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

(10) **DE 601 33 453 T2** 2009.05.07

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 256 104 B1**
(21) Deutsches Aktenzeichen: **601 33 453.1**
(86) PCT-Aktenzeichen: **PCT/SE01/00321**
(96) Europäisches Aktenzeichen: **01 904 767.9**
(87) PCT-Veröffentlichungs-Nr.: **WO 2001/061657**
(86) PCT-Anmeldetag: **15.02.2001**
(87) Veröffentlichungstag der PCT-Anmeldung: **23.08.2001**
(97) Erstveröffentlichung durch das EPA: **13.11.2002**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **02.04.2008**
(47) Veröffentlichungstag im Patentblatt: **07.05.2009**

(51) Int Cl.[8]: ***G07F 7/10*** (2006.01)
G06K 19/07 (2006.01)

(30) Unionspriorität:
507087 **18.02.2000** **US**

(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:
Cypak AB, Täby, SE

(74) Vertreter:
Mitscherlich & Partner, Patent- und Rechtsanwälte, 80331 München

(72) Erfinder:
EHRENSVÄRD, Jakob, S-183 77 Täby, SE; GRIP, Stina, S-183 77 Täby, SE

(54) Bezeichnung: **VERFAHREN UND VORRICHTUNG ZUR IDENTIFIZIERUNG UND AUTHENTISIERUNG**

Beschreibung

Gebiet der Erfindung

[0001] Die vorliegende Erfindung bezieht sich auf ein Verfahren und eine Einrichtung zum Durchführen sicherer Transaktionen zwischen einem Dienstbereitsteller, beispielsweise einer Institution, einer Bank, einem Finanzinstitut, einem Einzelhandelsgeschäft, einem Datenbankserver, einem Dateiserver usw., und einem Halter der Einrichtung, d. h., einem Transaktionskunden, welcher ein Kunde oder ein Benutzer eines Systems sein kann.

Hintergrund der Erfindung

[0002] Wenn eine Transaktion und eine Identifikation in einer allgemeinen Form (Kreditkarte, Clubmitglied, Gründungsmitglied, Maklerkontakte, Zugriffssteuerung, usw.) durchgeführt wird, identifiziert ein Kunde oder Benutzer sich selbst, indem er einen einmaligen Personenidentifizierer liefert, beispielsweise einen Namen, eine Kundennummer, eine Kreditkartennummer, eine Sozialversicherungsnummer, usw.. Die Transaktion kann entweder angenommen werden oder weitere Authentifizierung erfordern, beispielsweise Liefern eines geheimen Informationsabschnitts, beispielsweise eines Passworts oder eines PIN-Codes (persönlicher Identifikations-Nummerncode). Wenn eine Nachschlagetabelle in der Kunden/Benutzerdatei die Authentifizierungsantwort als korrekt identifiziert, wird die Transaktion als gültig angesehen. Im Fall der verwendeten Authentifizierung richtet sich das Problem auf die Tatsache, dass der Dienstbereitsteller durch kein Mittel verifizieren kann, dass der Benutzer die Person ist, die er zu sein vorgibt.

[0003] Mehrere Probleme treten hinsichtlich der Sicherheit auf, da diese Art an Verarbeitung häufig über "Funk" durchgeführt wird, d. h., dass sie abgehört und aufgezeichnet werden kann. Der betrügerische Benutzer kann dann die gleiche Identität und Authentifizierung liefern, wobei dem Dienstbereitsteller dies dann so erscheint, dass er der legale Benutzer ist. Eine Kreditkartenummer über eine Telefonverbindung oder in Form eines Faxes zu liefern, ist eine große Unbequemlichkeit für viele Benutzer. Außerdem ist die betrügerische Verwendung von persönlichen Codes und Kreditkartennummern ein Hauptproblem in der automatisierten Welt von heute.

[0004] Das Anwachsen des Internethandels hat zu mehreren Sorgen über die Sicherheit geführt, wenn sich Kunden in Bezug auf einen fernen Dienstanbieter selbst identifizieren müssen. Es gibt ein allgemeines Verständnis, dass ein ernster Beschränkungsfaktor für die Öffentlichkeit, einen Handel durchzuführen und Dienste zu nutzen, die reale Gefahr ist, dass die vertrauliche Information während der Übertragung von Rechnungsnummern und Kreditkartennummern, welche entsprechende Passwörter oder PINs haben, abgehört werden.

[0005] Es gibt mehrere Verfahren und Einrichtungen, welche sich auf diese Sorgen richten, einschließlich der Verschlüsselung von Sicherheitsinformation und Transaktionsidentifikationscodes (TID). Letzteres bezieht sich auf das Verfahren des Dienstanbieters (SP), der einen Einzelverwendungscode ausgibt, der in einer nichtlinearen Weise übertragen wird, welcher für jeden Benutzer einzig ist, und dann zurück zum SP übertragen wird. Der SP führt dann die gleiche nichtlineare Transformation durch und vergleicht das Ergebnis, welches von dem entfernten Ort zurückgebracht wird. Wenn die Ergebnisse übereinstimmen, wird die Transaktion als gültig angesehen.

[0006] Ein allgemeiner Weg zum Durchführen einer sicheren Transaktion bezieht sich auf das Konzept eines Zertifikats, beispielsweise X.509, welches als offener Standard definiert ist. Das Zertifikat verlässt sich auf das Konzept von TIDs und wird durch den SP ausgegeben. Das Zertifikat ist ein Informationsabschnitt, welcher in das Softwarepaket installiert wird, welches verwendet wird, Transaktionen durchzuführen, beispielsweise in einem Internet-Browser. Der Benutzer aktiviert die Geheiminformation im Zertifikat, wobei er einen PIN-Code bereitgestellt, der mit dem vorgegebenen Code im Zertifikat verglichen wird.

[0007] Das Zertifikatverfahren hat mehrere Nachteile, wobei der offensichtlichste die Tatsache ist, dass das Zertifikat lediglich in einem Computer verbleibt. Es gibt keinen allgemeinen Weg, ein Zertifikat von Computer zu Computer zu befördern, oder in einer allgemeineren Form, von Endgerät zu Endgerät. Außerdem gibt es einen Sicherheitsnachteil im Hinblick auf die Tatsache, dass das Zertifikat auf einem nichtentnehmbaren Medium gespeichert ist und daher theoretisch durch irgendjemand geöffnet werden kann, der den Computer verwendet, wo das Zertifikat gespeichert ist.

[0008] Die Tatsache, dass Schriftsprachen, beispielsweise Java und VBScript, die allgemein verwendet werden, ein programmatischeres Verhalten von Internet-Seiten durchzuführen, allgemein betrügerische Aktionen durchführen können, beispielsweise das Abhören des PIN-Codes, der eingegeben wird, wenn ein Zertifikat geöffnet wird, ist das Kopieren der Zertifikatinformation und dann das Transferieren der Information zurück zu einem fremden Dienstanbieter möglich.

[0009] Einige SP geben Transaktionsendgeräte aus, welche kleine rechnerartige Einrichtungen sind, welche eine Anzeigeeinrichtung, eine Tastatur und in

einigen Fällen ein Schlitz haben, um eine IC-Karte mit Benutzerinformation einzuführen. Dieses Verfahren löst das Problem in Verbindung mit der Mobilität, bringt jedoch zusätzliche Kosten für die Einrichtung mit sich. Der größte Nachteil dieses Verfahrens ist die Tatsache, dass alles manuell ausgeführt wird. Um eine TID einzugeben und dann das verarbeitete Ergebnis wieder zu vergleichen, ist ein zeitaufwendiger und fehlerbehafteter Prozess. Die Anzahl von Zeichen, die eingegeben werden und die wieder verglichen werden, muss ein Kompromiss zwischen Sicherheit einerseits sein, und der Annehmlichkeit, einen kurzen Code auf der anderen Seite zu haben. Man kann weiter annehmen, dass diese manuellen Schritte ein Hindernis für den Benutzer sind, was ein Grund sein kann, eine gewünschte Aktion nicht durchzuführen.

[0010] Das Konzept zur Verschlüsselung verlasst sich allgemein auf die Annahme, dass die Zeit, die für eine "Umkehrverarbeitung" erforderlich ist, d. h., um zu entschlüsseln, die verschlüsselte Information lang genug ist, um es in der Praxis sogar unmöglich zu machen, zu versuchen, das Verschlüsselungsverfahren zu knacken. Das märchenhafte Wachsen von sowohl Computerverarbeitungsleistung als auch der Entdeckung neuer mathematischer Algorithmen hat sich in vielen Fällen bestätigt, dass diese Annahme gefährlich ist. Umkehrverfahrensaktionen, für die man einmal dachte, dass dies mehrere Jahre braucht, dass sie für die leistungsfähigste Maschine verfügbar sind, können nun in Minuten durchgeführt werden, indem neue Algorithmen und massive Computerleistung angewandt werden.

[0011] Verschlüsselungsverfahren, beispielsweise der Datenverschlüsselungsstandard (DES), der früher als kaum zu knackendes Verfahren bekannt war, werden nunmehr als "schwach" betrachtet. Primzahl-Verfahren, beispielsweise RSA, versuchen, dies zu überspringen, wobei immer längere Schlüssel verwendet werden. 56-Bit-RSA-Verfahren sind heutzutage bekannt, als beträchtlich sicher zu sein, wobei sich jedoch eine Hochsicherheitsanwendungen auf 1024-Bit-Zahlen verlassen. Man kann erwarten, dass dieser Wettlauf an Zahlen sich fortsetzt.

[0012] Ein Problem mit Hochsicherheits-Verschlüsselungsverfahren ist die Tatsache, dass diese üblicherweise eine starke numerische Verarbeitung benötigen. Durch stationäre Einrichtungen, welche mit Hochleistungsmikroprozessoren ausgerüstet sind, beispielsweise ein PC, ist dies allgemein kein Hauptproblem. Jedoch haben batteriebetriebene preiswerte mobile Einrichtungen, beispielsweise Zellulartelefone, tragbare Notebooks usw. allgemein begrenzte Ressourcen für numerische Verarbeitung.

[0013] Die Folgerung ist die, dass es ratsam sein würde, ein Verfahren und eine Einrichtung bereitzustellen, welche sich an diese Wünsche adressiert und welche in der Lage ist, zweifellos zu bestätigen, dass eine Transaktion sicher ist. Vorzugsweise sollte das Verfahren einfach zu erklären sein und sich nicht auf die Tatasche verlassen, dass Teile des Verfahrens streng geheim gehalten werden müssen.

[0014] Die US 4 295 039 zeigt ein Verfahren und eine Vorrichtung zum Identifizieren eines individuellen Halters einer nichtänderbaren kreditkartenartigen Einrichtung in einem Benutzerendgerät, wo ein einmaliger Benutzereingabeschlüssel in einer sicheren Weise gehandhabt wird. Das System erlaubt die Eingabe eines einmaligen Benutzerschlüssels durch einen Halter der Karte, entweder auf ein Tastenfeld auf dem Endgerät oder ein Tastenfeld auf einem speziellen mobilen Endgerät, in welches die Karte eingeführt werden kann. Die Karte enthält einen Zufallswortgenerator, und das erzeugte Wort wird durch den eingegebenen Benutzerschlüssel sowie durch einen gespeicherten echten Schlüssel in der Karte verschlüsselt. Das Zufallswort, welches unter dem eingegebenen Schlüssel verschlüsselt wurde, wird im Endgerät gespeichert, und das Zufallswort, welches durch den echten Schlüssel verschlüsselt wurde, wird in der Karte gespeichert. Das Endgerät kann bewirken, dass das Wort, welches in der Karte gespeichert ist, zum Endgerät übertragen werden kann, wo die beiden Verschlüsselungen verglichen werden können.

Aufgabe der Erfindung

[0015] Eine Aufgabe der vorliegenden Erfindung besteht darin, ein Verfahren und eine Einrichtung bereitzustellen, welche in der Lage sind, eine sichere Transaktion automatisch über ein Datennetzwerk durchzuführen, sobald der Transaktionsanforderer eine gültige persönliche Identifikation in die Einrichtung eingegeben hat.

Überblick über die Erfindung

[0016] Gemäß einem Merkmal der Erfindung wird ein Verfahren zur Identifikation und Authentifizierung eines Halters eines mobilen elektronischen Transaktionsgeräts in einem elektronischen Transaktionsvorgang zwischen einem Transaktions-Dienstleister und einem Transaktionsendgerät bereitgestellt, welche über ein Computernetzwerk miteinander kommunizieren, wobei das mobile Transaktionsendgerät
Sende-Empfangsmittel zur Übermittlung von Information zum Transaktionsendgerät und für den Empfang von Information von denselben,
Dateneingabemittel
Datenverarbeitungsmittel
Datenspeichermittel mit darin gespeicherten Informationen, wobei die Information eine von außen zugängliche Gerätekennung, eine nichtabrufbare Bezugs-Benutzeridentifikation und
einen nichtabrufbaren Geheimschlüssel, der von den

Verarbeitungsmitteln verarbeitet und von den Empfangsmitteln in der Kommunikation mit dem Dienstleister über das Netzwerk und das Transaktionsendgerät verwendet wird, um eine Transaktion zu validieren, und
Mittel zur Stromversorgung des Geräts aufweist,
wobei das Verfahren dadurch gekennzeichnet ist, dass bei der Verwendung des mobilen elektronischen Transaktionsgeräts in einem elektronischen Transaktionsvorgang zwischen dem Transaktion-Dienstleister und dem Transaktionsendgerät, die über ein Computernetzwerk miteinander kommunizieren,
das Gerät die Gerätekennung an das Transaktionsendgerät übermittelt, der Dienstleister über das Transaktionsendgerät eine Transaktionskennungs-Aufforderung an das Gerät übermittelt;
der Inhaber mit den Eingabemitteln eine Benutzeridentifikation eingibt; das Verarbeitungsmittel die Authentizität der eingegebenen Identifikation durch Vergleichen mit der Bezugs-Benutzeridentifikation erkennt; und nur dann, wenn die Identifikationseingabe als authentisch erkannt wurde:

– das Verarbeitungsmittel an Hand des Geheimschlüssels eine Verschlüsselung der Transaktionskennung durchführt; und
– über das Transaktionsendgerät ein Antwort-Resultat der Verschlüsselung an den Dienstleister übermittelt, um die Transaktion zu validieren.

[0017] Gemäß einem weiteren Merkmal der Erfindung wird ein elektronisches Transaktionsgerät zur Identifikation und Authentifizierung des Inhabers des Geräts in einem elektronischen Transaktionsvorgang zwischen einem Transaktion-Dienstleister und einer Transaktionsendgerät bereitgestellt, welche über ein Computernetzwerk miteinander kommunizieren, wobei das mobile Transaktionsgerät aufweist:
Dateneingabemittel zum Eingeben einer Benutzeridentifikation durch den Benutzer,
Datenverarbeitungsmittel,
Datenspeichermittel zum Speichern von Information, wobei die Information eine von außen zugängliche Vorrichtungs-Identität umfassen,
Sende-Empfangsmittel zum Übermitteln von Information zum und vom Transaktionsendgerät, einschließlich der Übermittlung der Gerätekennung zum Transaktionsendgerät,
Mittel zur Stromversorgung des Geräts, wobei das Gerät dadurch gekennzeichnet ist, dass
die Sende-Empfangs-Mittel in der Lage sind, über das Transaktionsendgerät eine Transaktionskennungsauforderung vom Dienstleister zu empfangen,
die Datenspeichermittel zum Speichern von Information einen nichtabrufbare Bezugs-Benutzeridentifikation und einen nichtabrufbaren Geheimschlüssel aufweisen, der von den Verarbeitungsmitteln verarbeitet und von den Empfangsmitteln in der Kommunikation mit dem Dienstleister über das Netzwerk und das Transaktionsendgerät verwendet wird,
die Verarbeitungsmittel in der Lage sind, die Authentizität einer Benutzeridentifikationseingabe durch den Vergleich der eingegebenen Benutzeridentifikation mit der nichtabrufbaren Bezugs-Benutzeridentifikation in den Speichermitteln zu erkennen, und nur dann, wenn die Identifikationseingabe als authentisch erkannt wurde, an Hand des in den Speichermitteln gespeicherten Geheimschlüssels eine Verschlüsselung der Transaktionskennung durchgeführt wird,
wobei die Sende-Empfangsmittel auch in der Lage sind, ein Antwort-Resultat der Verschlüsselung über das Transaktionsendgerät an den Dienstleister zu übermitteln, um die Transaktion zu validieren.

[0018] Die Transaktionseinrichtung gemäß der Erfindung hat vorzugsweise die Größe einer Kreditkarte und ist eingerichtet, mit einem Dienstleister (SP) über ein Datennetzwerk, insbesondere das Internet, über ein Transaktionsendgerät (TT) zu kommunizieren, welches eine Kommunikationsschnittstelle hat, beispielsweise einen Kartenleser (CR).

[0019] Der SP ist eine Bank, ein Internet-Geschäft, ein Einzelhandelsgeschäft, usw.. Der SP hält eine Datenbank aller Kunden, die autorisiert sind, Transaktionen durchzuführen. Das TT ist eine stationäre Einrichtung, welche mit dem SP über ein Netzwerk verbunden ist. Die Verbindung kann entweder fortlaufend oder intermittierend sein. Das TT kann entweder speziell für den Zweck ausgebildet sein oder kann ein Standardpersonalcomputer sein. Der CR, der mit dem TT verbunden ist, enthält eine Sende-Empfangs-Einrichtung zur bidirektionalen Kommunikation mit der Einrichtung. Die Karte ist vorzugsweise eine preiswerte Einrichtung, welche durch den Kartenhalter getragen wird, d. h., den Kunden. Die Karte kann aktiv einen Datenaustausch mit dem TT unter Verwendung des CR durchführen. Bei der bevorzugten Ausführungsform wird der Datenaustausch durch drahtlose kapazitive Nahbereichs-Datenübertragung und Spannungsversorgung für die Karte durchgeführt.

Kurzbeschreibung der Zeichnungen

[0020] Fig. 1 ist eine Vorderansicht, wobei Teile einer Transaktionskarte gemäß der Erfindung weggebrochen sind;

[0021] Fig. 2 ist eine grafische Darstellung, welche eine Transaktionskarte gemäß Fig. 1 in Kommunikation mit einem Dienstleister in einem Netzwerk zeigt;

[0022] Fig. 3 ist eine Vorderansicht, wobei Teile von einem flachen Feld weggebrochen sind, welche einen Kartentransaktionsanschluss hat, der im Feldaufbau eingebettet ist;

[0023] Fig. 4 zeigt eine erste Ebene, welche auf einer Bodenschicht aufgedruckt ist, einer Transaktions-

karte gemäß der Erfindung, und welche kapazitive Leiterflecken aufweist;

[0024] Fig. 5 zeigt eine zweite gedruckte Ebene auf der ersten Ebene der Bodenschicht, und welche einen Isolationsfleck aufweist;

[0025] Fig. 6 zeigt eine dritte Ebene, welche auf die zweite Ebene der Bodenebenen gedruckt ist und welche elektrische Schaltungen aufweist;

[0026] Fig. 7 ist ein Funktionsdiagramm eines Transaktionsendgeräts gemäß der Erfindung;

[0027] Fig. 8 ist ein Funktionsdiagramm einer Transaktionseinrichtung gemäß der Erfindung; und

[0028] Fig. 9 ist ein Block- und Schaltungsdiagramm eines Systems einschließlich eines Transaktionsendgeräts und einer Transaktionseinrichtung gemäß der Erfindung.

Beschreibung der bevorzugten Ausführungsform

[0029] Eine bevorzugte Ausführungsform der mobilen preiswerten elektronischen Transaktionseinrichtung ist in Fig. 1 bis Fig. 5 gezeigt.

[0030] Die Einrichtung hat die äußere Form einer Karte **10**, vorzugsweise einer Kreditkarte, und ist optional mit einem Magnetstreifen (nicht gezeigt) und mit einem eingeprägten Textfeld versehen, um als herkömmliche Kreditkarte verwendet werden zu können. Jedoch kann eine Transaktion gemäß der Erfindung andere Formen aufweisen, beispielsweise die Form eines kleinen Rechners.

[0031] Wie aus Fig. 1 ersichtlich ist, besteht die Karte **10** vorzugsweise aus drei beschichteten Folien **12**, **18**, **24**, vorzugsweise aus Polyester-Kunststoffmaterial, und hat eine kombinierte Dicke von ungefähr 0,8 mm, d. h., die Dicke der herkömmlichen Kreditkarte.

[0032] Bei der bevorzugten Ausführungsform ist die Karte mit einer Eingabeeinrichtung versehen, beispielsweise einem Tastenfeld **14**, einer Datenspeicher- und Verarbeitungseinrichtung, einschließlich einer integrierten Schaltung (IC) **50** und einer Sende-Empfangs-/Energieversorgungseinrichtung einschließlich eines kapazitiven Senders/Empfängers oder eines bidirektionalen Übertragers **38**, wobei Teile davon in Fig. 6 bis Fig. 9 gezeigt sind.

[0033] Das Tastenfeld **14**, welches geeignet an einem oberen Teil der vorderen Kartenfläche vorgesehen ist, besitzt **12** Tasten zur manuellen Eingabe der Zahlen 0–9, sowie für "Eingabe-" und "Lösch"-Befehle. Das Tastenfeld **14** ist vorzugsweise ein Membran-Tastenfeld, welches in die Karte **10** eingebettet ist. Genauer besteht das dünne federnde Polyester-Kunststoffmaterial aus einer Kopffolie **12**, welche gedruckte Tastensymbole auf ihrer vorderen Fläche hat, und bildet die Tastenfeld-Tasten-Membranen. Auf der Bodeninnenseitefläche der Kopffolie **12** sind elektrisch-leitfähige Schaltflecken **16** aufgedruckt. Die Zwischenfolie **18** funktioniert als Abstandsebene, welche kreisförmige Ausnehmungen **20** aufweist, fluchtend mit den Schaltflecken **16**, und welche außerdem eine Rechteckausnehmung **22** aufweist, welche den IC **50** beherbergt. Die Bodenfolie **24** hat eine oberste gedruckte Schaltungsebene **26** (siehe auch Fig. 4) einschließlich Schaltbereichen **28**, welche mit den Schaltflecken **16** und den kreisförmigen Ausnehmungen **20** fluchten. Die Anordnung ist derart, dass, wenn ein Kartenhalter eine Taste auf das Tastenfeld **14** drückt, der entsprechende leitfähige Schaltpfad **16** den Raum von ungefähr 0,5 mm überbrückt, der durch die entsprechende Ausnehmung **22** gebildet wird und in Kontakt mit dem in fluchtenden Schaltbereich **28** kommt. Eine entsprechende elektrische Schaltung **32**, welche normalerweise durch ein dichtes Muster von Leitern **30** unterbrochen ist, welche in Kontakt im Schaltbereich **28** kommt, wird dadurch geschlossen. Jede elektrische Schaltung **32** ist mit dem IC **50** über gedruckte Verbinderflecken einer Verbindungsschnittstelle **54** verbunden.

[0034] Wie oben erwähnt bildet die gedruckte Schaltungsebene **26** eine Kopfebene in der Bodenfolie **24**. Wie in Fig. 5 und Fig. 6 gezeigt ist, hat die Innenseite der Bodenfolie **24** zwei darunterliegende zusätzliche gedruckte Ebenen, nämlich eine gedruckte elektrische isolierende Zwischenebene **34** und eine gedruckte kapazitive Bodenebene **36**. Die Bodenebene **36**, welche ein Teil des kapazitiven Sende-Empfangs-Geräts **38** bildet (Fig. 9), was später beschrieben wird, umfasst drei kapazitive Flecken **40**, **42**, **44**, welche elektrisch mit dem IC **50** über gedruckte Leiterflecken **46**, **47**, **48** verbunden sind. Diese sind wiederum mit Verbindungsflecken **56**, **58**, **58** der Verbindungsschnittstelle **54** (Fig. 4) verbunden, wenn die Kopfschaltungsebene **26** auf die isolierende Zwischenschicht **34** gedruckt wird.

[0035] In einer durch den Stand der Technik bekannten Weise hat der IC **50** eine Datenspeicher-, Verarbeitungs- und Eingabe-/Ausgabeeinrichtung, welche für den bestimmten Zweck und zur Verwendung der Karte als Transaktionseinrichtung bestimmt ist. Insbesondere ist die Speichereinrichtung in der Lage, in ihr einen persönlichen Identifikationscode (PIN) von üblicherweise vier Zeichen und einen Geheimschlüssel (SK) einer beträchtlichen Länge zu speichern. Der PIN und der SK, welche vorzugsweise schon im Speicher gespeichert sind, wenn die Karte an den Halter ausgegeben wird, kann durch kein Mittel von der Karte **10** abgerufen werden. Der SK wird lediglich einmal in die Karte durch den Kartenherausgeber programmiert. In einer ansich bekannten Weise durch den Stand der Technik auf dem Gebiet der

Mikroelektronik sind die Software- und/oder Hardware-Einrichtung eingerichtet, das Lesen und das Ändern des PINs und des SKs zu verhindern. Der PIN kann jedoch optional einmal von einem vorher programmierten Anfangswert durch den Halter geändert werden, bevor die Transaktionskarte **10** verwendet wird.

[0036] Fig. 2 zeigt eine Transaktionskarte **10**, die zur Verwendung bereit ist, welche auf einer Kartenschnittstelle (CI) angeordnet ist, welche einen eng benachbarten kapazitiven Sende-Empfänger in Form eines Kartenlesers **60** über ein Kabel **66** aufweist.

[0037] Der Kartenleser **60** hat eine Kartenaufnahmefläche **62**, auf welcher die Karte beim Validieren einer Transaktion mit einem Dienstleister (SP **72**) angeordnet wird, der mit dem Kartenleser über ein Netzwerk **70** kommuniziert, und einen Transaktionsanschluss (TT) **68**, der mit dem Kartenleser **60** verbunden ist. Der gezeigte Kartenleser **60** besitzt außerdem eine alphanumerische Anzeige **64**, um über notwendige Aktionen während eines Transaktionsprozesses zu informieren.

[0038] Da die Transaktionseinrichtung gemäß der Erfindung von einem externen Tastenfeld unabhängig ist, kann die Kartenleseschaltungsanordnung hinter einer flachen Fläche **62'** eingebettet sein, wie in Fig. 3 gezeigt ist. Beispielsweise kann die Fläche **62'** eine hygienisch leicht zu reinigende dazu passende Glas-Kopffläche in einem Geschäft sein. In diesem Fall kann die elektrisch-leitende Schaltung einschließlich der kapazitiven Bereiche fast unsichtbar angebracht werden, beispielsweise auf einer inneren Fläche von Glasfolienlagen, durch Ablagerung eines Indium-Tin-Oxids-Schaltungsmusters (ITO). Die flache Fläche **62'** kann außerdem eine vertikale Feldfläche mit einer zerklüfteten Außenstruktur sein, welche gegenüber gelegentlichen Vandalismus unempfänglich ist.

[0039] Der SP **72** ist eine Bank, ein Internet-Laden, ein Einzelhandelgeschäft usw.. Der SP **72** hält eine Aufzeichnung in einer Datenbank **74** alle Kunden, die zum Durchführen von Transaktionen berechtigt sind.

[0040] Das TT **68** ist eine stationäre Einrichtung, welche mit dem SP über ein Netzwerk verbunden ist. Die Verbindung kann entweder fortlaufend oder intermittierend sein. Das TT **68** kann entweder speziell für den Zweck ausgebildet sein, oder es kann ein Standardpersonalcomputer sein.

[0041] Der Sender-Empfänger des Kartenlesers **60** ist zu einer bidirektionalen Kommunikation mit Karten in der Lage. Der Kartenleser **60** ist als eigenständige Einrichtung dargestellt, jedoch kann dieser auch ein integriertes Teil (nicht gezeigt) des TT **68** sein.

[0042] Die Karte kann einen Datenaustausch mit dem TT unter Verwendung des CI/Kartenlesers **60** durchführen. Wie oben erwähnt wird bei der bevorzugten Ausführungsform der Datenaustausch über eine Drahtloseinrichtung unter Verwendung einer kapazitiven Nahbereichs-Datenübertragung und Spannungsversorgung für die Karte ausgeführt.

[0043] Fig. 7 und Fig. 8 zeigen grafisch funktionelle Anordnungen von jeweils einem Kartenleser **60** und einer Karten/Transaktionseinrichtung **10**, während Fig. 9 spezifische Komponenten des kombinierten Systems zeigt.

[0044] Wie in Fig. 9 gezeigt ist, werden die kapazitiven Flecken **40**, **42**, **44** der Karte **10** mit den entsprechenden kapazitiven Flecken **40b**, **42b**, **44b** fluchten, welche den Flecken **40**, **42**, **44** in enger Nachbarschaft zugewandt sind, wenn die Karte **10** auf der Empfangsfläche **62** (Fig. 2) angeordnet wird. Die Karte **10** und der Kartenleser **60** werden dann den kapazitiven Schaltkreis bilden, der in Fig. 9 gezeigt ist, der in der Lage ist, elektrische Leistung zum Schaltkreis der Karte **10** zu liefern und die Digitaldaten zwischen der Karte **10** und dem Kartenleser **60** wie folgt auszutauschen:
In der nachfolgenden Beschreibung wird der Kartenleser **60** als eine externe Host-Einheit **60** betrachtet, welche eine kapazitive Schnittstelle in enger Nachbarschaft zur Karte **10** anteilig nutzt, welche als Gasteinheit angesehen wird und welche eine integrierte Schaltung **50** aufweist, welche über eine Schnittstelle **126** angeschaltet ist. Die drei Paare der leitfähigen Bereiche **40**–**40b**, **42**–**42b** und **44**–**44b** bilden eine gemeinsame kapazitive Schnittstelle.

[0045] Das Transaktionsendgerät **68**, welches ein Standardpersonalcomputer sein kann, ist üblicherweise mit einer V.24/V.28-Schnittstelle als Standard ausgerüstet. Das Transaktionsendgerät **68** ist mit einer Eigentumssoftware-Ansteuerung (nicht gezeigt) ausgerüstet, um den Datenfluss für die Host-Einheit **60** zu steuern. In Abhängigkeit von der gewünschten Funktionalität kann diese Ansteuerung entweder ein installiertes Ansteuermodul oder ein Teil eines Anwendungsprogramms sein.

[0046] Die CCITT-V.24/V.28-Elektro-Spezifikation legt eine minimale Spannungsausgangsleistungsschwankung bei einem festgelegten Lastzustand fest. Sogar, obwohl die Anwendung selbst nicht festlegt, dass eine angebrachte Einrichtung von der Schnittstelle mit Leistung versorgt wird, solange die festgelegte maximale Belastung nicht überstiegen wird, ist es ein Vorteil, unabhängig von einer externen Leistung zu sein. Wo es nicht erwünscht wird, weitere Last auf den seriellen Port zu legen oder der serielle Port selbst nicht mit den Ansteuererfordernissen zurecht kommt, welche bei der Anwendung festgelegt sind, kann externe Spannung von einem AC/DC-Ad-

apter oder von Batterien, welche in der Host-Einheit enthalten sind, angelegt werden. Wenn gewünscht kann ein Schnittstellensteuersignal verwendet werden, um die Leistung der Host-Einheit **60** zu steuern, wo ein Zustand ein Niedrigspannungszustand, ein Bereitschaftszustand oder der andere ein aktiver Vollleistungszustand ist.

[0047] Eine Hauptschaltung der Host-Einheit **60** kann wie folgt ausgeführt werden:
Die Host-Einheit **60** ist so ausgebildet, dass sie mit einem seriellen Standard-V.24/V.28-Port verbunden wird, wo die Spannungspegel der Ausgänge RTS und DTR durch die Schnittstellensoftware so programmiert sind, um auf einem hohen Pegel zu sein, wodurch eine positive Versorgungsspannung für die Schaltungselemente bereitgestellt wird. Die Empfangsdaten-Eingangsschnittstelle (R × D) hat einen Markierungspegel bei einem negativen Pegel, wodurch eine negative Versorgung für einen Pegelschieber **98** bereitgestellt wird. Zusätzliche Schwingkreis- und Glättungskondensatoren **82**, **96** sind vorgesehen, und sie können mit einem Spannungsstabilisierungselement ergänzt werden, beispielsweise einer parallelen Zener-Diode (nicht gezeigt).

[0048] Ein Pegelschieber **84** liefert Verschieben von Eingangsspannungen zur Host-Einheit, und liefert ein logisches hohes Ausgangssignal, wenn das Eingangssignal beim Markierungspegel, d. h., inaktiv ist. Eine Oszillator-Schmitt-Trigger-NAND-Schaltung **86** wird dann bei einer Frequenz schwingen, welche hauptsächlich durch eine LC-Resonanzschaltung festgelegt ist, welche aus einem Widerstand **90**, einer Induktivität **92** und einem Kondensator **94** besteht, welche bei dem Ausgang des Schmitt-Triggers **88** vorgesehen sind. Diese Resonanzschaltung liefert ein Trägerausgangssignal hinsichtlich des Leitbereichs **42b**. Durch die Widerstandsrückführung liefert diese Ausbildung eine automatische Abstimmung der Resonanzschaltung, um auf ihrer Spitzenwert-Ausgangsamplitude zu arbeiten, relativ unabhängig von der komplexen Impedanzlast von **42b**. Durch Auswählen eines CMOS/HCMOS-Schmitt-Triggers **88** kann der Wert der Widerstandsrückführung hoch gehalten werden, um die Last der Resonanzschaltung zu reduzieren. Weitere Vorteile einer Verwendung von HCMOS-Einrichtungen umfassen eine niedrige Betriebsleistung, niedrige Ausgangsimpedanz, Ausgangsschwingung von Schiene zu Schiene und Eingangsschutzdioden, wodurch eine hohe Ausgangsschwingung der Resonanzschaltung mit einem Minimum von Ausbildungskomplexität bereitgestellt wird.

[0049] Wenn ein Raumpegel auf der Eingangsseite des Pegelschiebers **84** vorhanden ist, sperrt ein logisches niedriges Ausgangssignal die Oszillatorfunktion, so dass das Ausgangssignal der Resonanzschaltung schwankt, und ein DC-Pegel auf dem Anschluss **42b** vorhanden ist. Wenn ein serieller Datenstrom auf dem Eingang des Pegelschiebers **84** empfangen wird, wird der Ausgang der Resonanzschaltung einen pulsmodulierten Trägerbereich bereitstellen, der dann kapazitiv darüber mit der tragbaren Einrichtung gekoppelt ist.

[0050] Die Gasteinheit **10** hat eine hohe Eingangsimpedanz und wird nachstehend in der ausführlichen Beschreibung der Transaktionseinrichtungs-Schnittstelle erläutert.

[0051] Wenn folglich kapazitive Schnittstellenplatten **40** und **42**/**44** in enger Nachbarschaft zu den entsprechenden Platten **40b**, **42b** und **44b** angeordnet werden, werden Kondensatoren durch die Platten **40**–**40b**, **42**–**42b** und **44**–**44b** gebildet. Die tatsächlichen Kondensatorwerte werden hauptsächlich durch die Plattengröße, den Abstand zwischen den Platten und die Art des dielektrischen Materials (Materialien), welches zwischen diesen vorhanden ist, vorgegeben.

[0052] Die Ausbildung, wo die Platten **42** und **44** miteinander verbunden sind, bezieht eine reduzierte Streukapazität ein, welche eine Kopplung zwischen den Platten **42b** und **44b** bildet. Ein weiterer Vorteil ist der, dass die tragbare Einrichtung symmetrisch ist, d. h., sie in den Schritten von 180° ohne Verlust an Funktionalität gedreht werden kann.

[0053] Eine erste kapazitive geschlossene Schleife wird durch nachfolgendes Ausbilden des Ausgangssignals der Resonanzschaltung in der Host-Einheit **60** über Platten **42b**–**42** zur Gasteinheit **10** über eine Gleichrichterbrücke **120**, welche vier Dioden **122** hat, über die parallele Impedanzschaltung **114**, welche einen Kondensator **116** und einen Widerstand **118** aufweist, und zurück zur Masse in der Host-Einheit **60** über die Platten **40**–**40b** gebildet.

[0054] Eine zweite geschlossene kapazitive Schleife wird nachfolgend durch die Ausgangsschaltung der Resonanzschaltung in der Host-Einheit **60** über Platten **42b**–**42**, **44**–**44b** und über die Eingangsdiode **106** und den Widerstand **102** nach unten zur Masse in der Host-Einheit **60** gebildet.

[0055] Wenn die Oszillatorschaltung **16** in der Host-Einheit **10** freigegeben wird, induziert die erste kapazitive Schleife eine Spannung auf den Anschluss RX in der Gasteinheit **10**. Durch eine optionale Spitzenhalte-Diode und einen Speicherkondensator (nicht gezeigt) kann dann ein Niedrigstromschaltkreis in der Gasteinheit **10** mit Leistung versorgt werden, ohne ernsthaft die Signalübertragung zwischen der Host-Einheit **60** und der Gasteinheit **10** zu beeinträchtigen.

[0056] Wenn der Oszillator **88** durch einen Datenstrom von dem Transaktionsendgerät **68** moduliert

wird, wird ein entsprechendes demoduliertes Ausgangssignal am Anschluss RX in der Gasteinheit **10** gebildet. Durch einen optionalen Spannungsbegrenzer und den Schmitt-Trigger (nicht gezeigt) hinsichtlich RX kann ein sauberes, demoduliertes Signal unmittelbar durch die integrierte Schaltung **50** in der Gasteinheit **10** verarbeitet werden.

[0057] Die Gasteinheit **10** weist außerdem einen Transistor **112** auf, der parallel zur Impedanzschaltung **114** geschaltet ist. Die Digitaldateninformation kann zurück von der Gasteinheit **10** zur Host-Einheit **60** übertragen werden, wobei der Transistor **112** von einem TX-Anschluss in der Gasteinheit **10** gesteuert wird. Wenn der Transistor **112** leitfähig ist, wird der Eingang auf der Platte **42** wirksam auf Masse über die Platten **40**–**40b** kurzgeschlossen, wodurch die Spannung auf der Platte **44**, welche mit der Platte **44b** verbunden ist, gedämpft wird. Die ruhige Kopplung des Trägers, der im Eingangsnetzwerk gefiltert ist, der mit dem Pegelschieber **98** in der Host-Einheit **60** verbunden ist, wird dann gedämpft. Ein passend ausgewählter Schwellenwert des Eingangssignals zum Pegelschieber **98** zusammen mit einer Hysterese führen die Demodulation der Information durch, welche von der Gasteinheit **10** zum Transaktionsendgerät **68** übertragen wird, durch.

[0058] Im Fall einer Leistungsübertragung von der Host-Einheit **60** zur Gasteinheit **10** ist es ein nicht erwünschter Effekt, dass NRZ-Modulationsdaten (keine Rückkehr auf Null) die Spannung auf dem RX-Anschluss in der Gast-Einheit **10** sperren. Durch Anwenden eines anderen Modulationsverfahrens, welches durch den Stand der Technik bekannt ist, beispielsweise PPI, FM oder Manchester, kann die Abschaltzeit reduziert werden, wodurch eine stetigere Spannung in der Gasteinheit **10** ermöglicht wird.

[0059] Diese bevorzugte Ausführungsform hat eine preiswerte, leicht durchzuführende, selbstabstimmende Ausbildung, mit entspannten Erfordernissen der reaktiven Komponenten. Komponenten, welche eine relativ geringe Toleranz von ungefähr ±10% gegenüber Idealwerten haben, sind im System verwendbar und sind breit bei geringen Kosten verfügbar. Die kapazitive Belastung, welche durch die Gasteinheit **10** gebildet wird, sowie unterschiedliche Streukapazitäten, verschieben unmittelbar leicht die Oszillatormittenfrequenz, ohne ernsthaft die Ausgangssignalamplitude zu beeinträchtigen.

[0060] Da die Host-Einheit **60** mit niedriger Leistung arbeitet, kann sie unmittelbar von den Schnittstellensignalen mit Leistung versorgt werden, wodurch die Notwendigkeit auf eine externe Leistung beseitigt wird, beispielsweise die, welche von einem AC-Adapter oder einem Batteriesatz bereitgestellt wird.

[0061] Die Gasteinheit arbeitet virtuell mit einem ruhigen Nullstrom, ohne die Fähigkeiten in Frage zu stellen, Daten zu irgendeiner Zeit zu empfangen.

[0062] Alternativ zur oben beschriebenen Ausführungsform kann die Karte als sogenannte Smart-Card (intelligente Karte) ausgebildet werden, um Daten galvanisch zu kommunizieren, d. h., über Leiterflecken, welche auf der vorderen Fläche der Karte (nicht gezeigt) frei sind. In diesem Fall und auch alternativ bei der oben beschriebenen Ausführungsform kann die elektrische Energie in einer Dünnfilmbatterie gespeichert sein, welche eine Ebene in der Karte (nicht gezeigt) bildet. Eine Karte, welche eine eigene Energiequelle hat, erlaubt es dem Halter, den PIN selbst mit geringerer Gefahr einzugeben, den PIN an andere zu enthüllen, bevor die Karte auf den Kartenleser angeordnet wird. Wenn die Transaktionseinrichtung gemäß der Erfindung als dickerer Kreditkarten-Rechner ausgebildet ist, kann sie natürlich eine kleine herkömmliche Batteriezelle als elektrische Energiequelle haben.

[0063] Der IC **50** hat Datenverarbeitungsfähigkeiten, um eine nichtreversible Transformation durchzuführen, unter Verwendung einer nichtlinearen Funktionstransformation oder Hash-Funktion, y = h(x), welche die folgenden Kennmerkmale erfüllt.:
Das Ausgangssignal hat eine feste Ausgangslänge für jeden Eingangswert von x.

[0064] Es gibt keine Umkehr, d. h., x kann nicht von einem bestimmten Wert von y berechnet werden.

[0065] Es ist einfach, dies hinsichtlich der Verarbeitungsleistung zu berechnen und man ist in der Lage, durch grundsätzliche ganzzahlige arithmetische und logische Funktionen ausgewertet zu werden, einschließlich einer Nachschlagetabelle.

[0066] Eine Einrichtung gemäß der Erfindung ist dazu beabsichtigt, in Kombination mit dem SP **72** wie folgt verwendet zu werden:
Die Medien zwischen dem SP **72** und der TT **68** sowie zwischen dem TT **68** und der Karte **10** werden angesehen, unsicher zu sein, und die gesamte Information, welche in jeder Richtung übertragen wird, kann abgehört werden und im Klartext durch irgendjemand zu jeder Zeit gelesen werden. Die eingeprägte Kartennummer wird so angesehen, dass sie keine Beziehung mit einer optionalen Kreditkartennummer hat, oder einer anderen Information, welche nützlich sein kann, wenn durch irgendeinen abgehört zu werden.

[0067] Der SP **72** kann einen Transaktionsidentifizierer (TID) einer beträchtlichen Länge an das TT **68** ausgeben. Die TIDs werden in einer Zufallsweise ausgegeben, so dass die Wahrscheinlichkeit, dass zwei identische Nummern während der Lebensdauer einer einzelnen Karte gesendet werden, extrem klein

ist oder niemals überhaupt auftreten sollten.

[0068] Die Karte enthält eine Kartenidentität (CID), welche im IC **50** gespeichert ist, der für den Kartenhalter einzig ist. Die CD wird betrachtet, um öffentlich zu sein und kann auf die Karte **10** gedruckt werden, da diese nicht verwundbar ist und zum Durchführen einer Transaktion verwendbar ist, ohne die Karte selbst. Die CD muss keine Verknüpfung zu einer optionalen Kreditkartennummer haben, wenn diese auf die Karte eingeprägt ist und auf dem Magnetstreifen oder der CR **60** aufgezeichnet ist. Die CD kann automatisch von der Karte zu jeder Zeit durch den Magnetstreifen oder CR **60** gelesen werden.

[0069] Wenn gewünscht kann die Karte ein Signal dem TT **68** für jede betätigte Taste auf der Tastatur **14** bereitstellen, um eine hörbare und/oder sichtbare Rückführung dem Benutzer zu liefern. Dieses Rückführsignal hat keine Beziehung auf die betätigte Tastenposition.

[0070] Der Geheimschlüssel (SK), welcher im IC **50** gespeichert ist, kann durch kein Mittel von der Karte irgendeiner Form abgerufen werden und ist lediglich einmal durch den Kartenherausgeber programmiert. Die Software- und/oder Hardware-Einrichtung verhindert das Lesen oder das Ändern des Geheimschlüssels.

[0071] Wie oben erwähnt enthält die Karte eine persönlichen Identifikationsnummerncode (PIN), welche im IC **50** gespeichert ist. Dieser PIN kann durch kein Mittel von der Karte in irgendeiner Form abgerufen werden.

[0072] Die Karte weist Datenverarbeitungsfähigkeiten auf, um eine nichtreversible Transformation durchzuführen, unter Verwendung eines Einzelverwendungscodes von der SP über das TT **68**, welches vom TID geliefert wird, und überträgt dies zurück zum SP **72** über das TT. Da zwei identische TIDs niemals während der Lebensdauer der Karte auftreten sollten, kann ein fremdes System keine Wiedergabe einer aufgezeichneten Antwort wiedergeben, um dadurch eine betrügerische Transaktion im Fall zuzulassen, dass eine vorherige Antwort aufgezeichnet ist.

[0073] Um eine Karte zu identifizieren, werden die folgenden Schritte durchgeführt:

1. Das TT fordert die CID von der Karte an.
2. Die Karte überträgt die CID zurück zur TT. In Abhängigkeit von der Anwendung kann die CID zurück zur SP übertragen werden.

[0074] Optional können die folgenden Merkmale in Abhängigkeit von der Anwendung hinzugefügt werden:
Das TT kann entsprechend eine CID anfordern.

[0075] Wenn eine Karte auf dem Lesegerät angeordnet ist, leitet die Anwendung im TT automatisch dem Benutzer zurück ein programmiertes Anwendungsprogramm oder URL im Internet.

[0076] Weitere Information über die Karte kann von der SP angefordert werden. Um eine sichere Transaktion durchzuführen oder um Authentifizierung durchzuführen, dass der Kartenhalter gültig ist, werden die folgenden allgemeinen Schritte durchgeführt:

1. Das TT überträgt die CID, welche wie oben abgerufen wurde, an den SP.
2. Der SP gibt eine TID aus, welche über das TT auf die Karte übergeleitet wird.
3. Der Kartenhalter wird informiert, die PIN einzugeben.
4. Eine gültige PIN entriegelt den SK und führt eine Hash-Transformation des TID durch und überträgt das Ergebnis zurück über das TT zum SP.
5. Der SP führt die gleiche Verarbeitung wie die im Schritt S4 durch und vergleicht das abgerufene Ergebnis. Wenn die Ergebnisse übereinstimmen, wird die Transaktion als gültig angesehen.

[0077] Um eine weitere Sicherheitstransaktion durchzuführen, werden die Schritte vom Schritt 2 an wiederholt.

[0078] Um die Sicherheit weiter zu verbessern, können die folgenden Schritte wie folgt ausgeführt werden.

[0079] Es wird lediglich eine Transaktion für jede empfangene TID zugelassen. Jede neue Transaktion muss durch eine neue TID validiert werden.

[0080] Ein Zeitablauf wird festgelegt, nachdem eine Forderung-TID für die Karte empfangen wird. Ein Zeitablauf erfordert eine neue TID, welche vom SP auszugeben ist.

[0081] Die Karte ist vorprogrammiert, um eine vorher festgelegte Anzahl von Transaktionen durchzuführen, bevor sie abläuft. Die Karte wird dann permanent zur weiteren Verwendung durch nichtreversibles Ändern einer einmal aufzubauenden Speicherzelle blockiert.

[0082] Die Karte wird mit einem nichtflüchtigen Zähler vorprogrammiert, der permanent die Karte blockiert, wenn mehr als eine vorher programmierte Anzahl ungültiger PINs eingegeben wird. Der Zähler wird zurückgesetzt jedes Mal dann, wenn eine gültige PIN eingegeben ist.

[0083] Karten, welche als verloren und/oder gestohlen registriert sind, bleiben permanent zur weiteren Verwendung blockiert, wobei der SP verwendet wird, der eine Blockierungs-TID ausgibt, der permanent

die Karte zur weiteren Verwendung blockiert, und, wenn erwünscht, Verkaufspersonal alarmiert wird. Die TID wird einmalig oder zufallsmäßig für jede Karte programmiert und ist lediglich durch den SP und in der Karte bekannt, und erscheint als normale TID für einen Fremden, der die TID abhört.

[0084] Jede Karte kann mit einer TID-Sequenzkarte vorprogrammiert sein, welche zwischen ausgegebenen Karten zufallsmäßig ausgewählt wird, welche eine Karte von TIDs mit einer bestimmten Charakteristik lediglich zulässt. Diese Sequenz oder das Verfahren muss sorgfältig ausgewählt werden, um nicht erwünschte Effekte bei der nichtlinearen Transformation zu bewirken, was zu einem statistisch verzerrten Antwortmuster führen wird. Wenn eine empfangene TID nicht zu dem genannten Verfahren passt, wird die Karte unmittelbar ablaufen, wodurch somit die Wahrscheinlichkeit einer frühen Erfassung vergrößert wird und die Beendigung eines Fremdversuchs, um vorgetäuschte TIDs auszugeben.

[0085] Jede Karte kann programmiert sein, um unterschiedliche Transformationsalgorithmen zu verwenden, in Abhängigkeit von einem vorprogrammierten Auswahlverfahren, welches von der TID erfassbar ist. Das Verfahren kann in die Karte vorprogrammiert werden und lediglich durch den SP sowie in der Karte bekannt ist.

[0086] Wie oben erläutert kann ein erstmaliger PIN-Code optional durch den Kartenhalter initialisiert werden. Der PIN-Code kann dann nicht geändert werden und ist danach lediglich dem Kartenhalter bekannt.

[0087] Da jede Antwort von der Karte eine vollständige und validierte PIN-Eingabe erfordert, wird angenommen, dass ein Fremdversuch, eine vorgetäuschte TID in die Karte einzugeben, um Information über den Geheimschlüssel in der Karte herauszufinden, nicht erfolgreich sein wird. Der verbesserte Sicherheitspegel zum Blockieren der Karte nach einer vorprogrammierten Anzahl von Transaktionen stärkt außerdem diese Annahme.

[0088] Eine statistisch bestätigte Auswahl der Schlüssellänge, ein nichtlinearer Transformationsalgorithmus und der Kartenablaufzähler sollten es ermöglichen, dieses Verfahren für alle praktischen Einrichtungen so zu machen, dass dies nicht geknackt werden kann. Dies erfordert außerdem ein sorgfältig ausgewähltes Zufallsverfahren, welches auszuführen ist, so dass keine erfassbare Verknüpfung zwischen der CID und dem SK existiert, oder dass keine verzerrenden Effekte bei dem Transformationsprozess auftreten.

[0089] Optional können die folgenden Merkmale hinzugefügt werden, und zwar in Abhängigkeit von der Anwendung:
Die Karte kann einen Lese-/Schreibspeicherbereich enthalten, der verwendet werden kann, um persönliche Information in der Karte selbst zu speichern, d. h., Internet-Cookies, Benutzerprofile, usw.. Dieser Speicherbereich kann entweder offen sein, zu jeder Zeit gelesen zu werden oder so ausgeführt werden, das Entsperren durch einen gültigen PIN-Code anzufordern.

[0090] Der Kartenhalter kann außerdem weitere Transaktionsdaten auf dem Tastenfeld der Karte eingeben, beispielsweise einen Transaktionsbetrag, verfügbare Optionen, geheime Abstimmungen, usw.

[0091] Die CID zusammen mit unterschiedlichen Eingaben kann auch so eingerichtet sein, um automatisch eine Benutzeranwendungsumgebung zu steuern, um eine vorgegebene Stelle zu verbinden, beispielsweise ein URL des Internets, eine bestimmte Hausstelle eines Mailbox-Betrags usw..

[0092] Weitere vorteilhafte Merkmale der Transaktionseinrichtung sind:
Die einfache Ausbildung des Lesers erlaubt die Verwendung von Zuhause, wo ein Personal-Desktop oder ein Palmtop-Computer als TT verwendet werden kann, mit einer einfachen herunterladbaren Internet-Software.

[0093] Eine Festkörper-, ein Drahtlos- und eine geschlossene Ausbildung erlaubt das geschlossene TT, ohne Teile oder Schlitze zu bewegen.

[0094] Keine Verschlechterung aufgrund von Wasser, Feuchtigkeit, Korrosion, Magnetfeldern, usw..

[0095] Die kapazitive Kopplung verhindert eine drahtlose Abhörung an Information, was bei Funkfrequenzkarten, welche heutzutage verfügbar sind, nicht der Fall ist.

[0096] Konstruktive Ausbildung niedriger Leistung der CI und der Karte.

Patentansprüche

1. Verfahren zur Identifikation und Authentifizierung des Inhabers eines mobilen elektronischen Transaktionsgeräts (**10**) in einem elektronischen Transaktionsvorgang zwischen einem Transaktion-Dienstleister (**72**) und einem Transaktion-Endgerät (**68**), die über ein Computernetzwerk (**70**) miteinander kommunizieren, wobei das mobile Transaktionsgerät
Sende-Empfangsmittel (**38**) zur Übermittlung von Informationen zum Transaktion-Endgerät und für den Empfang von Informationen von demselben,
Dateneingabemittel (**14**),
Datenverarbeitungsmittel (**50**),

Datenspeichermittel (**50**) mit darin gespeicherten Informationen, wobei die Informationen eine von aussen zugängliche Gerätekennung (ID), eine nicht abrufbare Bezugs-Benutzeridentifikation (PIN) und
einen nicht abrufbaren Geheimschlüssel (SK), der von den Verarbeitungsmitteln verarbeitet und von den Sende-Empfangsmitteln in der Kommunikation mit dem Dienstleister über das Netzwerk und das Transaktions-Endgerät verwendet wird, um eine Transaktion zu validieren, und
Mittel zur Stromversorgung des Geräts aufweist,
dadurch gekennzeichnet, dass bei der Verwendung des mobilen elektronischen Transaktionsgeräts in einem elektronischen Transaktionsvorgang zwischen dem Transaktion-Dienstleister (**72**) und dem Transaktion-Endgerät (**68**), die über ein Computernetzwerk (**70**) miteinander kommunizieren, das Gerät die Gerätekennung (ID) an das Transaktion-Endgerät (**68**) übermittelt;
der Dienstleister (**72**) über das Transaktion-Endgerät eine Transaktionskennungsaufforderung (TID) an das Gerät übermittelt;
der Inhaber mit den Eingabemitteln (**14**) eine Benutzeridentifikation eingibt;
das Verarbeitungsmittel (**50**) die Authentizität der eingegebenen Identifikation durch Vergleichen mit der Bezugs-Benutzeridentifikation (PIN) erkennt; und
nur dann, wenn die Identifikationseingabe als authentisch erkannt wurde:
– das Verarbeitungsmittel (**50**) anhand des Geheimschlüssels (SK) eine Verschlüsselung der Transaktionskennung (TID) durchführt; und
– über das Transaktion-Endgerät ein Antwort-Resultat der Verschlüsselung an den Dienstleister übermittelt, um die Transaktion zu validieren.

2. Verfahren nach Anspruch 1, wobei der Inhaber die Bezugsidentifikation vor der ersten Verwendung des Transaktiongeräts eingibt.

3. Verfahren nach Anspruch 1, wobei die Sende-Empfangsmittel automatisch mit dem Dienstleister kommunizieren, wenn das Gerät in unmittelbare Nähe zum Transaktion-Endgerät gebracht wird.

4. Mobiles elektronisches Transaktionsgerät (**10**) zur Identifikation und Authentifizierung des Inhabers des Geräts in einem elektronischen Transaktionsvorgang zwischen einem Transaktions-Dienstleister (**72**) und einem Transaktion-Endgerät (**68**), die über ein Computernetzwerk (**70**) miteinander kommunizieren, wobei das mobile Transaktionsgerät beinhaltet:
Dateneingabemittel (**14**) zum Eingeben einer Benutzeridentifikation durch den Benutzer,
Datenverarbeitungsmittel (**50**),
Datenspeichermittel (**50**) zum Speichern von Informationen, wobei die Informationen eine von aussen zugängliche Vorrichtungs-Identität (ID) umfassen,
Sende-Empfangsmittel (**38**) zum Übermitteln von Informationen zum und vom Transaktion-Endgerät, einschliesslich der Übermittlung der Gerätekennung zum Transaktion-Endgerät,
Mittel zur Stromversorgung des Geräts, dadurch gekennzeichnet, dass
die Sende-Empfangsmittel (**38**) in der Lage sind, über das Transaktions-Endgerät (**68**) eine Transaktionskennungsaufforderung (TID) vom Dienstleister zu empfangen,
die Datenspeichermittel zum Speichern von Informationen eine nicht abrufbare Bezugs-Benutzeridentifikation (PIN) und einen nicht abrufbaren Geheimschlüssel (SK) beinhalten, der von den Verarbeitungsmitteln (**50**) verarbeitet und von den Sende-Empfangsmitteln (**38**) in der Kommunikation mit dem Dienstleister (**72**) über das Netzwerk (**70**) und das Transaktion-Endgerät (**68**) verwendet wird,
die Verarbeitungsmittel (**50**) in der Lage sind, die Authentizität einer Benutzeridentifikationseingabe durch den Vergleich der eingegebenen Benutzeridentifikation mit der nicht abrufbaren Bezugs-Benutzeridentifikation (PIN) in den Speichermitteln (**50**) zu erkennen, und nur dann, wenn die Identifikationseingabe als authentisch erkannt wurde, anhand des in den Datenspeichermitteln (**50**) gespeicherten Geheimschlüssels (SK) eine Verschlüsselung der Transaktionskennung (TID) durchgeführt wird,
wobei die Sende-Empfangsmittel (**38**) auch in der Lage sind, ein Antwort-Resultat der Verschlüsselung über das Transaktion-Endgerät (**68**) an den Dienstleister (**72**) zu übermitteln, um die Transaktion zu validieren.

5. Gerät nach Anspruch 4, wobei die Sende-Empfangsmittel einen ersten Sende-Empfänger beinhalten, um mit dem Dienstleister zu kommunizieren, wenn das Gerät in die Nähe eines zweiten Sende-Empfängers gebracht wird, der zum Transaktions-Endgerät gehört.

6. Gerät nach Anspruch 5, wobei der erste und der zweite Sende-Empfänger den ersten bzw. den zweiten Teil einer elektrischen Schaltung bilden, wobei der erste Teil im Gerät und der zweite Teil im Transaktion-Endgerät enthalten ist und die Schaltung physisch in die genannten Einheiten unterteilt ist in einem Bereich, der das jeweilige Dielektrikum einer Mehrzahl von an der Schaltung angeschlossenen Kondensatoren bildet, wenn die Karte in die Nähe des Transaktion-Endgeräts gebracht wird.

7. Gerät nach Anspruch 6, wobei das Mittel zur Stromversorgung des Geräts in dem ersten und dem zweiten Teil der elektrischen Schaltung enthalten ist.

8. Gerät nach Anspruch 4, wobei das Gerät die Form einer Kreditkarte hat.

Es folgen 5 Blatt Zeichnungen

Anhängende Zeichnungen

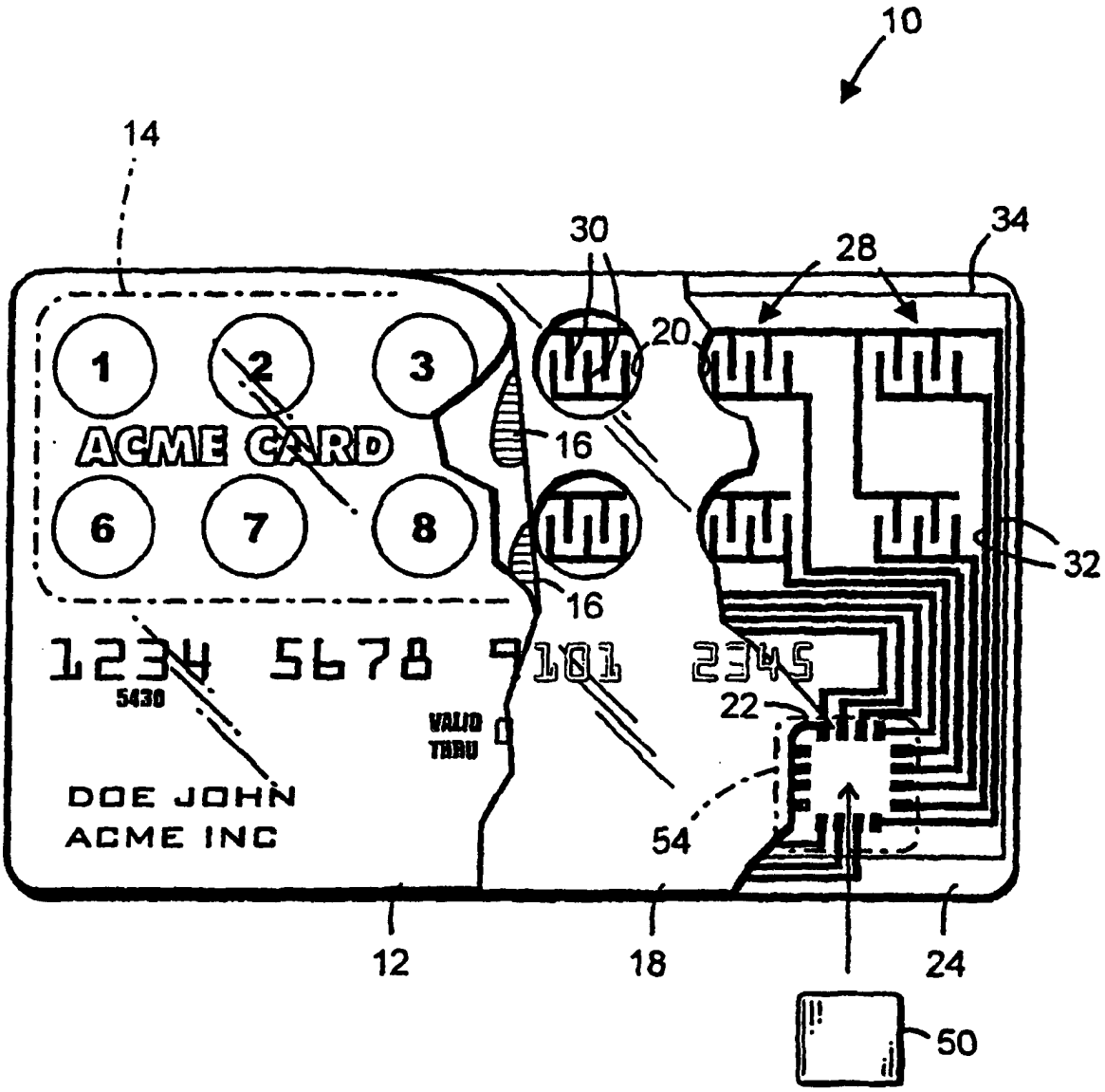

Fig. 1

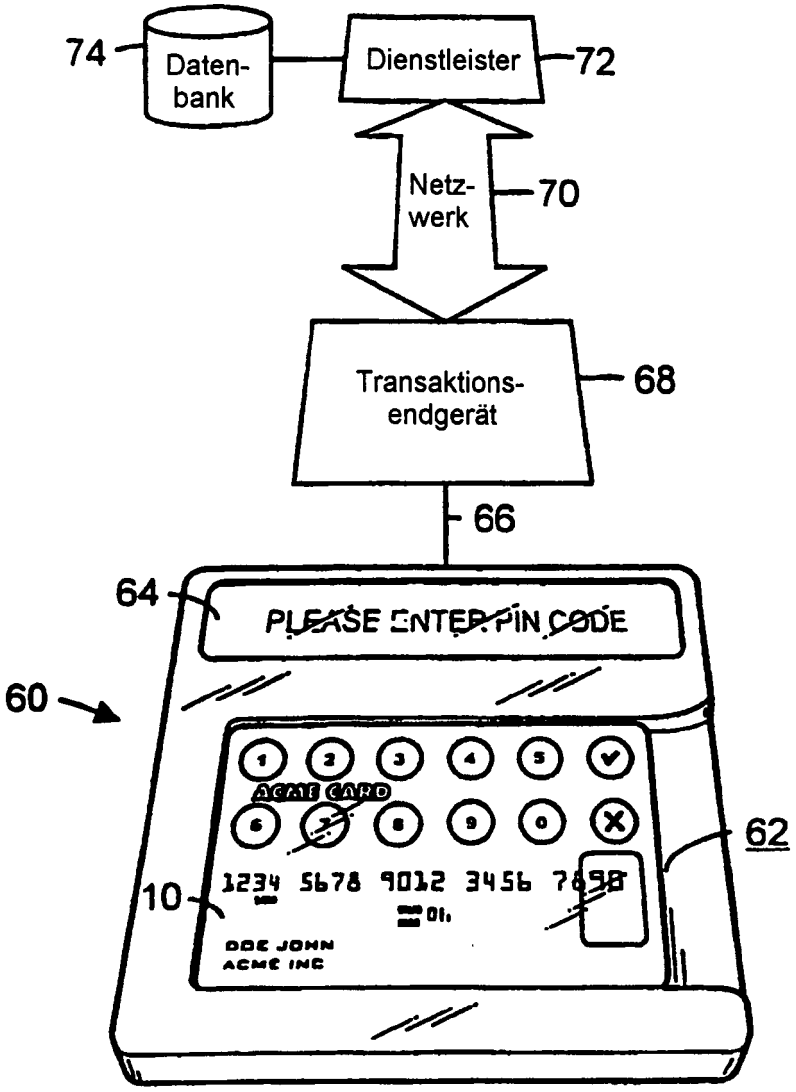
74
Daten-
bank
Dienstleister
72
Netz-
werk
70
Transaktions-
endgerät
68
66
64
PLEASE ENTER PIN CODE
60
ACME CARD
62
1234 5678 9012 3456 7890
10
DOE JOHN
ACME INC

Fig. 2

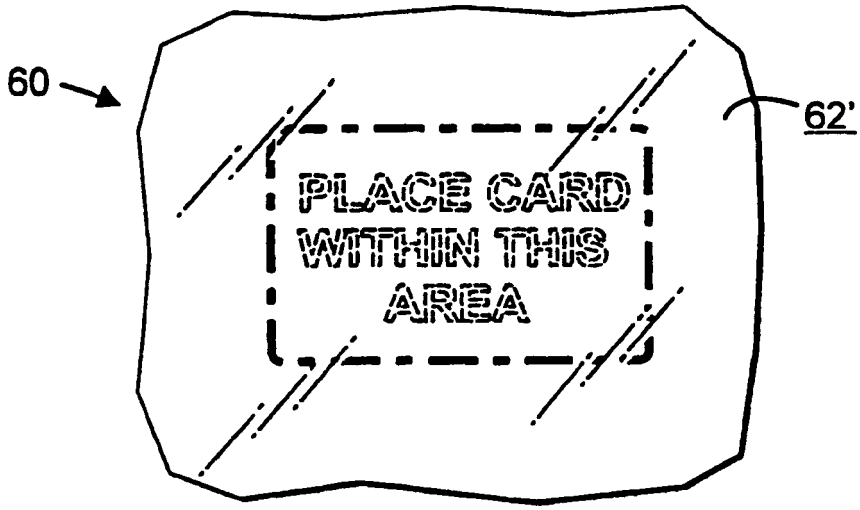
60
62'
PLACE CARD
WITHIN THIS
AREA

Fig. 3

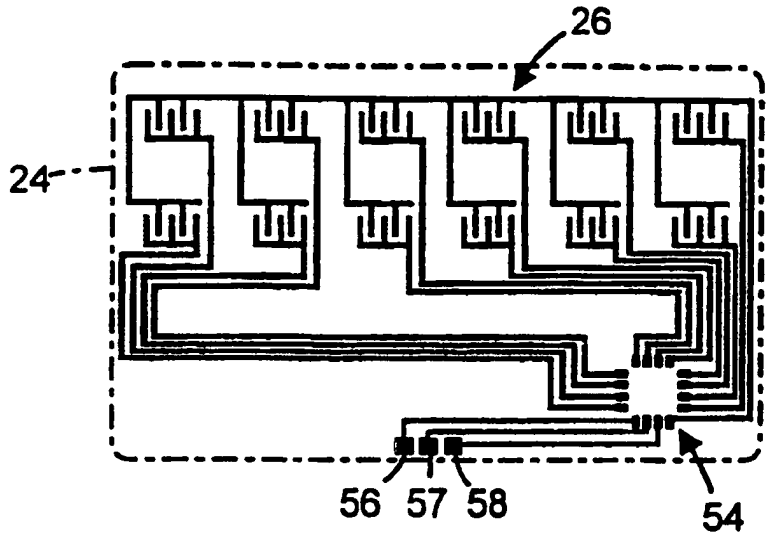

Fig.4

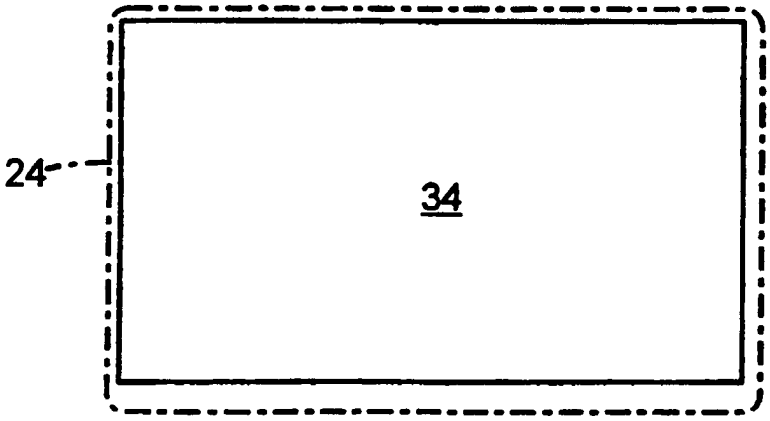

Fig.5

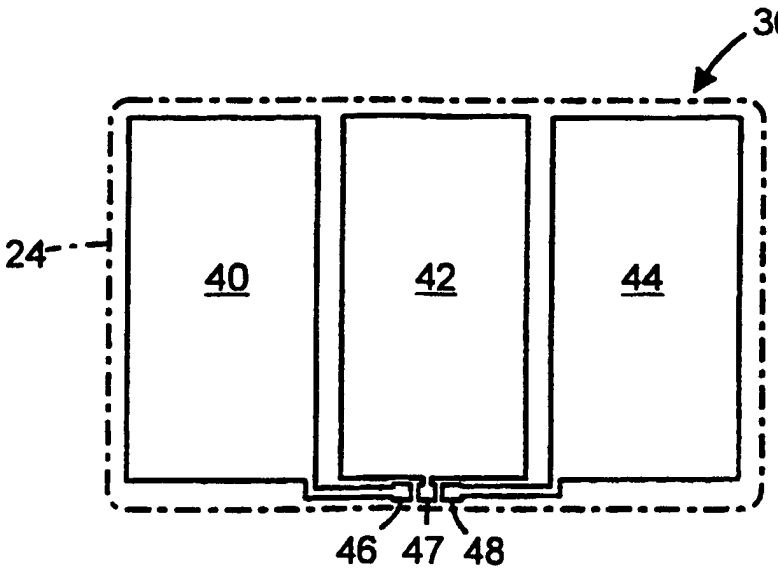

Fig.6

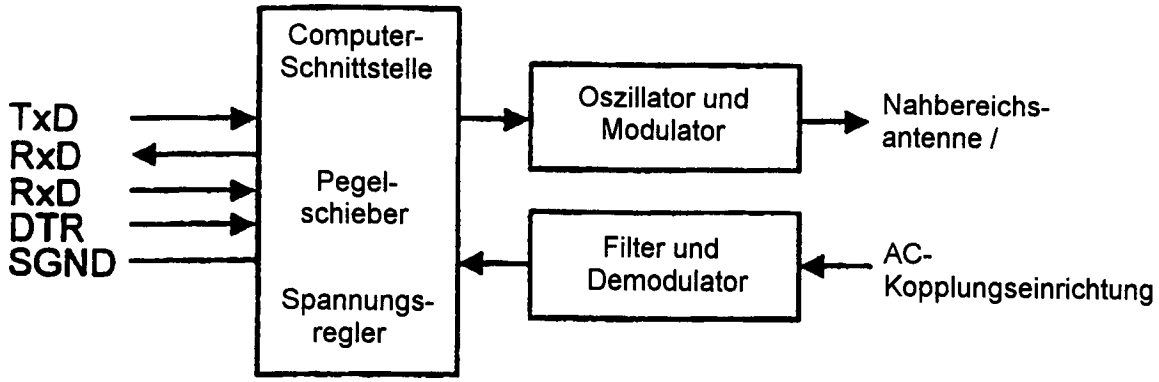
TxD
RxD
RxD
DTR
SGND
Computer-Schnittstelle
Pegel-schieber
Spannungs-regler
Oszillator und Modulator
Filter und Demodulator
Nahbereichs-antenne /
AC-Kopplungseinrichtung

Fig. 7

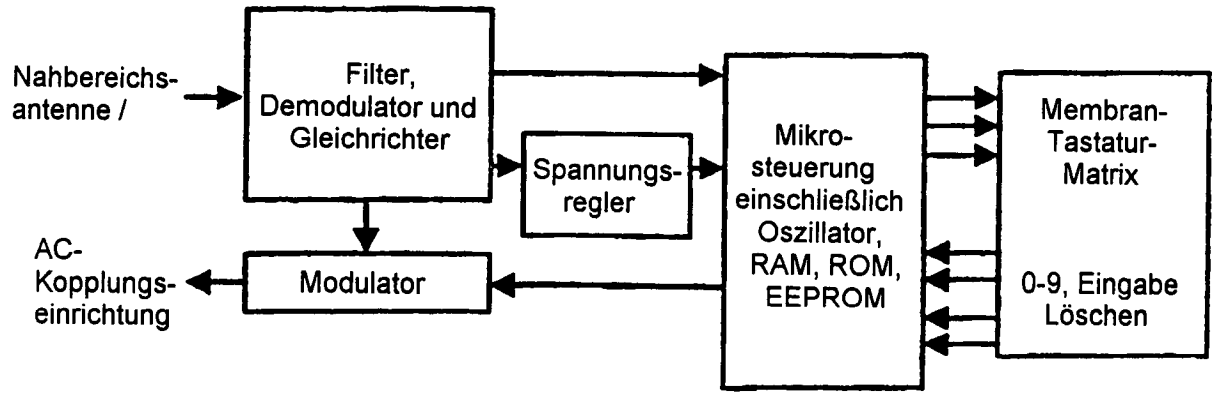
Nahbereichs-antenne /
Filter, Demodulator und Gleichrichter
Spannungs-regler
Mikro-steuerung einschließlich Oszillator, RAM, ROM, EEPROM
Membran-Tastatur-Matrix
0-9, Eingabe Löschen
AC-Kopplungs-einrichtung
Modulator

Fig. 8

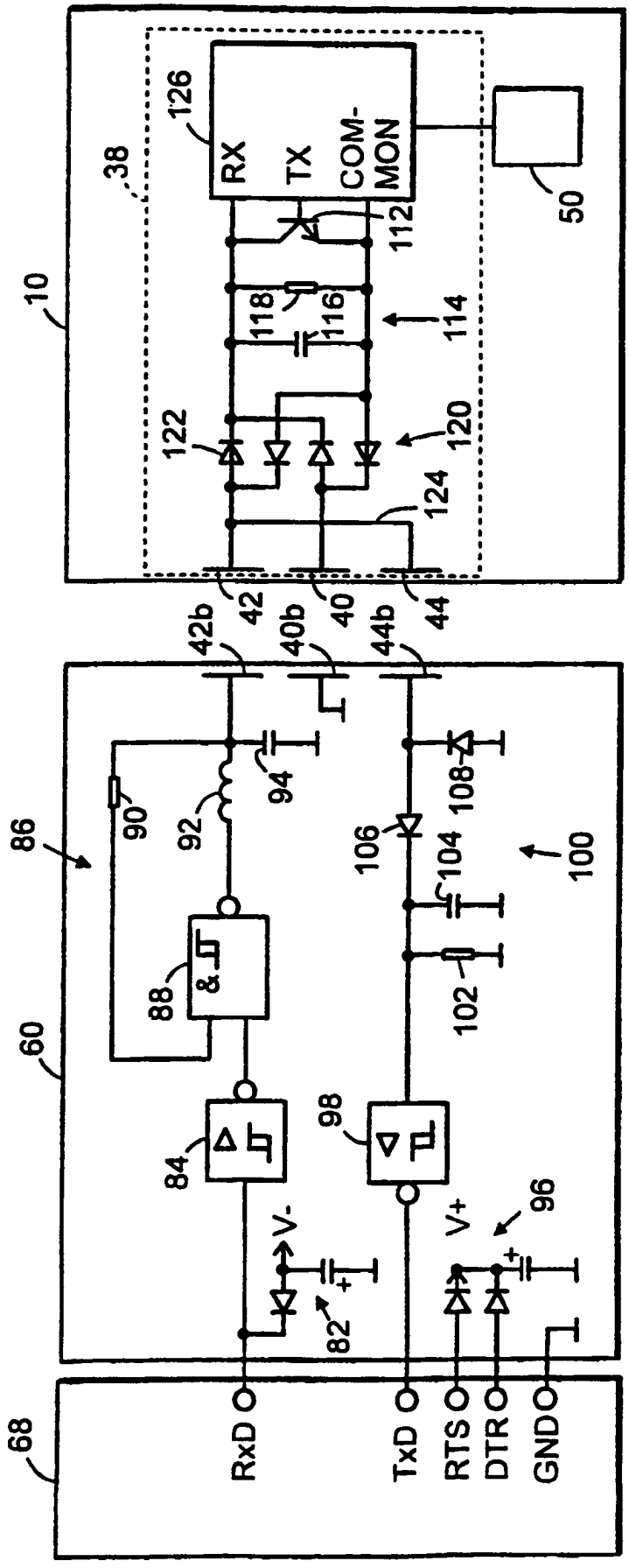
10
38
126
RX
TX
COM-
MON
50
112
118
116
114
122
120
124
42
40
44
42b
40b
44b
86
90
92
94
108
106
104
100
88
102
60
84
98
V-
V+
96
82
68
RxD
TxD
RTS
DTR
GND

Fig. 9