



(19)
Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 697 23 882 T2 2004.07.29**

(12)

Übersetzung der europäischen Patentschrift

(97) **EP 1 008 256 B1**

(21) Deutsches Aktenzeichen: **697 23 882.2**

(86) PCT-Aktenzeichen: **PCT/FR97/01685**

(96) Europäisches Aktenzeichen: **97 942 090.8**

(87) PCT-Veröffentlichungs-Nr.: **WO 98/013984**

(86) PCT-Anmeldetag: **25.09.1997**

(87) Veröffentlichungstag

der PCT-Anmeldung: **02.04.1998**

(97) Erstveröffentlichung durch das EPA: **14.06.2000**

(97) Veröffentlichungstag

der Patenterteilung beim EPA: **30.07.2003**

(47) Veröffentlichungstag im Patentblatt: **29.07.2004**

(51) Int Cl.⁷: **H04M 1/274**
G06F 1/00

(30) Unionspriorität:

9611912 25.09.1996 FR

(73) Patentinhaber:

Audiosmartcard International S.A., Paris, FR

(74) Vertreter:

Eisenführ, Speiser & Partner, 28195 Bremen

(84) Benannte Vertragsstaaten:

**AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LI,
LU, MC, NL, PT, SE**

(72) Erfinder:

**ROSSET, Franck, F-75011 Paris, FR; GAYET, Alain,
F-92400 Courbevoie, FR; MOULIN, Jean, F-92210
Draveil, FR**

(54) Bezeichnung: **VERFAHREN UND EINRICHTUNG ZUR SICHERUNG DER DIENSTLEISTUNGEN WELCHE ÜBER
EIN COMPUTERNETZ VOM INTERNET-TYP ANGEBOten WERDEN**

Anmerkung: Innerhalb von neun Monaten nach der Bekanntmachung des Hinweises auf die Erteilung des europäischen Patents kann jedermann beim Europäischen Patentamt gegen das erteilte europäische Patent Einspruch einlegen. Der Einspruch ist schriftlich einzureichen und zu begründen. Er gilt erst als eingelegt, wenn die Einspruchsgebühr entrichtet worden ist (Art. 99 (1) Europäisches Patentübereinkommen).

Die Übersetzung ist gemäß Artikel II § 3 Abs. 1 IntPatÜG 1991 vom Patentinhaber eingereicht worden. Sie wurde vom Deutschen Patent- und Markenamt inhaltlich nicht geprüft.

Beschreibung

[0001] Die Erfindung betrifft die Datenübertragung in einem Computernetz vom Internet-Typ.

[0002] Genauer betrifft die Erfindung ein Verfahren und ein System, das den Benutzern eines Computernetzes vom Internet-Typ, ausgestattet mit Multimedia-Terminals, die ein Mikrophon umfassen und an das Computernetz vom Internet-Typ angeschlossen sind und sich in Entfernung von einem Dienstleistungsanbieter bzw. Service Provider befinden, den sicheren und schnellen Zugang zu den Dienstleistungen ermöglicht, die der Dienstleistungsanbieter bzw. Service Provider den Benutzern des Computernetzes vom Internet-Typ bietet.

[0003] Das Problem besteht darin, einem böswilligen Benutzer den unbefugten Zugang zu den Dienstleistungen der Dienstleistungsanbieter bzw. Service Provider, ohne die entsprechenden Gebühren zu zahlen oder unter Behauptung, die in Rechnung gestellten Dienstleistungen nicht bestellt zu haben, unmöglich zu machen.

[0004] Um dieses Problem zu lösen, wurde die Benutzung von Zugangsschlüsseln vorgeschlagen, die der Benutzer mittels seines Multimedia-Terminals oder mit Hilfe von Peripheriegeräten erzeugt. Diese Lösungen sind nicht nur kostspielig, sondern auch zeitraubend. Tatsächlich kann das Problem nur dann effektiv gelöst werden, wenn man gleichzeitig in der Lage ist, ein anderes Problem zu lösen: nämlich die Konzeption eines bequemen, schnell einzusetzenden und wirtschaftlichen Verfahrens sowie eines dazu passenden Systems. In der Tat, wenn man eine breite Öffentlichkeit anspricht, werden Einfachheit der Benutzung und Zeitgewinn zu wichtigen Problemen, die man nicht beiseite schieben kann.

[0005] Es wurde der Einsatz einer Karte vorgeschlagen (Dokument WO 96 04741 im Namen von Andrew MARK), die verschlüsselte akustische Signale vom Typ DTMF sendet, um Telefonnummern zu wählen. So würde der Träger einer solchen Karte durch Kopeln derselben mit dem Mikrofon des Telefonhörers automatisch seine Identifikationszeichen übermitteln. Da diese verschlüsselt sind, kann man davon ausgehen, dass eine dritte Person nicht in der Lage sein wird, den Inhalt zu verstehen.

[0006] Die Lösung von A. MARK betrifft demnach ein ganz anderes technisches Gebiet als das der Sicherheit von Daten, die über ein Computernetz vom Internet-Typ gesendet werden. Darüber hinaus ist es möglich, die von der Karte von A. MARK gesendeten Signale aufzuzeichnen, und ein Betrüger, der sich im Besitz dieser Aufzeichnung befindet, kann den Platz des Kartenbesitzers einnehmen. Die Karte von A. MARK würde demnach einen böswilligen Benutzer nicht daran hindern, unbefugt in die Dienstleistungen von Dienstleistungsanbietern bzw. Service Providern in Computernetzen vom Internet-Typ einzudringen.

[0007] Die Patentanmeldung DE,A,43 25 459 im Namen von Raymund H. EISELE beschreibt einen

Taschenrechner, der akustische Identifizierungssignale sendet, die sich bei jeder Operation ändern. Das Aufzeichnen solcher akustischen Signale wäre demnach für einen Betrüger ohne Interesse. Jedoch erlauben die platzraubenden Abmessungen des Geräts, seine geringfügige Handhabbarkeit, seine schwierige Benutzung und sein hoher Preis nicht das Erreichen der Ziele der Erfindung, nämlich das Bereitstellen eines Verfahrens und eines Systems, die einfach zu handhaben, schnell einzusetzen und preiswert sein sollen. In der Tat wird ein Benutzer nur dann die Dienstleistungen eines Dienstleistungsanbieters bzw. Service Providers in einem Computernetz vom Internet-Typ nur dann in Anspruch nehmen, wenn der Zugang dazu einfach und schnell ist. [0008] Die von der Erfindung gesetzten Ziele werden erreicht und die technischen Probleme nach dem bisherigen Stand der Technik werden nach der Erfindung mit Hilfe des folgenden Verfahrens gelöst:

- der Dienstleistungsanbieter bzw. Service Provider stellt jedem Benutzer des Computernetzes vom Internet-Typ, die Abonnenten seiner Dienstleistungen sind, eine Karte zur Verfügung, die das Format einer Kreditkarte aufweist und durch für jeden Abonnenten und jede Karte spezifische Identifikationsdaten personalisiert ist, wobei jede dieser Karten kurze akustische Identifizierungssignale vom Typ DTMF sendet, die zumindest teilweise verschlüsselt sind und sich bei jeder Betätigung der Karte durch den Benutzer des Computernetzes vom Internet-Typ ändern,
- die erwähnten akustischen Identifizierungssignale werden vom Mikrophon des Multimedia-Terminals empfangen und über das Computernetz vom Internet-Typ an die Computerzentrale des Dienstleistungsanbieters bzw. Service Providers übertragen,
- die übertragenen Signale und die Identifizierungsdaten des Abonnenten und der Karte, die in der Computerzentrale gespeichert sind, werden von der Computerzentrale des Dienstleistungsanbieters bzw. Service Providers elektronisch verarbeitet und verglichen, so dass bei Übereinstimmung der Daten, der Abonnent sofort Zugang zu den Dienstleistungen des Dienstleistungsanbieters bzw. Service Providers erhält.

[0009] Dank dieses Verfahrens ist der Dienstleistungsanbieter bzw. Service Provider sicher, dass es sich bei der Karte des Anrufers um eine echte Karte und nicht um eine informatische Täuschung handelt. Er konnte ebenfalls den Halter der Karte als zum Nutzen seiner Dienstleistungen befugte Person identifizieren. Andererseits haben Betrüger keine Möglichkeit, sich die Identifizierungsdaten unbefugt anzueignen, da diese automatisch in verschlüsselter Form gesendet werden. Ferner wird das Aufzeichnen der akustischen Signale in jeglicher Art dem Betrüger nichts nutzen, wenn er versucht, von den EDV-Diensten des Dienstleistungsanbieters bzw. Service Provi-

ders identifiziert zu werden. Die akustischen Signale ändern sich nämlich bei jeder Operation, d. h., bei jeder Betätigung der Karte.

- [0010] Bevorzugterweise wird die Karte
- die Zahl $C(p, n)$ ihrer Betätigungen durch das Element zählen,
 - akustische Signale senden, die für die Zahl $C(p, n)$ ihrer Betätigungen repräsentativ sind,
 - die akustischen Signale als Funktion der Zahl $C(p, n)$ ihrer Betätigungen verschlüsseln.

[0011] Ebenfalls in bevorzugter Weise werden die EDV-Verarbeitungsmittel der Computerzentrale, welche die übertragenen Signale und die Identifizierungsdaten des Kunden und der Karte, die in der Computerzentrale des Dienstleistungsanbieters bzw. Service Providers gespeichert sind, elektronisch verarbeiten und vergleichen, folgendes ausführen:

- die Zahl $C(p, m)$ der Betätigungen der Karte während der letzten validierten Transaktionen speichern,
- die Zahl $C(p, n)$ der Betätigungen der Karte während der laufenden Transaktion mit der gespeicherten Zahl von Betätigungen $C(p, m)$ vergleichen,
- die laufende Transaktion abrechnen, wenn $C(p, n)$ kleiner oder gleich $C(p, m)$ ist und die Prüfung der laufenden Transaktion fortsetzen, wenn $C(p, n)$ größer als $C(p, m)$ ist,
- die elektronischen Signale $S'(p, n)$ als Funktion der Identifizierungsdaten und der Zahl der Betätigungen der Karte $C(p, n)$ im Verlauf der laufenden Transaktion neu berechnen und sie dann mit den übertragenen elektronischen Signalen $S(p, n)$ vergleichen, so dass bei Übereinstimmung, der Abonnent sofort Zugang zu den Dienstleistungen des Dienstleistungsanbieters bzw. Service Providers erhält.

[0012] Es sei darauf hingewiesen, dass die Verwendung einer Mikroschaltung zum Verschlüsseln von zwischen einem Sender und einem Empfänger ausgetauschten Identifizierungscodes mittels eines Zählers in der von NANOTEK LIMITED eingereichten Patentanmeldung EP 0 459 781 A1 beschrieben wurde.

[0013] Um die Sicherheit des Verfahrens zu erhöhen, umfasst das Verfahren bei einer Ausführungsvariante ferner den folgenden Schritt: der Abonnent sendet mittels einer dem Multimedia-Terminal und/oder der Karte zugeordneten Tastatur einen vertraulichen Code, wobei nach Übertragung an die Computerzentrale des Dienstleistungsanbieters bzw. Service Providers über das Computernetz vom Internet-Typ, dieser vertrauliche Code verarbeitet und mit dem in der Computerzentrale des Dienstleistungsanbieters bzw. Service Providers gespeicherten persönlichen vertraulichen Code des Abonnenten verglichen wird.

[0014] Somit hat der Dienstleistungsanbieter bzw. Service Provider die Sicherheit, dass der Anrufer tat-

sächlich die Person ist, welche dazu befugt ist, seine Dienstleistungen zu nutzen. Eine gestohlene Karte kann vom Dieb nicht benutzt werden, da er den vertraulichen Code nicht kennt.

[0015] Bei einer weiteren Ausführungsvariante, und ebenfalls um die Sicherheit des Verfahrens zu erhöhen und um zu verhindern, dass der Abonnent den von ihm an den Dienstleistungsanbieter bzw. Service Provider gerichteten Anruf in Frage stellen kann, umfasst das Verfahren ferner die folgenden Schritte:

- die vom Abonnenten an die Dienstleistungen des Dienstleistungsanbieters bzw. Service Providers erteilten Anweisungen werden vom Abonnenten durch Betätigung der Karte validiert, um sicherzustellen, dass ein verschlüsseltes akustisches Validierungssignal von der Karte gesendet wird,
- das Validierungssignal wird von der Computerzentrale des Dienstleistungsanbieters bzw. Service Providers aufgezeichnet, verarbeitet und entschlüsselt, wobei in bevorzugter Weise der Abonnent eine Empfangsbestätigung erhält.

[0016] Dank dieses Verfahrens hat der Abonnent die an den Dienstleistungsanbieter bzw. Service Provider erteilte Anweisung durch eine elektronische Unterschrift validiert.

[0017] Mindestens drei Ausführungsvarianten ermöglichen das Senden der akustischen Identifizierungssignale an die Computerzentrale des Dienstleistungsanbieters bzw. Service Providers.

[0018] Nach der ersten Variante umfasst das Verfahren der Erfindung ferner die folgenden Schritte:

- die Computerzentrale des Dienstleistungsanbieters bzw. Service Providers lädt eine Konversionssoftware in das Multimedia-Terminal herunter,
- die Konversionssoftware konvertiert die vom Mikrophon des Multimedia-Terminals aufgenommenen akustischen Identifizierungssignale in eine Bitfolge,
- diese Bitfolge wird über das Computernetz vom Internet-Typ an die Computerzentrale des Dienstleistungsanbieters bzw. Service Providers gesendet, insbesondere nach Empfang einer von der Computerzentrale gesendeten Übertragungsanweisung,

so dass die vom Multimedia-Terminal kommenden Signale als Bitfolge eintreffen.

[0019] Nach der zweiten Ausführungsvariante werden die vom Mikrophon des Multimedia Terminals empfangenen akustischen Identifizierungssignale über das Computernetz vom Internet-Typ an die Computerzentrale des Dienstleistungsanbieters bzw. Service Providers gesendet, insbesondere nach Empfang einer von der Computerzentrale kommenden Sendeanweisung durch das Multimedia Terminal. Bei dieser Variante werden die vom Multimedia Terminal kommenden Signale als Schalldatei gesen-

det. Die Verarbeitung dieser Schalldatei und seine Umwandlung in eine Folge von Bits (Binärelemente) erfolgt in der Computerzentrale des Dienstleistungsanbieters bzw. Service Providers.

[0020] Nach der dritten Ausführungsvariante umfasst das Verfahren noch die folgenden Schritte:

- der Dienstleistungsanbieter bzw. Service Provider stellt jedem Benutzer des Computernetzes vom Internet-Typ, der Abonnent seiner Dienstleistungen ist, eine Konversionssoftware zur Verfügung, die im Multimedia-Terminal zur Anwendung kommen soll,
- die vom Mikrophon des Multimedia-Terminals aufgenommenen akustischen Identifizierungssignale werden in eine Bitfolge konvertiert, bevor sie über das Computernetz vom Internet-Typ an die Computerzentrale des Dienstleistungsanbieters bzw. Service Providers gesendet werden.

[0021] Die Erfindung betrifft ebenfalls ein System, das den Benutzern des Computernetzes vom Internet-Typ die über Multimedia-Terminals verfügen, welche ein Mikrophon umfassen und an das Computernetz vom Internet-Typ angeschlossen sind und sich in Entfernung von einem Dienstleistungsanbieter bzw. Service Provider befinden, schnellen und sicheren Zugang zu den Dienstleistungen gewährt, die der Dienstleistungsanbieter bzw. Service Provider seinen Abonnenten bietet. Dieses System ist dadurch gekennzeichnet, dass es die Mittel zum Anwenden des oben definierten Verfahrens und seiner Ausführungsvarianten umfasst.

[0022] Genauer gesagt:

- umfasst das System nach der Erfindung eine Karte im Kreditkartenformat, die durch für jede Karte und für jeden Abonnenten spezifische Identifizierungsdaten personalisiert und die dem Abonnenten zur Verfügung gestellt wird. Diese Karte umfasst folgendes:
 - Mittel zum Senden kurzer Identifizierungssignale des Typs DTMF, die vom Abonnenten mittels eines Elementes betätigt werden, das von außerhalb der Karte zugänglich ist,
 - Verschlüsselungsmittel, die das Verschlüsseln von mindestens einem Teil und das Variieren der akustischen Signale bei jeder Betätigung der Karte ermöglichen.
- Das System der Erfindung umfasst in den Multimedia-Terminals untergebrachte Übertragungsmittel der akustischen Signale, welche diese akustischen Signale über das Computernetz vom Internet-Typ in die Ferne senden können,
- Das System der Erfindung umfasst EDV-Verarbeitungsmittel, die von der Computerzentrale des Dienstleistungsanbieters bzw. Service Providers abhängig sind, an das Computernetz vom Internet-Typ angeschlossen sind und die von den Multimedia-Terminals kommenden Signale empfangen, wobei diese EDV-Verarbeitungsmittel folgendes umfassen:

- eine Datenbank, in der die Referenzdaten der Karten der Abonnenten sowie deren Identifizierungsdaten gespeichert sind,
- Mittel zum Verarbeiten und zum Vergleichen der elektronischen Signale mit den in der Datenbank gespeicherten Identifizierungsdaten,

so dass bei Übereinstimmung, der Abonnent sofort Zugang zu den Dienstleistungen des Dienstleistungsanbieters bzw. Service Providers erhält.

[0023] So hat dank dieses Systems der Dienstleistungsanbieter bzw. Service Provider die Sicherheit, dass der Anrufer tatsächlich im Besitz einer echten Karte und nicht einer informatischen Täuschung ist. Er konnte den Besitzer der Karte ebenfalls als Person identifizieren, die zum Nutzen der von ihm angebotenen Dienstleistungen befugt ist.

[0024] Andererseits ist es Betrugern nicht möglich, die Identifizierungsdaten zu stehlen, da diese automatisch in verschlüsselter Form gesendet werden. Ferner wird das Aufzeichnen der akustischen Signale in jeglicher Art dem Betrüger nichts nutzen, wenn er versucht, von den EDV-Diensten des Dienstleistungsanbieters bzw. Service Providers identifiziert zu werden. Die akustischen Signale ändern sich nämlich bei jeder Operation, d. h., bei jeder Betätigung der Karte.

[0025] Bevorzugterweise umfasst die Karte außerdem:

- einen Schrittzähler, der mit den Sendemitteln und mit den Verschlüsselungsmitteln verbunden ist und bei jeder Betätigung der Karte mit Hilfe des Elementes um mindestens eine Einheit weitergestellt wird,

so dass der Zustand des Schrittzählers an die EDV-Verarbeitungsmittel weitergeleitet wird und, dass die akustischen Signale als Funktion des Status des Schrittzählers verschlüsselt werden.

[0026] In ebenfalls bevorzugter Weise umfassen die EDV-Verarbeitungsmittel noch:

- Mittel zum Speichern des Status $C(p, m)$ des Schrittzählers bei der letzten validierten Transaktion,
- Mittel zum Vergleichen des Status $C(p, n)$ des Schrittzählers, die bei der laufenden Transaktion herausgegeben wurden, mit dem gespeicherten Status $C(p, m)$ des Schrittzählers,

so dass die Prüfung der laufenden Transaktion abgebrochen wird, wenn $C(p, n)$ kleiner oder gleich $C(p, m)$ ist und weitergeführt wird, wenn $C(p, n)$ streng größer als $C(p, m)$ ist.

[0027] Ebenfalls in bevorzugter Weise verfügen die Mittel zum Verarbeiten und zum Vergleichen der elektronischen Signale mit den in der Datenbank gespeicherten Identifizierungsdaten über Mittel, mit denen

die elektronischen Signale als Funktion des Status $C(p, n)$ des Schrittzählers und der Identifizierungsdaten neu berechnet werden können und dann mit den gesendeten elektronischen Signalen verglichen werden, so dass bei Übereinstimmung der Abonnent sofort Zugang zu den Dienstleitungen des Dienstleistungsanbieters bzw. Service Providers erhält.

[0028] Um die Sicherheit des Systems zu erhöhen, verfügt es bei einer Ausführungsvariante ferner über zweite Vergleichsmittel eines in der Datenbank gespeicherten vertraulichen, für den Abonnenten persönlichen Code mit einem vom Abonnenten mittels einer mit dem Multimedia-Terminal und/oder mit der Karte assoziierten Tastatur gesendeten vertraulichen Code, welcher an die EDV-Verarbeitungsmittel des Dienstleistungsanbieters bzw. Service Providers über das Computernetz vom Internet-Typ gesendet wird.

[0029] So ist der Dienstleistungsanbieter bzw. Service Provider sicher, dass die anrufende Person tatsächlich befugt ist, seine Dienstleistungen zu verwenden. Eine gestohlene Karte kann nicht benutzt werden, weil der Dieb den vertraulichen Code nicht kennt.

[0030] Bei einer anderen Ausführungsvariante und ebenfalls mit dem Zweck, die Sicherheit des Systems zu erhöhen und um zu verhindern, dass der Abonnent den von ihm an den Dienstleistungsanbieter bzw. Service Provider gerichteten Anruf in Frage stellen kann, umfasst das System:

- eine Validierungssoftware der vom Abonnenten an den Dienstleistungsanbieter bzw. Service Provider erteilten Anweisungen, nach Erfassung eines von der vom Abonnenten betätigten Karte abgegebenen verschlüsselten akustischen Signals,
- eine Software zum Ausstellen einer Empfangsbestätigung der erteilten Anweisungen, die dem Abonnenten zugesandt wird.

[0031] Somit hat der Abonnent seine Anweisungen an den Dienstleistungsanbieter bzw. Service Provider mit einer elektronischen Signatur validiert.

[0032] Mindestens drei Ausführungsvarianten ermöglichen das Senden der akustischen Identifizierungssignale an die Computerzentrale des Dienstleistungsanbieters bzw. Service Providers.

[0033] Nach der ersten Variante umfassen die von der Computerzentrale des Dienstleistungsanbieters bzw. Service Providers abhängigen EDV-Verarbeitungsmittel folgendes:

- Mittel zum Aufladen einer Konversionssoftware in das Multimedia-Terminal, wobei diese Software die vom Mikrophon des Multimedia-Terminals aufgenommenen akustischen Identifizierungssignale in eine Bitfolge umwandelt,
- Mittel zum Herausgeben eines Sendebefehls für die Bitfolge vom Multimedia-Terminal zur Computerzentrale des Dienstleistungsanbieters bzw. Service Providers über das Computernetz vom Internet-Typ,

so dass die vom Multimedia-Terminal kommenden Signale als Bitfolge auftreten.

[0034] Nach der zweiten Ausführungsvariante umfasst das Multimedia-Terminal Mittel zum Senden der vom Mikrophon des Multimedia-Terminals empfangenen akustischen Identifizierungssignale in der Form einer Schalldatei. Diese Schalldatei wird über das Computernetz vom Internet-Typ zur Computerzentrale des Dienstleistungsanbieters bzw. Service Providers gesendet. Im Rahmen dieser Variante erfolgen die Verarbeitung der Schalldatei und ihre Umwandlung in eine Bitfolge durch die EDV-Verarbeitungsmittel des Dienstleistungsanbieters bzw. Service Providers.

[0035] Nach der dritten Variante umfasst das System eine Konversionssoftware, die im Multimedia-Terminal zum Einsatz kommt. Diese Konversionssoftware wandelt die vom Mikrophon des Multimedia-Terminals empfangenen und gesendeten akustischen Signale in Bitfolgen um, die über ein Computernetz vom Internet-Typ in die Ferne gesendet werden können.

[0036] Weitere Eigenschaften und Vorteile der Erfindung werden beim Lesen der nachfolgenden Beschreibung von Ausführungsvarianten der Erfindung verdeutlicht, die als nicht einschränkende Beispiele vorgestellt werden. Es zeigen:

[0037] **Fig. 1:** eine schematische perspektivische Ansicht des Systems und des Verfahrens nach der Erfindung,

[0038] **Fig. 2:** die Karte in Form eines Blockdiagramms,

[0039] **Fig. 3:** den Prüfalgorithmus für die Echtheit des gesendeten Signals,

[0040] **Fig. 4:** die erste Ausführungsvariante in Form eines Blockdiagramms, wobei diese Variante dadurch gekennzeichnet ist, dass die EDV-Verarbeitungsmittel des Dienstleistungsanbieters bzw. Service Providers eine Konversionssoftware in das Multimedia-Terminal aufladen,

[0041] **Fig. 5:** die zweite Ausführungsvariante in Form eines Blockdiagramms, wobei diese Variante dadurch gekennzeichnet ist, dass die EDV-Verarbeitungsmittel des Dienstleistungsanbieters bzw. Service Providers eine vom Multimedia-Terminal gesendete Schalldatei empfangen,

[0042] **Fig. 6:** die dritte Ausführungsvariante in Form eines Blockdiagramms, wobei diese Variante dadurch gekennzeichnet ist, dass die EDV-Verarbeitungsmittel des Dienstleistungsanbieters bzw. Service Providers Bits empfangen, die vom Multimedia-Terminal mit Hilfe einer spezifischen Software erzeugt wurden.

[0043] Es wird nun mit Bezug auf **Fig. 1** das System und das Verfahren der Erfindung vorgestellt. Das System und das Verfahren der Erfindung ermöglichen den Benutzern **11** eines Computernetzes vom Internet-Typ **15**, ausgestattet mit Multimedia-Terminals **16**, die ein Mikrophon **17** umfassen, schnellen

und sicheren Zugang zu den Dienstleistungen **30**, die der Dienstleistungsanbieter bzw. Service Provider **12** den Benutzern **11** bietet. Das Multimedia-Terminal **16**, das sich in Entfernung von den EDV-Verarbeitungsmitteln **18** des Dienstleistungsanbieters bzw. Service Providers **12** befindet, ist mit dem Computernetz vom Internet-Typ **15** verbunden.

[0044] Das System umfasst eine Karte **10** im Kreditkartenformat, die durch spezifische Identitätsmerkmale personalisiert ist, und zwar für jede Karte und für jeden Abonnenten **11**. Diese Karte wird den abonnierten Benutzern **11** vom Dienstleistungsanbieter bzw. Service Provider **12** und seinen Dienstleistungen **40** zur Verfügung gestellt. Die Karte **10** umfasst Sendemittel, insbesondere einen Lautsprecher **13**, der kurze akustische Identifizierungssignale **20** vom Typ DTMF sendet. Diese Signale werden gesendet, wenn die Sendemittel **13** und die sie steuernden Organe vom Kunden mit Hilfe der Taste **14** betätigt werden, die vom Äußeren der Karte her zugänglich ist (in **Fig. 1** nicht ersichtlich, weil sie sich auf der anderen Kartenseite befindet). Diese Sendemittel **13** werden von einem Generator für DTMF-Signale **99** angeregt, der von einem Mikroprozessor **104** gesteuert wird, welcher selbst von einer Batterie **106** mit Energie versorgt und von einem Resonator **107** gesteuert wird. Der in der Karte enthaltene Mikroprozessor **104** umfasst Mittel zum Verschlüsseln **103**, mit denen die akustischen Signale **20** zumindest teilweise verschlüsselt werden können, da er einen Verschlüsselungsalgorithmus **108** und spezifische Identifizierungsmerkmale **109** für jede Karte **10** und für jeden Abonnenten **11** aufweist, insbesondere der vom Verschlüsselungsalgorithmus **108** genutzte Geheimschlüssel **250**.

[0045] Die akustischen Signale **20** werden vom Mikrophon **17** des Telefonapparats empfangen, an das der Kunde die Karte **10** legt. Das System umfasst ebenfalls Mittel **19** zum Senden der akustischen Signale **20**, die im Multimedia-Terminal **16** untergebracht sind. Diese Sendemittel **19** senden, nach ihrer Verarbeitung und Konversion zu elektronischen Signalen, die akustischen Signale über das Computernetz vom Internet-Typ **15** in die Ferne.

[0046] Das System umfasst ebenfalls EDV-Verarbeitungsmittel **21**, die von der Computerzentrale **18** des Dienstleistungsanbieters bzw. Service Providers abhängig sind und mit dem Computernetz vom Internet-Typ **15** verbunden sind und welche die vom Multimedia-Terminal **16** kommende Signale empfangen.

[0047] Die EDV-Verarbeitungsmittel **21** umfassen:

- Aktivierungsmittel **22** der Sendemittel **19** der Multimedia-Terminals **16**,
- eine Datenbank **23**, in der die Daten der Abonnentenkarten und deren Identifizierungsdaten gespeichert sind,
- Verarbeitungsmittel **24** und Vergleichsmittel **25** für die EDV-Signale mit denen in der Datenbank **23** gespeicherten Identifizierungsdaten,
- in der Datenbank **23** gespeicherte Identifizie-

rungsdaten sowie charakteristische Daten der Abonnenten und der Karten,

so dass bei Übereinstimmung, die Dienstleistungen **30** des Dienstleistungsanbieters bzw. Service Providers **12** sofort dem Abonnenten zugänglich sind.

[0048] Der Mikroprozessor **104** und die Verschlüsselungsmittel **103** sind derart konzipiert, dass das akustische Signal **20** bei jeder Operation ein anderes ist. Das Verschlüsseln eines Identifizierungscode besteht darin, ihn in eine Folge von für jedermann unverständlichen Informationen umzuwandeln, die nur vom Inhaber des entsprechenden Schlüssels zu entschlüsseln sind. Dies verhindert in keiner Weise das Kopieren des verschlüsselten Identifizierungscode, entweder während der akustischen Übertragung (Tonaufnahmegerät) oder durch unerlaubtes Abhören der Telefonleitung. Bei ihrer unbefugten Benutzung durch einen Betrüger, wird diese Kopie vom Empfangssystem so verarbeitet, als hätte sie alle Eigenschaften des Originals, und dann interpretiert, um die Identifizierungsmerkmale der Karte zu prüfen.

[0049] Es stellt sich demnach das folgende Problem: wie kann man jeden Kopierversuch verhindern? Es werden nachfolgend verschiedene Ausführungsvarianten des allgemeinen Mittels beschrieben, mit dem bei der Analyse des empfangenen verschlüsselten Signals durch die EDV-Verarbeitungsmittel **21** unter Kopie und Original dadurch unterschieden wird, dass in dem von der Karte **10** gesendeten Signal **20** des Typs DTMF ein Unterscheidungselement eingefügt wird.

[0050] Eine Variante besteht im Benutzen einer so genannten Datum- und Zeitfunktion (wie beispielsweise im Patent US Nr. 4 998 279 beschrieben). Diese Datum- und Zeitfunktion nutzt den Parameter „Zeit“, der sich ständig ändert. Die „Kopie“ ist somit beim Senden bereits verspätet. Diese Lösung bedarf der Synchronisierung zwischen den Sendemitteln **13** und den EDV-Verarbeitungsmitteln **21**. Dafür müssen beide über eine „Zeitbasis“ und ein „Frequenznormalmaß“ verfügen. Jede dieser Zeitbasen hat ihre eigene Genauigkeit und ihre eigene Drift. Daher geht langsam aber fortschreitend ihre Synchronisierung verloren. Um diese technische Schwierigkeit zu überwinden, wird eine gewisse Drift zwischen den Zeitbasen der Sendemittel **13** und der EDV-Verarbeitungsmittel **21** geduldet. Je größer die Drift, desto größer wird die Ungewissheit bezüglich der „Gültigkeit“ der empfangenen Daten und damit die Betrugsgefahr. Wird demnach eine Drift von einer Minute geduldet, so wird jede unbefugte Kopie des gesendeten verschlüsselten Signals, die innerhalb von 30 Sekunden mit böswilliger Absicht genutzt wird, vom Analysensystem der EDV-Verarbeitungsmittel **21** als gültig anerkannt.

[0051] Eine andere Variante besteht im Einsatz von Schrittlisten (wie beispielsweise im Patent US Nr. 4 928 098 beschrieben). Die Sendevorrichtung und die

Empfangsvorrichtung sind jeweils im Besitz der geordneten Liste der aufeinander folgenden Verschlüsselungen des Identifizierungscodes, oder sie verfügen über die Algorithmen, mit denen sie fortschreitend aufgestellt werden können. Zu einem gegebenen Zeitpunkt erwarten die EDV-Verarbeitungsmittel **21** das verschlüsselte Ergebnis $C(n)$. Empfangen sie die Meldung $C(n)$, wird die Operation für gültig erklärt. Die EDV-Verarbeitungsmittel **21** können jedoch eine andere Meldung erhalten, beispielsweise kann der Kartenbenutzer mehrere Male die Sendemittel **13** der Karte betätigt haben, aus Spielerei oder aus Ungeschicklichkeit, so dass die Karte bei ihrer nächsten Verwendung mit den EDV-Verarbeitungsmitteln **21** das verschlüsselte Ergebnis $C(n + p)$ sendet. Empfangen die EDV-Verarbeitungsmittel **21** eine andere Meldung, so suchen sie vorwärts in der Liste der aufeinander folgenden verschlüsselten Ergebnisse, ob es eine Meldung $C(n + p)$ gibt, die mit der empfangenen identisch ist. Um die Zweideutigkeit „handelt es sich um eine gültige Meldung seitens des Absenders?“ oder „handelt es sich um eine betrügerische Meldung?“ aufzuheben, besteht die Lösung im Abfragen oder Abwarten der Sendung der nachfolgenden Meldung. Ist diese mit $C(n + p + 1)$ identisch, so erklärt das System die Meldung für gültig und stellt sich in Erwartung der nächsten Sendung auf den Zustand $C(n + p + 2)$ ein. Ist sie verschieden, wird die Meldung nicht validiert und das Analysensystem verbleibt in Erwartung der Meldung $C(n)$. Eine solche Ausführungsvariante ist nicht sehr ergonomisch, da sie den Kartenbenutzer zwingt, diese mehrere Male zu betätigen.

[0052] Nach einer bevorzugten Ausführung weist, um das echte Signal von der Kopie zu unterscheiden, der in der Karte **10** eingebaute Mikroprozessor **104** einen Schrittzähler **105** auf. Bei jeder Verwendung der Karte schreitet der Schrittzähler **105** um eine oder um mehrere Einheiten fort. Es ist selbstverständlich, dass er, wie ein Sperrklinkenrad nicht zurücklaufen, sondern nach jeder Anwendung nur nach vorne laufen kann.

[0053] Bei dieser Ausführungsvariante interveniert der Zustand $C(p, n)$ **242** des Zählers **105** bei der Berechnung der von den Sendemitteln **13** gesendeten verschlüsselten Meldung **244**. Der kodierte Teil $S(p, n)$ **241** wird vom Algorithmus **108** berechnet (deren entsprechender Algorithmus **247** von den EDV-Verarbeitungsmitteln **21** gespeichert wird), mit Hilfe des für jede Karte und für den Zustand $C(p, n)$ **242** des Zählers **105** spezifischen Geheimschlüssels **250**. Neben der Identifizierungszahl $I(p)$ **240** für die Karte und des verschlüsselten Identifizierungscodes $S(p, n)$ **241**, sendet die Karte **10** den Zustand $C(p, n)$ **242** des Schrittzählers **105** bei jeder Übertragung. Die EDV-Verarbeitungsmittel **21** speichern den Zustand $C(p, n)$ **242** des Schrittzählers **105** bei der letzten für gültig erklärten Operation in der Datenbank **23**. So können bei jedem Meldungsempfang **244** die Vergleichsmittel **25** der EDV-Verarbeitungsmittel **21** die

bezüglich des Zustandes $C(p, n)$ **242** des Zählers **105** empfangene Information mit der vorhergehenden empfangenen und im Speicher **23** gehaltenen Information $C(p, m)$ **246** vergleichen **245**.

a) Ist der in der Meldung **244** ausgedrückte Zustand $C(p, n)$ **242** des Zählers **105** (Fig. 2) streng größer ($n > m$) als der Zustand $C(p, m)$ **246** der vorher empfangenen Meldung, so wird die Meldung **244** angenommen und die Analyse fortgeführt.

b) Ist der in der Meldung **244** ausgedrückte Zustand $C(p, n)$ **242** des Zählers **105** kleiner als der oder gleich ($n \leq m$) dem Zustand $C(p, m)$ **246** der vorher empfangenen Meldung, so wird die Meldung abgelehnt. Die empfangene Meldung kann nur eine vorher gefertigte Kopie oder eine informative Täuschung sein.

[0054] Sind die unter dem obigen Punkt a) definierten Bedingungen erfüllt, ermöglichen die EDV-Verarbeitungsmittel **21** das Lesen des festen Teils $I(p)$ **240** und das Suchen in der eigenen Datenbank **23**, **230** des der Karte zugeordneten Geheimschlüssels. Die Rechenmittel der Verarbeitungsmittel **24** können dann mit Hilfe des Algorithmus **247**, des Zustands des Zählers $C(p, n)$ **242** und des Geheimschlüssels $Clé(p)$ **250** den von den EDV-Verarbeitungsmitteln **21** erwarteten verschlüsselten Code berechnen. Der so berechnete verschlüsselte Code $S'(p, n)$ **248** wird mit dem tatsächlich empfangenen Code $S(p, n)$ **241** durch die Vergleichsmittel **25** verglichen **249**. Dieses Verfahren und diese Mittel erlauben es demnach, die Meldung zu bestätigen oder abzulehnen **244**, ohne dass der Kartenbenutzer diese mehrere Male zu tätigen braucht, wie es der Fall bei der oben beschriebenen Ausführungsvariante war.

[0055] Das Vorhandensein eines Schrittzählers **105** innerhalb der Karte **10** ermöglicht ohne zusätzliche Kosten das Feststellen der Höchstzahl von Benutzungen der Karte bei ihrer individuellen Programmierung. Ist diese Höchstzahl erreicht, so sendet die Karte keine kohärente Meldung mehr und wird somit von den EDV-Verarbeitungsmitteln **21** abgelehnt.

[0056] Für eine gegebene Karte (p) umfasst das gesendete Raster **244** folgendes:

- einen festen Teil $I(p)$ **240** (die Identifizierungszahl der Karte),
- einen variablen, fortschreitenden Teil $C(p, n)$ **242** (der Zählerzustand),
- einen angeblich aleatorischen variablen Teil $S(p, n)$ **241** (das Ergebnis der Anwendung eines Verschlüsselungsalgorithmus **108** auf den für die Karte (p) spezifischen Geheimschlüssel **250**).

[0057] Das gesendete Raster

- ist stets von Karte zu Karte verschieden,
- ist, für eine gegebene Karte, bei jeder Übertragung verschieden.

[0058] Die EDV-Verarbeitungsmittel **21** ermöglichen

für eine gegebene Karte (p):

- das Lesen des festen Teils I(p) **240** (die Identifizierungszahl der Karte),
- das Suchen des dieser Karte zugeordneten Geheimschlüssels **250** sowie die letzte Eintragung des empfangenen Zustandes des Zählers **105** C(p, m) **245** der Karte in der eigenen Datenbank **23**,
- das Ablehnen des Rasters **244**, wenn der Zählerzustand C(p, n) **242** der laufenden Operation kleiner als der oder gleich dem vorher empfangenen Zustand C(p, m) **246** ist, sowie das Weiterführen der Überprüfung des Vorgangs, wenn der Zustand C(p, n) **242** streng größer als der vorher empfangene C(p, m) **246** ist,
- das „Entschlüsseln“ der empfangenen Meldung **244** und das Bestätigen ihres Inhaltes durch ihre Wiederberechnung mit Hilfe des Verschlüsselungsalgorithmus **247**, des kartenspezifischen Schlüssels **250** sowie des Zählerzustandes C(p, n) **242**, gefolgt vom Vergleich des Berechnungsergebnisses mit der empfangenen Meldung.

[0059] So ist es möglich, dank dieser Kombination von Mitteln, mit Hilfe einer Karte im Kreditkartenformat akustische Identifizierungsfrequenzen des Typs DTMF zu senden, die vom Mikrophon einer an das Telefonnetz angeschlossenen Ausrüstung empfangen werden, wobei man sich der Echtheit der rufenden Karte sicher ist und alle Betrüger abweisen kann, die irgendeine akustische Aufnahme oder EDV-Kopie oder informatische Täuschung einzusetzen versuchen.

[0060] Um die Sicherheit des Systems zu erhöhen weist, in der in **Fig. 1** dargestellten Ausführungsvariante, das System ferner zweite Vergleichsmittel **26** auf. Diese Vergleichsmittel ermöglichen den Vergleich eines in der Datenbank gespeicherten und dem Abonnenten persönlich zugeordneten vertraulichen Codes mit dem vom Abonnenten gesendeten vertraulichen Code. Dieser Code wird mit Hilfe einer Tastatur **27** gesendet, die dem Multimedia-Terminal **16** und/oder der Karte **10** zugeordnet ist und den EDV-Bearbeitungsmitteln des Dienstleistungsanbieters bzw. Service Providers über das Computernetz **15** gesendet wird.

[0061] Somit hat der Dienstleistungsanbieter bzw. Service Provider die Sicherheit, dass der Anrufer **11** tatsächlich zur Nutzung seiner Dienstleistungen befugt ist. Eine gestohlene Karte ist für den Dieb wertlos, da er den vertraulichen Code nicht kennt.

[0062] Um ebenfalls die Sicherheit des Systems zu erhöhen und zu vermeiden, dass der Abonnent seine Anfrage an den Dienstleistungsanbieter bzw. Service Provider in Frage stellt, umfassen die EDV-Verarbeitungsmittel **21** (in der in **Fig. 1** dargestellten Ausführungsvariante):

- eine Validierungssoftware **21a** für Anweisungen des Abonnenten an den Dienstleistungsanbieter bzw. Service Provider, nach Erfassung eines ver-

schlüsselten akustischen Signals, das nach Betätigung durch den Abonnenten von der Karte gesendet wird,

- eine Software **21b** für die Ausstellung einer Empfangsbestätigung der erteilten Anweisungen, die dem Abonnenten zugeschickt werden.

[0063] Dank dieses Systems hat der Abonnent durch eine elektronische Signatur seine Anweisung an den Dienstleistungsanbieter bzw. Service Provider bestätigt.

[0064] Mit Bezug auf die **Fig. 4, 5 und 6** sollen nun drei Ausführungsvarianten beschrieben werden, mit denen die akustischen Identifizierungssignale **20** an die EDV-Verarbeitungsmittel **21** des Dienstleistungsanbieters bzw. Service Providers **12** gesendet werden können. Es wurden in diesen Figuren die gleichen Referenzen für die Organe und Mittel verwendet, wie die im Zusammenhang mit **Fig. 1** beschrieben.

[0065] Nach der ersten Ausführungsvariante (**Fig. 4**) umfassen die von der Computerzentrale **18** des Dienstleistungsanbieters bzw. Service Providers abhängigen EDV-Verarbeitungsmittel **21** Mittel zum Laden **200** einer Konversionssoftware der in Bits ausgedrückten Schalldatei in das Multimedia-Terminal **16**, so dass die von diesem Multimedia-Terminal **16** kommenden Signale in der Form einer Bitfolge auftreten.

[0066] Nach der zweiten Ausführungsvariante (**Fig. 5**) verfügt das Multimedia-Terminal **16** über Mittel zum Konvertieren und zum Senden **300** der vom Mikrophon des Multimedia-Terminals empfangenen akustischen Identifizierungssignale als Schalldatei. Diese Schalldatei wird insbesondere nach Empfang eines von den EDV-Verarbeitungsmitteln **18** des Dienstleistungsanbieters bzw. Service Providers gesendeten Signals übermittelt. Dieses Signal wird nach Zustandekommen der telefonischen Verbindung zwischen dem Terminal und der Computerzentrale gesendet. Im Falle dieser Variante erfolgen die Bearbeitung der Schalldatei und ihre Umwandlung in eine Bitfolge durch die EDV-Verarbeitungsmittel **21** der Computerzentrale **18** des Dienstleistungsanbieters bzw. Service Providers.

[0067] Nach der dritten Ausführungsvariante (**Fig. 6**) stellt der Dienstleistungsanbieter bzw. Service Provider dem Abonnenten eine Konversionssoftware zur Verfügung (**400**), die dieser in sein Multimedia-Terminal **16** einspielt. Dieses Konversionssoftware wandelt die vom Mikrophon **17** des Multimedia-Terminals **16** empfangenen und gesendeten akustischen Signale in Digitalsignale, die über das Computernetz vom Internet-Typ **15** gesendet werden können.

Patentansprüche

1. Verfahren, das den Benutzern (**11**) eines Computernetzes vom Internet-Typ, ausgestattet mit Multi-

media-Terminals (16), die ein Mikrophon (17) umfassen und an das Computernetz (15) vom Internet-Typ angeschlossen sind und sich in Entfernung von einem Dienstleistungsanbieter bzw. Service Provider (12) befinden, den sicheren und schnellen Zugang zu den Dienstleistungen (30) ermöglicht, die der Dienstleistungsanbieter bzw. Service Provider (12) den Benutzern (11) des Computernetzes vom Internet-Typ bietet,

wobei das Verfahren die folgenden Schritte umfasst:

- der Dienstleistungsanbieter bzw. Service Provider (12) stellt jedem Benutzer (11) des Computernetzes vom Internet-Typ, die Abonnenten seiner Dienstleistungen sind, eine Karte (10) zur Verfügung, die das Format einer Kreditkarte aufweist und durch für jeden Abonnenten und jede Karte spezifische Identifikationsdaten personalisiert ist, wobei jede dieser Karten (10) kurze akustische Identifizierungssignale (20) vom Typ DTMF sendet, die zumindest teilweise verschlüsselt sind und sich bei jeder Betätigung (14) der Karte durch den Benutzer (11) des Computernetzes vom Internet-Typ ändern,
- die erwähnten akustischen Identifizierungssignale (20) werden vom Mikrophon (17) des Multimedia-Terminals (16) empfangen und über das Computernetz (15) vom Internet-Typ an die Computerzentrale (18) des Dienstleistungsanbieters bzw. Service Providers übertragen,
- die übertragenen Signale und die Identifizierungsdaten des Abonnenten und der Karte, die in der Computerzentrale (18) gespeichert sind (23), werden von der Computerzentrale (18) des Dienstleistungsanbieters bzw. Service Providers (12) elektronisch verarbeitet (24) und verglichen (25), so dass bei Übereinstimmung der Daten, der Abonnent (11) sofort Zugang zu den Dienstleistungen (30) des Dienstleistungsanbieters bzw. Service Providers (12) erhält.

2. Verfahren nach Anspruch 1,

- wobei die Karte (10):
- ferner die Zahl $C(p, n)$ (242) ihrer Betätigungen durch das Element (14) berechnet (105),
- akustische Signale (20) sendet, die für die Zahl $C(p, n)$ (242) ihrer Betätigungen repräsentativ sind,
- die akustischen Signale als Funktion der Zahl $C(p, n)$ (242) ihrer Betätigungen verschlüsselt (103),
- wobei die EDV-Verarbeitungsmittel (21) der Computerzentrale (18), welche die übertragenen Signale und die Identifizierungsdaten des Kunden und der Karte, die in der Computerzentrale (18) des Dienstleistungsanbieters bzw. Service Providers gespeichert sind (23), elektronisch verarbeiten (24) und vergleichen (25):
- die Zahl $C(p, m)$ (246) der Betätigungen der Karte während der letzten validierten Transaktionen speichern (23),
- die Zahl $C(p, n)$ (242) der Betätigungen der Karte während der laufenden Transaktion mit der gespeicherten Zahl von Betätigungen $C(p, m)$ (246) vergleichen (245),

- die laufende Transaktion abbrechen, wenn $C(p, n)$ (242) kleiner oder gleich $C(p, m)$ (246) ist und die Prüfung der laufenden Transaktion fortsetzen, wenn $C(p, n)$ (242) größer als $C(p, m)$ (246) ist,
- die elektronischen Signale $S'(p, n)$ (248) als Funktion der Identifizierungsdaten und der Zahl der Betätigungen der Karte $C(p, n)$ (242) im Verlauf der laufenden Transaktion neu berechnen (247) und sie dann mit den übertragenen elektronischen Signalen $S(p, n)$ (241) vergleichen (249),
- so dass bei Übereinstimmung, der Abonnent (11) sofort Zugang zu den Dienstleistungen (30) des Dienstleistungsanbieters bzw. Service Providers (12) erhält.

3. Verfahren nach einem der Ansprüche 1 oder 2, das ferner den folgenden Schritt umfasst:

- der Abonnent (11) sendet mittels einer dem Multimedia-Terminal (16) und/oder der Karte (10) zugeordneten Tastatur (27) einen vertraulichen Code, wobei nach Übertragung an die Computerzentrale (18) des Dienstleistungsanbieters bzw. Service Providers (12) über das Computernetz (15) vom Internet-Typ, dieser vertrauliche Code verarbeitet und mit dem in der Computerzentrale (18) des Dienstleistungsanbieters bzw. Service Providers (12) gespeicherten (23) persönlichen vertraulichen Code des Abonnenten verglichen wird.

4. Verfahren nach einem der Ansprüche 1, 2 oder 3, das ferner den folgenden Schritt umfasst:

- die vom Abonnenten (11) an die Dienstleistungen (30) des Dienstleistungsanbieters bzw. Service Providers (12) erteilten Anweisungen werden vom Abonnenten durch Betätigung der Karte (10) validiert, um sicherzustellen, dass ein verschlüsseltes akustisches Validierungssignal von der Karte gesendet wird,
- das Validierungssignal wird von der Computerzentrale (18) des Dienstleistungsanbieters bzw. Service Providers (12) aufgezeichnet,
- so dass der Abonnent (11) die an den Dienstleistungsanbieter bzw. Service Provider (12) erteilte Anweisung durch eine elektronische Unterschrift validiert.

5. Verfahren nach einem der Ansprüche 1, 2, 3 oder 4, das ferner die folgenden Schritte umfasst:

- die vom Mikrophon (17) des Multimedia-Terminals (16) aufgenommenen und über das Computernetz (15) vom Internet-Typ an die Computerzentrale (18) des Dienstleistungsanbieters bzw. Service Providers (12) gesendeten akustischen Identifizierungssignale (20) werden in der Form einer Schalldatei gesendet.

6. Verfahren nach einem der Ansprüche 1, 2, 3 oder 4, das ferner die folgenden Schritte umfasst:

- die Computerzentrale (18) des Dienstleistungsanbieters bzw. Service Providers (12) lädt eine Konversionssoftware in das Multimedia-Terminal herunter,
- die Konversionssoftware konvertiert die vom Mikrophon (17) des Multimedia-Terminals (16) aufgenom-

menen akustischen Identifizierungssignale (20) in eine Bitfolge,
 – diese Bitfolge wird über das Computernetz (15) vom Internet-Typ an die Computerzentrale (18) des Dienstleistungsanbieters bzw. Service Providers (12) gesendet,
 so dass die vom Multimedia-Terminal kommenden Signale als Bitfolge eintreffen.

7. Verfahren nach einem der Ansprüche 1, 2, 3 oder 4, das ferner die folgenden Schritte umfasst:

– der Dienstleistungsanbieter bzw. Service Provider (12) stellt jeden Benutzer (11) des Computernetzes (15) vom Internet-Typ, der Abonnent seiner Dienstleistungen (30) ist, eine Konversionssoftware zur Verfügung, die im Multimedia-Terminal (16) zur Anwendung kommen soll,
 – die vom Mikrophon (17) des Multimedia-Terminals (16) aufgenommenen akustischen Identifizierungssignale (20) werden in eine Bitfolge konvertiert bevor sie über das Computernetz (15) vom Internet-Typ an die Computerzentrale (18) des Dienstleistungsanbieters bzw. Service Providers gesendet werden.

8. System, das den Benutzern des Computernetzes (15) vom Internet-Typ, die über Multimedia-Terminals (16) verfügen, welche ein Mikrophon (17) umfassen und an das Computernetz (15) vom Internet-Typ angeschlossen sind und sich in Entfernung von einem Dienstleistungsanbieter bzw. Service Provider (12) befinden, schnellen und sicheren Zugang zu den Dienstleistungen (30) gewährt, die der Dienstleistungsanbieter bzw. Service Provider (12) seinen Abonnenten (11) bietet,

wobei das System folgendes umfasst:

– eine Karte (10) im Kreditkartenformat, die durch für jede Karte und für jeden Abonnenten spezifische Identifizierungsdaten personalisiert und die dem Abonnenten zur Verfügung gestellt wird, wobei die Karte (10) folgendes umfasst:

– Mittel zum Senden (13) kurzer Identifizierungssignale (20) des Typs DTMF, die vom Abonnenten mittels eines Elementes (14) betätigt werden, das von außerhalb der Karte (10) zugänglich ist,

– Verschlüsselungsmittel (103), die das Verschlüsseln von mindestens einem Teil und das Variieren der akustischen Signale (20) bei jeder Betätigung (14) der Karte (10) ermöglichen,

– in den Multimedia-Terminals (16) untergebrachte Übertragungsmittel (19) der akustischen Signale (20), welche diese akustischen Signale (20) über das Computernetz (15) vom Internet-Typ in die Ferne senden können,

– EDV-Verarbeitungsmittel (21), die von der Computerzentrale (18) des Dienstleistungsanbieters bzw. Service Providers (12) abhängig sind, an das Computernetz (15) vom Internet-Typ angeschlossen sind und die von den Multimedia-Terminals (16) kommenden Signale empfangen, wobei diese EDV-Verarbeitungsmittel (21) folgendes umfassen:

– eine Datenbank (23), in der die Referenzdaten der Karten (10) der Abonnenten (11) sowie deren Identifizierungsdaten gespeichert sind,

– Mittel zum Verarbeiten (24) und zum Vergleichen (25) der elektronischen Signale mit den in der Datenbank (23) gespeicherten Identifizierungsdaten, so dass bei Übereinstimmung, der Abonnent (11) sofort Zugang zu den Dienstleistungen (30) des Dienstleistungsanbieters bzw. Service Providers (12) erhält.

9. System nach Anspruch 8,

– wobei die Karte (10) ferner folgendes umfasst:

– einen Schrittzähler (105), der mit den Sendemitteln (13) und mit den Verschlüsselungsmitteln (103) verbunden ist und bei jeder Betätigung der Karte (10) mit Hilfe des Elementes (14) um mindestens eine Einheit weitergestellt wird,

so dass der Zustand des Schrittzählers (105) an die EDV-Verarbeitungsmittel (21) weitergeleitet wird und, dass die akustischen Signale als Funktion des Status des Schrittzählers verschlüsselt werden,

– wobei die EDV-Verarbeitungsmittel (21) ferner folgendes umfassen:

– Mittel zum Speichern (23) des Status $C(p, m)$ (246) des Schrittzählers (105) bei der letzten validierten Transaktion,

– Mittel zum Vergleichen (25) des Status $C(p, n)$ (242) des Schrittzählers (105), die bei der laufenden Transaktion herausgegeben wurden, mit dem gespeicherten Status $C(p, m)$ (246) des Schrittzählers (105), so dass die Prüfung der laufenden Transaktion abgebrochen wird, wenn $C(p, n)$ (242) kleiner oder gleich $C(p, m)$ (246) ist und weitergeführt wird, wenn $C(p, n)$ (242) streng größer als $C(p, m)$ (246) ist,

– wobei die Mittel zum Verarbeiten (24) und zum Vergleichen (25) der elektronischen Signale mit den in der Datenbank gespeicherten Identifizierungsdaten über Mittel verfügen, mit denen die elektronischen Signale als Funktion des Status $C(p, n)$ (242) des Schrittzählers (105) und der Identifizierungsdaten neu berechnet werden können (247) und dann mit den gesendeten elektronischen Signalen verglichen werden (249),

so dass bei Übereinstimmung, der Abonnent (11) sofort Zugang zu den Dienstleistungen (30) des Dienstleistungsanbieters bzw. Service Providers (12) erhält.

10. System nach einem der Ansprüche 8 oder 9, wobei die EDV-Verarbeitungsmittel (21) ferner folgendes umfassen:

– zweite Vergleichsmittel (26) eines in der Datenbank (23) gespeicherten vertraulichen, für den Abonnenten persönlichen Codes, mit einem vom Abonnenten mittels einer mit dem Multimedia-Terminal (16) und/oder mit der Karte (10) assoziierten Tastatur (27) gesendeten vertraulichen Code, welcher an die EDV-Verarbeitungsmittel (21) des Dienstleistungsanbieters bzw. Service Providers (12) über das Computernetz (15) vom Internet-Typ gesendet wird.

11. System nach einem der Ansprüche 8, 9 oder 10, wobei die EDV-Verarbeitungsmittel (21) ferner folgendes umfassen:

- eine Validierungssoftware (21a) der vom Abonnenten (11) an den Dienstleistungsanbieter bzw. Service Provider (12) erteilten Anweisungen, nach Erfassung eines von der vom Abonnenten betätigten Karte (10) abgegebenen verschlüsselten akustischen Signals,
- eine Software (21b) zum Ausstellen einer Empfangsbestätigung der erteilten Anweisungen, die dem Abonnenten zugesandt wird.

12. System nach einem der Ansprüche 8, 9, 10 oder 11,

- wobei das Multimedia-Terminal über Mittel zum Senden (300) der vom Mikrophon (17) des Multimedia-Terminals (16) aufgenommenen akustischen Identifizierungssignale (20) in Form einer akustischen Datei über das Computernetz (15) vom Internet-Typ an die Computerzentrale (18) des Dienstleistungsanbieters bzw. Service Providers (12) verfügt.

13. System nach einem der Ansprüche 8, 9, 10 oder 11,

- wobei die von der Computerzentrale (18) des Dienstleistungsanbieters bzw. Service Providers (12) abhängigen EDV-Verarbeitungsmittel (21) folgendes umfassen:

- Mittel zum Aufladen (200) einer Konversionssoftware in das Multimedia-Terminal (16), wobei diese Software die vom Mikrophon (17) des Multimedia-Terminals (16) aufgenommenen akustischen Identifizierungssignale (20) in eine Bitfolge umwandelt,
- Mittel zum Herausgeben eines Sendebefehls für die Bitfolge vom Multimedia-Terminal (16) zur Computerzentrale (18) des Dienstleistungsanbieters bzw. Service Providers, über das Computernetz (15) vom Internet-Typ, so dass die vom Multimedia-Terminal kommenden Signale als Bitfolge auftreten.

14. System nach einem der Ansprüche 8, 9, 10 oder 11, das folgendes umfasst:

- eine Konversionssoftware, die im Multimedia-Terminal (16) zum Einsatz kommen soll, wobei diese Software die vom Mikrophon (17) des Multimedia-Terminals aufgenommenen und gesendeten akustischen Signale (20) in digitale Signale umwandelt, die in die Ferne über das Computernetz (15) vom Internet-Typ gesendet werden können.

Es folgen 3 Blatt Zeichnungen

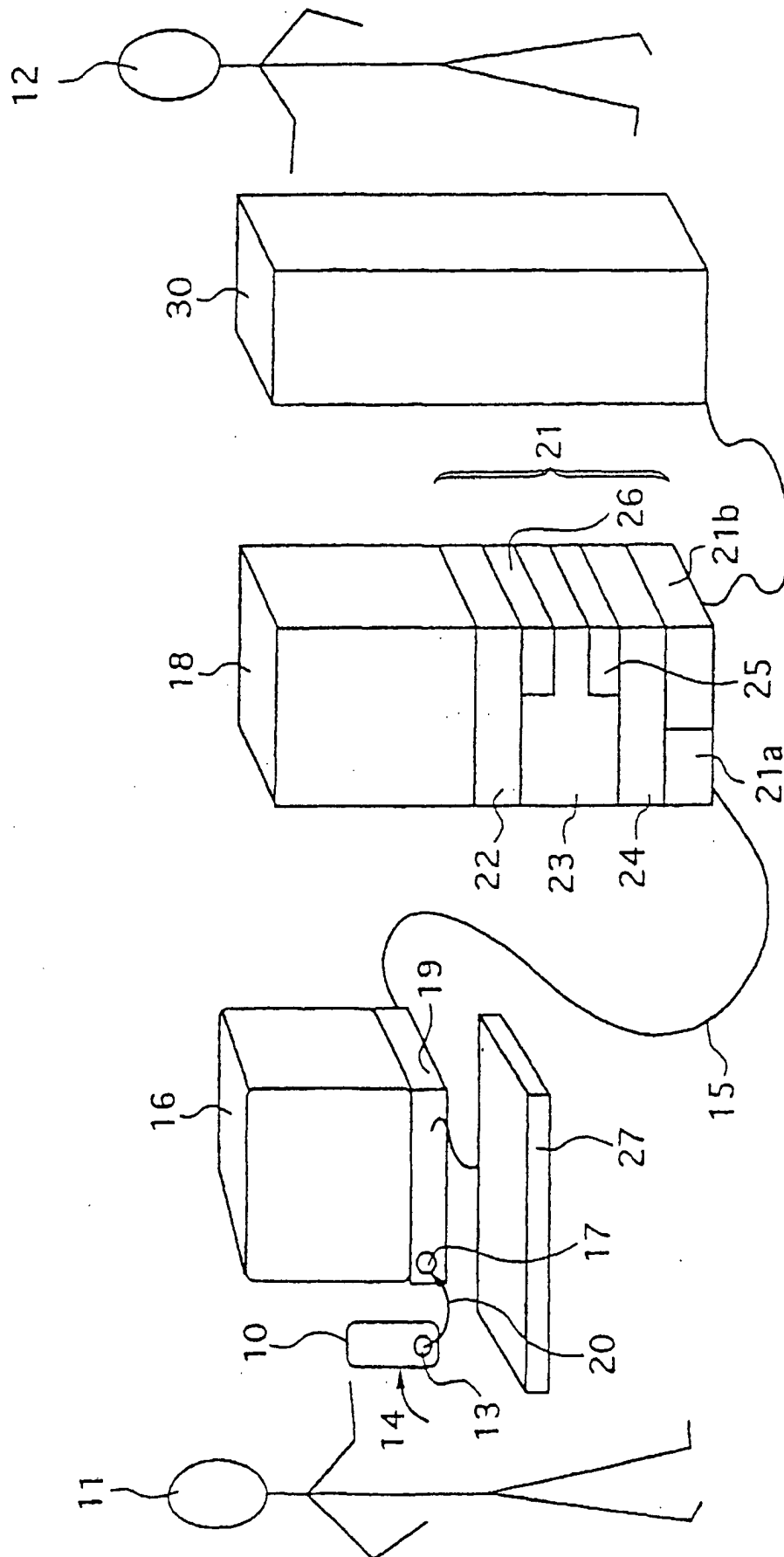


Fig. 1

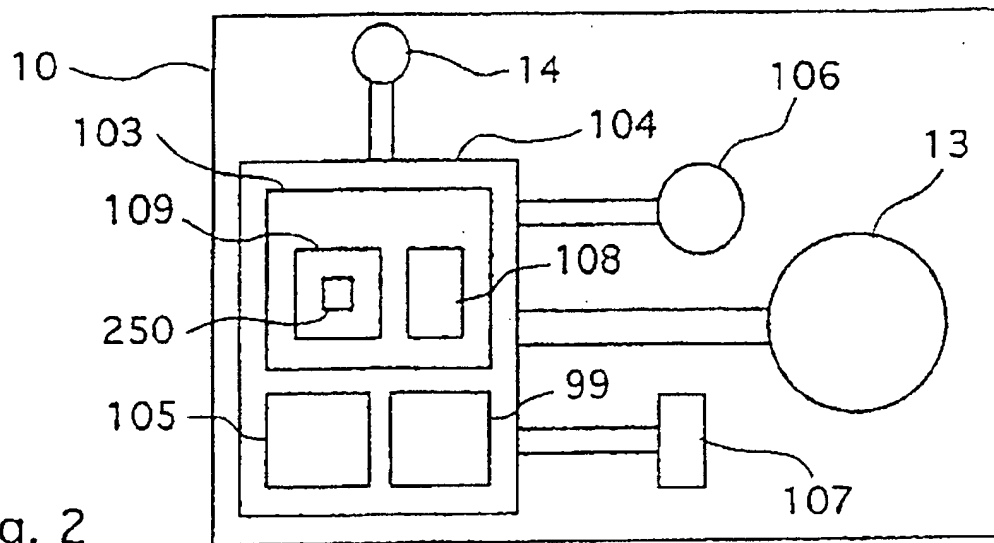


Fig. 2

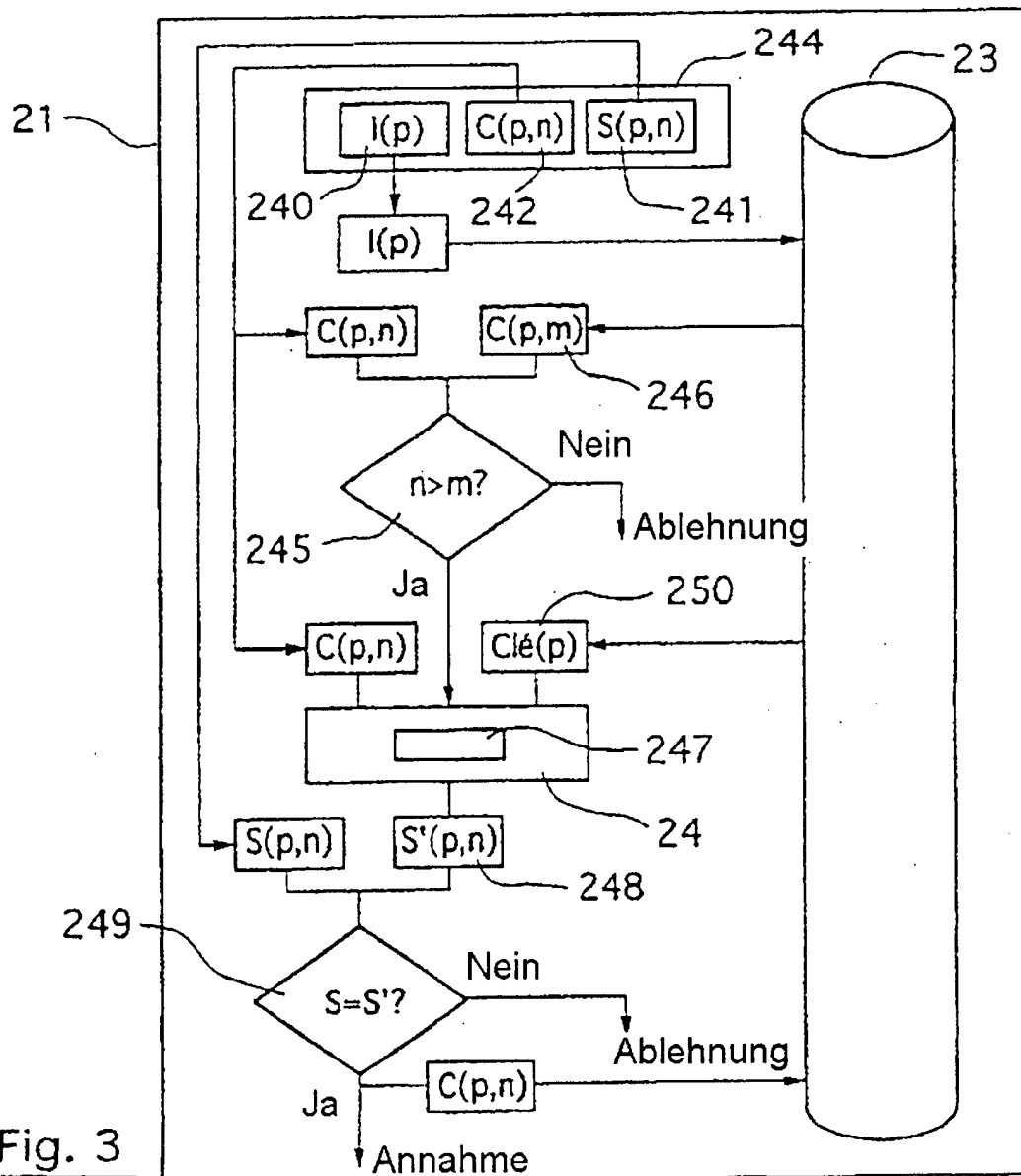


Fig. 3

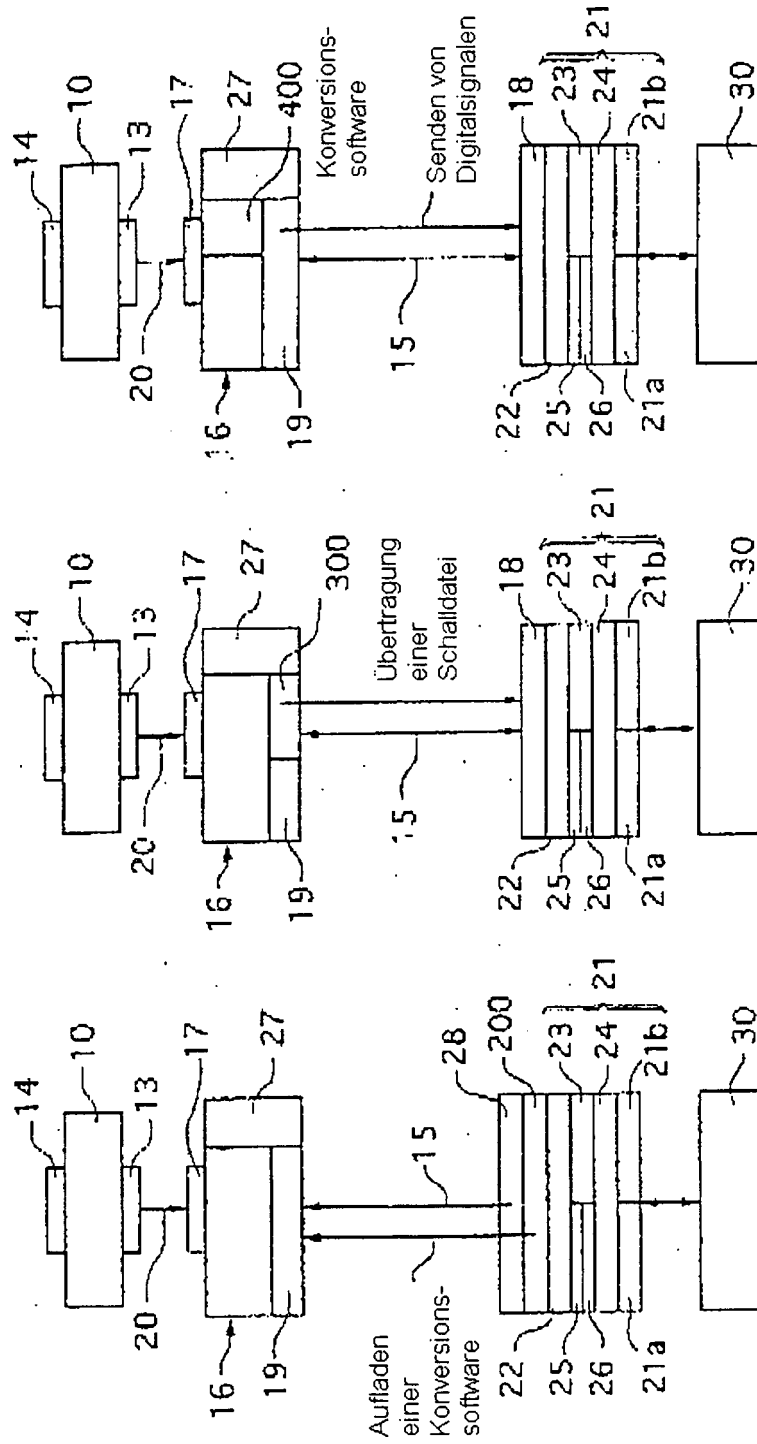


Fig. 6

Fig. 5

Fig. 4