(19) Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 42 30 866 B4** 2004.02.05

(12) # Patentschrift

(21) Aktenzeichen: **P 42 30 866.6**
(22) Anmeldetag: **16.09.1992**
(43) Offenlegungstag: **17.03.1994**
(45) Veröffentlichungstag
der Patenterteilung: **05.02.2004**

(51) Int Cl.[7]: **G07F 7/08**
G07F 7/10, G06K 19/067, G11C 7/00

Innerhalb von 3 Monaten nach Veröffentlichung der Erteilung kann Einspruch erhoben werden.

(71) Patentinhaber:
Venture Engineering Managementgesellschaft mbH, 45468 Mülheim, DE

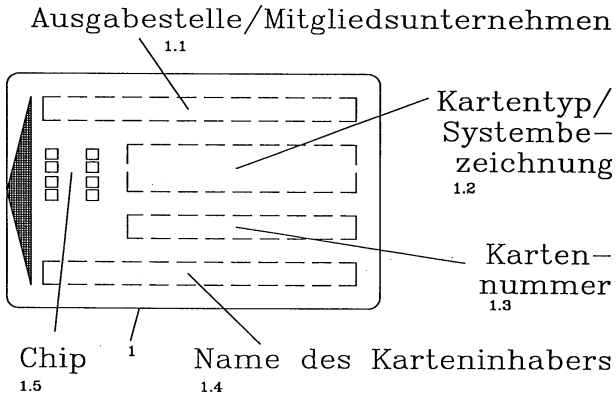
(74) Vertreter:
Patent- und Rechtsanwaltskanzlei Dipl.-Ing. P.-C. Sroka, Jan Sroka, 40545 Düsseldorf

(72) Erfinder:
Dietz, Christian, 45470 Mülheim, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:
DE 38 11 378 C2
DE 37 36 854 C2
DE 30 31 470 C2
DE 28 40 325 C2
DE 40 13 147 A1
DE 39 29 879 A1
DE 39 06 349 A1
DE 37 04 814 A1
US 46 97 072
MEULEN van der, Y.J.; PROEBSTER,W.E.: Memory Access to a Chip Card. In: IBM Technical Disclosure Bulletin, Vol.24,No.7B, Dec.1981, S.3883-3884;

(54) Bezeichnung: **Datenaustauschsystem**

(57) Hauptanspruch: Datenaustauschsystem, bestehend aus mindestens einer Einausgabeeinrichtung (2) und mindestens einem, einen oder mehrere integrierte Schaltkreise enthaltenden, portablen Datenträger (1), in welchem sich ein Wertspeicher (1.6) befindet, in den ein Zahlenwert einspeicherbar ist, der auslesbar, dekrementierbar und wiederholt inkrementierbar ist, wobei mindestens eine Einausgabeeinrichtung (2) zum Auslesen und Dekrementieren des im Wertspeicher (1.6) gespeicherten Zahlenwertes und mindestens eine Einausgabeeinrichtung (2) zum Inkrementieren des im Wertspeicher (1.6) gespeicherten Zahlenwertes ausgerüstet ist und der Datenträger (1) Einrichtungen (1.7) enthält, die ein beliebiges Auslesen sowie ein Dekrementieren des im Wertspeicher (1.6) gespeicherten Zahlenwertes von der Einausgabeeinrichtung (2) aus zulassen, während sie das Inkrementieren des im Wertspeicher (1.6) gespeicherten Zahlenwertes von der Einausgabeeinrichtung (2) aus nur nach Eingabe einer Legitimationsinformation zulassen.



Beschreibung

[0001] Gegenstand der Erfindung ist ein Datenaustauschsystem, bestehend aus mindestens einer Einausgabeeinrichtung und mindestens einem, einen oder mehrere integrierte Schaltkreise enthaltenden, portablen Datenträger, in welchem sich ein Wertspeicher befindet, in den ein Zahlenwert einspeicherbar ist, wobei der Zahlenwert mittels der Einausgabeeinrichtung auslesbar und dekrementierbar ist.

Stand der Technik

[0002] Derartige Datenaustauschsysteme sind an sich bekannt. Sie bestehen im wesentlichen aus einer Einausgabeeinrichtung in Form von einem oder mehreren Terminals und einem oder mehreren portablen, je einen oder mehrere integrierte Schaltkreise enthaltenden Datenträger, z.B. in Form einer Chipkarte. Ein bekanntes Beispiel für ein derartiges Datenaustauschsystem ist das öffentliche Kartentelefon der Deutschen Bundespost. Als Datenträger dient eine als "Wertkarte" oder auch "Guthaben-Karte" bezeichnete Chipkarte, in deren Wertspeicher ein Zahlenwert eingespeichert ist, der einen Geldbetrag repräsentiert. Durch Dekrementieren des Zahlenwertes nach dem Einstecken der Chipkarte in das Kartentelefon wird der Geldbetrag elektronisch verringert bis er schließlich verbraucht ist. Die nicht wiederverwendbare Wertkarte wird sodann vom Benutzer zurückgegeben und vernichtet und es wird eine neue Wertkarte gekauft, in die wiederum ein den gewünschten Geldbetrag repräsentierender Zahlenwert eingespeichert ist. Eine derartige Wertkarte ist beispielsweise in der EP 0 328 124 A2 beschrieben. Ein Nachteil des bekannten Datenaustauschsystems besteht darin, daß der Benutzer die Wertkarte nicht selbst wieder aufladen kann, sondern eine neue Wertkarte erwerben muß und daß die Verwendung der Wertkarte nur für einen sehr eng umgrenzten Zweck, beispielsweise zum Telefonieren, verwendbar ist.

[0003] Es sind auch über Chipkarten steuerbare Kommunikationssysteme bekannt, bei denen die Chipkarte selbst keinen Wertspeicher enthält und somit auch keinen Geldbetrag repräsentiert, sondern lediglich zur Legitimation von Buchungsvorgängen dient, bei denen von einem Abbuchungskonto des Karteninhabers bestimmte Beträge abgebucht werden. Beispiele für derartige Chipkarten sind Kreditkarten, Scheckkarten oder Zugangsberechtigungskarten. Bei ihnen muß, bevor die gewünschte Abbuchung vorgenommen oder der gewünschte Zugang freigegeben wird, überprüft werden, ob der Kartenbenutzer zur Benutzung berechtigt ist. Dies kann beispielsweise durch Eingabe einer sogenannten "PIN-Nummer" an der Einausgabeeinrichtung geschehen. Es sind eine Reihe von Verfahren entwickelt worden, um bei derartigen Systemen den Mißbrauch oder die Manipulation der Chipkarte zu verhindern und die Geheimhaltung der in ihr gespeicherten Daten sicherzustellen. Es wird hierzu beispielsweise hingewiesen auf die DE 26 21 269 C2, die DE 38 09 028 A1 und die EP 0 203 543 B1.

[0004] Die Systeme der zweitgenannten Kategorie haben den Nachteil, daß bei ihrer Verwendung zum Erwerb von Waren oder Dienstleistungen die Anonymität nicht sichergestellt ist und daß sowohl die Handhabung durch den Benutzer als auch die ständig notwendigen Überprüfungsverfahren einen relativ hohen technischen und zeitlichen Aufwand erfordern.

[0005] In DE 28 40 325 C2 ist eine Anordnung zum Verbuchen vorbestimmter gleichartiger Einheiten beschrieben mit einem beispielsweise als Chipkarte ausgebildeten Informationsträger, der einen Speicher zum Speichern der Informationen aufweist, sowie einer externen Vorrichtung, durch die auf die auf dem Speicher gespeicherte Information eingewirkt werden kann, und eine Einrichtung zum Ankoppeln des Informationsträgers an die externe Vorrichtung, um Daten auszutauschen. Bei dieser bekannten Anordnung ist der Speicher in mehrere Zonen aufgeteilt, welche durch Eingabe eines Informationsbits in ein Freigabefeld zur Abbuchung freigegeben werden. Es werden jeweils nur soviele Zonen freigegeben, wie vom Benutzer bezahlt worden sind. Der Maximalwert des Speicherinhalts ist von vornherein festgelegt und im Speicher vorhanden. Nach Freigabe und Verbrauch der letzten Zone ist der Speicher leer und kann nicht wieder aufgeladen werden, wodurch die Karte unbrauchbar wird.

[0006] Der Erfindung liegt die Aufgabe zugrunde, ein Datenaustauschsystem der eingangs beschriebenen Art so auszugestalten, daß mit einem portablen Datenträger, z.B. in Form einer Chipkarte, dem Benutzer der bargeldlose Zugang zu sehr unterschiedlichen Dienstleistungen oder Warenkäufen ermöglicht wird. Dabei sollte einerseits die Inanspruchnahme der Dienstleistung oder des Warenkaufs ohne großen technischen Aufwand und völlig anonym möglich sein, andererseits sollte eine "Wiederaufladung" des Datenträgers möglich sein, die sowohl eine Legitimationsprüfung als auch vielfältige Möglichkeiten zum Schutz gegen Mißbrauch umfaßt.

[0007] Die Lösung dieser Aufgabe geschieht erfindungsgemäß mit den Merkmalen aus dem Patentanspruch 1. Vorteilhafte Weiterbildungen der Erfindung sind in den Unteransprüchen beschrieben.

[0008] Der Grundgedanke der Erfindung besteht darin, daß die Eigenschaften einer üblichen Wertkarte – wie z.B. einer Telefonkarte – mit den Eigenschaften einer Kreditkarte verknüpft sind. Die Benutzung des Datenträgers bei der Inanspruchnahme einer Dienstleistung oder beim Kauf einer Ware geht ohne Identifikation des Benutzers, ohne hohen technischen Aufwand und völlig anonym vor sich. Der Datenträger wird am "point-of-sale" (d.h. beim Dienstleister bzw. Verkäufer) von einer Einausgabeeinrichtung gelesen, und der Preis wird von dem im Datenträger gespeicherten Zahlenwert abgebucht. Es ist

keine aufwendige Kommunikation mit einer zentralen Stelle erforderlich, welche die Berechtigung prüft, die Abbuchung vornimmt oder sonstige Transaktionen durchführt. Es müssen am point-of-sale keine "schwarzen Listen" geführt werden. Da die Identität des Benutzers bei diesem Vorgang nicht registriert wird, bleibt er völlig anonym. In jeder dieser Beziehungen hat der Datenträger also die Qualität von Bargeld.

[0009] Die Anwendungsbereiche des erfindungsgemäßen Datenaustauschsystems, bzw. eines solchen Datenträgers, sind sehr vielfältig. Neben dem Gebrauch an öffentlichen Telefonen kann ein solcher Datenträger vor allem bei der Nutzung von öffentlichen oder privaten Dienstleistungen eingesetzt werden, wie z.B. im öffentlichen Personennahverkehr, im ruhenden Verkehr (Parkhäuser, Parkplätze) oder bei Freizeiteinrichtungen. Hierzu ist der Datenträger dann in einen "Abbuchungsautomaten" einzugeben, der den für die jeweilige Nutzung nötigen Betrag von dem Datenträger abbucht. Der abgebuchte Betrag wird dann so weiter verarbeitet, daß er zwischen der Ausgabestelle des Datenträgers und dem Inhaber des "Abbuchungsautomaten" abgerechnet wird.

[0010] Ein solcher einmal erworbener Datenträger ist theoretisch unbegrenzte Zeit verwendbar, da er immer wieder "aufgeladen" werden kann. Hierfür sind verschiedene Einrichtungen und Verfahren denkbar. Einerseits könnte das "Aufladen" an speziell hierzu autorisierten "Aufladestellen" möglich sein, an denen der Datenträger durch Zahlung mit Bargeld oder Kreditkarte aufgeladen wird. Andererseits sind Automaten denkbar, an denen dieser Vorgang vom Benutzer selbständig durchgeführt werden kann.

[0011] Verfügt der Benutzer dagegen über ein eigenes Verrechnungskonto, welches für ihn beim Erwerb des Datenträgers eingerichtet wurde, so kann er den Datenträger auch in ein spezielles Einausgabesystem eingeben, welches das Aufladen der Karte vornimmt und gleichzeitig sein Verrechnungskonto mit dem Gegenwert des geladenen Betrages belastet. Die Legitimation dieses Vorgangs könnte das Einausgabesystem z.B. dadurch überprüfen, daß die Einausgabeeinrichtung die Berechtigung des Benutzers überprüft und dieser sich mittels Eingabe einer persönlichen Geheimnummer identifiziert. Ein solcher "Aufladevorgang" einschließlich der Überprüfung der Berechtigung und Legitimation kann sowohl selbstständig über eine Einausgabeeinrichtung als auch mittels einer on-line-Verbindung zu einem übergeordneten System abgewickelt werden. Im letzteren Fall sind als "Einausgabeeinrichtung" die verschiedensten Vorrichtungen denkbar. Hierzu könnten z.B. vorhandene Automaten wie Fahrkarten- oder Geldausgabeautomaten benutzt werden. Auch ist denkbar, daß dieser Aufladevorgang an speziell hierfür ausgerüsteten Telefonen durchgeführt werden kann, über welche die genannte On-line-Verbindung hergestellt wird.

[0012] Die Wirkungsweise üblicher portabler Datenträger mit nichtflüchtigen Speichern – insbesondere von Chipkarten – ist an sich bekannt. Von außen wird in Form elektrischer Signale, in der Regel als Zeichenfolge, die Adresse eines bestimmten Speicherplatzes vorgegeben und dessen Inhalt – in der Regel ein Zeichen – wird gelesen und nach außen übermittelt, oder ein ebenfalls von außen übertragenes Zeichen wird in den Speicherplatz eingeschrieben. Bei einer einfachsten Form dieses Verfahrens kann auf alle Speicherplätze lesend und schreibend zugegriffen werden. Wie bereits oben erwähnt, sind darüber hinaus Chipkarten bekannt, die Schutzmechanismen in Form logischer Schaltungen enthalten, welche den lesenden und/oder schreibenden Zugriff auf alle oder bestimmte Speicherplätze verhindern, wenn nicht vorher von außen ein bestimmter Code (z.B: die sogenannte PIN) übermittelt und auf Übereinstimmung mit einem in der Chipkarte enthaltenen, von außen nicht zugreifbaren Code überprüft wurde.

[0013] Zur Lösung des der Erfindung zugrunde liegenden Problems sind diese bekannten Anordnungen nicht geeignet, da bei ihnen der Zugriff auf bestimmte Speicherplätze entweder frei oder erst nach Eingabe der Legitimationsinformation möglich ist. Das der Erfindung zugrunde liegende Problem liegt darin, daß der Zugang zum Wertspeicher, der den Zahlenwert enthält, welcher einen Geldbetrag repräsentiert, beim bloßen Auslesen und beim Abbuchen frei sein soll, während er beim Wiederaufladen nur bei gegebener Legimitation möglich oder völlig frei sein soll. Der Unterschied liegt darin, daß in einem Fall der Inhalt erniedrigt wird oder unverändert bleibt, während er in dem anderen Fall erhöht werden soll. Die Erfindung sieht hierfür eine logische Anordnung auf dem Datenträger vor, welche bei bestimmten Speicherplätzen die von außen übermittelte, neue Information mit dem alten Inhalt vergleicht und das Beschreiben mit dem neuen Wert nur zuläßt, wenn er entweder gleich dem alten oder niedriger als dieser ist, oder, falls dies nicht zutrifft, wenn eine Legitimation vorliegt.

[0014] Wie weiter unten anhand eines Ausführungsbeispiels näher erläutert, sind bei dem erfindungsgemäßen Datenaustauschsystem unterschiedliche Verfahren zur Überprüfung der Legitimation und zur Verhinderung von Mißbrauch in technisch einfacher Weise verwirklichbar. Die Einrichtungen im Datenträger zum Ein/Auslesen von Daten sowie zum Vergleichen und/oder Verschlüsseln und Entschlüsseln von Codes können einerseits durch logische Schaltungen verwirklicht sein, andererseits ist es aber auch möglich, diese Funktionen mittels eines im Datenträger angeordneten programmierbaren Prozessors mit Speicher durchzuführen.

[0015] Weiterhin kann es für bestimmte Anwendungsarten zweckmäßig sein, wenn das erfindungsgemäße Datenaustauschsystem eine Vielzahl von Einausgabeeinrichtungen enthält, von denen eine erste Gruppe lediglich mit Vorrichtungen zum Auslesen und Dekrementieren des im Wertspeicher ge-

speicherten Zahlenwertes ausgerüstet ist, während eine zweite Gruppe allein oder zusätzlich mit Einrichtungen zum Inkrementieren des im Wertspeicher gespeicherten Zahlenwertes ausgerüstet ist.

Ausführungsbeispiel

[0016] Im folgenden werden anhand der beigefügten Zeichnungen Ausführungsbeispiele für Datenaustauschsysteme nach der Erfindung sowie für die mit ihnen durchführbaren Verfahren zum Austausch von Daten und zur Sicherung gegen Mißbrauch des Datenträgers oder der Einausgabevorrichtung näher erläutert.

[0017] In den Zeichnungen zeigen:

[0018] **Fig.** 1 einen Datenträger im Form einer Chipkarte; **Fig.** 2 in einem Prinzipschaltbild eine Einausgabeeinrichtung sowie einen Datenträger mit den Einrichtungen zum Ein/Auslesen des Wertspeichers;

[0019] **Fig.** 3 in einer Darstellung analog **Fig.** 2 die Einausgabeeinrichtung und den Datenträger mit den Einrichtungsteilen zum Ein/Auslesen eines Speichers für eine PIN;

[0020] **Fig.** 4 in einer Darstellung analog **Fig.** 2 die Einausgabeeinrichtung und den Datenträger mit den Einrichtungsteilen zum Ein/Auslesen eines Speichers für einen Super-Code;

[0021] **Fig.** 5 in einer Darstellung analog **Fig.** 2 die Einausgabeeinrichtung und den Datenträger mit den Einrichtungsteilen zum Ein/Auslesen eines Speichers für einen festen System-Code;

[0022] **Fig.** 6 in einer Darstellung analog **Fig.** 2 die Einausgabeeinrichtung und den Datenträger mit den Einrichtungsteilen zum Ein/Auslesen eines Speichers für einen variablen System-Code;

[0023] **Fig.** 7 in einer Darstellung analog **Fig.** 2 die Einausgabeeinrichtung und den Datenträger mit Mitteln zur Authentizitätsprüfung der Einausgaebeinrichtung;

[0024] **Fig.** 8 in einer Darstellung analog **Fig.** 2 die Einausgabeeinrichtung und den Datenträger mit Mitteln zur Authentizitätsprüfung des Datenträgers;

[0025] **Fig.** 9 in einer Darstellung analog **Fig.** 2 die Einausgabeeinrichtung und den Datenträger mit Mitteln zur Blockierung des Ein/Auslesens des Datenträgers nach einer vorgegebenen Anzahl von Fehlern;

[0026] **Fig.** 10 ein Beispiel für eine Einausgabeeinrichtung und einen Datenträger mit einer Kombination verschiedener Einrichtungsteile zum Ein/Auslesen von Daten und Codes;

[0027] **Fig.** 11 in einer schematischen perspektivischen Darstellung eine Einausgabeeinrichtung in Form einer Abbuchungsvorrichtung für den öffentlichen Personennahverkehr;

[0028] **Fig.** 12 in einer schematischen perspektivischen Darstellung eine Einausgabeeinrichtung in Form einer Abbuchungsvorrichtung in einem Parkhaus;

[0029] **Fig.** 13 in einer schematischen perspektivischen Darstellung eine Ausgabe- und Aufladestation für Benutzer ohne persönliches Verrechnungskonto;

[0030] **Fig.** 14 in einer schematischen perspektivischen Darstellung eine Aufladestation für Benutzer mit persönlichem Verrechnungskonto;

[0031] **Fig.** 15 in einem Blockschaltbild die technischen Merkmale einer On-line-Aufladestation.

[0032] In **Fig.** 1 ist ein Datenträger zur Verwendung bei einem Datenaustauschsystem nach der Erfindung dargestellt. Es handelt sich um einen Datenträger für einen Benutzer mit persönlichem Verrechnungskonto. Der Datenträger besitzt die Form einer üblichen Chip-Karte **1**, in der integrierte elektronische Schaltkreise "sogenannte Chips" **1.5** angeordnet sind. Auf der Außenseite der Karte sind Beschriftungsfelder **1.1** für die Ausgabestelle bzw. das Mitgliedsunternehmen, **1.2** für den Kartentyp bzw. die Systembezeichnung, **1.3** für die Kartennummer und **1.4** für den Namen des Karteninhabers angeordnet.

[0033] Im folgenden wird anhand der **Fig.** 2 bis 10 erläutert, welche Einausgabeverfahren für Daten in Form der einen Geldbetrag repräsentierenden Zahlenwerte sowie der verschiedenen Codes mit einem solchen Datenträger und der entsprechend ausgerüsteten Einausgabeeinrichtung verwirklichbar sind. Dabei sind jeweils nur die für die beschriebene Funktion unmittelbar notwendigen Einrichtungsteile angegeben, während insbesondere die üblichen und an sich bekannten Einrichtungsteile einer Einausgabeeinrichtung nicht näher dargestellt sind.

[0034] In **Fig.** 2 ist ein Datenträger **1** dargestellt, der mit einer Einausgabeeinrichtung **2** zusammenwirkt. Der Datenträger **1** besitzt einen Wertspeicher **1.6**, in dem der den Geldbetrag repräsentierende Zahlenwert gespeichert ist. Von einer Werteingabevorrichtung **2.1** der Einausgabeeinrichtung **2** aus wird ein neuer Zahlenwert in einen Zwischenspeicher **1.8** im Datenträger **1** eingegeben. Aus dem Wertspeicher **1.6** wird der in ihm gespeicherte alte Wert in einen Zwischenspeicher **1.9** eingegeben. Mittels eines Vergleichers **1.7** werden der neue Wert und der alte Wert miteinander verglichen und festgestellt, ob der neu eingegebene Wert gleich oder niedriger ist als der alte, oder, falls dies nicht zutrifft, ob eine Legitimationsinformation vorliegt. Über ein ODER-Glied O1 und ein UND-Glied U1 wird der neue Wert in den Wertspeicher **1.6** nur eingeschrieben, wenn er entweder niedriger ist als der alte Wert, oder wenn die Legitimationsinformation vorliegt.

[0035] Eine Möglichkeit der Eingabe einer Legitimationsinformation ist die Eingabe eines Codes, beispielsweise in Gestalt einer mehrstelligen PIN durch den Benutzer, der nur dem Benutzer bekannt ist. Wie aus **Fig.** 3 ersichtlich, wird von der Einausgabeeinrichtung **2** über die "Eingabe PIN" **2.2** der Code in den Zwischenspeicher **1.12** des Datenträgers **1** eingegeben und dort mittels des Vergleichers **1.11** mit der im aus dem PIN-Speicher **1.10** abgerufenen und im Zwischenspeicher **1**.13 abgelegten alten Wert der PIN verglichen. Im Falle der Übereinstimmung wird die Legitimationsinformation an das ODER-Glied O1 aus

Fig. 2 abgegeben. Der im Datenträger **1** fest einprogrammierte Code wechselt von Datenträger zu Datenträger und ist über die Einausgabeeinrichtung nicht aus dem Datenträger auslesbar. Dies verhindert, daß ein Dritter, der durch Verlust oder Diebstahl in den Besitz des Datenträgers gelangt – aber den Benutzer-Code nicht kennt – den Datenträger zu Lasten des rechtmäßigen Inhabers wieder auflädt.

[0036] Eine Variante dieses Verfahrens ist in **Fig.** 4 dargestellt. Hierbei kann der Benutzer mittels einer geeigneten Einausgabeeinrichtung **2** in den Datenträger **1** einen neuen Benutzer-Code seiner Wahl eingeben. Allerdings ist hierfür zuvor die Eingabe eines nur ihm bekannten Super-Codes notwendig, der ebenfalls nicht auslesbar in einem Super-Code-Speicher **1.14** im Datenträger eingespeichert ist. Der Super-Code wird über ein Eingabeterminal **2.3** der Einausgabeeinrichtung **2** in einen Zwischenspeicher **1.16** des Datenträgers **1** eingegeben und über einen Vergleicher **1.15** mit dem aus dem Speicher **1.14** in den Zwischenspeicher **1.17** abgerufenen Super-Code verglichen. Besteht Übereinstimmung, so wird über ein UND-Glied U2 dem Speicher ein Freigabesignal für die Eingabe einer neuen PIN zugeführt.

[0037] Dies schützt den rechtmäßigen Inhaber vor der befürchteten Inbesitznahme des Datenträgers durch eine Person, die den bisher gültigen Benutzer-Code kennt.

[0038] Nun ist es denkbar, daß ein technisch versierter, rechtmäßiger Inhaber eines Datenträgers eine Vorrichtung baut oder sich eine entsprechende Einausgabeeinrichtung beschafft und diese modifiziert, so daß er den Aufladevorgang unter Umgehung des hierfür vorgesehenen Datenaustauschsystems und der Belastung seines Kontos aber unter Verwendung seines Benutzer-Codes beliebig oft vornehmen kann. Um dieses betrügerische Vorgehen unmöglich zu machen, ist es möglich, eine zusätzliche Schutzvorrichtung mit System-Codes vorzusehen. Sie besteht in einer ersten Variante gemäß **Fig.** 5 darin, daß auf dem Datenträger **1** ein von außen nicht lesend zugreifbarer, für alle Datenträger identischer System-Code in einem System-Code-Speicher **1.8** gespeichert ist. Dieser System-Code wird über den Zwischenspeicher **1.21** einem Vergleicher **1.19** zugeführt und dort mit einem Code verglichen, der automatisch von der Code-Eingabeeinrichtung **2.4** der Einausgabeeinrichtung **2** dem Zwischenspeicher **1.20** im Datenträger **1** zugeführt wird. Nur im Falle der Übereinstimmung wird eine entsprechende Legitimationsinformation abgegeben.

[0039] Um zu verhindern, daß der betrügerische Inhaber des Datenträgers in Kenntnis auch dieses festen System-Codes den Datenträger wie oben beschrieben auflädt, ist gemäß einer zweiten in **Fig.** 6 dargestellten Variante ein variabler System-Code vorgesehen. Dieser System-Code wird am Ende jedes Aufladevorgangs in der Einausgabeeinrichtung **2** oder einem übergeordneten System, beispielsweise als Zufallszahl, erzeugt und dort mit den Inhaber-Daten zusammen registriert und an den Datenträger **1** übermittelt, welcher ihn im Speicher **1.22** speichert. Zu Beginn des nächsten Aufladevorgangs wird dieser variable Code von der Code-Eingabeeinrichtung **2.5** aus dem Zwischenspeicher **1.24** im Datenträger **1** zugeführt und dort mittels des Vergleichers **1.23** mit dem in den Zwischenspeicher **1.25** überführten, zuletzt gespeicherten System-Code verglichen. Nur im Falle der Übereinstimmung wird die Legitimationsinformation abgegeben und über das UND-Glied U3 der jeweils neue System-Code in den Speicher **1.22** eingegeben. Da der betrügerische Inhaber diesen Code nicht kennt, kann er die Karte nicht unter Umgehung des Datenaustauschsystems aufladen.

[0040] Eine weitere Möglichkeit des Schutzes vor betrügerischem Aufladen des Datenträgers besteht darin, daß der Datenträger selbst die Authentizität der Einausgabeeinrichtung überprüft, mit welcher er gerade kommuniziert. Wie aus **Fig.** 7 zu ersehen, erzeugt zu diesem Zweck die Einausgabeeinrichtung **2** zu Beginn der Transaktion mit einem Zufallsgeber **2.6** eine Zufallszahl, die in einer Verschlüsselungseinrichtung **2.8**, beispielsweise mittels eines systemspezifischen Codes **2.7**, verschlüsselt wird. Sowohl die Zufallszahl selbst als auch das Ergebnis der Verschlüsselung werden an den Datenträger **1** übermittelt. Einem Vergleicher **1.8** wird einerseits die von der Einausgabeeinrichtung **2** verschlüsselt übermittelte Zufallszahl und andererseits die im Datenträger **1** mittels der Verschlüsselungseinrichtung **1.26** aufgrund eines systemspezifischen Codes **1.27** verschlüsselte von der Einausgabeeinrichtung **2** direkt übermittelte Zufallszahl zugeführt. Bei Übereinstimmung wird die Legitimationsinformation abgegeben.

[0041] In einem analogen Verfahren, das in **Fig.** 8 dargestellt ist, kann auch die Einausgabeeinrichtung **2** davor geschützt werden, daß sie ausspioniert wird. Auch hier sendet die Einausgabeeinrichtung **2** von einem Zufallsgeber **2.9** aus dem Datenträger direkt eine Zufallszahl zu, die dort in einer Verschlüsselungseinrichtung **1.29** aufgrund eines systemspezifischen Codes **1.3** verschlüsselt und an die Einausgabeeinrichtung **2** zurückgesendet wird. Sie wird in der Einausgabeeinrichtung **2** in einem Vergleicher **2.12** mit der gleichen Zufallszahl verglichen, die in der Verschlüsselungseinrichtung **2.11** der Einausgabeeinrichtung **2** aufgrund des systemspezifischen Codes **2.10** verschlüsselt worden ist. Auch hier wird nur bei Übereinstimmung an die übrigen Einrichtungen der Einausgabeeinrichtung **2** eine Information abgegeben, gemäß der der Datenträger authentisch ist.

[0042] Die Beeinflussung der Verschlüsselungsergebnisse durch systemspezifische Code verhindert, daß ein Betrüger in Kenntnis des Verschlüsselungsverfahrens eine Manupilation des Datenträgers versucht. Dieser die Verschlüsselung beeinflußende systemspezifische Code ist entweder für alle Datenträger und Einausgabeeinrichtungen identisch, oder es können je nach Verwendungsort und -zweck des Datenträgers verschiedene Codes in Frage kommen.

[0043] Schließlich ist es vorstellbar, daß ein Betrüger den Benutzer-Code, den festen System-Code, den Karten-Code oder das verwendete Verschlüsselungsverfahren herausfindet, wenn er nur einen oder mehrere Datenträger, in deren Besitz er gelangt, lange genug mit einer geeigneten Vorrichtung verbindet und die Reaktionen des Datenträgers auf die Übermittlung gezielter Daten untersucht. Um dies zu verhindern, ist es möglich, wie in **Fig.** 9 dargestellt, den Datenträger mit Einrichtungen zu versehen, die fehlerhafte Versuche des Zugriffs registieren und nach einer bestimmten Zahl solcher Versuche den Datenträger für jede weitere Benutzung gleich welcher Art sperren. Hierzu ist beispielsweise im Datenträger **1** für den PIN-Vergleich ein Vergleicher **1.31** und für den Code-Vergleich ein Vergleicher **1.32** vorgesehen, der bei sofortiger korrekter Eingabe, beispielsweise über ein UND-Glied U4, eine Legitimationsinformation abgibt, während fehlerhafte Vergleichsergebnisse jeweils einem Zähler **1.33** bzw. **1.34** zugeführt werden. Nach einer voreingestellten Zahl n von Zählvorgängen geben die Zähler **1.33** und **1.34** über ein ODER-Glied O2 ein Signal ab, welches die Karte blockiert.

[0044] Die oben beschriebenen Möglichkeiten zur Mißbrauchsverhinderung können selbstverständlich innerhalb eines Datenträgers und einer Einausgabeeinrichtung miteinander kombiniert werden. Eine derartige Einrichtung ist in **Fig.** 10 dargestellt. In **Fig.** 10 sind für Einrichtungsteile, die analog den Einrichtungen nach den **Fig.** 2 bis 9 aufgebaut sind, die gleichen Bezugsziffern unter Hinzufügung eines ' oder eines " verwendet. Hinzu kommen in der Einausgabeeinrichtung **2** ein Fehlerzähler **2.13** zur Verhinderung des Ausspionierens einer Einausgabeeinrichtung durch manipulierte oder gefälschte Datenträger, eine Steuervorrichtung **2.14** für das Aufladen, ein Code-Nummernsender **2.15** mit einem Verschlüssler **2.16**, ein Zwischenspeicher **2.17** für den neu eingegebenen Zahlenwert sowie einen Speicher **2.18** für den aus dem Datenträger **1** ausgelesenen alten Wert. Im Datenträger **1** kommen hinzu ein Entschlüsseler **1.35** für die verschlüsselt übermittelte PIN sowie die Code-Nummer, ein zusätzlicher Fehlerzähler **1.36** für die Authentizitätsprüfung der Einausgabeeinrichtung **2** sowie UND-Glieder U5, U6 und U7, die in aus dem Schaltbild abzulesender Weise bestimmte Funktionen innerhalb des Datenträgers freigeben.

[0045] Insgesamt ist das in **Fig.** 10 dargestellte Schaltbild aus sich heraus verständlich und wird daher nicht näher erläutert.

[0046] **Fig.** 11 illustriert eine Anwendungsmöglichkeit des beschriebenen Datenaustauschsystems im öffentlichen Personennahverkehr. In diesem Fall ist die als Fahrpreisabbuchungsautomat ausgebildete Einausgabeeinrichtung beispielsweise in den Fahrzeugen installiert und kann direkt bedient werden, indem die entsprechende Chipkarte in die Datenträgereingabe eingesteckt wird und über die Bedienungseinheit die notwendigen Eingaben durchgeführt werden. Ein Anzeigefeld zeigt die für den Benutzer notwendigen Informationen an.

[0047] **Fig.** 12 zeigt ein Beispiel einer Anwendung des beschriebenen Datenaustauschsystems in einem Parkhaus. An der Einfahrtstation und an der Ausfahrtstation sind entsprechende Buchungsautomaten aufgestellt. Über die Karteneingabe werden die Abbuchungsautomaten betätigt und auf der Anzeigeeinheit die entsprechenden Informationen für die Benutzer angezeigt.

[0048] Der in den Abbuchungsautomaten abgebuchte Betrag wird dann so weiter verarbeitet, daß er zwischen der Ausgabestelle des Datenträgers und dem Inhaber des Abbuchungsautomaten abgerechnet wird.

[0049] **Fig.** 13 zeigt einen Aufladeautomaten, in welchem der Datenträger durch Zahlung mit Bargeld oder Kreditkarte aufgeladen werden kann. Hierzu wird die Chip-Karte in die Datenträger Ein/Ausgabe eingegeben. Die Bezahlung erfolgt über den Münzeinwurf, den Banknotenprüfer oder die Kreditkarteneingabe. Über die Bedienungseinheit mit Tastatur werden die notwendigen Eingaben getätigt und der Bildschirm zeigt dem Benutzer die notwendigen Informationen an.

[0050] Verfügt der Benutzer über ein eigenes Verrechnungskonto, welches für ihn beim Erwerb des Datenträgers eingerichtet wurde, so kann die Aufladung an einem eigens hierfür installierten Automaten durchgeführt werden, wie er beispielsweise in **Fig.** 14 dargestellt ist. In **Fig.** 14 sind die einzelnen Schritte dieses Aufladevorgangs dargestellt, nämlich

1. Eingabe des Datenträgers,
2. Wahl der Funktion "Aufladen",
3. Eingabe der PIN-Nummer,
4. Eingabe des gewünschten Betrages,
5. Entnahme des Datenträgers.

[0051] Die Eingaben erfolgen über die Bedienungseinheit, und am Bildschirm können die notwendigen Informationen abgelesen werden.

[0052] In **Fig.** 15 sind ergänzend zu **Fig.** 14 in einer Prinzipschaltung die Einrichtungsteile einer On-line-Aufladestation dargestellt. Sie sind aus dem Schaltbild heraus verständlich und werden im folgenden nicht näher erläutert.

Patentansprüche

1. Datenaustauschsystem, bestehend aus mindestens einer Einausgabeeinrichtung (**2**) und mindestens einem, einen oder mehrere integrierte Schaltkreise enthaltenden, portablen Datenträger (**1**), in welchem sich ein Wertspeicher (**1.6**) befindet, in den ein Zahlenwert einspeicherbar ist, der auslesbar, dekrementierbar und wiederholt inkrementierbar ist, wobei mindestens eine Einausgabeeinrichtung (**2**) zum Auslesen und Dekrementieren des im Wertspeicher (**1.6**) gespeicherten Zahlenwertes und mindestens eine Einausgabeeinrichtung (**2**) zum Inkre-

mentieren des im Wertspeicher (**1.6**) gespeicherten Zahlenwertes ausgerüstet ist und der Datenträger (**1**) Einrichtungen (**1.7**) enthält, die ein beliebiges Auslesen sowie ein Dekrementieren des im Wertspeicher (**1.6**) gespeicherten Zahlenwertes von der Einausgabeeinrichtung (**2**) aus zulassen, während sie das Inkrementieren des im Wertspeicher (**1.6**) gespeicherten Zahlenwertes von der Einausgabeeinrichtung (**2**) aus nur nach Eingabe einer Legitimationsinformation zulassen.

2. Datenaustauschsystem nach Anspruch 1, dadurch gekennzeichnet, daß der Datenträger (**1**) einen Code-Speicher (**1.10**) enthält, in den ein Benutzer-Code eingespeichert ist, sowie einen Vergleicher (**1.11**) zum Vergleich eines über die Einausgabeeinrichtung (**2**) eingegebenen Codes, mit dem eingespeicherten Benutzercode und zur Abgabe eines Legitimationssignals an die Einrichtung zum Inkrementieren des im Wertspeicher (**1.6**) gespeicherten Zahlenwertes bei Übereinstimmung des eingegebenen Codes mit dem Benutzercode.

3. Datenaustauschsystem nach Anspruch 2, dadurch gekennzeichnet, daß der Benutzercode unveränderbar und nicht aus dem Datenträger (**1**) auslesbar eingespeichert ist.

4. Datenaustauschsystem nach Anspruch 2, dadurch gekennzeichnet, daß der Benutzercode veränderbar eingespeichert ist und der Datenträger (**1**) einen weiteren Codespeicher (**1.14**) enthält, in den ein Supercode unveränderbar und nicht aus dem Datenträger (**1**) auslesbar eingespeichert ist, sowie einen Vergleicher (**1.15**) zum Vergleich eines über die Einausgabeeinrichtung (**2**) eingegebenen Codes mit dem eingespeicherten Supercode und zur Abgabe eines die Änderung des eingespeicherten Benutzercodes über die Einausgabeeinrichtung (**2**) zulassenden Freigabesignals bei Übereinstimmung des eingegebenen Codes mit dem Supercode.

5. Datenaustauschsystem nach Anspruch 3, dadurch gekennzeichnet, daß der eingespeicherte Benutzercode ein unveränderbarer Systemcode ist und dem Vergleicher (**1.19**) über die Einausgabeeinrichtung (**2**) automatisch ein aus einem externen Speicher abgerufener Code zugeführt und mit dem Systemcode verglichen wird.

6. Datenaustauschsystem nach Anspruch 2, dadurch gekennzeichnet, daß der eingespeicherte Benutzercode ein veränderbarer Systemcode ist, der jeweils beim Inkrementieren des im Wertspeicher (**1.6**) gespeicherten Zahlenwertes verändert wird, indem über die Einausgabeeinrichtung (**2**) ein automatisch erzeugter und extern gespeicherter neuer Wert für den Systemcode an den Datenträger (**1**) übermittelt und dort im Codespeicher (**1.22**) eingespeichert wird und beim jeweils nächsten Inkrementierungsvorgang dieser neue Wert des Systemcodes über die Einausgabeeinrichtung (**2**) automatisch dem Vergleicher (**1.23**) des Datenträgers (**1**) zugeführt und mit dem eingespeicherten Systemcode verglichen wird.

7. Datenaustauschsystem nach Anspruch 6, dadurch gekennzeichnet, daß die Werte des Systemcodes als Zufallszahlen erzeugt werden und zusammen mit zusätzlichen Informationen extern gespeichert werden.

8. Datenaustauschsystem nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, daß im Datenträger (**1**) und der Einausgabeeinrichtung (**2**) Einrichtungen (**1.26**, **1.29**, **1.35**; **2.8**, **2.11**, **2.16**) zum Verschlüsseln und Entschlüsseln der ausgetauschten Daten angeordnet sind.

9. Datenaustauschsystem nach einem der Ansprüche 1 bis 8, dadurch gekennzeicnet, daß der Datenträger (**1**) mehrere Wertspeicher enthält.

10. Datenaustauschsystem nach einem der Ansprüche 1 bis 9, dadurch gekennzeichnet, daß im Datenträger eine Verschlüsselungseinrichtung (**1.29**) und in der Einausgabeeinrichtung eine Verschlüsselungseinrichtung (**2.11**) und ein Vergleicher (**2.12**) vorhanden sind zur Authentitätsprüfung des Datenträgers (**1**) durch Abgabe einer Zufallszahl an den Datenträger (**1**) von der Einausgabeeinrichtung (**2**) aus, Verschlüsselung der Zufallszahl im Datenträger, Rückübertragung der verschlüsselten Zufallszahl an die Einausgabeeinrichtung (**2**) und Vergleich der vom Datenträger (**1**) verschlüsselten Zufallszahl, mit der ursprünglich von der Einausgabeeinrichtung (**2**) abgegebenen und verschlüsselten Zufallszahl.

11. Datenaustauschsystem nach einem der Ansprüche 1 bis 10, dadurch gekennzeichnet, daß im Datenträger (**1**) eine Verschlüsselungseinrichtung (**1.26**) und ein Vergleicher (**1.28**) und in der Einausgabeeinrichtung (**2**) eine Verschlüsselungseinrichtung (**2.8**) vorhanden sind zur Authentitätsprüfung der Einausgabeeinrichtung (**2**) durch Abgabe einer Zufallszahl in verschlüsselter und unverschlüsselter Form an den Datenträger (**1**) von der Einausgabeeinrichtung (**2**) aus und Vergleich der im Datenträger verschlüsselten Zufallszahl mit der in der Einausgabeeinrichtung verschlüsselten Zufallszahl im Datenträger (**1**) und Freigabe der geschützten Speicherplätze im Datenträger bei Übereinstimmung.

12. Datenaustauschsystem nach den Ansprüchen 10 oder 11, dadurch gekennzeichnet, daß die Verschlüsselung und Entschlüsselung von zwischen der Einausgabeeinrichtung (**2**) und dem Datenträger (**1**) ausgetauschten Daten unter Einbeziehung eines im Datenträger fest und nicht aus dem Datenträger auslesbar eingespeicherten Kartencodes erfolgt, der in der Einausgabeeinrichtung (**2**) gespeichert, oder

aus einem externen Speicher von ihr abrufbar ist.

13. Datenaustauschsystem nach Anspruch 12, dadurch gekennzeichnet, daß der Kartencode für alle Datenträger (**1**) identisch ist.

14. Datenaustauschsystem nach Anspruch 12, dadurch gekennzeichnet, daß unterschiedliche Kartencodes entsprechend dem Ort oder Zweck der Benutzung des Datenträgers verwendet werden.

15. Datenaustauschsystem nach einem der Ansprüche 1 bis 14, dadurch gekennzeichnet, daß der Datenträger (**1**) Einrichtungen (**1.31**, **1.32**, **1.33**, **1.34**) enthält, durch die nach einer vorgegebenen Anzahl von falsch an den Datenträger (**1**) übermittelten oder falsch entschlüsselten Codes der Datenaustausch abgebrochen und/oder ein Sperrsignal abgegeben wird, das eine die weitere Verwendung des Datenträgers (**1**) ausschließende Veränderung auslöst.

16. Datenaustauschsystem nach einem der Ansprüche 1 bis 15, dadurch gekennzeichnet, daß die Einausgabeeinrichtung (**1**) Einrichtungen (**2.13**) enthält, durch die nach einer vorgegebenen Anzahl falsch an die Einausgabeeinrichtung (**2**) übermittelten oder falsch entschlüsselten Codes der Datenaustausch abgebrochen und/oder ein Sperrsignal abgegeben wird, das eine die weitere Verwendung der Einausgabeeinrichtung (**2**) mindestens für einen vorgegebenen Zeitraum ausschließende Veränderung auslöst.

17. Datenaustauschsystem nach einem der Ansprüche 1 bis 16, dadurch gekennzeichnet, daß die Verbindung des Datenträgers (**1**) mit der Einausgabeeinrichtung (**2**) über eine Schnittstelle mit drahtloser Signalübertragung erfolgt.

18. Datenaustauschsystem nach einem der Ansprüche 1 bis 17, dadurch gekennzeichnet, daß die Einrichtungen im Datenträger (**1**) zum Ein/Auslesen von Daten, sowie zum Vergleich und/oder Verschlüsseln und Entschlüsseln von Codes durch logische Schaltungen verwirklicht sind.

19. Datenaustauschsystem nach einem der Ansprüche 1 bis 17, dadurch gekennzeichnet, daß die Einrichtungen im Datenträger zum Ein/Auslesen von Daten, sowie zum Vergleich und/oder Verschlüsseln und Entschlüsseln von Codes durch einen programmierbaren Prozessor mit Speicher verwirklicht sind.

20. Datenaustauschsystem nach einem der Ansprüche 1 bis 19, dadurch gekennzeichnet, daß es eine Vielzahl von Einausgabeeinrichtungen (**2**) enthält, von denen eine erste Gruppe lediglich mit Einrichtungen zum Auslesen und Dekrementieren des im Wertspeicher gespeicherten Zahlenwertes ausgerüstet ist, während eine zweite Gruppe allein oder zusätzlich mit Einrichtungen zum Inkrementieren des im Wertspeicher gespeicherten Zahlenwertes ausgerüstet ist.

21. Datenaustauschsystem nach Anspruch 20, dadurch gekennzeichnet, daß mindestens ein Teil der mit Einrichtungen zum Inkrementieren ausgerüsteten Einausgabeeinrichtungen (**2**) über eine On-line-Verbindung mit einem Autorisierungsrechner verbunden ist.

22. Datenaustauschsystem nach Anspruch 20 oder 21, dadurch gekennzeichnet, daß mindestens ein Teil der mit Einrichtungen zum Inkrementieren ausgerüsteten Einausgabeeinrichtungen (**2**) als Fahrkartenautomat ausgebildet ist.

23. Datenaustauschsystem nach Anspruch 20 oder 21, dadurch gekennzeichnet, daß mindestens ein Teil der mit Einrichtungen zum Inkrementieren ausgerüsteten Einausgabeeinrichtungen (**2**) als Geldausgabeautomat ausgebildet ist.

24. Datenaustauschsystem nach den Ansprüchen 20 oder 21, dadurch gekennzeichnet, daß mindestens ein Teil der mit Einrichtungen zum Inkrementieren ausgerüsteten Einausgabeeinrichtungen (**2**) als Telefon ausgebildet ist.

Es folgen 8 Blatt Zeichnungen

Anhängende Zeichnungen

Fig. 1

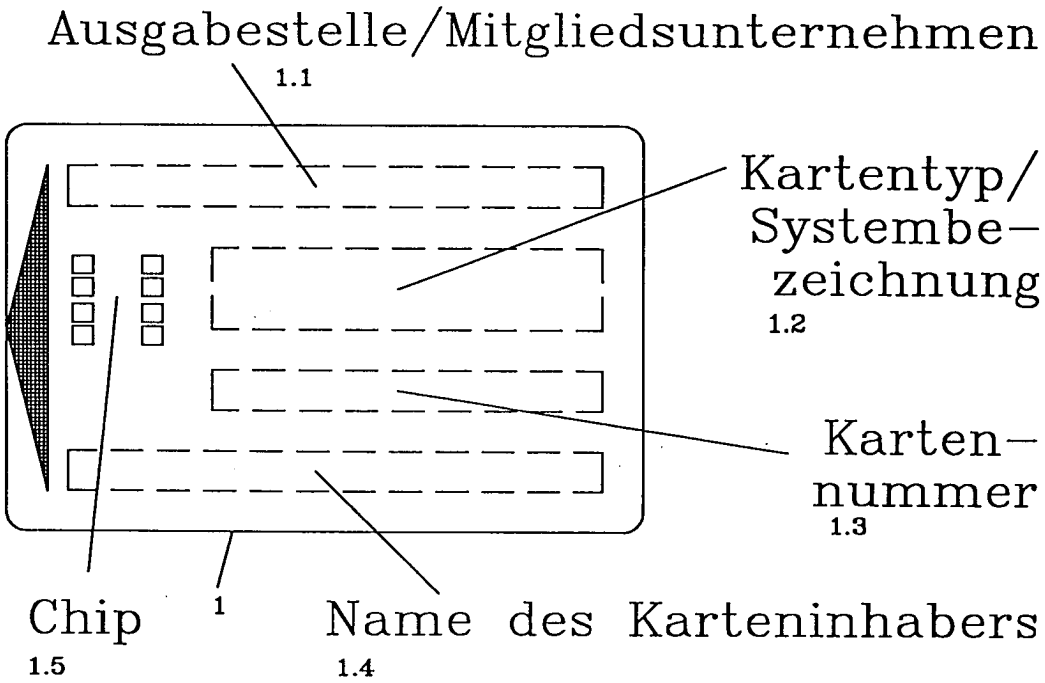


Fig. 2

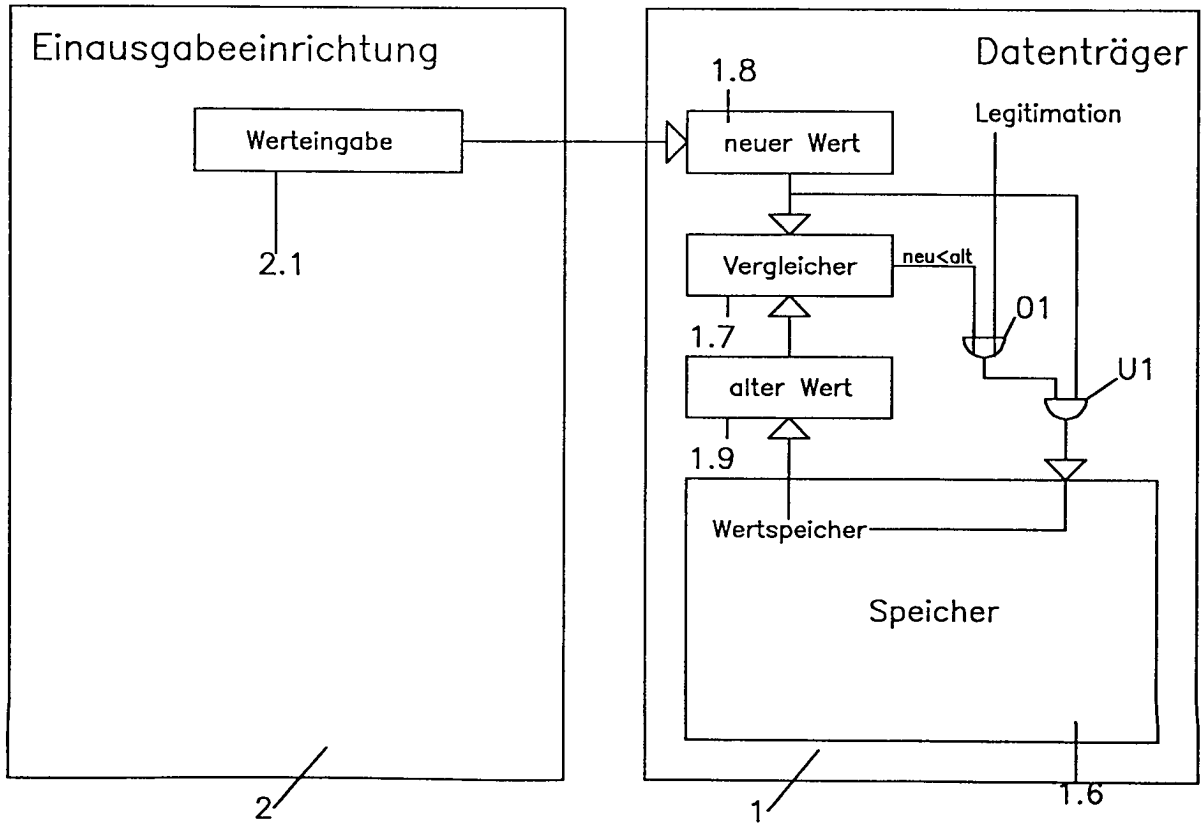


Fig. 3

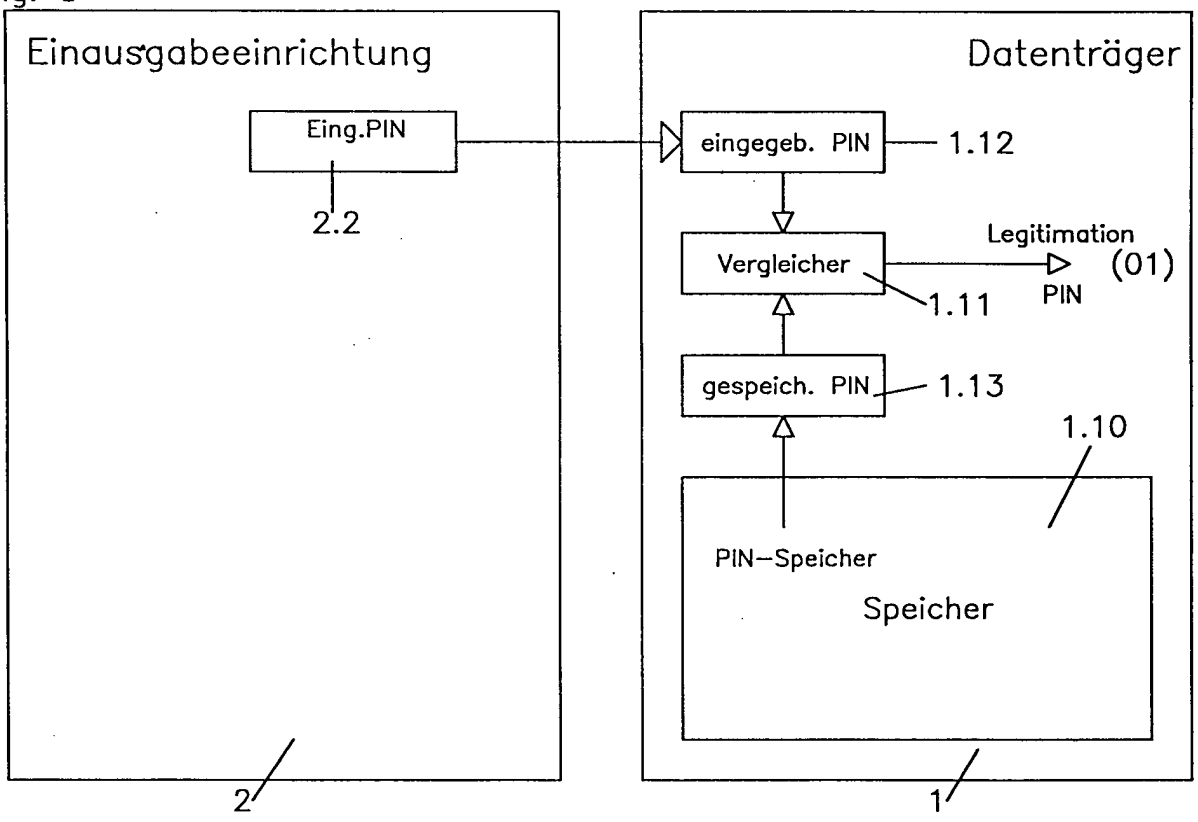

Einausgabeeinrichtung
Eing.PIN
2.2
2
Datenträger
eingegeb. PIN
1.12
Vergleicher
1.11
Legitimation
(01)
PIN
gespeich. PIN
1.13
1.10
PIN–Speicher
Speicher
1

Fig. 4

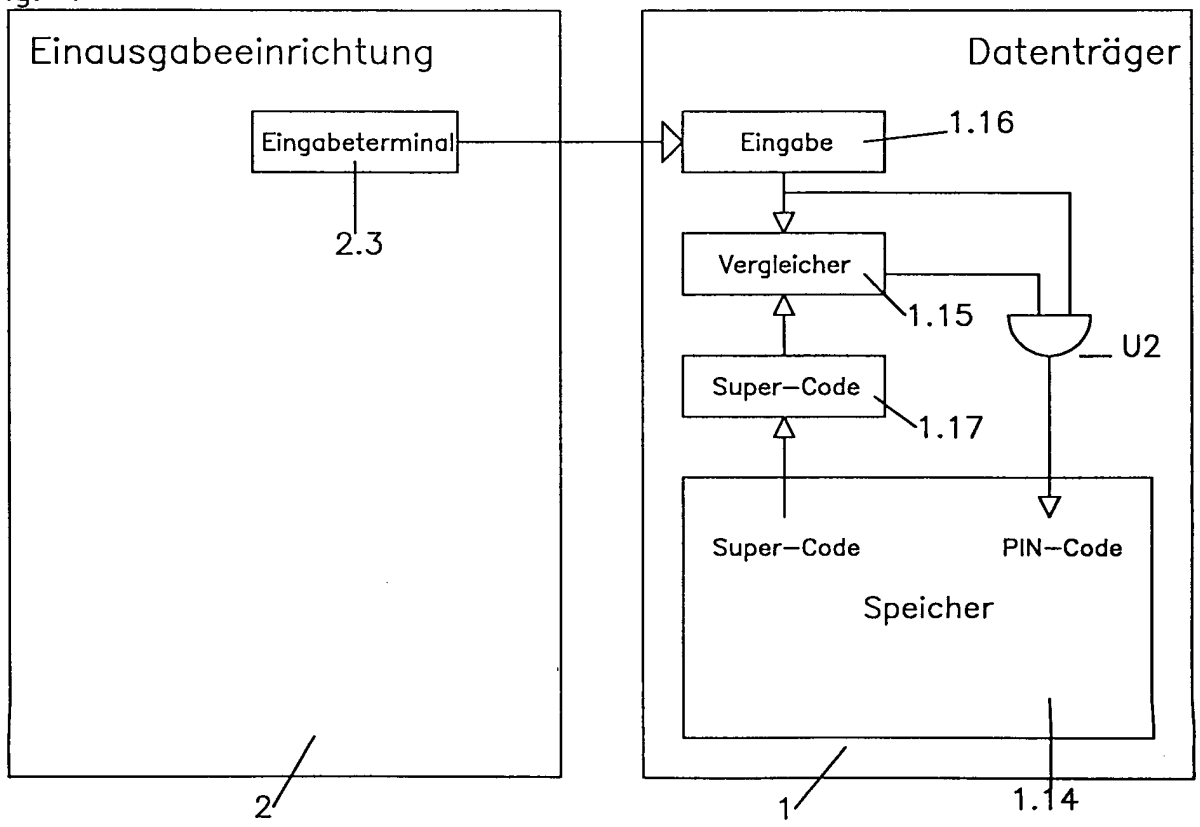

Einausgabeeinrichtung
Eingabeterminal
2.3
2
Datenträger
Eingabe
1.16
Vergleicher
1.15
U2
Super–Code
1.17
Super–Code
PIN–Code
Speicher
1
1.14

Fig. 5

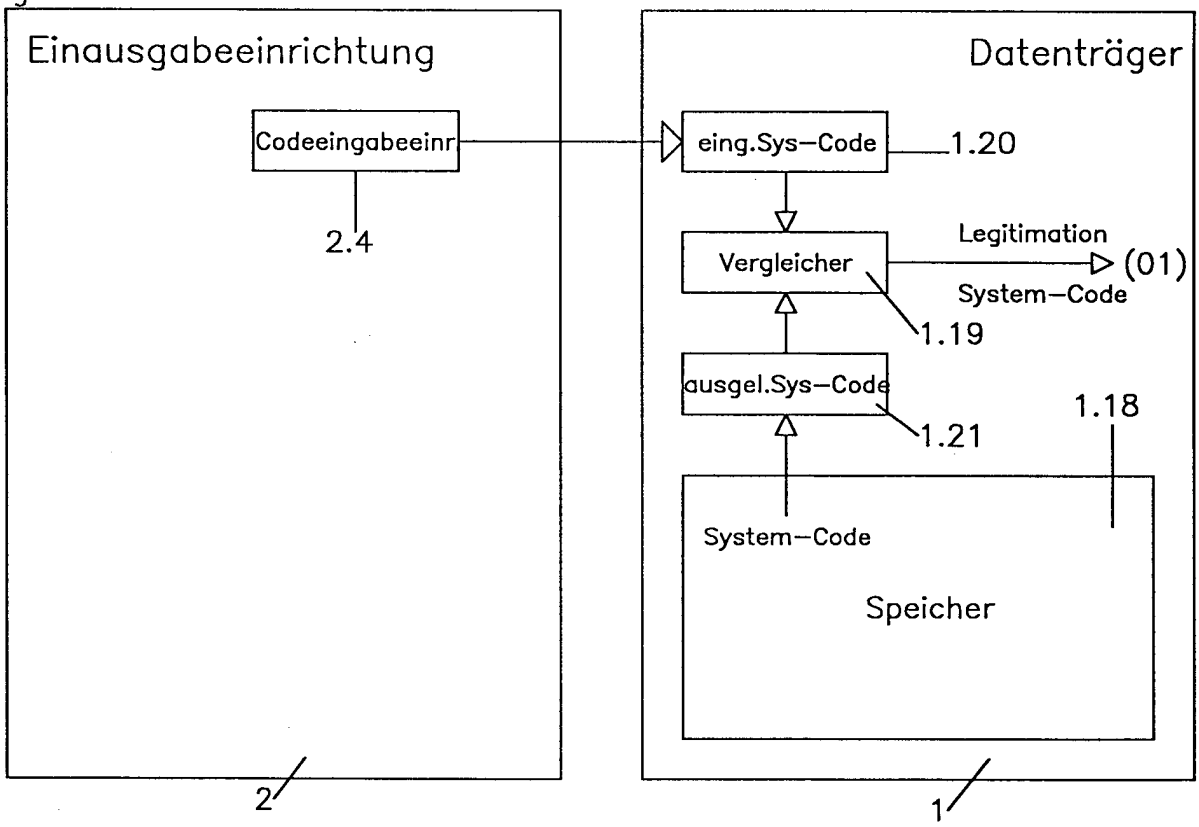

Einausgabeeinrichtung
Datenträger
Codeeingabeeinr
2.4
eing.Sys–Code
1.20
Vergleicher
Legitimation
(01)
System–Code
1.19
ausgel.Sys–Code
1.21
1.18
System–Code
Speicher
2
1

Fig. 6

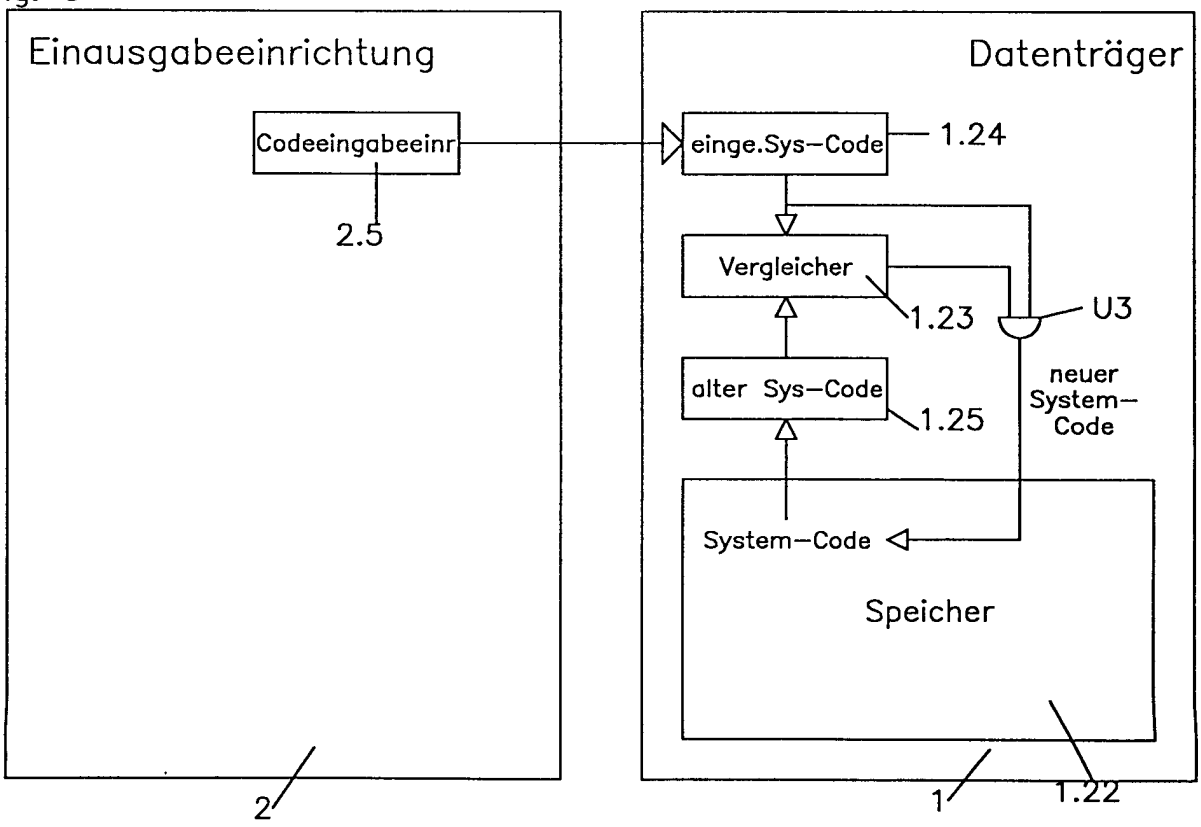

Einausgabeeinrichtung
Datenträger
Codeeingabeeinr
2.5
einge.Sys–Code
1.24
Vergleicher
1.23
U3
alter Sys–Code
1.25
neuer
System–
Code
System–Code
Speicher
2
1
1.22

Fig. 7

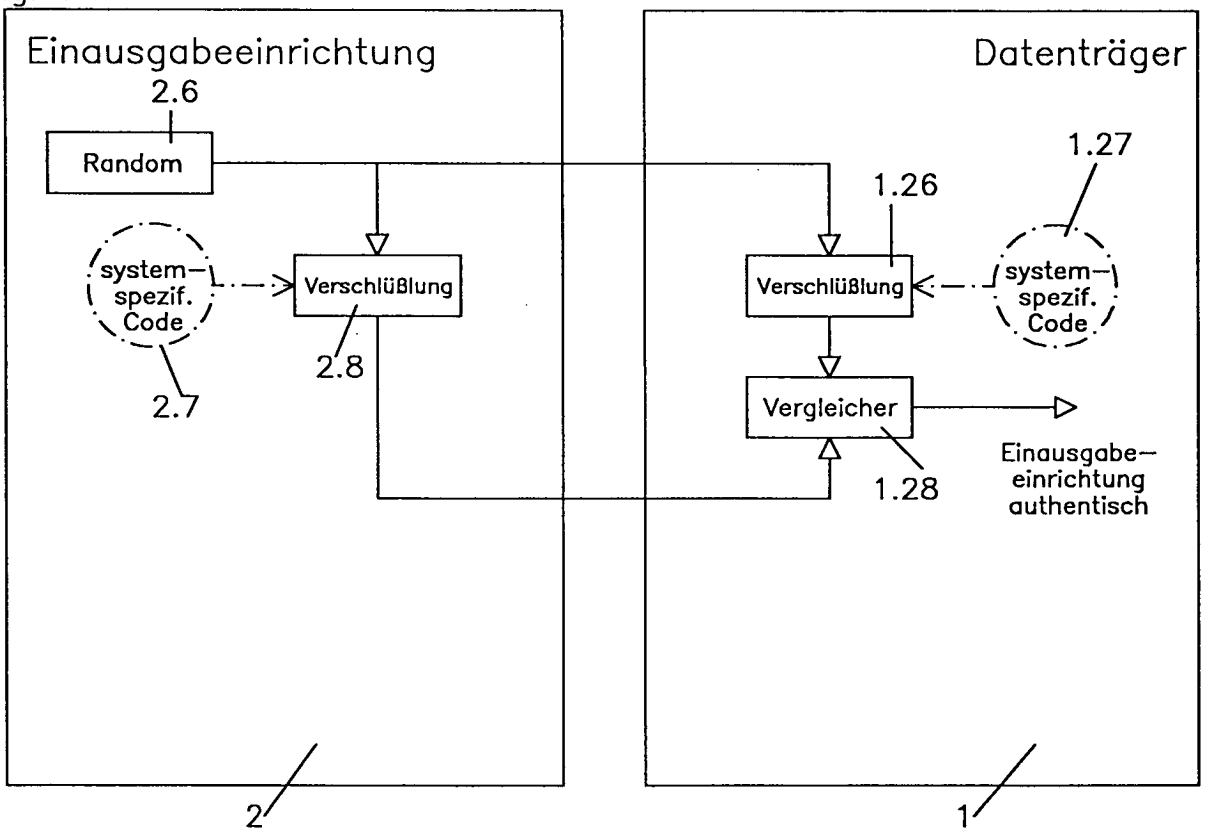

Einausgabeeinrichtung
Datenträger
2.6
Random
1.27
1.26
system–
spezif.
Code
Verschlüßlung
Verschlüßlung
system–
spezif.
Code
2.8
Vergleicher
2.7
1.28
Einausgabe–
einrichtung
authentisch
2
1

Fig 8

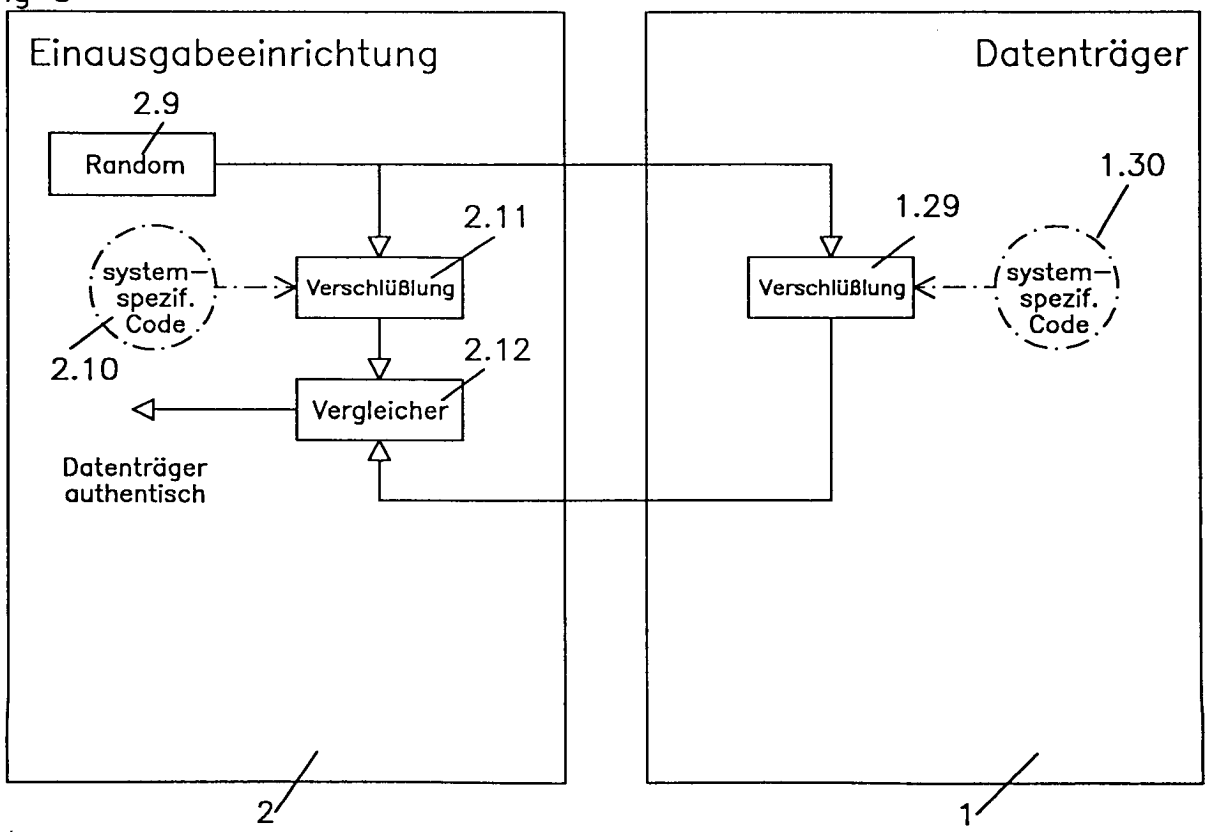

Einausgabeeinrichtung
Datenträger
2.9
Random
1.30
1.29
2.11
system–
spezif.
Code
Verschlüßlung
Verschlüßlung
system–
spezif.
Code
2.10
2.12
Vergleicher
Datenträger
authentisch
2
1

Fig. 9

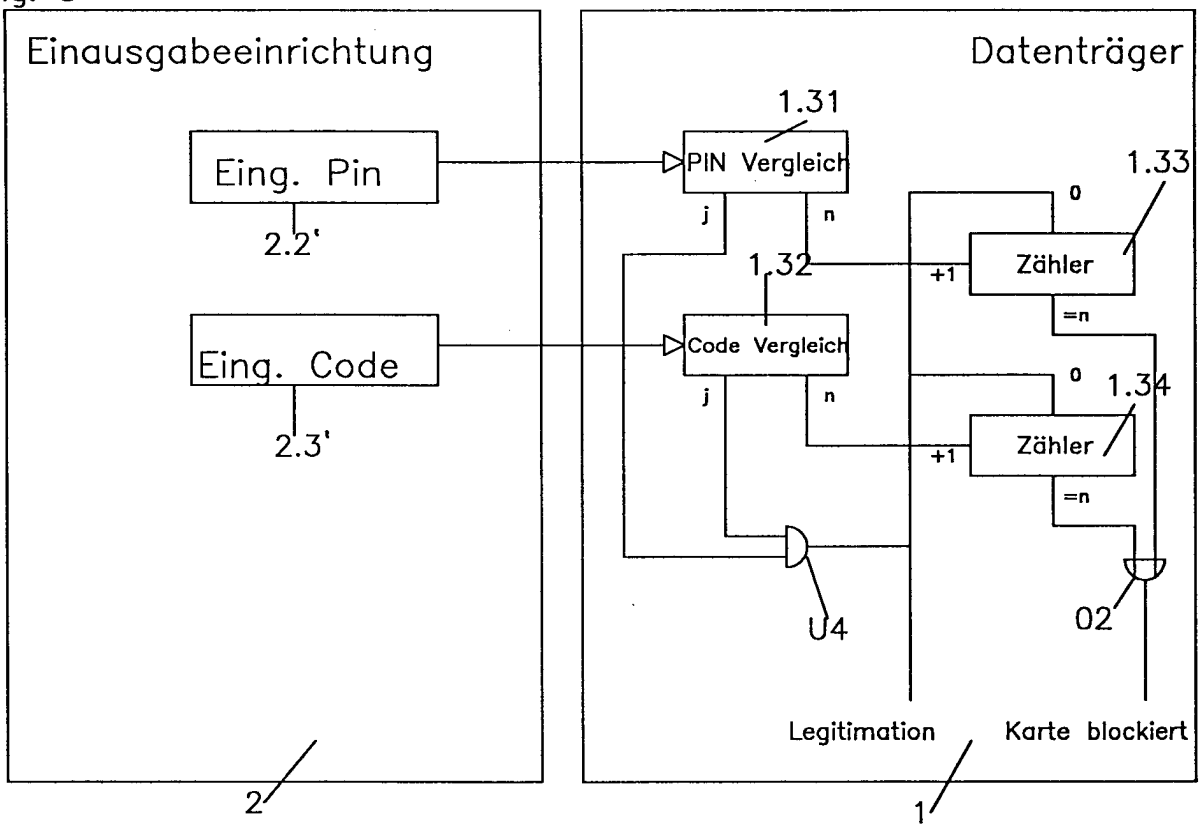

Einausgabeeinrichtung
Datenträger
Eing. Pin
2.2'
Eing. Code
2.3'
1.31
PIN Vergleich
j
n
1.32
Code Vergleich
j
n
1.33
0
Zähler
+1
=n
1.34
0
Zähler
+1
=n
U4
02
Legitimation
Karte blockiert
2
1

Fig. 11

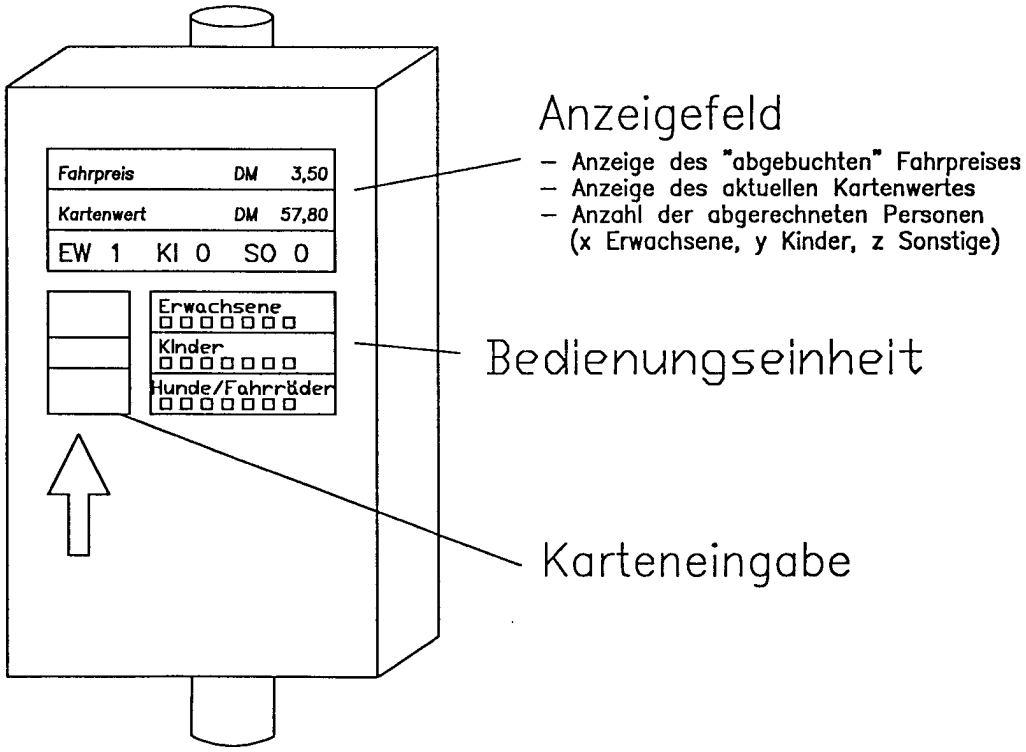

Fahrpreis DM 3,50
Kartenwert DM 57,80
EW 1 KI 0 SO 0
Erwachsene
Kinder
Hunde/Fahrräder
Anzeigefeld
– Anzeige des "abgebuchten" Fahrpreises
– Anzeige des aktuellen Kartenwertes
– Anzahl der abgerechneten Personen
(x Erwachsene, y Kinder, z Sonstige)
Bedienungseinheit
Karteneingabe

Fig. 10

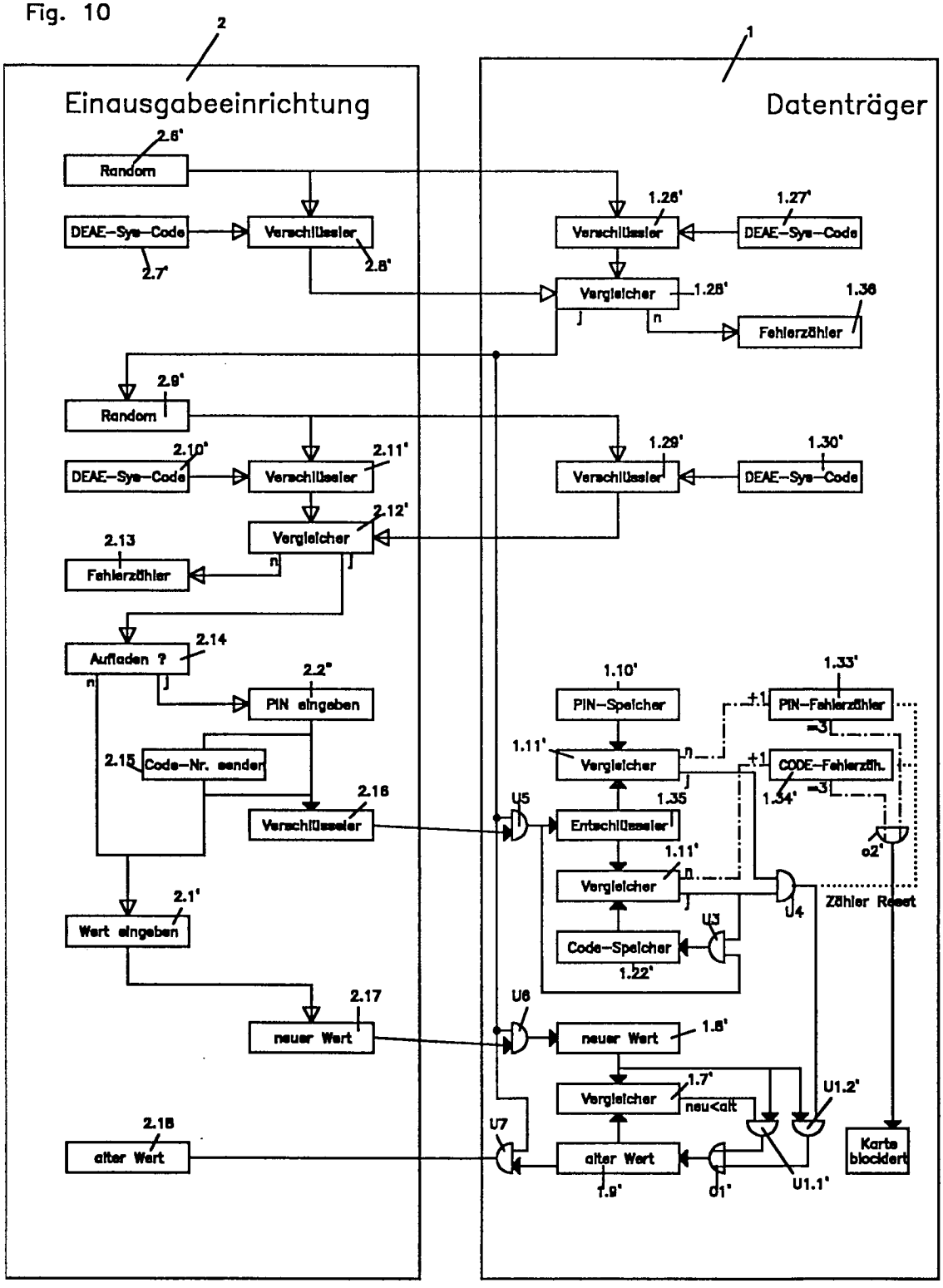

2
Einausgabeeinrichtung
1
Datenträger
2.6'
Random
DEAE-Sys-Code
2.7'
Verschlüsseler
2.8'
1.26'
Verschlüsseler
1.27'
DEAE-Sys-Code
Vergleicher
1.28'
1.36
Fehlerzähler
2.9'
Random
2.10'
DEAE-Sys-Code
Verschlüsseler
2.11'
1.29'
Verschlüsseler
1.30'
DEAE-Sys-Code
2.12'
Vergleicher
2.13
Fehlerzähler
2.14
Aufladen ?
2.2"
PIN eingeben
2.15
Code-Nr. senden
2.16
Verschlüsseler
2.1'
Wert eingeben
2.17
neuer Wert
2.18
alter Wert
1.10'
PIN-Speicher
1.33'
PIN-Fehlerzähler
1.11'
Vergleicher
CODE-Fehlerzäh.
1.34'
1.35
Entschlüsseler
U5
o2'
Zähler Reset
U4
U3
Code-Speicher
1.22'
U6
neuer Wert
1.8'
Vergleicher
1.7'
neu<alt
U1.2'
U7
alter Wert
1.9'
o1'
U1.1'
Karte blockiert

Fig. 12

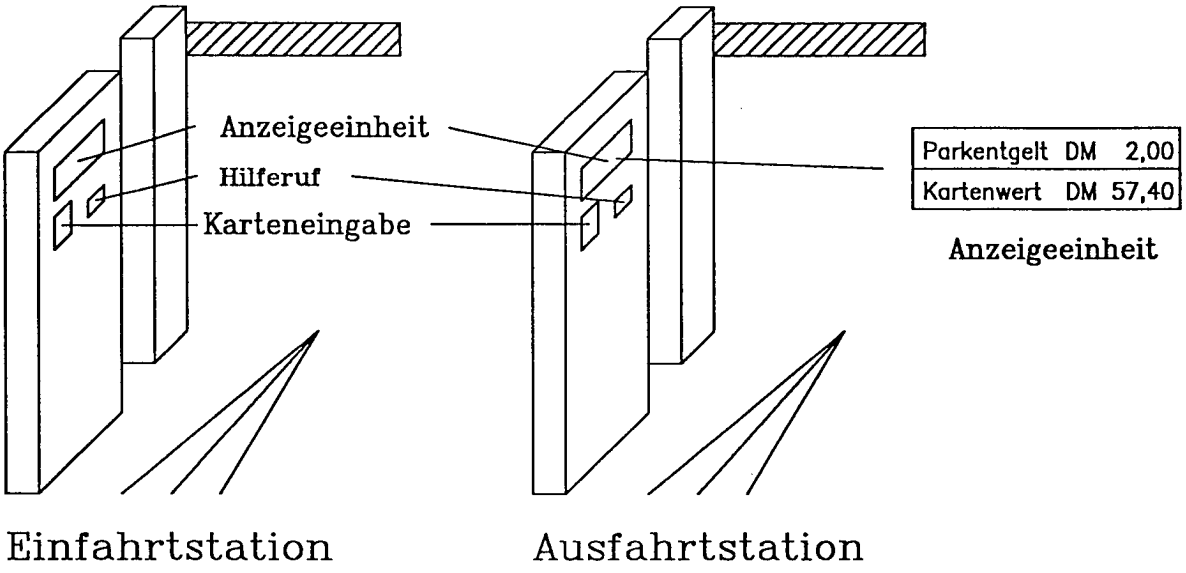

Anzeigeeinheit
Hilferuf
Karteneingabe
Parkentgelt DM 2,00
Kartenwert DM 57,40
Anzeigeeinheit
Einfahrtstation
Ausfahrtstation

Fig. 13

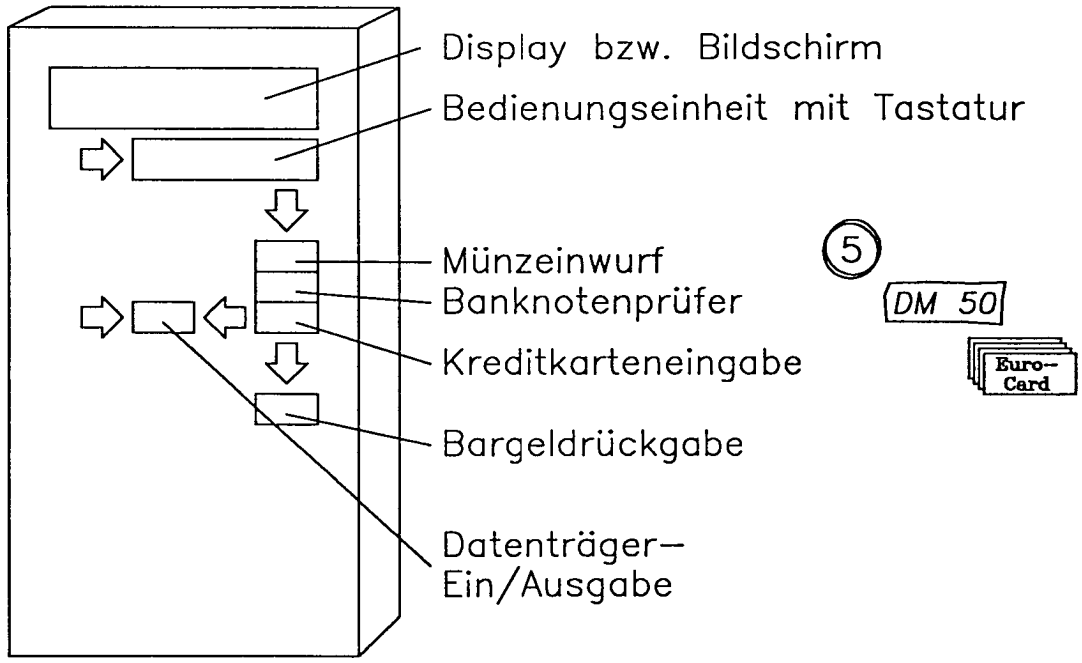

Display bzw. Bildschirm
Bedienungseinheit mit Tastatur
Münzeinwurf
Banknotenprüfer
Kreditkarteneingabe
Bargeldrückgabe
Datenträger–
Ein/Ausgabe
5
DM 50
Euro–
Card

Fig. 14

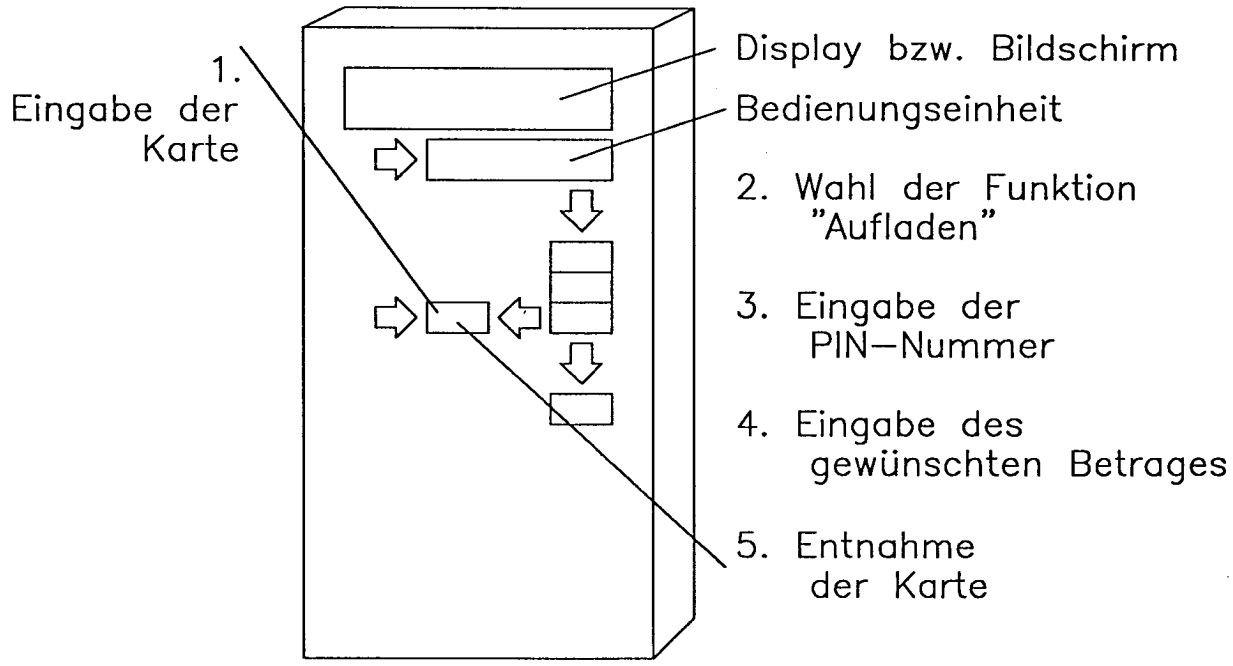
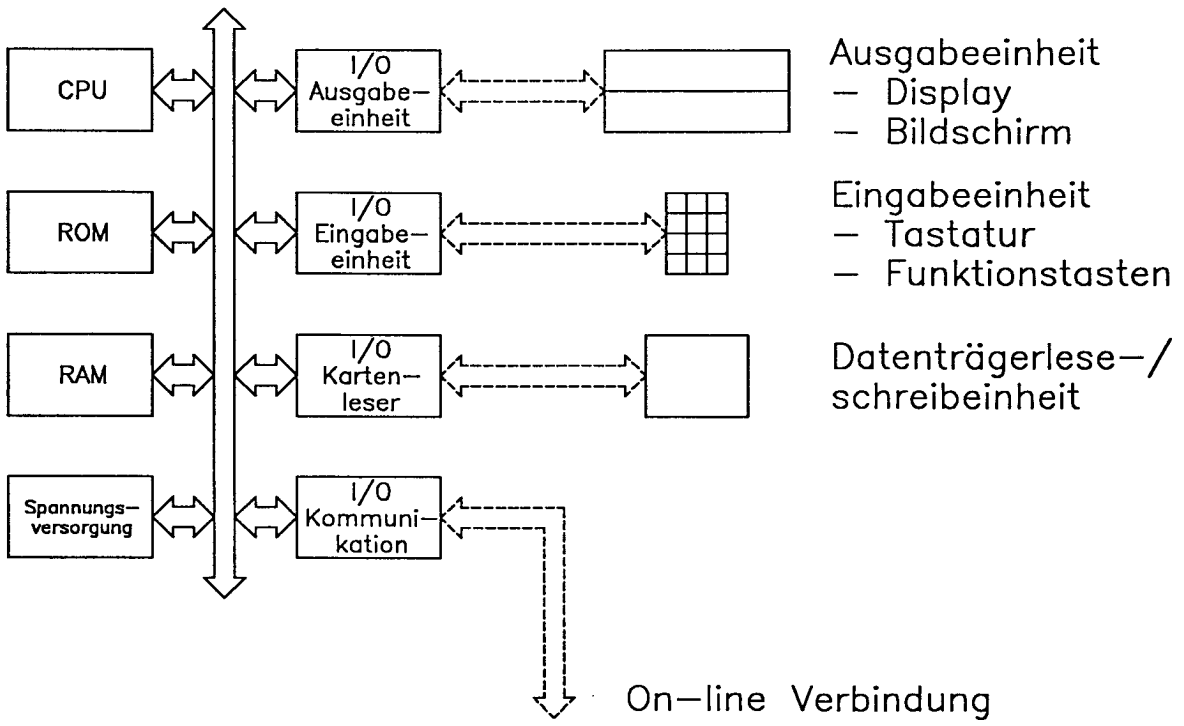

1.
Eingabe der
Karte
Display bzw. Bildschirm
Bedienungseinheit
2. Wahl der Funktion
"Aufladen"
3. Eingabe der
PIN–Nummer
4. Eingabe des
gewünschten Betrages
5. Entnahme
der Karte

Fig. 15


CPU
ROM
RAM
Spannungs–
versorgung
I/O
Ausgabe–
einheit
I/O
Eingabe–
einheit
I/O
Karten–
leser
I/O
Kommuni–
kation
Ausgabeeinheit
– Display
– Bildschirm
Eingabeeinheit
– Tastatur
– Funktionstasten
Datenträgerlese–/
schreibeinheit
On–line Verbindung