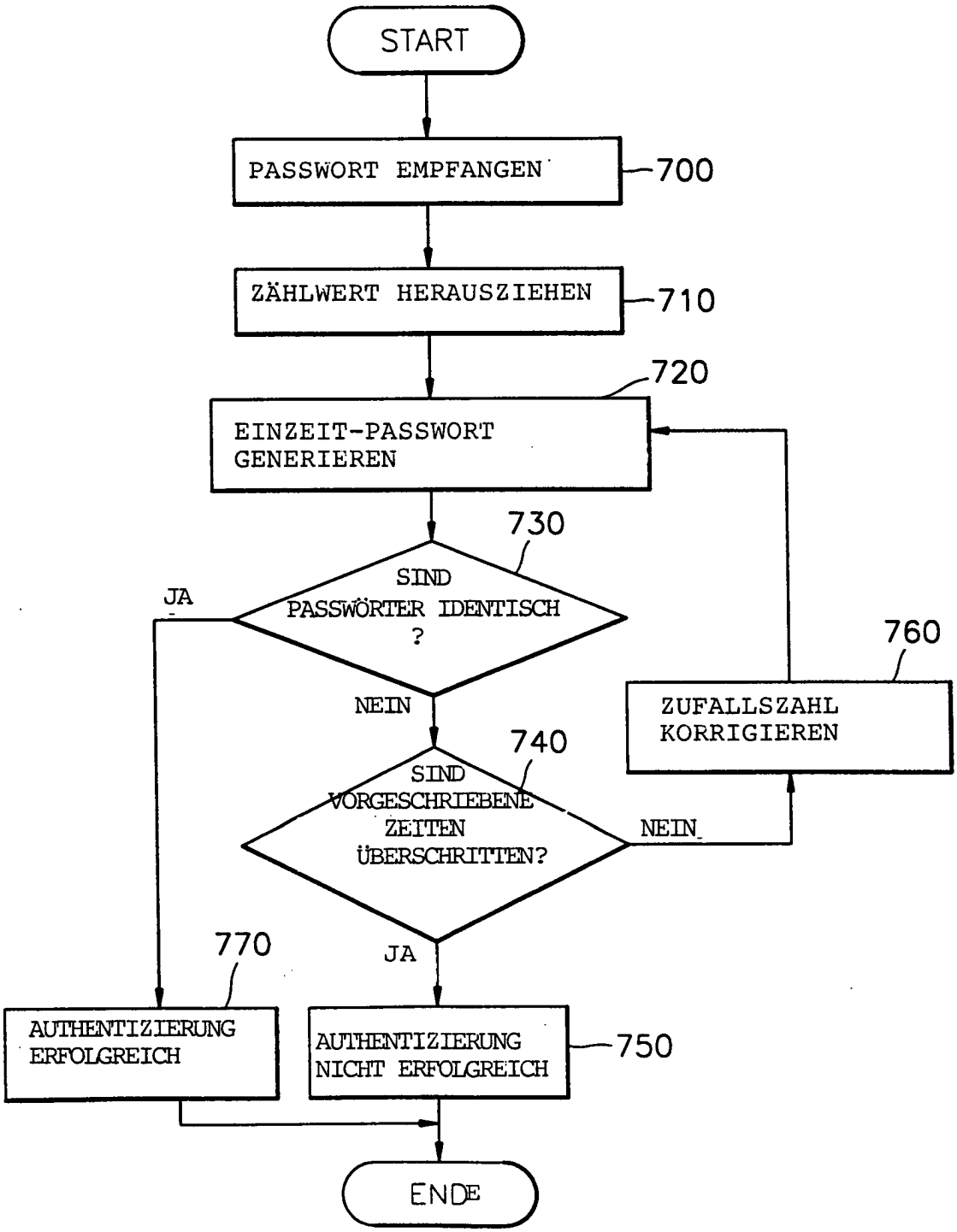

START
GEHEIMSCHLÜSSEL AUS IC-KARTE LESEN UND ZÄHLWERT UND ZUFALLSZAHL AUS SPEICHER LESEN
610
VERSCHLÜSSELUNG UNTER VERWENDUNG EINES SYMMETRISCH-SCHLÜSSEL-VERSCHLÜSSELUNGS-ALGORITHMUS
620
BERECHNEN BINÄRWERTE UNTER VERWENDUNG VON EINRICHTUNGS-HASH-FUNKTION
630
640
N=0?
a JA
NEIN
660
ZÄHLWERT (N) UND ZUFALLSZAHL (RN) INITIALISIEREN
N=N-1
RN=RN+1
650
ZÄHLWERT UND ZUFALLSZAHL IN SPEICHER AUFZEICHNEN
670
UMWANDLUNGSALGORITHMUS DURCHFÜHREN
(64~BIT-STROM ⟹ 8 STELLEN)
680
PASSWORT ANZEIGEN
690
ENDE

FIG. 7


START
PASSWORT EMPFANGEN
700
ZÄHLWERT HERAUSZIEHEN
710
720
EINZEIT-PASSWORT GENERIEREN
730
SIND PASSWÖRTER IDENTISCH ?
JA
NEIN
760
ZUFALLSZAHL KORRIGIEREN
740
SIND VORGESCHRIEBENE ZEITEN ÜBERSCHRITTEN?
NEIN
JA
770
AUTHENTIZIERUNG ERFOLGREICH
AUTHENTIZIERUNG NICHT ERFOLGREICH
750
ENDE