(19) **Bundesrepublik Deutschland**
Deutsches Patent- und Markenamt

(10) **DE 602 10 270 T2** 2006.12.14

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 354 288 B1**
(21) Deutsches Aktenzeichen: **602 10 270.7**
(86) PCT-Aktenzeichen: **PCT/IB02/00040**
(96) Europäisches Aktenzeichen: **02 729 487.5**
(87) PCT-Veröffentlichungs-Nr.: **WO 2002/056216**
(86) PCT-Anmeldetag: **09.01.2002**
(87) Veröffentlichungstag der PCT-Anmeldung: **18.07.2002**
(97) Erstveröffentlichung durch das EPA: **22.10.2003**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **29.03.2006**
(47) Veröffentlichungstag im Patentblatt: **14.12.2006**

(51) Int Cl.[8]: ***G06Q 20/00*** (2006.01)
G07F 19/00 (2006.01)

(30) Unionspriorität:
0100628 **16.01.2001** **FR**

(84) Benannte Vertragsstaaten:
AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LI, LU, MC, NL, PT, SE, TR

(73) Patentinhaber:
Axalto S.A., Montrouge, FR

(74) Vertreter:
Sparing · Röhl · Henseler, 40237 Düsseldorf

(72) Erfinder:
GUION, Christian, F-91370 Verrière le Buisson, FR;
SAUVEBOIS, Jean-Paul, F-92120 Montrouge, FR

(54) Bezeichnung: **Verfahren, bei de, elektronische Zahlkarten zum Sichern der Transaktionen eingesetzt werden**

Beschreibung

[0001] Die vorliegende Erfindung betrifft ein Verfahren und alle entsprechenden Vorrichtungen zur Umsetzung, bei denen die Zahlkarten zum Sichern der Handelstransaktionen und insbesondere der im Internet durchgeführten elektronischen Transaktionen eingesetzt werden. Die vorliegende Erfindung betrifft insbesondere die Anwendung von elektronischen Zahlkarten, auch Chipkarten genannt, um eine vorübergehende Zahlkartennummer zu bekommen.

[0002] Der Begriff „Zahlkarte" wird hier zur Bezeichnung von allen Geldkarten mit sofortiger oder späterer Abbuchung, allen Kreditkarten usw. verwendet, die von einer Bank oder einem speziellen Geldinstitut ausgestellt werden. Eine Zahlkarte bietet hauptsächlich folgende Dienstleistung an: Der Inhaber der Karte ist entsprechend bestimmten Bedingungen insbesondere hinsichtlich den Beträgen der Transaktionen (Betrag pro Transaktion und/oder pro Woche kumulierte Beträge usw.) dazu fähig, ein Produkt oder eine Dienstleistung bei einem zugelassenen Lieferanten durch einfache Signatur einer Rechnung zu bezahlen. Diese Signatur kann handschriftlich oder elektronisch sein; in diesem Fall muss man einen als PIN-Code (Personal Identification Number) bezeichneten geheimen Code eingeben, wie z. B. eine Folge von vier Ziffern oder aber auch eine alphanumerische Reihe beliebiger Länge.

[0003] Die Zahlkarten werden also auf Verlangen der Kundschaft von Geldinstituten für eine bestimmte Dauer (in der Regel ein bis zwei Jahre und verlängerbar) und für genau bestimmte Zahlungsbedingungen ausgestellt. Diese Karten sind sowohl für ihre Besitzer (Ausstellungsgebühr, Jahresgebühr...) als auch für die akkreditierten Lieferanten zahlungspflichtig, die einen Prozentsatz ihres mittels Geldkarten in Rechnung gestellten Umsatzes rücküberweisen.

[0004] Die dargestellten Vorteile der Zahlkarten sowohl für ihre Inhaber (man braucht kein Bargeld mehr verwalten, man kann auf Kredit bezahlen usw.) als auch für die Lieferanten (Gefahr von Zahlungsausständen praktisch null) führen dazu, dass sich heute die mit Zahlkarte bezahlten Transaktionen verallgemeinern.

[0005] Die Zahlkarten werden materiell von den Ausstellerbehörden in klassischer Form einer rechteckigen ca. 8 cm auf 5 cm großen Karte aus Plastik an ihre Inhaber ausgestellt. Auf der Vorderseite der Karte werden in Reliefschrift der Name des Karteninhabers, ein Verfalldatum, eine Kartennummer (mit 16 Ziffern) sowie eventuell eine Kontonummer geprägt. Die Karte trägt auch den Namen der Ausstellerbehörde sowie verschiedene Motive oder Hologramme, durch die ein Nachmachen erschwert werden soll. Auf der Rückseite der Karte ist ein Feld für die Unterschrift des Karteninhabers vorgesehen.

[0006] Die Zahlkarten sind auf herkömmliche Weise auch mit Magnetstreifen und/oder integrierten Schaltungen versehen, auf denen eine bestimmte Anzahl von Informationen und insbesondere ein Geheimcode, den nur der Karteninhaber alleine kennt, codiert sind. Dabei handelt es sich um den PIN-Code. Durch diese Magnetstreifen oder elektronischen Schaltungen können diese Karten als Zugriffs- und Zahlungsmittel in zahlreichen Automaten sowie in Geldautomaten verwendet werden. Diese Magnetstreifen oder elektronischen Schaltungen dienen auch zur Gewährleistung der Sicherheit der Transaktionen, da sie eine Kontrolle zulassen, ob der Kartenträger tatsächlich der Karteninhaber ist, der in der Tat seinen Geheimcode auf der Tastatur eines Kartenlesegeräts eingeben muss, das die Übereinstimmung der Nummern mit der, die auf den Magnetstreifen oder im elektronischen Schaltkreis abgelesen wird, prüft. Im letzteren Fall wertet das Kartenlesegerät einen Algorithmus mit Geheimschlüssel aus, der innerhalb der integrierten Schaltung der Karte implementiert ist.

[0007] Die Sicherheit der mittels Zahlkarten durchgeführten Transaktionen beruht heute auf zwei Elementen: auf der Kontrolle der Authentizität der vom Karteninhaber auf der Rechnung angebrachten Unterschrift, die handschriftlich oder elektronisch sein kann, und auf der Kontrolle der Authentizität und der Gültigkeit der Karte, indem die Ausstellerbehörde der Karte befragt wird, um die Genehmigung zu erhalten, diese Karte anzunehmen.

[0008] Diese zweifache Kontrolle wird üblicherweise vom Lieferanten vorgenommen, wenn er die Zahlkarte und ihren Inhaber vor sich hat. Die Prüfung der handschriftlichen oder elektronischen Signatur ist in der Tat einfach; dasselbe gilt für die vorausgehende Genehmigungsanfrage. Es gibt zudem Zahlungsterminale und Kartenlesegeräte, die sich zur automatischen Durchführung dieser Kontrollen eignen.

[0009] Der Karteninhaber gibt auf der Tastatur eines solchen Terminals den Geheimcode seiner Karte ein, den man auch PIN-Code nennt (PIN ist die Abkürzung für Personal Identification Number). Die elektronischen Schaltungen vergleichen dann den vom Inhaber eingegebenen Geheimcode mit dem in verschlüsselter Weise auf der Karte eingetragenen Code und validieren die laufende Transaktion, wenn beide übereinstimmen. Außerdem ist der Terminal ausgehend von den auf der Karte gelesenen Informationen in der Lage, über ein Telekommunikationsnetzwerk einen Server zur Zahlkartenverwaltung zu befragen, der bestätigt, ob die Karte tatsächlich gültig und nicht gesperrt ist. Diese Prüfung hinsichtlich der Gültigkeit der Karte kann „online" vor sich gehen, indem der Server während der Transaktion befragt wird

oder auch „offline", dank dem regelmäßigen Fernladen der Listen gesperrter Karten (schwarze Listen oder black lists) und/oder Listen authentischer Karten (positive Listen oder white lists). Es ist festzuhalten, dass durch die Anwendung von Karten mit elektronischen Schaltungen die Authentizität der Karte direkt kontrolliert werden kann.

[0010] Die Befragung der Verwaltungsserver, um den Status der Karte zu kennen, kombiniert mit der Anwendung eines Geheimcodes, den nur allein der Karteninhaber kennt, schränkt in der Regel den Betrug bei den mit Zahlkarten beglichenen Transaktionen ein und macht sie somit zu einem der sichersten Zahlungsmittel.

[0011] Das gleiche gilt allerdings nicht mehr, wenn der Karteninhaber und der Lieferant weit voneinander entfernt sind und wenn die Anwendung eines Zahlungsterminals und Kartenlesegeräts, insbesondere zum Testen des Geheimcodes der Karte, also nicht möglich ist.

[0012] In der Tat, zur Durchführung einer Transaktion, wenn der Karteninhaber und der Lieferant weit voneinander entfernt sind, zum Beispiel beim Kauf über Katalog und Versand oder bei einer telefonischen Reservierung oder auch bei einer elektronischen Transaktion im Internet, muss der Karteninhaber heute offen Informationen über seine Karte, wie z. B. die Nummer seiner Zahlkarte und deren Verfalldatum, mitteilen. Die Übertragung dieser einzigen Informationen reicht, um eine Rechnung zu validieren, die der Lieferant dann zur Begleichung der Ausstellerbehörde der Karte vorliegt.

[0013] Aufgrund des derzeitigen einfachen Mechanismus zur Zahlung per Zahlkarte der auf Distanz durchgeführten Transaktionen kommt es zu zahlreichen Betrügen, da jeder, der die Nummer einer Zahlkarte und deren Verfalldatum kennt, diese Informationen auf illegale Art verwenden kann, um Produkte oder Dienstleistungen zu kaufen und zwar solange bis der eigentliche Eigentümer der Karte die Veruntreuung merkt, der er zu Opfer gefallen ist und die Karte bei der Ausstellerbehörde gesperrt wird.

[0014] Zudem lässt das System auch übertriebene Verleugnungen seitens verantwortungsloser Käufer zu, die verweigern, dass ihr Konto belastet wird mit dem Vorwand, dass die Transaktionen ohne ihre Kenntnis durchgeführt wurden.

[0015] Dies gilt insbesondere für die im Internet vorgenommenen elektronischen Transaktionen, da es in einem derart offenen Kommunikationsnetzwerk besonders einfach ist, die hier ausgetauschten Informationen abzufangen. Diese Unsicherheit bremst derzeit den Handel im Internet sehr.

[0016] Es wurden zahlreiche Versuche unternommen, um diesen Nachteil zu beseitigen und die Transaktionen auf Distanz und vor allem die elektronischen Transaktionen sicherer zu gestalten.

[0017] Unter diesen Versuchen kann man die Systeme der Art SET aufführen, die darin bestehen, die im Internet ausgetauschten Informationen zu verschlüsseln. Mit solchen Systemen werden die Nummern von Geldkarten nicht mehr offen mitgeteilt und können also nicht mehr abgefangen werden.

[0018] Ein solches System erscheint in der Tat als relativ sicher, da man keinen Zugriff mehr auf die Nummer der Zahlkarte des Inhabers hat, es erscheint aber auch schwer und nur mit viel Aufwand umzusetzen, da es hundert Tausende von kommerziellen Webseiten, Tausende von Geldinstituten und Millionen von Kunden betrifft.

[0019] Um diese Nachteile abzuschaffen, besteht eine von der Patentanmelderin entwickelte Lösung darin, dass jeder Anwender von einem geeigneten Server, der von seinem Geldinstitut verwaltet wird, eine virtuelle Geldkarte erhält, die nur für eine begrenzte Anzahl von Transaktionen und vorzugsweise nur für eine einzige Transaktion gültig ist. Der Anwender beantragt diese also bei jeder Transaktion und sobald er sie erhalten hat, braucht er nur noch die Nummer dieser Karte bei der Bestätigungsphase mit der kommerziellen Site eingeben. Die kommerzielle Site nimmt diese Nummer an, ohne mit einer reellen Kartennummer zu unterscheiden und bearbeitet die Transaktion auf gleiche Art. Dieses System ist also hinsichtlich der Infrastruktur der kommerziellen Sites ganz neutral. Außerdem kann, wenn diese Nummer geraubt wird, sie nicht erneut verwendet werden, da die Nummer, sobald eine Transaktion verzeichnet wurde, inaktiviert wird und nicht mehr dazu dienen kann, das Konto des Anwenders zu belasten.

[0020] Es wurden unterschiedliche Arten des Ausstellens einer solchen Karte entwickelt und insbesondere die, die darin besteht, ein Handy dazu zu benutzen. Zum Beispiel beschreibt das Dokument WO-A-99/49424 ein gesichertes Transaktionssystem für den Kommerz zwischen einem Händler und einem Anwender, das auf der Anwendung von Kreditkarten mit beschränktem Einsatz besteht und damit die Funktionen einer Kreditkarte eröffnet, ohne dabei jemals die Nummer der Hauptkreditkarte des Anwenders preis zu geben. Ziel der vorliegenden Patentanmeldung ist es, eine besondere Art des Ausstellens einer virtuellen Karte darzustellen, die eine echte Zahlkarte benutzt.

[0021] Wie vorausgehend aufgeführt, ist eine echte Zahlkarte mit Mikroprozessor (oder Chip) in der Tat ein extrem gesichertes Instrument, wenn sie zusammen mit geeigneten Zahlungsterminals eingesetzt

wird.

[0022] Die vorliegende Erfindung zielt also darauf ab, eine neue Lösung zur Ausgabe der virtuellen Karten vorzuschlagen, wobei diese Erfindung echte Zahlkarten mit einbezieht und dabei trotzdem einfach und günstig bleibt.

[0023] Das erfindungsgemäße Verfahren strebt die Sicherung einer kommerziellen Transaktion zwischen einem Lieferanten und einem Käufer an, für die der Käufer persönliche Daten wie z. B. die Nummer einer Zahlkarte mitteilen muss.

[0024] Die Erfindung ist durch den Gegenstand von Anspruch 1 definiert. Das Verfahren besteht darin, mittels einer ersten Zahlkarte mit Mikroprozessor eine zweite Zahlkarte einer geeigneten Ausstellerbehörde zu erhalten und die Daten der zweiten Karte wie z. B. ihre Nummer bei der Transaktion zu verwenden, wobei die zweite Karte nur für eine begrenzte Anzahl von Transaktionen gültig ist.

[0025] Gemäß eines anderen Merkmals des erfindungsgemäßen Verfahrens wird die zweite Zahlkarte über das Internet erhalten, indem eine Verbindung mit einem Server hergestellt wird, der von der Ausstellerbehörde verwaltet wird.

[0026] Gemäß eines anderen Merkmals des erfindungsgemäßen Verfahrens identifiziert sich der Anwender bei dieser Verbindungsherstellung dadurch, dass er seine erste Zahlkarte verwendet, die in ein Lesegerät gesteckt und mit einem Computer verbunden ist, und dies, um eine geeignete Mitteilung an einen Server zu adressieren.

[0027] Gemäß eines anderen Merkmals des erfindungsgemäßen Verfahrens ist die Mitteilung, die vom Anwender über seine erste Karte an den Server adressiert wird, eine Authentifizierungs- und Unversehrtheitsbescheinigung des Ausstellers, die Daten und eine Signatur kombiniert, wobei die Signatur durch Verschlüsseln dieser Daten durch einen Verschlüsselungsalgorithmus erreicht wird, der in der besagten ersten Karte enthalten ist.

[0028] Gemäß eines anderen Merkmals des erfindungsgemäßen Verfahrens wird die Mitteilung, die vom Anwender über seine erste Karte an den Server adressiert wird, nach der Eingabe eines Geheimcodes erzeugt, der der ersten Karte zugeordnet ist und den nur der Anwender allein kennt.

[0029] Gemäß eines anderen Merkmals des erfindungsgemäßen Verfahrens wird die Mitteilung, die vom Anwender über seine erste Karte an den Server adressiert wird, vom Server benutzt, um die zweite Karte und insbesondere ihre Nummer zu erstellen.

[0030] Gemäß eines anderen Merkmals des erfindungsgemäßen Verfahrens ist die zweite Zahlkarte nur für eine einzige Transaktion gültig.

[0031] Gemäß eines anderen Merkmals des erfindungsgemäßen Verfahrens ist die zweite Zahlkarte nur für eine begrenzte Dauer zwischen mehreren zehn Sekunden und einigen Tagen gültig.

[0032] Gemäß eines anderen Merkmals des erfindungsgemäßen Verfahrens umfasst die zweite Zahlkarte eine Kartennummer und ein Verfalldatum, deren Formate mit denen der ersten Zahlkarte identisch sind, sodass sie von den Händlern nicht unterschieden werden können.

[0033] Gemäß eines anderen Merkmals des erfindungsgemäßen Verfahrens handelt es sich bei den betreffenden Transaktionen um elektronische Transaktionen im Internet und Web.

[0034] Anhand der folgenden Beschreibung einer Ausführungsweise der Erfindung, die als nicht einschränkendes Beispiel aufgeführt wird und in Anlehnung auf beiliegende Abbildung wird man die Zielsetzungen, Aspekte und Vorteile der vorliegenden Erfindung besser verstehen.

[0035] Die Fig. 1 ist eine schematische Darstellung des Systems, das für die Anwendung einer elektronischen Transaktion gemäß der vorliegenden Erfindung notwendig ist.

[0036] Bezugnehmend auf die Zeichnung wurden nur die für das Verständnis der Erfindung nützlichen Elemente aufgeführt.

[0037] Das gewählte Beispiel zur Darstellung des erfindungsgemäßen Verfahrens betrifft eine elektronische Transaktion, die über das Internet durchgeführt wird. Auch wenn sie sich besonders gut für die elektronischen Transaktionen im Internet eignet, beschränkt sich die Erfindung nicht auf diese Transaktionen allein, sondern bezieht sich ganz allgemein auf alle Transaktionen, die mittels Zahlkarten beglichen werden.

[0038] Mit dem in Fig. 1 dargestellten System kann also in aller Sicherheit eine elektronische Transaktion zwischen einem Anwender und einer entfernten kommerziellen Site, die mit **7** bezeichnet wird, abgewickelt werden.

[0039] Der nicht aufgeführte Anwender befindet sich vor einem Terminalgerät, das zum Beispiel sein PC **5** ist. Dieser Computer **5** ist an das Internet **6** angeschlossen und ermöglicht den Zugang zu einer kommerziellen Website **7**.

[0040] Der Anwender hat darüber hinaus eine Zahl-

karte **1** mit einem elektronischem Schaltkreis, die man auf herkömmliche Art bei einem geeigneten Geldinstitut erhält, das durch einen Server **10** für die rechnergestützte Verwaltung von Zahlkarten **1** dargestellt ist.

[0041] Die Zahlkarte **1** liegt in der herkömmlichen Form eines flachen Rechtecks aus Plastik mit den ISO-Abmessungen von ca. 8 cm auf 5 cm vor, in das ein Mikroprozessor eingesetzt ist. Diese Karte **1** kann versenkte elektrische Kontakte aufweisen oder aber auch kontaktlos sein.

[0042] Auf der Vorderseite der Karte sind der Namen **4** des Karteninhabers, ein Verfalldatum **3**, eine Kartennummer **2** mit 16 Ziffern, die auch PAN-Code bezeichnet wird, sowie eventuell eine Kontonummer eingetragen.

[0043] Die Karte **1** verfügt zudem über eine zusätzliche Nummer über drei Ziffern, die als CVV bezeichnet wird. Diese CVV-Nummer kann als Erweiterung zum PAN **2** dienen, wodurch letzterer auf 19 Ziffern gebracht wird (erweiterter PAN) und somit die Sicherheit der Transaktionen verbessert. Diese drei Ziffern sind zum Beispiel das Ergebnis einer Berechnung mit einem Verschlüsselungsschlüssel, der am PAN mit 16 Ziffern angewendet wird. Die CVV ist nicht auf der Karte eingeprägt, im Gegensatz zum PAN, und erscheint nur auf der Rückseite der Karte geschrieben, im Feld der Unterschrift. Die CVV erscheint also auf keinem Beleg und nur der, der die Karte in der Hand hält, kann diese Ziffern lesen und sie beim Ablesen angeben, wenn man von ihm seinen erweiterten PAN verlangt. Die von Hand im POS-Zahlungsterminal von einem Händler eingegebenen Ziffern werden von der Ausstellerbehörde der Karte bei der Anfrage um Genehmigung geprüft.

[0044] Es ist allseits bekannt und deshalb braucht man auch nicht weiter auf die Details eingehen, dass die Ausstellerbehörde der Karte **1** mit einem Server **10** ausgestattet ist, der sich zur Ausgabe und Verwaltung der Zahlkarten und der mittels dieser Karten vollzogenen Transaktionen eignet. Dieser Server **10** kann allein die Verwaltung seiner Karten übernehmen oder er kann sich an einen zentralen Server **9** wenden, der insbesondere im Auftrag von mehreren Geldinstituten die gültigen und gesperrten Karten verwaltet.

[0045] Auf genau dieselbe Art und Weise verfügt der Lieferant und Eigentümer der kommerziellen Site **7** über ein Bankkonto bei einem Geldinstitut, das einen Verwaltungsserver **8** besitzt, wobei das Geldinstitut des Lieferanten das gleiche sein kann wie das des Karteninhabers oder auch auch nicht.

[0046] Der Inhaber der Zahlkarte **1** ruft also auf seinem Computer **5** eine Seite des Servers der kommerziellen Site **7** auf, auf der man ihm einen Artikel zum Kauf anbietet. Nach dem Entschluss diesen Artikel über den Server der kommerziellen Site **7** zu erwerben, löst der Inhaber also die Bestellung aus, die er validieren muss, indem er die vom Lieferanten geforderten Zahlungsdaten vorliegt und insbesondere die Referenzen einer Zahlkarte.

[0047] Der Anwender vollzieht also, wie im Anschluss näher erklärt, die Eröffnung einer zweiten Sitzung über das Internet, um auf einen Server **101** Zugriff zu haben, der ihm eine virtuelle Zahlkarte **11** ausstellt, die im Anschluss als VPC bezeichnet wird. Nach Erhalt dieser virtuellen Zahlkarte **11** ist der Anwender dazu fähig, die Daten dieser Karte an den Server der kommerziellen Site **7** zu übertragen. Dazu tippt der Inhaber einfach diese Daten auf der Tastatur seines Computers **5** und überträgt sie über das Internet an den Server der kommerziellen Site **7**. Die Kommunikation verläuft nach dem für den Server der kommerziellen Site **7** gültigen Protokoll, d. h. auf offene Weise oder auf durch eine geeignete Verschlüsselungssoftware verdeckte Weise (DES, RSA usw.).

[0048] Der Lieferant prüft dann die Gültigkeit dieses Zahlungsmittels, entweder über sein Geldinstitut **8**, über den zentralen Server **9** oder aber direkt beim Server **101**. Nach rückwärtigen Erhalt der verlangten Genehmigung wird die Transaktion validiert bzw. das bestellte Produkt oder die bestellte Dienstleistung werden an den Anwender ausgeliefert. Der Lieferant braucht dann nur noch die entsprechende Rechnung an sein Geldinstitut übergeben, damit dieses den Transfer der Summen vollziehen kann.

[0049] Die VPC-Zahlkarten **11** entsprechen hinsichtlich den angebotenen Leistungen ganz und gar der Karte **1**; der wesentliche Unterschied liegt darin, dass sie nur für eine begrenzte Anzahl von Transaktionen gültig sind. Vorzugsweise sind die VPC-Karten **11** nur für eine einzige Transaktion gültig und vorzugsweise haben sie auch nur eine relativ kurze Lebensdauer zwischen mehreren zehn Sekunden und einigen Tagen.

[0050] Obwohl diese VPC-Zahlkarten **11** für alle kommerziellen Transaktionen verwendet werden können, eignen sie sich besonders gut für die Transaktionen auf Distanz und insbesondere die Transaktionen über das Internet. Die VPC-Zahlkarten **11** können insbesondere keinen materiellen Träger haben (vorübergehende Anzeige auf einem Bildschirm oder auch verbale Kommunikation) oder nur einen sporadischen materiellen Träger haben, wie z. B. ein einfaches Papierdokument (von einem Terminal ausgedrucktes Ticket, Fax, Schreiben usw.). Sie können jedoch auch denselben Träger haben wie eine herkömmliche Karte: Magnetkarte oder Karte mit elektronischem Schaltkreis.

[0051] Abgesehen , von diesen Unterschieden entsprechen die VPC-Zahlkarten **11** voll und ganz den anderen Karten, insbesondere hinsichtlich Format und Codierung ihrer PAN-Nummern **12** oder ihres Verfalldatums **13** (Format mit vier Ziffern: Monat/Jahr (08/00)). Daher umfasst jede PAN-Nummer **12** in Anlehnung an die herkömmlichen Zahlkarten **1**, die PAN-Nummern **2** mit 16 Ziffern umfassen, ebenfalls 16 Ziffern: die ersten sechs Ziffern bilden den BIN-Code des Geldinstituts, das zugleich Ausstellerbehörde ist und die letzte Ziffer den Authentifizierungscode von Luhn. Selbstverständlich ist das Format mit 16 Ziffern für die Erfindung nicht einschränkend, die PAN-Nummern **2** und **12** können jedes andere Format annehmen: eine Reihe mit 19 Ziffern, eine alphanumerische Reihe von bestimmter Länge usw.

[0052] Außerdem ist es möglich, jeder VPC-Karte **11** einen Geheimcode **14** zu erteilen, den man auch PIN-Code nennt (Personal Identification Number). Die Karte **11** umfasst also ebenfalls in genauerer Weise Datum und Uhrzeit des Gültigkeitsendes 16 (z. B. im Format Tag/Monat/Jahr Uhrzeit (22/08/00 10:31)). Diese Information 16 ist allein für den Inhaber der Karte **11** bestimmt, während die Information **13** zur Mitteilung an den Lieferanten bestimmt ist, wie bei einer Transaktion mit der Karte **1**.

[0053] Ebenso kann jede VPC-Karte **11** eine geeignete CVV-Nummer erhalten, durch die ein erweiterter PAN mit 19 Ziffern erreicht wird.

[0054] Der Inhaber der VPC-Karte **11** ist also ganz und gar in der Lage, auf dieselbe Weise wie mit seiner Karte **1** eine elektronische Transaktion mit der kommerziellen Site **7** zu bezahlen.

[0055] Da die vom Inhaber eingegebene PAN-Nummer **12** genau der PAN-Nummer **2** entspricht, braucht der Lieferant seine Verfahren für die Transaktionen nicht zu ändern, um die Bestellung des Inhabers der Karte **11** zu akzeptieren. Für den Lieferanten besteht damit kein Unterschied zwischen einer mittels einer VPC-Karte **11** bezahlten Transaktion und einer Transaktion, die mit einer herkömmlichen Zahlkarte **1** bezahlt wird. Der Lieferant hat übrigens keine Möglichkeit die Nummern und damit die Art der ihm übermittelten Zahlkarten zu unterscheiden.

[0056] Die Schaffung solcher VPC-Karten **11** ermöglicht, die bestehenden Validierungsverfahren der zwischen Lieferanten und Käufern eingerichteten Transaktionen nicht in Frage zu stellen.

[0057] Die Lieferanten bewahren auch ihre aktuellen Validierungsverfahren der von ihren Kunden erhaltenen Bankinformationen. Von ihnen wird einfach verlangt, die Gültigkeit der Karte zu überprüfen, von der sie die Daten erhalten haben, da die Karte nur eine sehr kurze Lebensdauer haben kann. Es handelt sich dabei jedoch um eine bereits bei fast allen der kommerziellen Sites angewendeten Aktion, die, bevor sie die Transaktion akzeptieren und das entsprechende Produkt oder die entsprechende Dienstleistung liefern, bei der Ausstellerbehörde oder einem zentralen Server **9** eine Genehmigung verlangen und zwar um zu prüfen, ob die Karte, die ihnen vorgelegt wird, tatsächlich authentisch ist, dass sie nicht gesperrt ist bzw. dass der Transaktionsbetrag nicht die finanzielle Stärke der Karte überschreitet.

[0058] Außerdem sind auf Seite der Geldinstitute von Lieferanten die Einzugsverfahren der Rechnungen identisch, unabhängig davon, ob sie von VPC-Zahlkarten **11** oder von traditionellen Karten **1** stammen.

[0059] Unabhängig von der Tatsache, ob eine VPC-Karte **11** nur für eine bestimmte Anzahl von Transaktionen und vorzugsweise für eine einzige Transaktion gültig ist, kann die durch Anwendung einer solchen Karte gebotene Sicherheit noch verstärkt werden, indem die Anwendung dieser Karte auf einen bestimmten Händler **7** begrenzt wird oder auf einen nach oben hin eingeschränkten Betrag oder auf den exakten Betrag der Transaktion, für die die VPC-Karte **11** verlangt wurde.

[0060] Der Anwender, der eine VPC-Karte **11** bekommen möchte, hat mehrere Möglichkeiten zur Auswahl. Insbesondere kann er den Server **101** über ein Handy anrufen, wie dies in der vorab genannten und vom Antragsteller angemeldeten Patentanmeldung WO 02/19284 detailliert wurde. Die vorliegende Erfindung hat eine andere Lösung zum Gegenstand, bei der das Internet **6** und die Bankkarten mit Mikroprozessor vom Typ **1** verwendet werden.

[0061] Gemäß der Erfindung verfügt der Server **101** also über eine IP-Adresse und ist ausgehend vom Computer **5** des Anwenders über das Internet **6** zugänglich. Der Anwender braucht also nur mit der Site des Servers **101** eine Internetverbindung herzustellen und eine VPC-Karte **11** zu verlangen, damit diese dafür auf dem Bildschirm seines Computers **5** angezeigt wird. Um die Sicherheit einer solchen Anfrage zu gewährleisten und jeglichen Betrug zu vermeiden, ist es erforderlich, dass der Anwender sich auf sichere Art beim Server **101** während seiner Verbindungsherstellung identifizieren kann.

[0062] Diese Identifizierung wird dank der Anwendung der Geldkarte mit Mikroprozessor **1** möglich, über die der Anwender verfügt, sowie dank den in dieser Karte **1** enthaltenen kryptografischen Ressourcen, wie z. B. ein Verschlüsselungsalgorithmus vom Typ DES (DES: Data Encryption Standard) oder anderer Art (RSA, usw.). Dazu braucht man nur bei der Verbindungsherstellung mit dem Server **101** an diesen eine Mitteilung senden, die mittels kryptogra-

fischer Ressourcen der Karte **1** verschlüsselte Daten enthält. Der Server **101**, der über entsprechende Ressourcen verfügt, ist also dazu fähig, die Authentizität der Mitteilung zu prüfen und daraus die Identität des Anwenders abzuleiten, da nur dieser allein dazu in der Lage ist, materiell über die Karte **1** zu verfügen und nur diese Karte **1** dazu fähig ist, eine solche Mitteilung abzugeben.

[0063] Die Umsetzung eines solchen Verfahrens ist relativ einfach, da das Senden einer solchen Mitteilung bereits in den Geldkarten mit Mikroprozessor **1** vorgesehen ist. Bei einer mittels Zahlungsterminal durchgeführten Transaktion adressiert der Terminal in der Tat die Daten der Transaktion an den Bankserver: Referenz des Händlers, Referenz der Karte, Betrag und Datum der Transaktion usw.

[0064] Diese Daten werden zusammen mit einer elektronischen Signatur, die aus der Verschlüsselung dieser Daten ausgehend von in der Geldkarte (Karte mit Mikroprozessor) oder im Terminal (Magnetkarte) enthaltenen kryptografischen Programmen gebildet wird, an den Bankserver adressiert. Diese Daten und Signatur bilden die Authentifizierungs- und Unversehrtheitsbescheinigung des Ausstellers, die auch CAI genannt wird. Diese CAI wird vom Bankserver geprüft, um die Transaktion zwischen dem Händler und seinem Kunden zu authentifizieren.

[0065] Der Bankserver prüft die CAI durch Vergleich der Signatur, die durch einen reziproken Verschlüsselungsalgorithmus bearbeitet wird, sowie den sie begleitenden Daten bzw. durch Anwendung des gleichen Verschlüsselungsalgorithmus auf diese Daten und durch Vergleich der erhaltenen Signatur mit der übertragenen. Es ist festzuhalten, dass die CAI (Daten und Signatur) vorzugsweise in verschlüsselter Form übertragen wird, sie kann jedoch auch in Klartext übertragen werden.

[0066] Die Berechnung der Signatur und das Senden der CAI wird in der Regel durch die Eingabe des Geheimcodes oder PIN-Codes durch den Anwender auf der Tastatur des Zahlungsterminals ausgelöst. Das Erkennen des PIN-Codes durch die Karte startet das Rechenprogramm der Signatur über die Daten der Transaktion, die vorab eingegeben worden sind.

[0067] Gemäß der Erfindung geht es also bei der Verbindungsherstellung zum Server **101** darum, ihm eine Mitteilung in der Art einer CAI zu adressieren, wobei die Prüfung dieser CAI durch den Server **101** die Identität des Anwenders garantiert.

[0068] Dazu muss der Anwender über ein Lesegerät für Geldkarten **51** verfügen, das an seinen Computer angeschlossen ist, um Zugang zu den Software-Ressourcen seiner Karte **1** zu bekommen.

[0069] Wenn der Computer eine entsprechende Software vom Typ Emulation eines Bankterminals POS hat, wird der Anwender mit seinem Computer und seinem Kartenlesegerät die Rolle eines solchen Bankterminals simulieren und an den Server **101** eine Authentifizierungs- und Unversehrtheitsbescheinigung bzw. CAI adressieren, und der Server **101** veranlasst erst nach Eingang und Prüfung dieser CAI das Senden einer VPC-Karte **11**.

[0070] Der Softwarezugriff auf die Karte erfolgt also auf herkömmliche Weise durch Vorlage des PIN-Codes. Man kann ein gesichertes Lesegerät **51** mit Tastatur **51** verwenden, aber man kann genauso gut auch ein Lesegerät ohne Tastatur verwenden, z. B. vom Typ Reflex **72**, das von der Firma Schlumberger kommerzialisiert wird; in diesem Fall wird der PIN-Code direkt über die Tastatur des Computers erfasst. Im Fall von Bankkarten mit Kryptoprozessor (Schlumberger-Karten Palmera Protect) kann man auch die Anwendung eines verschlüsselten PIN-Codes (vom Server ausgegeben) in Erwägung ziehen.

[0071] Die Eingabe des PIN-Codes als Klartext auf der Tastatur des Computers **5** stellt keine Gefahr dar. Der alleinige Zugriff auf einen PIN-Code ist nicht von Interesse, wenn man nicht gleichzeitig über die dazugehörige materielle Karte verfügt.

[0072] Sobald die Karte **1** den PIN-Code erkannt hat, ist diese dazu fähig, die Signatur einer Transaktion zu erzeugen und also eine Authentifizierungs- und Unversehrtheitsbescheinigung des Ausstellers oder CAI abzugeben. Die Karte **1** ermöglicht die Emission dieser Bescheinigung durch das Ablaufverfahren einer Transaktion.

[0073] Vor der Eingabe seines PIN-Codes als Klartext oder verschlüsselt gibt der Anwender also die Daten einer fiktiven Transaktion ein, die nur zum Erstellen einer CAI für den Server **101** dient und insbesondere einen Transaktionsbetrag, wobei dieser Betrag entweder derselbe ist als der der mit dem Server **7** laufenden Transaktion, für die die VPC-Karte **11** verlangt wurde oder aber auch nicht. Selbstverständlich wird diese Transaktion, die nur zum Erhalt einer VPC-Karte dient, nie vom Konto des Anwenders abgebucht.

[0074] Die Bescheinigung wird also mit dem Verschlüsselungsalgorithmus (DES usw.) der Karte **1** und eventuell mit einem Sendeschlüssel CTO berechnet. Unter den zu zertifizierenden Daten kann neben dem Betrag, wenn vorhanden, das Kennzeichen des Akzeptors aufgeführt werden oder ein vereinbarter Code.

[0075] Die Bescheinigung wird an den Server **101** gesendet, wo sie zur Prüfung durch Vergleich der durch einen reziproken Verschlüsselungsalgorithmus

bearbeiteten Signatur und den sie begleitenden Daten oder durch Anwendung desselben Verschlüsselungsalgorithmus an diesen Daten und durch Vergleich der erhaltenen Signatur mit der übertragenen neu berechnet wird. Diese CAI wird vorzugsweise in verschlüsselter Form an den Server **101** übertragen, aber sie kann auch im Klartext übertragen werden.

[0076] Nach der Prüfung der Authentizität der CAI durch den Server **101** ist dieser in der Lage, also auf sichere Weise den Anwender zu identifizieren, denn ein Dritter, der weder über die Karte **1** noch über den entsprechenden PIN-Code verfügt, nicht dazu fähig ist, eine authentische CAI zu erzeugen. Wenn der Anwender mit Gewissheit identifiziert wurde, kann ihm der Server **101** dafür also seine VPC-Karte **11** zusenden.

[0077] Es ist festzuhalten, dass die so vom Anwender an den Server **101** adressierte CAI verwendet werden kann, um die VPC-Karte **11** zu erstellen und insbesondere seine PAN-Nummer **12** oder auch die CVV.

[0078] Somit kann sich der Anwender dank der vorliegenden Erfindung auf sichere Weise beim Server **101** identifizieren und das Internet nutzen und dies ohne die Gefahr eines Betrugs, indem er einfach die Funktionen der aktuellen und zukünftigen Geldkarten nutzt und insbesondere ihre Fähigkeit eine CAI-Ausstellerbescheinigung als Mittel zur Authentifizierung und Identifikation zu erzeugen. Die vorliegende Erfindung erfordert also keine umfangreichen materiellen Ressourcen zu ihrer Umsetzung, da alle Arten von Kartenlesegeräten verwendbar sind und da es kein besonderes Kriterium für die Eingabe des PIN-Codes gibt, die im Klartext auf der Tastatur des Computers erfolgen kann.

[0079] Nachdem der Server **101** dem Anwender eine VPC-Karte **11** zugewiesen hat, teilt er ihm dafür auf seinem Computerbildschirm **5** die PAN-Nummer **12**, die Gültigkeitsdauer 16 sowie einen eventuellen Passmodus **14** und eine CVV-Anzahl mit, wodurch eine auf 19 Ziffern erweiterte PAN-Nummer erreicht wird.

[0080] Der Anwender kann dann seine Verbindung zum Server **101** abbrechen und die zum Server des Händlers **7** fortsetzen, indem er die Nummer seiner virtuellen VPC-Karte **11** eingibt. Sobald die Transaktion mit dem Server des Händlers **7** verzeichnet wurde, wird der Server **101** darüber informiert und storniert die VPC-Karte **11** (soweit diese Karte nur einmal gültig ist), sodass diese später nicht mehr verwendet werden kann.

[0081] Selbstverständlich wurde die dargestellte Ausführungsweise nur als Beispiel aufgeführt und ist in keinster Weise einschränkend für alle Lösungen, die dank der vorliegenden Erfindung umgesetzt werden können.

Patentansprüche

1. Verfahren zum Sichern einer Handelstransaktion zwischen einem Händler (**7**) und einem Anwender, für die der Anwender persönliche Daten wie zum Beispiel eine Zahlkartennummer angeben muss, wobei dieses Verfahren die Verbindungsherstellung über das Internet (**6**) zu einem Server (**101**) umfasst, der von einer geeigneten Ausstellerbehörde verwaltet wird, sowie das Adressieren einer geeigneten Mitteilung an den besagten Server (**101**), den Erhalt dafür einer zweiten Zahlkarte (**11**) der besagten geeigneten Ausstellerbehörde (**101**), die Anwendung der Daten dieser zweiten Karte (**11**) wie zum Beispiel ihre Nummer (**12**) bei der Transaktion, wobei diese zweite Karte (**11**) nur für eine begrenzte Anzahl von Transaktionen gültig ist, **dadurch gekennzeichnet**, dass es unter anderem die Identifizierung gegenüber dem Server (**101**) durch Anwendung einer ersten Zahlkarte mit Mikroprozessor umfasst, die in ein Lesegerät (**51**) geschoben und mit einem Computer (**5**) gekoppelt ist, sowie dadurch, dass die besagte Mitteilung eine Authentifizierungs- und Unversehrtheitsbescheinigung des Ausstellers (CAI) ist, die Daten und eine Signatur kombiniert, wobei die Signatur durch Verschlüsseln der besagten Daten durch einen in der ersten Karte enthaltenen Verschlüsselungsalgorithmus erhalten wird, und dadurch, dass der besagte Server (**101**) die besagte Mitteilung verwendet, um die besagte zweite Karte (**11**) auszustellen und insbesondere ihre Nummer (**12**).

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die besagte Mitteilung nach Eingabe eines Geheimcodes erstellt wird, der der besagten ersten Karte zugeordnet ist und dem alleinigen Anwender bekannt ist.

3. Verfahren nach einem beliebigen der vorausgehenden Ansprüche, dadurch gekennzeichnet, dass die besagte zweite Zahlkarte (**11**) nur für eine einzige Transaktion gültig ist.

4. Verfahren nach einem beliebigen der vorausgehenden Ansprüche, dadurch gekennzeichnet, dass die besagte zweite Zahlkarte (**11**) nur für einen begrenzten Zeitraum gültig ist, der von einigen Zehntelsekunden bis einige Tage reicht.

5. Verfahren nach einem beliebigen der vorausgehenden Ansprüche, dadurch gekennzeichnet, dass die besagte zweite Zahlkarte (**11**) eine Kartennummer (**12**) und ein Verfalldatum (**13**) umfasst, deren jeweiliges Format mit dem der besagten ersten Zahlkarte (**1**) identisch ist und zwar derart, dass es von den Händlern nicht unterschieden werden kann.

6. Verfahren nach einem beliebigen der vorausgehenden Ansprüche, dadurch gekennzeichnet, dass die betreffenden Transaktionen elektronische Transaktionen im Internet und Web sind.

Es folgt ein Blatt Zeichnungen

Anhängende Zeichnungen

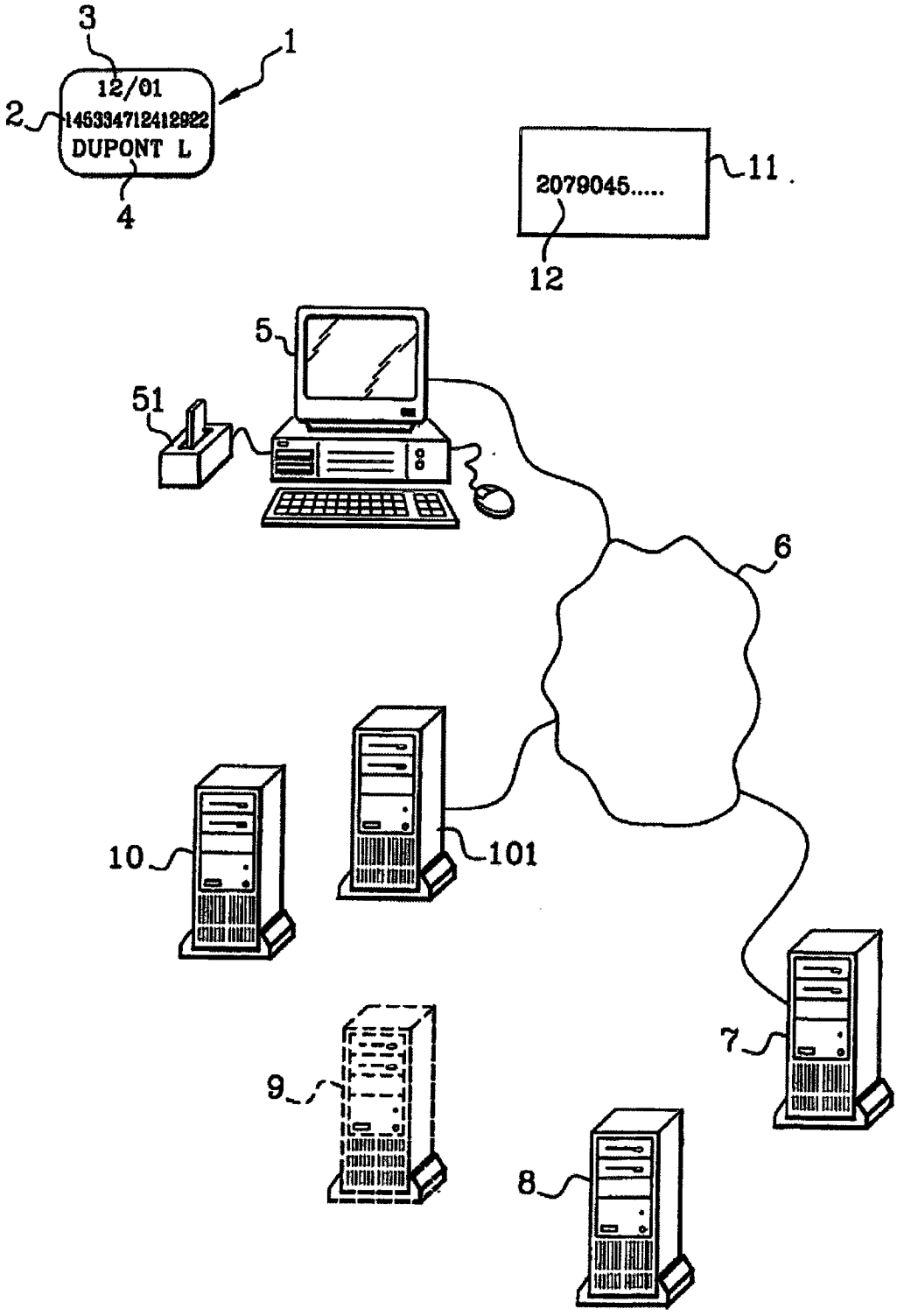

Fig. 1