

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

(19) Weltorganisation für geistiges Eigentum
Internationales Büro



(43) Internationales Veröffentlichungsdatum
8. Januar 2009 (08.01.2009)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2009/003605 A2

(51) Internationale Patentklassifikation:
Nicht klassifiziert

(21) Internationales Aktenzeichen: PCT/EP2008/005057

(22) Internationales Anmeldedatum:
23. Juni 2008 (23.06.2008)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2007 030 114.8 29. Juni 2007 (29.06.2007) DE
10 2007 048 976.7
12. Oktober 2007 (12.10.2007) DE

(71) Anmelder (für alle Bestimmungsstaaten mit Ausnahme von US): VOICE.TRUST AG [DE/DE]; Geisenhausenerstrasse 15, 81379 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder (nur für US): MUMM, Marc

[DE/DE]; 80686 München (DE). KUPPUSWAMY, Rajasekharan [DE/DE]; 80799 München (DE).

(74) Anwälte: HEINZE, Ekkehard usw.; Meissner, Bolte & Partner GbR, Postfach 86 06 24, 81633 München (DE).

(81) Bestimmungsstaaten (soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

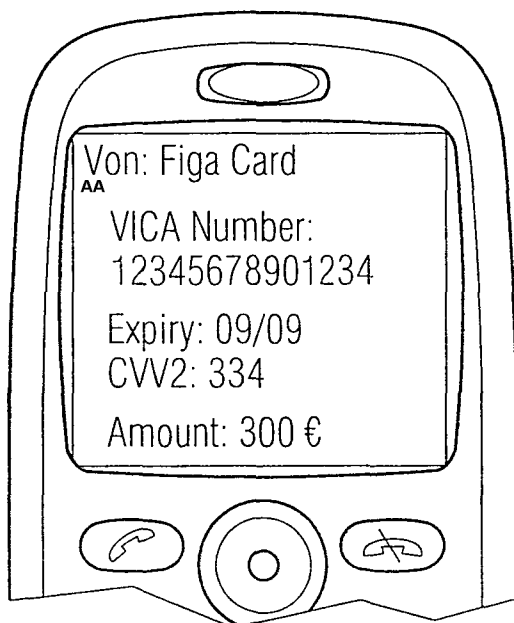
(84) Bestimmungsstaaten (soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU,

[Fortsetzung auf der nächsten Seite]

(54) Title: VIRTUAL PREPAID OR CREDIT CARD AND METHOD AND SYSTEM FOR PROVIDING SUCH AND FOR ELECTRONIC PAYMENT TRANSACTIONS

(54) Bezeichnung: VIRTUELLE PREPAID- ODER KREDITKARTE UND VERFAHREN UND SYSTEM ZUR BEREITSTELLUNG EINER SOLCHEN UND ZUM ELEKTRONISCHEN ZAHLUNGSVERKEHR

FIG 1



AA ...From:

(57) Abstract: A virtual prepaid or credit card, as a data record, free from a physical substrate, wherein the data are designed to authorize a holder in possession thereof to pay for a product or a service, particularly as part of an online transaction, or to obtain cash, wherein the data record is produced on the basis of a credit card account or a prepayment to a system account and in response to a control signal which is output as the result of a registration procedure by the holder, wherein the data record is available for display and sending on a telecommunication terminal, particularly a mobile telephone, of the registered holder.

(57) Zusammenfassung: Virtuelle Prepaid- oder Kreditkarte, als Datensatz, frei von einem physischen Substrat, wobei die Daten dazu ausgebildet sind, einen Inhaber zu autorisieren, der in ihrem Besitz ist, für ein Produkt oder einen Dienst zu zahlen, insbesondere im Rahmen einer Online-Transaktion, oder Bargeld zu erhalten, wobei der Datensatz auf der Basis eines Kreditkartenkontos oder einer Vorab-Zahlung auf ein Systemkonto und im Ansprechen auf ein im Ergebnis einer Registrierungsprozedur des Inhabers ausgegebenes Steuersignal erzeugt wird, wobei der Datensatz an einem Telekommunikations-Endgerät, insbesondere einem Mobiltelefon, des registrierten Inhabers zur Anzeige und zum Versenden verfügbar ist.

WO 2009/003605 A2



TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— *ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts*

Virtuelle Prepaid- oder Kreditkarte und Verfahren und System zur Bereitstellung einer solchen und zum elektronischen Zahlungsverkehr

Beschreibung

Diese Erfindung betrifft eine virtuelle Kreditkarte (d.h. einen Datensatz, der alle relevante Information einer physischen Kreditkarte enthält, z.B. eine Kreditkartennummer, ein Ablaufdatum, einen zweiten Sicherheitscode = CVV2..., und der mindestens bis zu einem vorbestimmten Grade deren Funktionen hat) und ein Verfahren und ein System zur Bereitstellung einer solchen virtuellen Kreditkarte.

Obgleich heute Kreditkarten weit verbreitet sind und im Internet genutzt werden, sind mit dieser Nutzung viele Bedenken, Beschränkungen und offene Fragen verbunden.

Die wachsende Anzahl von Kreditkartenbetrügereien, Phishing- und Pharming-Attacken schränkt die Bereitschaft von Kunden zur Nutzung von Kreditkarten sowohl online als auch offline ein. Mehr und mehr Nutzer sind nicht gewillt, ihre Kreditkarteninformation auf Websites einzugeben, weil sie befürchten, Opfer von ID- und Kreditkartenbetrug zu werden. Diebe würden unmittelbaren Zugriff zu ihrem Kreditkartenkonto haben, wobei der Betrug auf das Kreditlimit der Karte beschränkt ist.

Neben Online-Betrug, der nach Eingabe von Kreditkartendetails online vorkommen kann, können Karten außerdem verloren gehen, gestohlen werden, oder es können andere Arten von Betrug geschehen. Dies ist ein allgemeiner Nachteil solcher Arten physischer Karten, der seit langem bekannt ist, dem aber bisher nicht befriedigend beizukommen war.

5. Virtuelle Kredit- oder Prepaidkarte nach einem der vorangehenden Ansprüche, wobei diese definierende Datensatz mindestens ein sich auf die zugrunde liegende Registrierungsprozedur, die eine Bewertung biometrischer Merkmale der autorisierten Person einschließt, beziehendes Datum umfasst.
6. Verfahren zur Herstellung einer virtuellen Kredit- Prepaidkarte, als Datensatz, frei von einem physischen Substrat, wobei die Daten dazu ausgebildet sind, einen Inhaber zu autorisieren, der in ihrem Besitz ist, für ein Produkt oder einen Dienst zu zahlen, insbesondere im Rahmen einer Online-Transaktion, oder Bargeld zu erhalten, wobei das Verfahren die Auswertung von Kreditkarten-Kontendaten oder Vorab-Zahlungsdaten und eine Registrierungsprozedur, um den Datensatz zu bilden, und weiter die Übertragung des Datensatzes an ein Telekommunikations-Endgerät des registrierten Inhabers, insbesondere über ein Mobilfunknetz, einschließt.
7. Verfahren nach Anspruch 6, wobei die Registrierungsprozedur eine Auswertung biometrischer Merkmale des Inhabers, insbesondere seines Stimmprofils, einschließt.
8. Verfahren nach Anspruch 6 oder 7, wobei mindestens ein die Art und/oder das Ergebnis der Registrierungsprozedur kennzeichnendes Datum in den Datensatz eingefügt wird.
9. Verfahren nach einem der Ansprüche 6 bis 8, wobei eine eindeutige Endgerät-Kennung des Telekommunikations-Endgerätes des Inhabers erfasst und in den autorisierenden Datensatz eingefügt wird.
10. Verfahren zur Nutzung einer virtuellen Kredit- oder Prepaidkarte nach einem der Ansprüche 1 bis 5 zum elektronischen Zahlungsverkehr, wobei Zahlungsanweisungen als elektronische Nachrichten vom Telekommunikations-Endgerät des Inhabers an ein Gateway eines Autorisierungssystem-Servers

versandt, von diesem geprüft und bearbeitet und im Ansprechen auf ein positives Prüfungsergebnis an einen vom Inhaber bestimmten Zahlungsempfänger weitergeleitet werden.

11. Verfahren nach Anspruch 10, wobei der Versand als elektronische Nachricht an ein Daten- oder Telekommunikations-Endgerät des Zahlungsempfängers erfolgt.
12. Verfahren nach Anspruch 10 oder 11, wobei die Prüfung im Autorisierungssystem-Server die Prüfung eines Verfügungsrahmen-Datensatzes einschließt, welcher im Ansprechen auf eine Vorab-Zahlung auf ein Systemkonto durch den Inhaber in einem Zahlungsverkehrs-Server erzeugt wird, insbesondere einen ersten Teilschritt der Prüfung des Vorhandensein eines Verfügungsrahmens und, im Ansprechen hierauf, einen zweiten Teilschritt des Vergleichs eines vorhandenen Verfügungsrahmens mit einem in der Nachricht vom Inhaber spezifizierten Zahlungsbetrag.
13. Verfahren nach einem der Ansprüche 10 bis 12, wobei die Prüfung im Autorisierungssystem-Server eine Authentifizierung des Absenders der Zahlungsanweisung, insbesondere mit aktueller Erfassung und Vergleich biometrischer Merkmale mit während der Registrierungsprozedur gespeicherten biometrischen Merkmalen, umfasst.
14. Verfahren nach Anspruch 13, wobei zur Authentifizierung, insbesondere Erfassung der biometrischen Merkmale, im Ansprechen auf den Empfang der elektronischen Nachricht durch den Autorisierungssystem-Server ein Rückruf beim sendenden Telekommunikations-Endgerät und die Ausgabe einer Menüführung auf diesem ausgeführt wird.
15. Verfahren nach Anspruch 14, wobei zur Erfassung eines aktuellen Stimmprofils im Rahmen der Menüführung auf dem Telekommunikations-Endgerät nachzusprechende Ziffern, Textteile oder dergleichen angezeigt und die nachgesprochenen Ziffern, Textteile oder dergleichen akustisch erfasst wer-

- den und beim Autorisierungssystem-Server aus diesen ein aktuelles Stimmprofil errechnet wird.
16. Verfahren nach einem der Ansprüche 10 bis 15, wobei die Bearbeitung einer Zahlungsanweisung im Autorisierungssystem-Server die Übermittlung eines Zahlungs-Steuerdatensatzes an einen Zahlungsverkehrs-Server zur Steuerung eines elektronischen Übertrages eines in der Nachricht spezifizierten Zahlungsbetrages auf ein Systemkonto oder system-externes Konto des Zahlungsempfängers einschließt.
 17. Verfahren nach einem der Ansprüche 10 bis 16, wobei zur Aufladung der Prepaidkarte mit einem vorbestimmten Betrag eine elektronische Nachricht vom Telekommunikations-Endgerät des Inhabers an ein Gateway eines Autorisierungssystem-Servers versandt und die empfangene Nachricht im Server geprüft und bearbeitet und im Ansprechen auf ein positives Prüfungsergebnis ein Auflade-Steuerdatensatz an einen Zahlungsverkehrs-Server übermittelt wird, wodurch der Aufladungsbetrag auf das Systemkonto des Karteninhabers transferiert wird.
 18. Verfahren nach einem der Ansprüche 10 bis 17, wobei die vom der Inhaber abgesandte und/oder die an den bestimmten Zahlungsempfänger weitergeleitete elektronische Nachricht das SMS-Format hat.
 19. Verfahren nach Anspruch 18, wobei die Erstellung der elektronischen Nachricht im SMS-Format unter Benutzung von systemintern erzeugten Templates und die Bearbeitung empfangener SMS im Autorisierungssystem-Server unter Erkennung und Vergleich darin enthaltener Templates erfolgt.
 20. System zur Bereitstellung einer virtuellen Kredit- oder Prepaidkarte nach einem der Ansprüche 1 bis 5, wobei das System aufweist:
einen Zahlungsverkehrs-Server, der Kreditkarten- oder Vorab-Zahlungsdaten eines Nutzers speichert und verarbeitet und elektronische Systemkonten so-

wie Zahlungswegdaten für elektronische Transaktionen von/auf system-externen Konten speichert,
einen Autorisierungssystem-Server, der Nutzerauthentisierungsdaten, insbesondere einschließlich biometrischer Daten des Nutzers, speichert und verarbeitet,
eine Kartendatensatz-Erzeugungseinrichtung, die sowohl mit dem Zahlungsverkehrs-Server als auch dem Autorisierungssystem-Server zur Bildung des Datensatzes, der die virtuelle Kreditkarte definiert, und
eine Datensatz-Übertragungseinrichtung zum Übertragen des Kostendatensatzes über ein Telekommunikationsnetz, insbesondere ein Mobilfunknetz, an ein mit dem Netz verbundenes Telekommunikationsendgerät.

21. System nach Anspruch 20, wobei dem Zahlungsverkehrs-Server eine Systemkonten-Datenbasis zugeordnet ist, die jeweils einen registrierten Inhaber einer virtuellen Kredit- oder Prepaidkarte zugeordnete elektronische Systemkonten umfasst.
22. System nach Anspruch 21, wobei die Systemkonto-Datenbasis ein elektronisches Deckungs-Systemkonto aufweist, mit dem die Systemkonten durch interne Steuersignalleitungen verbunden sind.
23. System nach einem der Ansprüche 20 bis 22, wobei die Datensatz-Übertragungseinrichtung als SMS-Gateway zum Übertragen des Kartendatensatzes im SMS-Format ausgebildet ist.
24. Anordnung für den elektronischen Zahlungsverkehr, mit einem System nach einem der Ansprüche 20 bis 23, wobei der Autorisierungssystem-Server dazu ausgebildet ist, von den Telekommunikations-Endgeräten von Karteninhabern versandte elektronische Nachrichten zu prüfen, zu bearbeiten und gegebenenfalls weiterzuleiten, wobei die Prüfung eine Prüfung der Nutzerauthentisierungsdaten einschließt und die Bearbeitung die Erzeugung und Übermittlung von Steuerdatensätzen zum elektronischen Übertrag von Zah-

aktiviert werden, bzw. die Mobiltelefone, zu denen die virtuelle Kredit-/Prepaid-Karte gesandt wird, wie in Fig. 2 dargestellt.

Die Default-Flussdiagramme von Fig. 3 und 4 zeigen den Ablauf der Web-Registrierung und des Voice-Enrolment (Fig. 3) und die Nutzung des Dienstes (Fig. 4). Siehe auch die Figuren 5 und 6 für weitere Einzelheiten bezüglich des Enrolment- und Verifizierungsprozesses.

Zur Nutzung der virtuellen Prepaid-/Kreditkarte muss sich der Nutzer auf einer dedizierten Website registrieren. Während der Registrierung muss der Nutzer verschiedene Daten liefern. Die Web-Registrierung ist für alle Nutzer obligatorisch, die den Dienst nutzen wollen. Die stimmbasierte Registrierung/Authentifizierung ist ein zusätzliches Merkmal, welches die Nutzer zur Nutzung des Dienstes vom Mobiltelefon aus befähigt. Bezüglich der Details der stimmbasierten Authentifizierungsprozeduren und -systeme, die im Rahmen der vorliegenden Erfindung nutzbar sind, verweisen wir auf EP 1 172 770 B1 oder EP 1 172 771 B1, sowie auf verschiedene unveröffentlichte deutsche Patentanmeldungen der Anmelderin.

Web-Registrierung:

Die folgenden Daten sind durch die Nutzer bereitzustellen, um sich für die virtuelle Prepaid-/Kreditkarte zu registrieren. Ein Teil der Daten (Nutzername, Passwort, Telefonnummer...) wird später zur Identifizierung und Verifizierung des Nutzers verwendet, und ein Teil der Daten (Bankkonto oder Kreditkartendetails) ist erforderlich zur Handhabung des Geldes.

- > Login-Daten: Nutzername und Passwort
- > Persönliche Daten: Name, Adresse, Geburtsdatum
- > Default-Mobilrufnummer
- > Bankdetails: Bankkontendetails und/oder Kreditkartendetails

Option:

Der Nutzer kann wählen, welches Aufladeverfahren er benutzen möchte. Der Nutzer kann entweder eine virtuelle Prepaidkarte oder eine virtuelle Kreditkarte benutzen. Eine virtuelle Prepaidkarte bedeutet, dass der Betrag der virtuellen Karte vorbezahlt wird. Der Betrag ist nur nutzbar, wenn das Geld bezahlt ist. Optional kann der Nutzer eine normale virtuelle Kreditkarte benutzen. Dies bedeutet, dass die virtuelle Kreditkarte die gleichen Eigenschaften wie eine normale Kreditkarte hat und der Nutzer nicht vorab zahlen muss.

Stimmbasierte Registrierung

Nach einem erfolgreichen ersten Registrierungsschritt erhält der Nutzer/die Nutzerin eine an sein/ihr Mobiltelefon gesandte SMS mit einer PIN und einer Telefonnummer zur Vervollständigung des stimmbasierten Enrolment zur Nutzung des Dienstes direkt vom Mobiltelefon aus, nicht web-basiert. Dies garantiert, dass der Nutzer sich für den stimmbasierten Dienst registrieren bzw. enrolen kann, wann immer er dies zu tun wünscht.

Eine detaillierte Enrolment-Prozedur ist in Fig. 5 dargestellt.

Hinzufügung zusätzlicher Mobilrufnummern

Der Nutzer registriert sich immer mit einer Default-Nummer. Das mit dieser Nummer verknüpfte Mobiltelefon dient als Transportmittel für die virtuelle Kreditkarte, über das der Nutzer eine SMS mit den virtuellen Details erhält. Mit der Default-Nummer führt der Nutzer auch das stimmbasierte Enrolment aus. Im Falle der Hinzufügung einer neuen, zusätzlichen Nummer zur Ermächtigung von Kindern, Ehefrauen/Ehemännern oder anderen Personen gibt es verschiedene Optionen:

Option 1:

Nach Hinzufügung einer neuen Mobilrufnummer sendet das System eine SMS mit einem Bestätigungs-Code an die Mobilrufnummer des Default-Nutzers, um zu bestätigen, dass die neue Nummer korrekt hinzugefügt ist und kein Betrug auftreten kann.

Option 2:

Zu Bestätigungszwecken erhält der Nutzer eine E-Mail auf seinen E-Mail-Account mit einem Aktivierungscode, um die neuen Mobilrufnummern gültig zu machen. Nach Anklicken des Codes wird der Nutzer auf eine Website umgeleitet, um die neue Mobilrufnummer zu aktivieren.

Option 3:

Neue Nummern können zur existierenden und registrierten Default-Nummer hinzugefügt werden, ohne dass es einer Verifizierung einer neuen Nummer bedarf. Diese kann entweder auf der Website und dem Account des Nutzers hinzugefügt und gespeichert werden, oder sie muss jedes Mal eingetippt werden, wenn der Nutzer eine virtuelle Karte aktivieren will.

Option 4:

Die zusätzliche Mobilrufnummer muss jedes Mal eingegeben werden, wenn der Nutzer die virtuelle Kreditkarte an eine andere Mobilrufnummer senden will.

Eine Erläuterung der Nutzung oder der Aktivierungsprozedur der virtuellen Karte wird nachfolgend gegeben, wobei die beiden Basisszenarien, das web-basierte oder das mobiltelefon-basierte Szenario, betrachtet werden.

Web-basiertes Szenario

Um eine neue virtuelle Kreditkarte online zu aktivieren, muss sich der Nutzer online auf seinem Account einloggen. Nach dem Einloggen auf seinem Account kann der Nutzer eine neue virtuelle Karte basierend auf den gespeicherten Daten der physischen Kreditkarte oder des Bankkontos aktivieren. Optional kann der Nutzer wählen, ob er eine virtuelle Prepaidkarte oder ein virtuelle Kreditkarte aktivieren möchte. Dies kann von dem gewählten Zahlungsverfahren ebenso wie von den Vorlieben des Nutzers abhängen.

Als nächsten Schritt muss der Nutzer wählen, welchen Betrag er auf die Prepaidkarte bringen will, bzw. für welchen Betrag er die Kreditkarte aktivieren will. Optional kann der Nutzer auch das Ablaufdatum der Kredit-/Prepaid-Karte wählen.

Der Nutzer/die Nutzerin hat zu wählen, ob er/sie die virtuelle Kreditkarte an die Default-Mobilrufnummer oder eine andere registrierte Mobilrufnummer senden will. Optional kann der Nutzer eine neue Mobilrufnummer eingeben, ohne die neue Nummer zu autorisieren. Sobald der Nutzer die Aktivierung der virtuellen Karte eingeleitet hat, wird eine virtuelle Kartenummer erzeugt und per SMS an den Nutzer gesandt.

Die virtuelle Karte auf dem Mobiltelefon kann für jede Art von Transaktion bei einem Onlinehändler genutzt werden, so lange die Zahlung nicht den aktivierten oder auf die Karte gebrachten Betrag überschreitet.

Mobiltelefon-basiertes Szenario

Um eine virtuelle Karte vom Mobiltelefon aus zu aktivieren, muss der Nutzer von irgendwoher, wo er Mobilnetzabdeckung hat, eine dedizierte Nummer anrufen. Nach Anrufen der Nummer muss sich der Nutzer unter Nutzung der stimmbasierten Authentifizierung identifizieren und authentisieren.

Zur Identifizierung wird die MS-ISDN des Nutzers geprüft. Sie wird mit einer existierenden Datenbasis verglichen, und der Nutzer wird identifiziert. Optional muss der Nutzer eine Nutzer-ID oder einen Nutzercode unter Einsatz des DTMF-Verfahrens oder der Spracherkennung eingeben.

Wenn der Nutzer identifiziert ist, muss er einer Aufforderungs-/Antwort-Prozedur zur Authentifizierung folgen. Das System wird verschiedene Zahlen bereitstellen, die der Nutzer wiederholen muss, um sich zu authentisieren. Optional muss der Nutzer ein gemeinsames Geheimnis (shared secret) per DTMF für einen ersten Authentisierungsschritt eingeben.

Nach erfolgreicher stimmbasierter Authentifizierung wird der Nutzer mit den meisten Optionen wie beim web-basierten Aktivierungs-Szenario versorgt. Der Nutzer muss per DTMF den gewünschten Betrag eintippen, für den er die virtuelle Karte aktivieren will, und den Betrag bestätigen. Optional kann der Nutzer den Betrag

aus einer Liste verfügbarer Beträge unter Nutzung von DTMF oder der Spracherkennung auswählen.

Wenn der Nutzer die Aktivierung der virtuellen Karte initiiert hat, wird eine virtuelle Kartenummer erzeugt und per SMS an den Nutzer gesandt.

Textnachrichten im SMS-Format sind in einer aus derzeitiger Sicht bevorzugten Ausführung des Systems auch die Mittel zur Ausführung von Zahlungsvorgängen sowie zur Aufladung der virtuellen Prepaidkarte oder sogar von physischen Prepaidkarten. Zu ihrer Verarbeitung ist dem Zentralserver des Systems, hier auch als Autorisierungssystem-Server bezeichnet, ein SMS-Gateway als Nachrichtenschnittstelle zugeordnet. Es wird angemerkt, dass neben dem seit langem etablierten Versand von SMS in Mobilfunknetzen mittlerweile auch der Versand ähnlicher Nachrichten in Festnetzen technisch möglich und etabliert ist, so dass das erwähnte Gateway auch als Schnittstelle zu leitungsgebundenen TK-Netzen ausgebildet sein wird.

Sinnvollerweise sind im vorgeschlagenen System verschiedene Standardtypen von SMS oder Bausteinen (templates) für solche vorgegeben, die zur Ausführung bestimmter Vorgänge (Aktivierung der Karte, Aufladung, Zahlungsanweisungen) benutzt werden und nach Empfang beim Server-Gateway mit geringem Verarbeitungsaufwand und daher besonders schnell in Steuerdatensätze zur Auslösung verschiedener elektronischer Transaktionen beim Zahlungsverkehrsserver umgesetzt werden können.

Ein wesentliches Sicherheitsmerkmal des vorgeschlagenen Verfahrens und Systems in einer bevorzugten Ausführung besteht in einem per Rückruf an den Absender eines Transaktions-Auftrages ausgeführten Authentifizierungsschritt. Der Rückruf kann dabei auf dem gleichen Kanal erfolgen, auf dem die eine Transaktion beauftragende elektronische Nachricht versandt wurde (also bei einer Mobilfunk-SMS etwa über das gleiche Mobilfunknetz), es kann aber in Sonderfällen auch gezielt ein anderer Kanal (etwa das Festnetz oder eine Datennetzverbindung) gewählt werden. Zur Authentifizierung des Transaktions-Auftraggebers werden die weiter oben erwähnten oder sonstige bekannte Authentifizierungsmechanismen genutzt,

und sinnvollerweise wird im Rahmen des erwähnten Rückrufes dann eine nutzerfreundliche Menüführung präsentiert, um die benötigten Daten zu erfassen.

Bedeutsam für einen reibungslosen und auf hohe Nutzerakzeptanz orientierten Systembetrieb ist auch der Versand geeigneter Bestätigungsnachrichten (bevorzugt ebenfalls per SMS), sei es an den Auftraggeber einer Prepaidkarten-Aufladung oder sowohl an den Auftraggeber als auch an den Zahlungsempfänger einer elektronischen Überweisung.

Die Ausführung der Erfindung ist nicht auf die oben beschriebenen Beispiele und hervorgehobenen Aspekte beschränkt, sondern ebenso in einer Vielzahl von Abwandlungen möglich, die im Rahmen fachgemäßen Handelns liegen.

Patentansprüche

1. Virtuelle Prepaid- oder Kreditkarte, als Datensatz, frei von einem physischen Substrat, wobei die Daten dazu ausgebildet sind, einen Inhaber zu autorisieren, der in ihrem Besitz ist, für ein Produkt oder einen Dienst zu zahlen, insbesondere im Rahmen einer Online-Transaktion, oder Bargeld zu erhalten, wobei der Datensatz auf der Basis eines Kreditkartenkontos oder einer Vorab-Zahlung auf ein Systemkonto und im Ansprechen auf ein im Ergebnis einer Registrierungsprozedur des Inhabers ausgegebenes Steuersignal erzeugt wird, wobei der Datensatz an einem Telekommunikations-Endgerät, insbesondere einem Mobiltelefon, des registrierten Inhabers zur Anzeige und zum Versenden verfügbar ist.
2. Virtuelle Kredit- oder Prepaidkarte nach Anspruch 1, wobei dem diese definierenden Datensatz ein Verfügungsrahmen-Datensatz zugeordnet ist, der durch ein an das Telekommunikations-Endgerät gesendetes Steuersignal veränderbar ist.
3. Virtuelle Kredit- oder Prepaidkarte nach Anspruch 1 oder 2, wobei eine eindeutige Endgerät-Kennung des Telekommunikations-Endgerätes, insbesondere MSISDN des Mobiltelefons, Teil des die Kredit- bzw. Prepaidkarte definierenden Datensatzes ist.
4. Virtuelle Kredit- oder Prepaidkarte nach Anspruch 3, wobei die Endgerät-Kennung, insbesondere MSISDN, eine Empfangs- und Sendeadresse sämtlicher die Nutzung der Karte betreffenden Nachrichten an den und/oder von dem Inhaber der Karte bestimmt.
5. Virtuelle Kredit- oder Prepaidkarte nach einem der vorangehenden Ansprüche, wobei der diese definierende Datensatz mindestens ein sich auf die zugrunde liegende Registrierungsprozedur, die eine Bewertung biometrischer Merkmale der autorisierten Person einschließt, beziehendes Datum umfasst.

6. Verfahren zur Herstellung einer virtuellen Kredit- Prepaidkarte, als Datensatz, frei von einem physischen Substrat, wobei die Daten dazu ausgebildet sind, einen Inhaber zu autorisieren, der in ihrem Besitz ist, für ein Produkt oder einen Dienst zu zahlen, insbesondere im Rahmen einer Online-Transaktion, oder Bargeld zu erhalten, wobei das Verfahren die Auswertung von Kreditkarten-Kontendaten oder Vorab-Zahlungsdaten und eine Registrierungsprozedur, um den Datensatz zu bilden, und weiter die Übertragung des Datensatzes an ein Telekommunikations-Endgerät des registrierten Inhabers, insbesondere über ein Mobilfunknetz, einschließt.
7. Verfahren nach Anspruch 6, wobei die Authentifizierungsprozedur eine Auswertung biometrischer Merkmale des Inhabers, insbesondere seines Stimmprofils, einschließt.
8. Verfahren nach Anspruch 6 oder 7, wobei mindestens ein die Art und/oder das Ergebnis der Authentifizierungsprozedur kennzeichnendes Datum in den Datensatz eingefügt wird.
9. Verfahren nach einem der Ansprüche 6 bis 8, wobei eine eindeutige Endgerät-Kennung des Telekommunikations-Endgerätes des Inhabers erfasst und in den autorisierenden Datensatz eingefügt wird.
10. Verfahren zur Nutzung einer virtuellen Kredit- oder Prepaidkarte nach einem der Ansprüche 1 bis 5 zum elektronischen Zahlungsverkehr, wobei Zahlungsanweisungen als elektronische Nachrichten vom Telekommunikations-Endgerät des Inhabers an ein Gateway eines Autorisierungssystem-Servers versandt, von diesem geprüft und bearbeitet und im Ansprechen auf ein positives Prüfungsergebnis an einen vom Inhaber bestimmten Zahlungsempfänger weitergeleitet werden.
11. Verfahren nach Anspruch 10, wobei die Weiterleitung als elektronische Nachricht an ein Daten- oder Telekommunikations-Endgerät des Zahlungsempfängers erfolgt.

12. Verfahren nach Anspruch 10 oder 11, wobei die Prüfung im Autorisierungssystem-Server die Prüfung eines Verfügungsrahmen-Datensatzes einschließt, welcher im Ansprechen auf eine Vorab-Zahlung auf ein Systemkonto durch den Inhaber in einem Zahlungsverkehrs-Server erzeugt wird, insbesondere einen ersten Teilschritt der Prüfung des Vorhandensein eines Verfügungsrahmens und, im Ansprechen hierauf, einen zweiten Teilschritt des Vergleichs eines vorhandenen Verfügungsrahmens mit einem in der Nachricht vom Inhaber spezifizierten Zahlungsbetrag.
13. Verfahren nach einem der Ansprüche 10 bis 12, wobei die Prüfung im Autorisierungssystem-Server eine Authentifizierung des Absenders der Zahlungsanweisung, insbesondere mit aktueller Erfassung und Vergleich biometrischer Merkmale mit während der Registrierungsprozedur gespeicherten biometrischen Merkmalen, umfasst.
14. Verfahren nach Anspruch 13, wobei zur Authentifizierung, insbesondere Erfassung der biometrischen Merkmale, im Ansprechen auf den Empfang der elektronischen Nachricht durch den Autorisierungssystem-Server ein Rückruf beim sendenden Telekommunikations-Endgerät und die Ausgabe einer Menüführung auf diesem ausgeführt wird.
15. Verfahren nach Anspruch 14, wobei zur Erfassung eines aktuellen Stimmprofils im Rahmen der Menüführung auf dem Telekommunikations-Endgerät nachzusprechende Ziffern, Textteile oder dergleichen angezeigt und die nachgesprochenen Ziffern, Textteile oder dergleichen akustisch erfasst werden und beim Autorisierungssystem-Server aus diesen ein aktuelles Stimmprofil errechnet wird.
16. Verfahren nach einem der Ansprüche 10 bis 18, wobei die Bearbeitung einer Zahlungsanweisung im Autorisierungssystem-Server die Übermittlung eines Zahlungs-Steuerdatensatzes an einen Zahlungsverkehrs-Server zur Steuerung eines elektronischen Übertrages eines in der Nachricht spezifizierten Zahlungsbetrages auf ein Systemkonto oder system-externes Konto des Zahlungsempfängers einschließt.

17. Verfahren nach einem der Ansprüche 10 bis 16, wobei zur Aufladung der Prepaidkarte mit einem vorbestimmten Betrag eine elektronische Nachricht vom Telekommunikations-Endgerät des Inhabers an ein Gateway eines Autorisierungssystem-Servers versandt und die empfangene Nachricht im Server geprüft und bearbeitet und im Ansprechen auf ein positives Prüfungsergebnis ein Auflade-Steuerdatensatz an einen Zahlungsverkehrs-Server übermittelt wird, wodurch der Aufladungsbetrag auf das Systemkonto des Karteninhabers transferiert wird.
18. Verfahren nach einem der Ansprüche 10 bis 17, wobei die vom der Inhaber abgesandte und/oder die an den bestimmten Zahlungsempfänger weitergeleitete elektronische Nachricht das SMS-Format hat.
19. Verfahren nach Anspruch 18, wobei die Erstellung der elektronischen Nachricht im SMS-Format unter Benutzung von systemintern erzeugten Templates und die Bearbeitung empfangener SMS im Autorisierungssystem-Server unter Erkennung und Vergleich darin enthaltener Templates erfolgt.
20. System zur Bereitstellung einer virtuellen Kredit- oder Prepaidkarte nach einem der Ansprüche 1 bis 5, wobei das System aufweist:
 - einen Zahlungsverkehrs-Server, der Kreditkarten- oder Vorab-Zahlungsdaten eines Nutzers speichert und verarbeitet und elektronische Systemkonten sowie Zahlungsendungen für elektronische Transaktionen von/auf systemexternen Konten speichert,
 - einen Autorisierungssystem-Server, der Nutzerauthentisierungsdaten, insbesondere einschließlich biometrischer Daten des Nutzers, speichert und verarbeitet,
 - eine Kartendatensatz-Erzeugungseinrichtung, die sowohl mit dem Zahlungsverkehrs-Server als auch dem Autorisierungssystem-Server zur Bildung des Datensatzes, der die virtuelle Kreditkarte definiert, und
 - eine Datensatz-Übertragungseinrichtung zum Übertragen des Kostendatensatzes über ein Telekommunikationsnetz, insbesondere ein Mobilfunknetz, an ein mit dem Netz verbundenes Telekommunikationsendgerät.

21. System nach Anspruch 20, wobei dem Zahlungsverkehrs-Server eine Systemkonten-Datenbasis zugeordnet ist, die jeweils einen registrierten Inhaber einer virtuellen Kredit- oder Prepaidkarte zugeordnete elektronische Systemkonten umfasst.
22. System nach Anspruch 21, wobei die Systemkonto-Datenbasis ein elektronisches Deckungs-Systemkonto aufweist, mit dem die Systemkonten durch interne Steuersignalleitungen verbunden sind.
23. System nach einem der Ansprüche 20 bis 22, wobei die Datensatz-Übertragungseinrichtung als SMS-Gateway zum Übertragen des Kartendatensatzes im SMS-Format ausgebildet ist.
24. Anordnung für den elektronischen Zahlungsverkehr, mit einem System nach einem der Ansprüche 20 bis 23, wobei der Autorisierungssystem-Server dazu ausgebildet ist, von den Telekommunikations-Endgeräten von Karteninhabern versandte elektronische Nachrichten zu prüfen, zu bearbeiten und gegebenenfalls weiterzuleiten, wobei die Prüfung eine Prüfung der Nutzerauthentisierungsdaten einschließt und die Bearbeitung die Erzeugung und Übermittlung von Steuerdatensätzen zum elektronischen Übertrag von Zahlungsbeträgen auf/von den Zahlungsverkehrs-Server verwaltete Systemkonten einschließt.

FIG 1



FIG 2

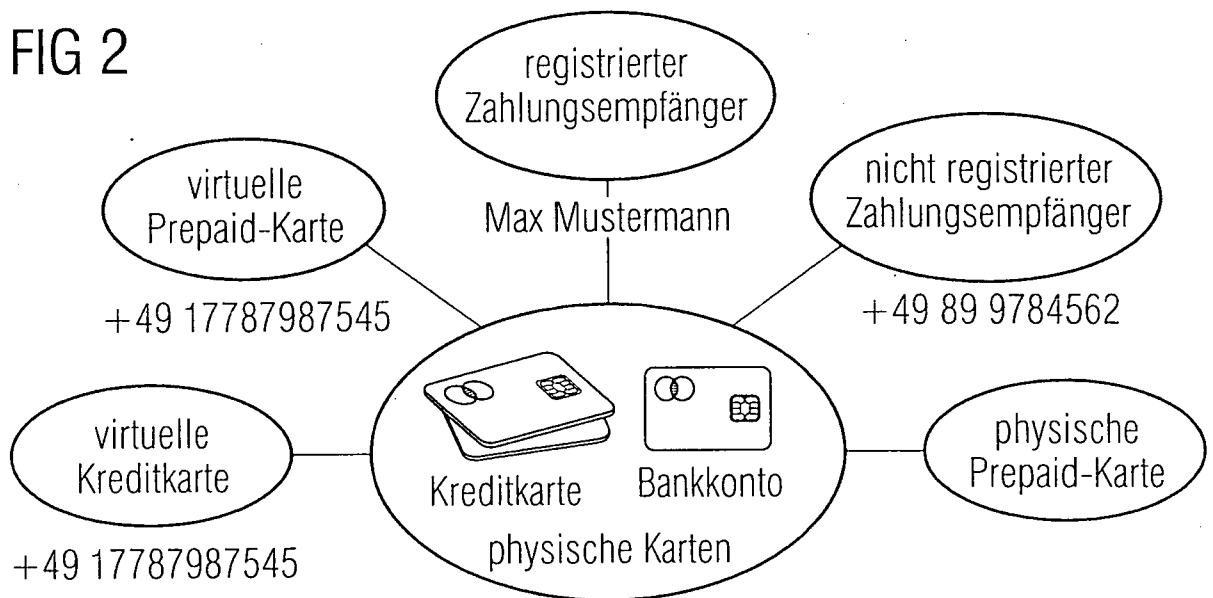


FIG 3

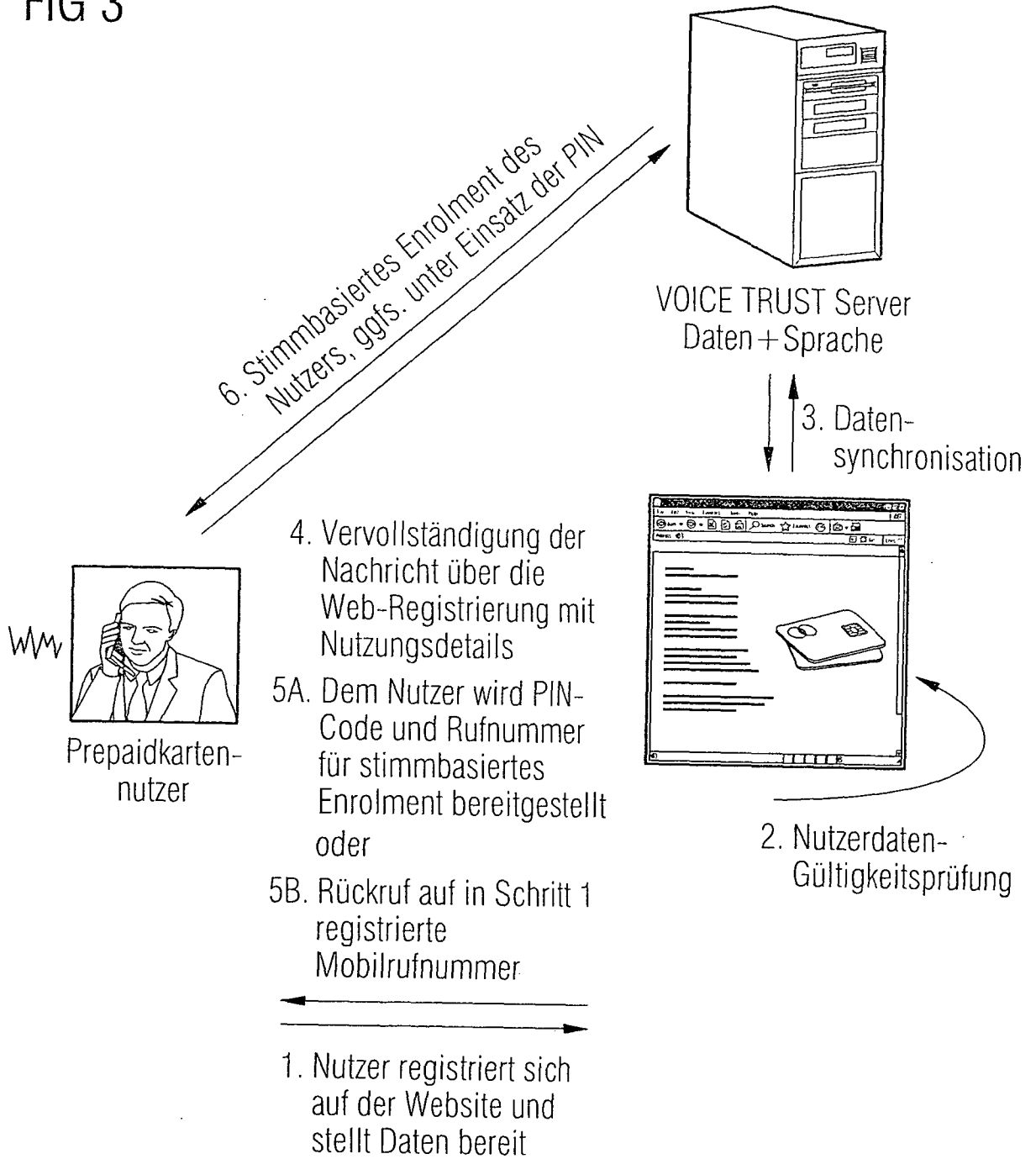
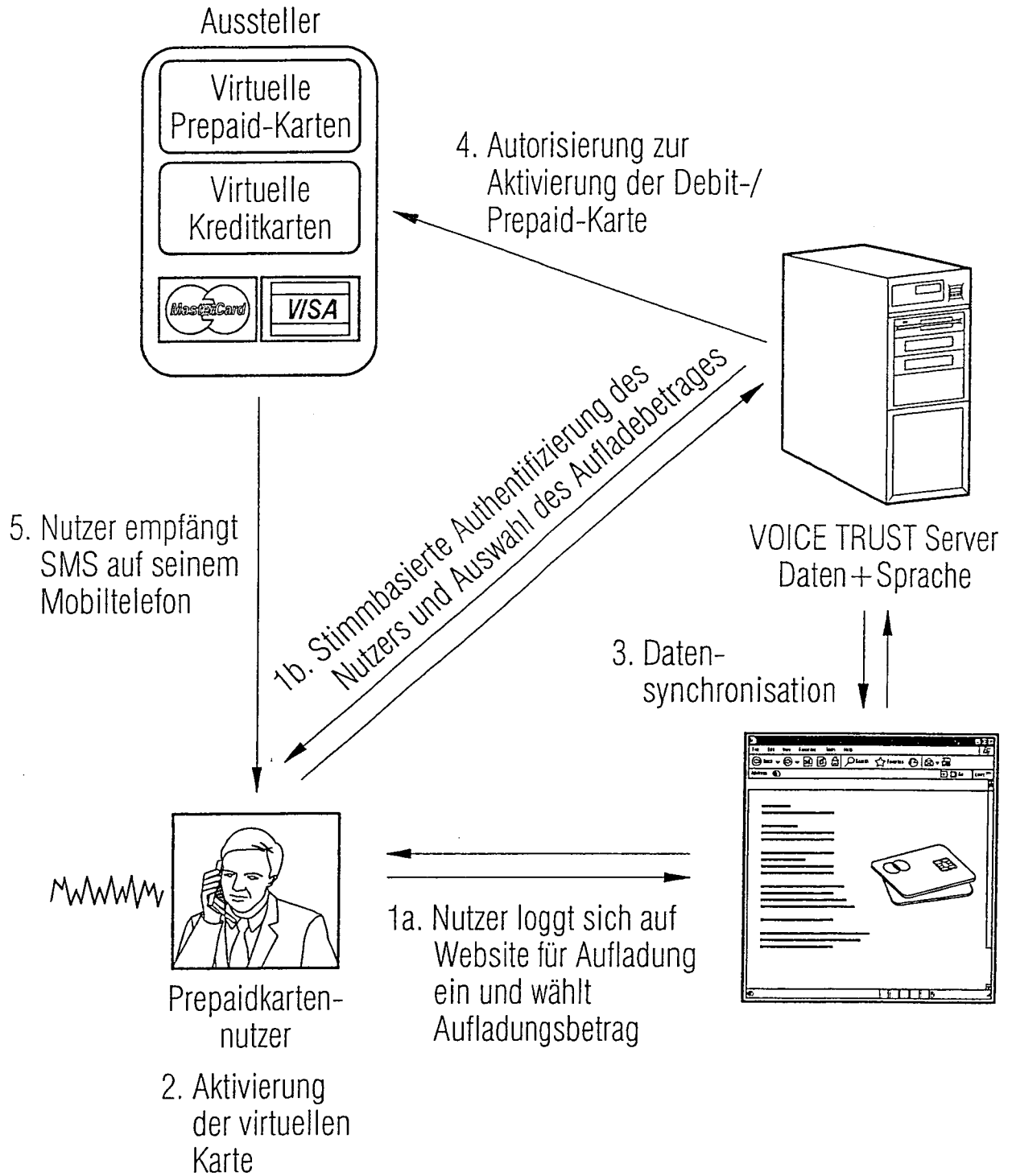


FIG 4



Enrolment

Option 1: Keine MS-ISDN-Prüfung
System: "Willkommen beim FlexCard-Dienst. Um zu starten, bitte geben Sie Ihre Mobilrufnummer ein."
Anrufer: "0-1-7-1-1-2-3-4-5-6-7"

Option 2: MS-ISDN Prüfung
System: <MS-ISDN-Prüfung wird ausgeführt> "Danke für Ihren Anruf."
System: "Als nächstes geben Sie aus Sicherheitsgründen bitte Ihre PIN ein."
Anrufer: "* _ * _ * _ *"
System: "Okay, um Sie in das System zu enrolen, werde ich nach einigen Informationen fragen, die ich nutzen werde, um Ihre Stimme kennen zulernen und Ihren einzigartigen Stimmabdruck zu erzeugen. Dann werde ich bei jedem Anruf von Ihnen in der Lage sein, Ihre Identität unter Nutzung Ihrer Stimme zu verifizieren."
System: "Als nächstes zählen Sie bitte von 0 bis 9 auf diese Weise: '0-1-2-3-4-5-6-7-8-9'. Bitte beginnen Sie jetzt zu zählen."
Anrufer: "0-1-2-3-4-5-6-7-8-9"
System: "Der letzte Schritt besteht darin, dass Sie einige Zufallszahlen wiederholen, denn dies ist das Verfahren, mit dem Ihr Stimmabdruck verifiziert wird, wenn Sie wieder anrufen. Es geht los. Bitte sprechen Sie diese vier Zufallszahlen: Null Zwei Drei Vier"
Anrufer: "0-2-3-4"
System: Bitte wiederholen Sie "Null Zwei Drei Vier"
Anrufer: "0-2-3-4"
System: "Okay Sie sind erfolgreich im System enrollt. Bitte drücken Sie eine beliebige Taste, um Ihre virtuelle Karte zu aktivieren."
Anrufer: "*"
System: "Drücken Sie 1 für eine virtuelle Prepaid-Karte und 2 für eine virtuelle Kreditkarte."
Anrufer: "2"
System: "Bitte geben Sie den Betrag in Euro ein, den Sie auf Ihrer virtuellen Karte aktivieren wollen."
Anrufer: "100"
System: "Sie haben 100 eingegeben. Drücken Sie 1, um die Aktivierung zu initiieren, drücken Sie 2, um einen anderen Betrag einzugeben."
Anrufer: "1"
System: "Danke für den Auftrag. Sie werden eine SMS mit den Details Ihrer virtuellen Kreditkarte erhalten. Auf Wiedersehen!"

Fig. 5

Verifizierung

Option 1: Keine MS-ISDN-Prüfung

System: "Willkommen beim FlexCard-Dienst. Um zu starten bitte geben Sie Ihre Mobilrufnummer ein."

Anrufer: "0-1-7-1-1-2-3-4-5-6-7"

Option 2: MS-ISDN Prüfung

System <MS-ISDN-Prüfung wird ausgeführt> "Danke für Ihren Anruf."

System: "Bitte geben Sie Ihr <gemeinsames Geheimnis> zur Authentifizierung ein."

Anrufer: "* _ * _ * _ * _ *"

System: "Als nächstes müssen Sie einige Zufallszahlen wiederholen. Es geht los. Bitte sagen Sie: Neun Sechs Sieben Vier."

Anrufer: "9-6-7-4"

System: Bitte wiederholen Sie "Neun Sechs Sieben Vier."

Anrufer: "9-6-7-4"

System: "Ihre Identität wurde verifiziert. Jetzt drücken Sie bitte eine beliebige Taste, um eine virtuelle Karte zu aktivieren."

Anrufer: "*"

System: "Drücken Sie 1 für eine virtuelle Prepaid-Karte und 2 für eine virtuelle Kreditkarte."

Anrufer: "2"

System: "Bitte geben Sie den Betrag in Euro ein, den Sie auf Ihrer virtuellen Karte aktivieren wollen."

Anrufer: "100"

System: "Sie haben 100 eingegeben. Drücken Sie 1, um die Aktivierung zu initiieren, drücken Sie 2, um einen anderen Betrag einzugeben."

Anrufer: "1"

System: "Danke für den Auftrag. Sie werden eine SMS mit den Details Ihrer virtuellen Kreditkarte erhalten. Auf Wiedersehen!"

Fig. 6

Enrollment

(Rückruf auf registrierter Nummer)

System: "Lassen Sie jetzt bitte Ihre Stimme registrieren."

System: "OK, um Sie im System zu registrieren, werde ich Sie nach einigen Informationen fragen, die ich verwenden werde, um Ihre Stimme kennen zu lernen und Ihren einzigartigen Stimmabdruck zu erzeugen. Dann werde ich jedes Mal, wenn Sie wieder anrufen, in der Lage sein, Ihre Identität unter Nutzung Ihrer Stimme festzustellen."

Option 1:

System: "Als nächstes, zählen Sie bitte von null bis neun auf diese Weise: 0-1-2-3-4-5-6-7-8-9. Bitte beginnen Sie jetzt zu zählen."

Anrufer: "0-1-2-3-4-5-6-7-8-9"

System: "Der letzte Schritt besteht darin, dass Sie einige Zufallszahlen wiederholen, da dies der Weg ist, auf dem Ihre Stimme verifiziert wird, wenn Sie zurückrufen. Es geht los. Bitte sprechen Sie folgende vier Zufallszahlen: 0-2-3-4."

Anrufer: "0-2-3-4"

System: "Bitte wiederholen Sie: 0-2-3-4."

Anrufer: "0-2-3-4"

Option 2:

System: "Als nächstes zählen Sie bitte auf diese Weise von null bis neun: 0-1-2-3-4-5-6-7-8-9. Bitte beginnen Sie jetzt zu zählen."

Anrufer: "0-1-2-3-4-5-6-7-8-9"

System: "Bitte lesen Sie die Sicherheits-PIN, die Sie auf dem Schirm sehen."

Anrufer: "1-2-3-4"

System: "Bitte lesen Sie die Sicherheits-PIN nochmals."

Anrufer: "1-2-3-4"

Option 3:

System: "Als nächstes nennen Sie bitte Ihren Vor- und Zunamen."

Anrufer: "Mike Miller"

System: "Bitte nennen Sie nochmals Ihren Vor- und Nachnamen."

Anrufer: "Mike Miller"

System: "OK, Sie wurden erfolgreich im System registriert."

Verifizierung

(Prüfung der Nummer und des Inhaltes der SMS, Übereinstimmung mit registrierten Daten)

(Rückruf auf der per MS-ISDN übertragenen Nummer)

Option 1:

System: "Bitte verifizieren Sie Ihre Transaktion. Als nächstes einige Zufallszahlen wiederholen. Es geht los. Bitte sprechen Sie: neun-sechs-sieben-vier"
Anrufer: "9-6-7-4"
System: "Bitte wiederholen Sie: 9-6-7-4."
Anrufer: "9-6-4-7".

Option 2:

System "Bitte verifizieren Sie Ihre Transaktion. Als nächstes lesen Sie bitte die auf Ihrem Schirm angezeigte Sicherheits-PIN.
Anrufer: "3-5-1-8"
System: "Bitte wiederholen Sie."
Anrufer: "3-5-1-8"

Option 3:

System: "Als nächstes sagen Sie bitte Ihren Vor- und Nachnamen."
Anrufer: "Mike Miller"
System: "Bitte sprechen Sie ihren Vor und –Nachnamen nochmals."
Anrufer: "Mike Miller"
System: "Ihre Identität wurde verifiziert. Ihre Transaktion ist ausgeführt. Auf Wiedersehen."

Fig. 8