(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Patentschrift**

(10) **DE 27 60 486 C 2**

(51) Int. Cl.[5]: **G 06 K 19/073**

(21) Aktenzeichen: P 27 60 486.0-53
(22) Anmeldetag: 24. 8. 77
(43) Offenlegungstag: 9. 3. 78
(45) Veröffentlichungstag der Patenterteilung: 2. 9. 93

DE 27 60 486 C 2

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

(30) Unionspriorität: (32) (33) (31)

06.09.76 AT 6599-76

(73) Patentinhaber:

GAO Gesellschaft für Automation und Organisation mbH, 81369 München, DE

(74) Vertreter:

Klunker, H., Dipl.-Ing. Dr.rer.nat.; Schmitt-Nilson, G., Dipl.-Ing. Dr.-Ing.; Hirsch, P., Dipl.-Ing., Pat.-Anwälte, 8000 München

(62) Teil aus: P 27 38 113.1

(72) Erfinder:

Dethloff, Jürgen, 2000 Hamburg, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:

DE-OS 25 12 902
US 39 06 460
US 36 37 994

(54) Einrichtung zur Durchführung von Bearbeitungsvorgängen mit wenigstens einem Identifikanden und einer Vorrichtung

DE 27 60 486 C 2

Beschreibung

Die Erfindung betrifft eine Einrichtung gemäß dem Oberbegriff des Anspruchs 1.

Ein Identifikand in diesem Sinne ist eine Kreditkarte, Scheckkarte, Automatenkarte oder dergleichen. Die Erfindung ist aber nicht auf die Kartenform beschränkt; sie kann auch mit einem Schlüssel durchführbar sein. Im folgenden wird daher der allgemeine Ausdruck Identifikand verwendet.

Die Identifikanden enthalten häufig neben der Kontonummer und einer persönlichen Merkzahl noch weitere, den Betrüger interessierende Daten, beispielsweise zeitliche und/oder mengenmäßige Beschränkungen, die der berechtigte Karteninhaber, aber auch der Betrüger leicht zu seinen Gunsten ändern kann, insbesondere, wenn diese Daten in einem Magnetstreifen der Karte eingetragen sind.

Aus dem umfangreichen Stand der Technik, der sich mit der Erhöhung der Sicherheit derartiger Einrichtungen gegen Mißbrauch befaßt, seien die Druckschriften DE-OS 25 12 902 und DE-OS 25 12 935 genannt.

Diese Druckschriften beschreiben eine Datenaustauscheinrichtung mit wenigstens einem tragbaren Datenträger und einer Vorrichtung zur Durchführung von Transaktionen, z. B. für Anwendungen im Bankwesen. Im integrierten Schaltkreis des Datenträgers sind ein sogenannter Identifizierungsspeicher, ein Guthaben-Speicher und ein Sollspeicher vorgesehen. Im Identifizierungsspeicher sind benutzerbezogene Daten, wie die Kontonummer oder die Geheimzahl gespeichert. Der Guthabenspeicher enthält alle im Lebenslauf einer Karte eingetragenen Guthaben, d. h. letztendlich das Kreditvolumen. Der Sollspeicher enthält alle im Lebenslauf der Karte entsprechend der getätigten Transaktionen anfallenden Sollbeträge.

Bei der bekannten Datenaustauscheinrichtung beginnt eine Transaktion mit dem Geheimzahlvergleich, um die Identität des rechtmäßigen Benutzers überprüfen zu können. Dazu tastet der Benutzer die nur ihm bekannte Geheimzahl über eine entsprechende Tastatur in die Vorrichtung ein, worauf die Steuerung des Terminals die im Identifizierungsspeicher abgelegte Geheiminformation abfordert und diese in das Terminal überträgt. Wenn der im Terminal durchgeführte Vergleich zwischen Identifikanden — Geheimzahl und eingetasteter Geheimzahl zu einem positiven Ergebnis führt, beginnt die eigentliche Transaktion. Dazu werden zunächst durch entsprechende Steuereinrichtungen in der Vorrichtung die Haben- und Solleinträge aus den entsprechenden Speichern in ein in der Vorrichtung befindliches Saldierwerk übertragen. Dieser Vorgang endet, sobald eine entsprechende in der Vorrichtung vorgesehene Erkennungslogik den ersten nicht beschriebenen Speicherplatz im Guthabenspeicher und im Sollspeicher festgestellt hat. Das Saldierwerk liefert ein Ergebnis darüber, ob das noch zur Verfügung stehende Guthaben ausreichend ist, um die beabsichtigte Transaktion durchführen zu können. Ist dies der Fall, dann wird wieder von der Vorrichtung gesteuert, die Transaktion eingeleitet sowie der der Transaktion entsprechende Schuldbetrag in den ersten noch unbeschriebenen Speicherplatz des Sollspeichers eingetragen. Mit diesem Eintrag ist die Transaktion beendet.

Aus der obigen Schilderung eines Transaktionsablaufs wird klar, daß die für den Ablauf wesentlichen Steuerfunktionen während der gesamten Betriebsdauer von der Vorrichtung aus eingeleitet und durchgeführt werden.

Daraus ergeben sich sicherheitstechnische Probleme, die eine mißbräuchliche Anwendung der bekannten Datenaustauscheinrichtung ermöglichen.

Da der Geheimzahlvergleich in der Vorrichtung durchgeführt wird und dazu die im Identifikationsspeicher des Identifikanden befindliche Geheimzahl zur Vorrichtung übertragen werden muß, kann die einem jeweiligen Identifikanden zugeordnete Geheimzahl entweder in der Vorrichtung oder aber auf der Schnittstelle zum Identifikanden auf vergleichsweise einfache Weise ermittelt werden. Nach Eingabe einer beliebigen Geheimzahl sendet der Identifikand auf Anforderung der Vorrichtung die in dessen Speicher enthaltene Geheimzahl, welche auf diesem Weg dann abhörbar ist. Mit der ermittelten Geheimzahl kann der Datenträger mißbräuchlich genutzt werden.

Unabhängig von der im Zusammenhang mit der Geheimzahl geschilderten Problematik ist auch die eigentliche Transaktion gegen mißbräuchliche Anwendung unzureichend geschützt. Alle Anschlüsse der verwendeten Speicher, d. h. alle Steuer- und Datenleitungen führen vom integrierten Schaltkreis des Identifikanden zur Vorrichtung und sind in dieser mit entsprechenden Steuereinrichtungen verbunden, die die zum Einschreiben oder Lesen benötigten Signale erzeugen und über die Leitungen zu den Speichern übertragen. Das heißt, daß durch einen entsprechenden Eingriff in die Vorrichtung, aber auch durch Manipulation an den Schnittstellen ohne großen Aufwand in die Speicherinhalte mißbräuchlich ermittelt, überschrieben oder manipuliert werden können. So kann beispielsweise im Habenspeicher das Kreditvolumen erhöht oder aber der im Sollspeicher im Zuge einer Transaktion einzutragende Schuldbetrag unterdrückt werden. Grundsätzlich können die Einträge auch nachträglich ungültig gemacht oder Einträge geringeren Wertes geladen werden.

Es sind zwar bei den bekannten Datenaustauscheinrichtun- gen Sicherheitsmaßnahmen in dem Sinne vorgesehen, daß bestimmte Speicherbereiche gegen ein Überschreiben oder Lesen geschützt sind. Dies gilt für die Kontonummer und auch die Geheimzahl. Diese bekannten Schutzmaßnahmen können aber prinzipiell nicht für alle Speicherbereiche wie Guthabenspeicher und Sollspeicher vorgesehen werden, da diese systembedingt bei jeder Transaktion sowohl bezüglich des Lesens als auch des Schreibens zugreifbar sein müssen.

Eine Datenaustauscheinrichtung mit einem Identifikanden mit integriertem Schaltkreis und einer Vorrichtung zur Durchführung von Transaktionen ist auch aus der US-PS 39 06 460 bekannt. Bei dieser bekannten Einrichtung wird zwar ein Geheimzahlvergleich im Identifikanden durchgeführt, es führen aber auch bei dieser Einrichtung die Datenleitungen der verwendeten Speicher vom integrierten Schaltkreis zur Vorrichtung, so daß über diese Leitungen von außen ein direkter Zugriff auf die Speicher möglich ist.

Der Anmeldung liegt die Aufgabe zugrunde, die bekannte Einrichtung dahingehend weiterzubilden, um einem Betrüger jegliche Möglichkeit eines direkten Zugriffs von außen auf die einzelnen Speicher des Identifikanden zu nehmen.

Die Aufgabe wird durch die im kennzeichnenden Teil des Hauptanspruches angegebenen Merkmale gelöst.

Demnach liegt der Grundgedanke der Erfindung darin, daß alle Speicher- und Verarbeitungsvorgänge vom Identifikanden der Datenaustauscheinrichtung eigenständig veranlaßt werden, wobei die Vorgänge durch

den Anstoß der Vorrichtung eingeleitet sein können. Die Steuereinrichtung im Identifikanden ist ein Mikroprozessor, der in jedem Fall den gewünschten externen Zugriff auf Schaltkreise und Speicherinhalte im Identifikanden überwacht und kontrolliert.

Der Mikroprozessor wird durch den Inhalt eines ebenfalls im Identifikanden vorgesehenen nichtflüchtigen Programmspeichers gesteuert.

Da die im Identifikanden geschützten Daten aufgrund der erfindungsgemäßen Lösung nicht von außen feststellbar sind, ist auch keine weitere Geheimhaltung erforderlich. Der potentielle Betrüger könnte alle Einzelheiten der Vorrichtung kennen und dann doch nicht mit Erfolg in das System einbrechen oder es mißbrauchen.

Gemäß einer Weiterbildung der Erfindung wird der gesamte Datentransfer zwischen der Vorrichtung und dem Identifikanden unter der Kontrolle eines Mikroprozessors über eine Ein-/Ausgabeeinheit, die auch Bestandteil des Identifikanden ist, abgewickelt. Über diese seriell ausgebildete Schnittstelle ist es bei interner paralleler Verarbeitung der Daten im Identifikanden möglich, den gesamten Datentransfer zwischen dem Identifikanden und der Vorrichtung in serieller Form über eine Übertragungsstrecke durchzuführen. Damit ist es prinzipiell nicht möglich, über die von außen zugängliche Schnittstelle des Identifikanden auf einzelne Daten oder Steuerleitungen im integrierten Schaltkreis des Identifikanden Einfluß zu nehmen.

Gemäß einer weiteren Ausführungsform der Erfindung ist in der integrierten Schaltung des Identifikanden zusätzlich ein Programmierteil vorgesehen, das in der Lage ist, die nichtflüchtigen Speicher zu programmieren, d. h. die im Zuge einer Transaktion notwendigen Daten in die Speicher einzuschreiben. Mit dieser Maßnahme erübrigt es sich, die zur Programmierung des nichtflüchtigen Speicher im allgemeinen notwendige Programmierspannung separat von außen zuzuführen. Darauf bezogene Manipulationsmöglichkeiten entfallen ebenfalls.

Gemäß einer weiteren Ausführungsform der Erfindung sind alle Speicher und Steuerschaltungen in einem einzigen integrierten Schaltkreis vereint. Durch diese Vorgehensweise kann die Sicherheit des Identifikanden gegen mißbräuchliche Nutzung weiter erhöht werden, da durch diese Maßnahme auch die Schnittstellen innerhalb des Identifikanden, d. h. die die einzelnen Komponenten verbindenen Leitungen, praktisch unzugänglich sind.

Wie erwähnt, hat die Erfindung eine ganze Reihe von Vorteilen gegenüber den bekannten Systemen und Karten. Es ist sowohl ein Mißbrauch durch den berechtigten Karteninhaber als auch durch Unbefugte im Sinn von Änderungen der Benutzungsbedingungen und/oder der Benutzungsdaten praktisch unmöglich.

Weitere Merkmale und Vorteile der Erfindung ergeben sich aus den Patentansprüchen und der nachfolgenden Beschreibung eines Ausführungsbeispiels, bei dem als Identifikand eine Automatenkarte dient. Es zeigen:

Fig. 1 einen Identifikanden,

Fig. 2 einen IC des Identifikanden gemäß **Fig.** 1,

Fig. 3 einen gegenüber **Fig.** 2 erweiterten IC,

Fig. 4 u. 5 Ausführungsbeispiele von einfachen Prüfgeräten,

Fig. 6 ein Funktionsdiagramm der Prüfung von Identifikanden,

Fig. 7 ein Blockbild eines Automaten und

Fig. 8 den Funktionsablauf des Automaten gemäß **Fig.** 7.

Fig. 1 zeigt einen Identifikanden **1**, der als Kreditkarte oder Eurocheque-Karte ausgebildet ist. Er enthält ein Namensfeld **2** des Karteninhabers, ein Feld **3** für die Identifizierungs- oder Kontonummer in Klarschrift, ein Fotofeld **4** sowie ein Unterschriftsfeld **5**. Das Feld **3** ist parallel zu einer Schmalseite vorgesehen, damit die Kontonummer von außen lesbar bleibt, wenn die Karte in das Prüfgerät eingeführt ist.

Die Karte enthält ferner eine integrierte Schaltung IC **6** mit einer Anschlußleiste **7** für die Versorgungsspannung sowie die Datenein- und Ausgabe. Der IC ist unsichtbar in die Karte implantiert.

Eine bestimmte, den IC umgebende Fläche **8** ist von leitenden Materialien freigehalten, damit bei Benutzung der Karte in einem Automaten geprüft werden kann, ob von sich außerhalb eines Automaten befindlichen Simulationsschaltungen Verbindungsleitungen zur Karte im Automaten geführt sind. Da die Totalfälschung einer Karte mit einem identischen IC aufgrund von Wirtschaftlichkeitserwägung als ausgeschlossen angenommen werden kann, wird durch diese Maßnahme verhindert, daß ein Betrüger, vorausgesetzt, ihm wäre die Funktionsweise des IC's bekannt, eine Ersatzschaltung aus diskreten Bauelementen aufbaut und diese Schaltung z. B. über Drähte mit einer hierfür als Adapter wirkenden Karte verbindet.

Der Automat prüft außerdem, ob andersartige Verbindungen über das Umfeld nach außen hergestellt sind.

Fig. 2 zeigt ein Blockschaltbild des IC's **6**. Alle einzeln dargestellten Teile sind in Wirklichkeit in einer einzigen Schaltung integriert. Die Versorgung des IC's mit Strom sowie die Eingänge und die Ausgänge für Daten laufen über eine Kontaktleiste **9**. Diese Kontaktleiste kann entweder galvanische Kontakte oder eine induktive Kopplungsschleife aufweisen. Wenn die Einkopplung von Daten und die Stromversorgung über eine Induktivschleife erfolgt, enthält die Kontaktleiste **9** auch noch die hierfür benötigten Umsetzer.

Der IC enthält eine Zentraleinheit **10**. Diese Zentraleinheit ist ein spezieller Mikroprozessor, der mit einem fest eingebauten Programm aus einem Programmspeicher **11** arbeitet. Die Zentraleinheit **10** und der Programmspeicher **11** können in einer anderen Ausführungsform auch als fest verdrahtete Logik innerhalb einer integrierten Schaltung ausgebildet sein.

Die Stromversorgung erfolgt über einen integrierten Stromversorgungsteil **12**, in dem die von außen eingespeiste Versorgungsspannung in die für die Zentraleinheit **10** notwendigen Werte umgeformt wird. Von außen muß dabei stets eine so hohe Stromversorgung zur Verfügung gestellt werden, daß ein Programmierteil **19** des IC in der Lage ist, Datenspeicher **13** ... **17** zu programmieren. Im Versorgungsteil **12** wird deshalb überprüft, ob die Versorgungsspannung hoch genug ist, um stets die Zentraleinheit **10** betätigen zu können und ob sie bei Ausführungsformen der Karte, die bei Erkennen von Mißbrauch eine Selbstzerstörung des IC's vorsehen, auch ausreichend für die Zerstörung des IC's ist. Wenn die Versorgungsspannung zu niedrig ist, arbeitet der IC nicht. Die Selbstzerstör-Einrichtung des IC's kann durch eine Umprogrammierung eines Tores **24** verifiziert werden. Normalerweise bleibt dieses Tor immer geöffnet, und die Benutzungsbedingungen sind aus dem Speicher **16** auslesbar. Wenn während der Identifikationsprüfung eine endgültige Sperrung dieses Identifikanden erforderlich wird, wird das Tor **24** gesperrt, und damit sind keine Benutzungsbedingungen mehr aus lesbar.

Die Zentraleinheit arbeitet nur, wenn Benutzungsbe-

dingungen gelesen werden können.

Diese Selbstzerstörung kann sowohl von der Karte selbst durch entsprechende Steuerung des Programmspeichers **11** ausgelöst werden als auch durch ein Auslösesignal von außen. Dieses Auslösesignal kann bei Automatenkarten vom Automaten erzeugt werden, wenn zusätzliche Prüfungen im Automaten eine Zerstörung erforderlich machen.

Alle Dateneln- und -ausgaben erfolgen über eine Ein/Ausgabeeinheit **18**. Die Zentraleinheit **10** ist per Programm in der Lage, alle bisher beschriebenen Funktionen auszuführen. Wenn die Versorgungsspannung von außen angelegt wird, läuft der Mikroprozessor der Zentraleinheit **10** von alleine an und überprüft als erstes, ob die Versorgungsspannung groß genug ist.

Danach wird die Zentraleinheit **10** über Dateneingaben zu weiteren Funktionen veranlaßt. Welche Funktionen ablaufen können, wird weiter unten beschrieben. Die Ausgabe von Rückmeldungen nach Überprüfung einer eingegebenen persönlichen Merkzahl und anderer Informationen erfolgt über die Ein-/Ausgabeeinheit **18**.

Alle bisher beschriebenen Teile des IC's werden bei der Herstellung des IC's in ein Stück integriert. Die außerdem noch notwendigen Datenspeicher **13 ... 17** sind PROM-Speicher und können insgesamt oder einzeln beim Herstellungsprozeß entweder in den vorerwähnten IC integriert oder als gesonderter Speicher-IC ausgebildet sein.

In diese PROM-Speicher werden in unten beschriebenen einzelnen Schritten zu verschiedenen Zeiten verschiedene Daten eingeschrieben, und damit wird aus einer neutralen eine bestimmte Identifizierungskarte erzeugt. Die Datenspeicher **13 ... 17** werden unterschiedlich behandelt. Einige Speicher sind nur über Tore **20 ... 24** programmierbar. Diese Programmier-Sperrschaltungen lassen sich außer Funktion setzen, so daß keine weiteren Veränderungen der Speicherinhalte nachträglich mehr möglich sind. Die Datenspeicher sind außerdem unterschiedlich, was ihre Lesbarkeit anbetrifft, d. h. nur einige vorbestimmte Speicher sind von außerhalb der Karte lesbar, andere nicht. Welche Teile wann und warum programmierbar oder lesbar sind, wird unten erläutert.

Der Datenspeicherteil des IC's enthält, wie bereits gesagt, die Speicher **13 ... 17**.

Der Speicher **13**, in den ein Schutzcode zum Schutz der Karte auf dem Weg von der Fabrik zur Ausgabestelle eingespeichert ist, ist nur programmierbar, solange das Tor **20** in Funktion ist und nur intern lesbar über das Tor **21**.

Der Speicher **14** dient zur Speicherung der persönlichen Merkzahl, die nur eingeschrieben werden kann, wenn das Tor **22** in Funktion ist. Die Merkzahl kann nicht aus der Karte herausgelesen, sondern nur in die Zentraleinheit **10** abgespeichert werden, wo sie zu Vergleichszwecken zur Verfügung steht.

Der Speicher **15** dient zur Aufnahme von Daten, die zur Identifizierung des jeweiligen Kontoinhabers dienen. In diesen Speicher werden also die Kontonummer oder eine beliebige andere — auch alphanumerische — zur Identifizierung des Kontoinhabers dienende Angabe eingeschrieben. Erst nach dieser Programmierung ist der Identifikand einem Kunden zugeordnet. Der Speicher **15** ist nur solange programmierbar, wie das Tor **23** in Funktion ist. Nach der Programmierung wird das Tor **23** zerstört. Der Speicher **15** bleibt danach trotzdem lesbar für die Zentraleinheit **10**.

Der Speicher **16** dient zur Aufnahme von Benutzungsbedingungen, wie z. B. Periodenlänge, Periodenlimit, Tageslimit. Diese Daten können nur bei der Ausgabe der Karte, d. h. der Initialisierung, eingeschrieben werden, und zwar über das Tor **24**.

In dem Speicher **17** werden für jede Bedienung die Daten gespeichert, wie Datum, Anzahl der Fehlversuche bei der Eingabe der persönlichen Merkzahl, Kontobewegung etc.

Im folgenden seien nun im Zusammenhang die Initialisierung und die Benutzung der Karte am Beispiel einer Karte für monetäre Anwendungen beschrieben.

Nach dem letzten Arbeitsgang bei der Herstellung der Karte wird ein Schutzcode als numerischer Begriff in einem Zufallsgenerator erzeugt und in den Speicher **13** eingeschrieben. Gleichzeitig wird dieser Schutzcode auf einen getrennten Beleg gebucht. Nach der Einspeicherung wird das Tor **20** zerstört, so daß eine Veränderung des Schutzcodes oder das Einschreiben einer anderen Codezahl in den Speicher **13** nicht mehr möglich ist. Der Beleg wird unter Geheimhaltungsbedingungen automatisch in einen Umschlag eingeführt und der Umschlag anschließend versiegelt. Die Karte und der Umschlag erhalten dann eine visuell lesbare identische Kennzeichnung, z. B. dieselbe laufende Nummer. Die so mit einem Schutzcode versehenen Karten und Umschläge werden getrennt zu dem ausgebenden Institut gebracht und dort getrennt gelagert und verwaltet. Bis hierhin sind die Karten noch neutral. Bei der Ausgabe einer Karte an einen Kunden wird die betreffende neutrale Karte mit dem dieselbe laufende Nummer tragenden Beleg zusammengeführt. Sodann wird der Umschlag geöffnet, vorzugsweise von dem Kunden selbst, und der visuell lesbare Schutzcode entnommen.

Die Karte wird dann in das beim ausgebenden Institut befindliche Eingabegerät eingeführt, um die kundenspezifischen Daten in die Karte einzuschreiben. Hierzu wird zunächst die gelesene Schutzcode-Nummer eingetastet und über die Eingabe-/Ausgabeeinheit **18** in die Zentraleinheit **10** der Karte eingespeichert, wo ein Vergleich mit der in dem Speicher **13** gespeicherten Schutzcode-Nummer stattfindet. Ist der Vergleich negativ, dann wird nach einer vorgegebenen Anzahl von negativen Versuchen eine Selbstzerstörung des IC's bewirkt.

Ist der Vergleich positiv, dann gibt der IC ein Freigabesignal an das Eingabegerät, so daß dann die weiteren Daten eingegeben werden können.

Zunächst tastet der Kunde die von ihm selbst gewählte persönliche Merkzahl geheim ein, die dann wieder in die Zentraleinheit **10** übertragen und von dort in den Speicher **14** eingespeichert wird. Nach der Einspeicherung wird das Tor **22** automatisch zerstört, so daß die persönliche Merkzahl nicht mehr verändert werden kann.

Hiernach werden durch das Institut die zur Identifizierung des Kunden dienenden Daten eingegeben. So wird in den Speicher **15** die Kontonummer des Kunden eingespeichert und danach das Tor **23** automatisch zerstört, so daß auch diese Daten nicht mehr verändert werden können.

Die Benutzungsvorschriften werden in den Speicher **16** gespeichert, und danach wird das Tor **24** automatisch zerstört. Als letztes kann noch in den Speicher **17** der Anfangskontostand eingespeichert werden.

Nachdem diese Einspeicherungen vorgenommen sind, wird das Ausgabetor **21** des Speichers **13** zerstört, so daß die Karte nicht ein zweites Mal mittels des gebrauchten Schutzcodes initialisiert werden kann, da eine Prüfung dieses Schutzcodes nicht mehr möglich ist.

Die so vorbereitete Karte wird dem Kunden ausgehändigt.

Soll eine Karte nach Ablauf ihrer Gültigkeit wiederholt gültig gemacht werden können, dann werden weitere Schutzcodes verwendet, die wie vorstehend behandelt werden; entsprechend ist der Speicher **13** mit den Toren **20** und **21** mehrfach vorgesehen.

Dies zeigt **Fig. 3**, die die entsprechenden Erweiterungen gegenüber der **Fig. 2** aufweist. Wie man sieht, sind die Speicher für den Schutzcode und für die Kontenführung mit den zugeordneten Toren mehrfach vorgesehen.

Wenn der zuvor beschriebene Zeitraum für eine Karte abgelaufen oder ihr Geldvolumen verbraucht ist, geht der Kunde mit der Karte zu seiner Bank. Bei der Bank kann für die Karten außer dem zuvor beschriebenen ersten Schutzcode von vornherein ein zweiter, dritter usw. Schutzcode in weiteren verschlossenen und versiegelten Umschlägen aufbewahrt sein. Die Karte wird jetzt – wie beim ersten Schutzcode bereits beschrieben – nach Eingabe des zweiten Schutzcodes neu initialisiert.

Bei dieser Initialisierung wird das Tor **26** zerstört, so daß in den ersten Konto-Speicher **17** keine weiteren Daten mehr eingeschrieben werden können.

Außerdem wird das Tor **30** jetzt durch eine besondere Programmierung geöffnet, so daß nunmehr die Kontoführung über das "Konto-2", Speicher **29**, erfolgt.

Die Tore **27** und **28** entsprechen in ihrer Funktion den Toren **20** und **21**, der Speicher **41** dem Speicher **13** für den Schutzcode.

Der zweite und alle weiteren Schutzcode-Speicher werden bei der Herstellung (letzter Arbeitsgang) mit dem Schutzcode "2", "3" usw. programmiert.

Diese Erweiterung um weitere Schutzcodes und weitere Konto-Speicher führt zu einer längeren Lebensdauer und besseren Ausnutzung der elektronischen Teile der Karte.

Zur Benutzung der Karte wird diese in das entsprechende Prüfgerät oder den entsprechenden Automaten eingeführt, wo zunächst innerhalb des Identifikanden geprüft wird, ob die Versorgungsspannung die erforderliche Höhe hat, insbesondere für eine eventuell notwendig werdende Selbstzerstörung des IC's.

Die Prüfung des Benutzers auf seine Inhaber-Identität erfolgt durch Eingabe der persönlichen Merkzahl und Vergleich mit der gespeicherten Merkzahl in der Zentraleinheit **10**. Die persönliche Merkzahl kann also nicht extern gelesen werden. Bei positivem Ergebnis kann als nächstes die Kontonummer geprüft werden, während bei dem n-ten Fehlversuch der IC automatisch zerstört wird. Außerdem wird die Anzahl der eventuellen Fehlversuche in die Karte eingetragen.

Zur Prüfung der Kontonummer kann diese bei konventionellen Karten sichtbar außen an der Karte aufgebracht sein, so daß sie abgelesen und in ein Prüfgerät eingetastet werden kann. Die Prüfung erfolgt wieder in dem IC der Karte selbst.

Bei dieser Prüfung wird nach dem n-ten Fehlversuch ein Alarmausgelöst, da man dann nämlich davon ausgehen kann, daß die auf der Karte befindliche Kontonummer verändert wurde, um die Belastung eines anderen Kontos zu erreichen. Auch hier wird in der Karte die Anzahl eventueller Fehlversuche vermerkt.

Zusätzlich zu den vorbeschriebenen Prüfungen werden weitere Prüfmaßnahmen ergriffen, die im Identifikanden eine derartige Ausbildung der Funktions- und Speicherschaltungen bedingen, daß diese mit handelsüblichen, also nicht speziell für den erfindungsgemäßen Zweck hergestellten, Schaltungen nicht darstellbar ist.

Hierdurch wird verhindert, daß Betrüger mit handelsüblichen, in Fälschungen von Identifikanden untergebrachten Schaltungen ein "Gut" -Signal erzeugen, ohne daß zuvor die vorerwähnten zusätzlichen Prüfungen stattgefunden haben.

Nach diesen Prüfungen kann nun die eigentliche Bedienung erfolgen, z. B. die Geldausgabe eingeleitet werden. Wenn diese Bedienung unerlaubt ist, z. B. weil das Ausgabelimit überschritten, d. h. zuviel Geld angefordert wurde, erhält der Kunde automatisch einen entsprechenden Hinweis. Die Prüfung, ob eine Transaktion erlaubt ist, erfolgt in der Zentraleinheit **10**. Wenn die Kontonummer auch aus der Karte in dem Automaten lesbar sein soll, muß der Programmspeicher **11** das entsprechende Programm enthaltend.

Die Kontoführung erfolgt in dem Speicher **17**, und zwar werden alle Vorgänge nacheinander abgespeichert, wobei ein Auslesen jederzeit möglich ist. Da die alten Kontostände bei Kontobewegungen nicht gelöscht werden können, steht die gesamte Historie des Kontos zur Verfügung. Auch Kontoauszüge können so mit Hilfe der Karte erstellt werden.

Die Erfindung ist weder auf das Beispiel für banktechnische Transaktionen noch auf die Verwendung von kartenförmigen Identifikanden beschränkt. So können durch das neue System auch die Zugänge zu Arealen dadurch geschützt werden, daß nur ausgesuchten Personen, die sich mit einem gültigen und unverfälschten Identifikanden als berechtigte Inhaber des Identifikanden ausweisen, Zutritt gewährt wird.

Ferner können die Identifikanden dazu benutzt werden, nur als berechtigt erkannten Personen den Zugang zu Einrichtungen oder deren zweckbestimmte Inbetriebsetzung zu gestatten, die dem Speichern oder Abrufen von Informationen dienen.

Besonders vorteilhaft ist, daß unveränderbar speicherbare Benutzungsbedingungen auch im off-line-Betrieb alle möglichen Anwendungen den Benutzern einen vorbestimmten Spielraum zuweisen.

Anhand der **Fig. 4** und 5 werden zwei Ausführungsbeispiele einer Aufnahmeeinrichtung A_1, A_2 in Form einfacher Prüfgeräte zur Prüfung des als Eurochequekarte oder Kreditkarte ausgebildeten Identifikanden erläutert. Die vereinfachten Prüfgeräte dienen zur Prüfung der Benutzeridentität und zur Prüfung, ob die von außen aufgedruckte Kontonummer verändert wurde, und sie dienen insgesamt zur Prüfung der Echtheit der Karte, indem mittels der beiden vorgenannten Prüfungen festgestellt wird, ob der erforderliche IC in der Karte vorhanden ist.

Beide Ausführungsformen unterscheiden sich nur durch ein in **Fig. 4** vorhandenes numerisches Anzeigefeld **31**, das dazu dient, zum Vergleich der Kontonummern die aus der Karte automatisch ausgelesene Nummer anzuzeigen, damit sie visuell mit der außen auf der Karte **1** aufgebrachten Nummer **3** verglichen werden kann.

In der Ausführungsform nach **Fig. 5** ist dieses Anzeigefeld nicht enthalten. Die Prüfung, d. h. der Vergleich der außen aufgebrachten Nummer, die hier über eine Tastatur **32** eingetastet wird, erfolgt im Inneren der Karte mittels des IC's **6**. Entsprechend dem Ergebnis des Vergleichs gibt der IC ein Signal an das Prüfgerät, das entweder die Anzeige "Freigabe" oder "Richtig" in einem Feld **33** oder "Alarm" oder "Nicht richtig" in einem Feld **34** bewirkt.

Die Anzeigen in den Feldern 33 und 34 dienen in gleicher Weise dem Vergleich der persönlichen Merkzahl. Ein Schalter 35 dient zum Inbetriebsetzen des Geräts, während eine Löschtaste 36 zur Beendigung einer Teilprüfung und zur Löschung von Fehleingaben dient.

Auch bei dieser einfachen Art Ausweisprüfung ist im Prinzip eine Selbstzerstörung des IC's nach einer vorbestimmten Anzahl von Fehlversuchen bei der Eingabe der persönlichen Merkzahl oder der Kontonummer möglich. Für eine solche Selbstzerstörung ist im Prüfgerät die erforderliche elektrische Leistung bereitgestellt.

In **Fig. 6** ist nach der oben erläuterten Funktion von **Fig. 4** und **Fig. 5** ein selbsterklärendes Funktionsdiagramm der Prüfung von Identifikanden in konventionellen-Kredit-/Eurochequekarten oder in entsprechenden Nicht-Automaten-Anwendungen dargestellt.

In **Fig. 7** ist ein Blockbild und in **Fig. 8** der Funktionsablauf einer Aufnahmeeinrichtung A_3 in Form eines Automaten wiedergegeben, der auch zum Bewirken einer Kontoführung im Identifikanden geeignet ist.

Der Automat enthält als Prüfeinrichtung einen Leseteil 37, in den der Identifikand 1 eingeführt werden kann. Der Leseteil ist in der Lage, den Identifikanden mit Strom zu versorgen und Daten zum Identifikanden zu schicken oder bzw. von dort zu empfangen. Die Steuerung des Automaten erfolgt durch die Zentraleinheit 10 mit dem Programmspeicher 11, die zur Vereinfachung der Darstellung außerhalb des Identifikanden dargestellt sind. Die Eingabe von Daten erfolgt über eine eingebaute Tastatur 38. Bei der Prüfung können Hinweise und Alarme nach außen und nach einer bestandenen Prüfung ein Freigabesignal an den Funktionsteil des Automaten gegeben werden, um die entsprechende Transaktion zu veranlassen. Außer der Kontoführung im Identifikanden wird in einem solchen Automaten eine Speicherung der Daten in einem Datenspeicher 39 vorgenommen. Dieser Datenspeicher wird entweder in Zeitabständen ausgewechselt und in einer Zentrale in die EDV übernommen oder bei on-line-Betrieb von der zentralen EDV abgefragt.

Der Automat enthält ferner eine Prüfeinrichtung 40, mit der festgestellt werden kann, ob von der Stelle im Identifikanden, an der bei echten Karten der IC angeordnet ist, Verbindungen zum Außenraum des Leseteils oder des Automaten bestehen. Hiermit soll das System gegen Rechtsbrecher gesichert werden, die den Funktions-Komplex des IC's im Identifikanden durch eine Simulationsschaltung aus diskreten Bauelementen außerhalb des Identifikanden ersetzen wollen.

Auch kann der Identifikand einbehalten werden.

Die Anordnung zur Einführung des Identifikanden in einem Automaten kann so ausgebildet sein, daß nach dem Einführen des Identifikanden durch den Benutzer eine Klappe oder ein Deckel manuell durch den Benutzer zu schließen ist oder die Klappe oder der Deckel automatisch geschlossen werden. Klappe oder Deckel sind so ausgeführt, daß sie eventuell vom Identifikanden nach außen führende Verbindungsleitungen beliebiger Art durch den Schließvorgang unterbrechen, z. B. abschneiden, und daß sie ferner den im Automaten befindlichen Identifikanden im Zusammenwirken mit einer fest um den Identifikanden-Leseteil des Automaten angebrachten Abschirmung gegen nicht leitungsabhängige Verbindungen, z. B. elektromagnetische oder mechanische Wellen, abschirmen. Der Verschluß ist so gestaltet, daß die Funktionen des Automaten nur bei vollständig geschlossener Klappe oder Deckel ablaufen und beim Öffnen unterbrochen werden.

Die weitere Prüfung erfolgt zunächst ähnlich wie bei dem vereinfachten Prüfgerät nach den **Fig. 4** und **5**, indem die persönliche Merkzahl eingegeben wird. Die persönliche Merkzahl wird zum Identifikanden übertragen und innerhalb des Identifikanden auf Übereinstimmung geprüft.

Vom Identifikanden kommt nur ein Signal zurück, mit dem Übereinstimmung oder Nicht-Übereinstimmung angezeigt wird.

Wenn die persönliche Merkzahl falsch eingegeben wird, erfolgt ein Hinweis. Die Eingabe kann maximal n-mal wiederholt werden. Als n wird in der Praxis üblicherweise die Zahl von drei Versuchen gewählt. Nach der n-ten Eingabe wird von einer Fehlversuch-Zähleinrichtung, die ebenfalls im Identifikanden ausgebildet sein kann, ein Alarmsignal ausgegeben, der IC im Identifikanden elektrisch zerstört und in dem Identifikanden ein Hinweis auf die Fehlversuche eingetragen.

Wurde die persönliche Merkzahl richtig eingegeben, können anschließend aus dem Identifikanden die Daten des Datenspeichers ausgegeben werden, die zur Identifizierung des Benutzers notwendig sind. Ebenso werden die Benutzungsdaten und die Kontodaten gelesen und im Automaten gespeichert. Nachdem diese Daten aus dem Identifikanden gelesen worden sind, kann die gewünschte Transaktion in den Automaten eingegeben werden.

Mit Hilfe der Benutzungsbedingungen und der Benutzungsdaten wird geprüft, ob die gewünschte Transaktion erlaubt ist. Ist die Transaktion nicht erlaubt, kann ein Hinweis ausgegeben werden, und ein geänderter Transaktionswunsch muß eingegeben werden. Wird die Transaktion als erlaubt befunden, wird als nächster Schritt die Kontofortschreibung im Identifikanden veranlaßt, und außerdem werden die Transaktionsdaten im Automaten aufgezeichnet und/oder zur Auswertung in die EDV-Zentrale übertragen. Danach erfolgt ein Freigabesignal aus dem Prüfteil des Automaten, und die Transaktion wird ausgeführt.

Bei off-line-Betrieb wird der Datenspeicher in gewissen Zeitabständen gegen einen leeren Datenspeicher ausgewechselt, und die aufgezeichnet Daten werden zur Auswertung in die EDV-Zentrale gebracht. In der EDV Zentrale erfolgt dann eine Fortschreibung der Konten der Inhaber der Identifikanden, so daß die Zentrale in Abhängigkeit vom Wechsel-Rhythmus des Datenspeichers im Transaktions-Automaten die Konten à jour halten kann.

Patentansprüche

1. Einrichtung zur Durchführung von Bearbeitungsvorgängen mit wenigstens einem Identifikanden und einer Vorrichtung zur Kommunikation mit dem Identifikanden, wobei der Identifikand eine integrierte Schaltung aufweist, die eine Steuereinrichtung und mindestens einen Speicher besitzt, auf welchen die Vorrichtung Schreib-/Lesezugriff hat, wobei über eine Schnittstelle zwischen Identifikand und Vorrichtung Daten aus dem Identifikanden ausgelesen und Daten in den Identifikanden eingeschrieben werden, **dadurch gekennzeichnet,**

— daß die Speicher **(13 ... 17)** nichtflüchtige programmierbare Schreib-/Lesespeicher (PROM) sind,

— daß die Steuereinrichtung ein Mikroprozessor **(10)** ist, der durch den Inhalt eines nichtflüchtigen Programmspeichers **(11)** gesteuert

wird, und

— daß der Schreib-/Lesezugriff auf die PROM-Speicher durch den Mikroprozessor gesteuert wird, wobei der Zugriff von außen zu den Speichern (13 ... 17) nur über den Mikroprozessor (10) möglich ist, während das Auslesen und Einschreiben im Innern der integrierten Schaltung freigegeben ist.

2. Einrichtung nach Anspruch 1, dadurch gekennzeichnet, daß ein Speicher (14) zur Speicherung einer persönlichen Merkzahl und ein Speicher (17) zur Speicherung der Anzahl von Fehlversuchen bei der Eingabe von Geheimzahlen vorgesehen sind.

3. Einrichtung nach Anspruch 2, dadurch gekennzeichnet, daß die persönliche Merkzahl ausschließlich im Mikroprozessor (10) mit der von außen in den Identifikanden eingegebenen persönlichen Merkzahl verglichen wird.

4. Einrichtung nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß ein Speicher (16) zur Speicherung von Benutzungsbedingungen vorgesehen ist, die nach n-maliger, vorzugsweise dreimaliger Falscheingabe der persönlichen Merkzahl und entsprechender Registrierung im Speicher (17) nicht mehr auslesbar sind.

5. Einrichtung nach Anspruch 4, dadurch gekennzeichnet, daß der Mikroprozessor (10) nur arbeitet, wenn die Benutzungsbedingungen auslesbar sind.

6. Einrichtung nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, daß eine Eingabe-/Ausgabe-Einheit (18) in der integrierten Schaltung (6) vorgesehen ist, über die alle Dateneingaben und Datenausgaben erfolgen.

Hierzu 4 Seite(n) Zeichnungen

– Leerseite –

Nummer: DE 27 60 486 C2
Int. Cl.[5]: G 06 K 19/073
Veröffentlichungstag: 2. September 1993

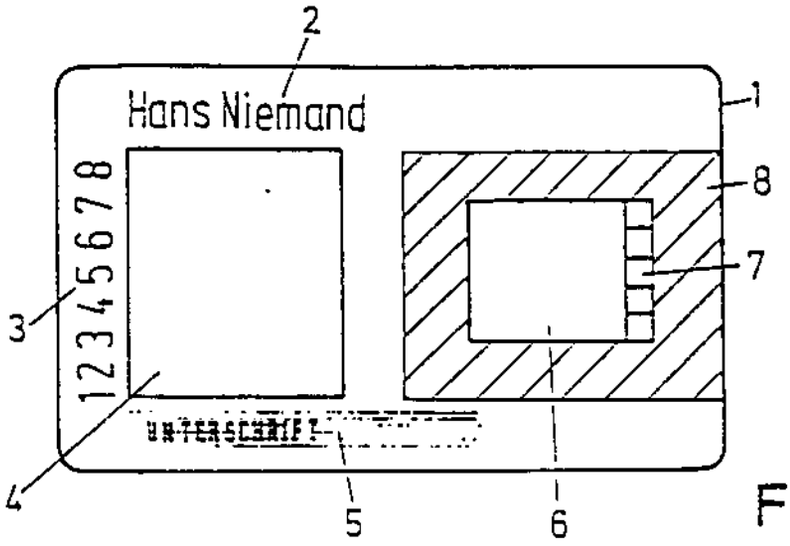

Fig. 1

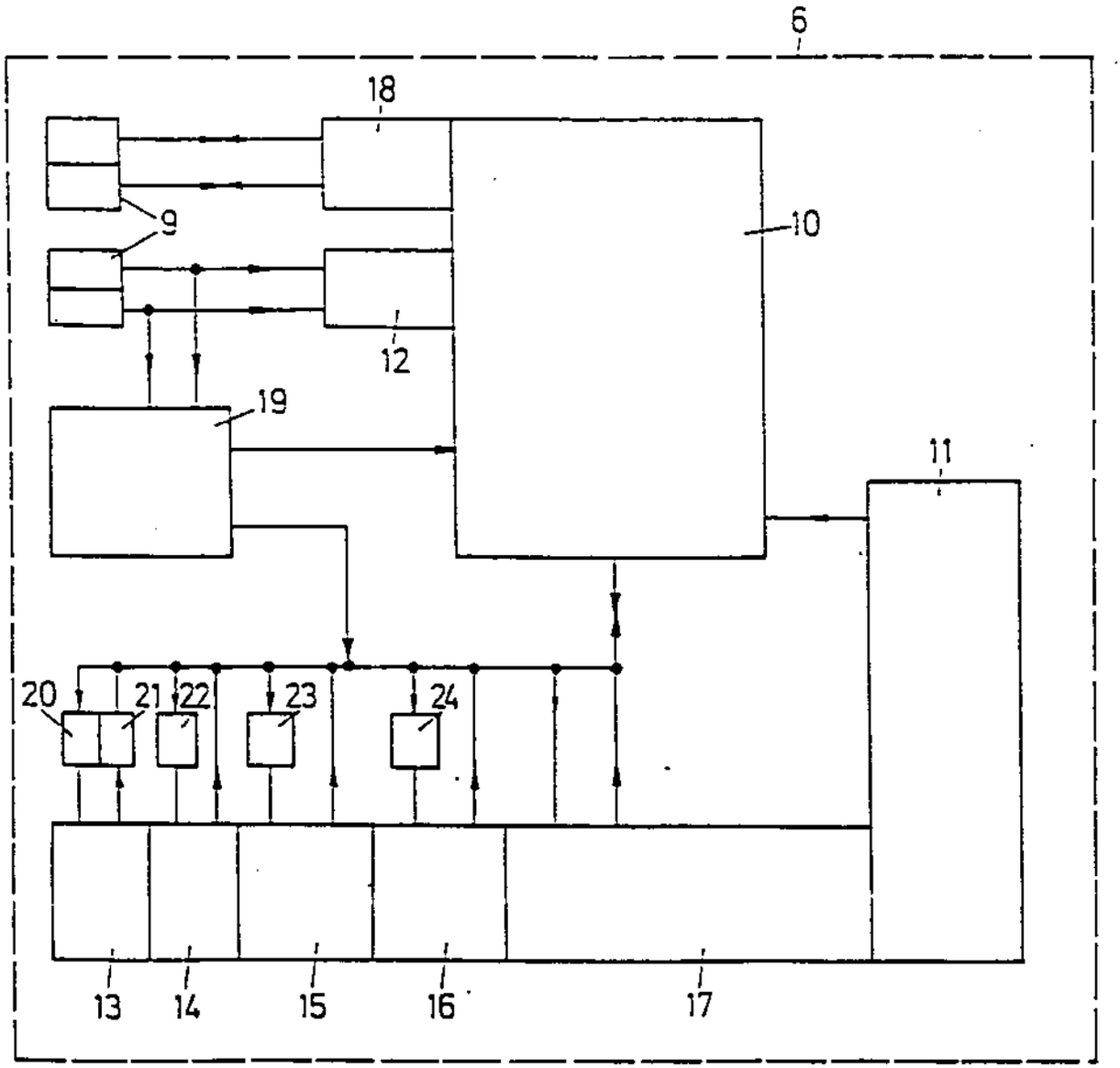

Fig. 2

Nummer: DE 27 60 486 C2
Int. Cl.[5]: G 06 K 19/073
Veröffentlichungstag: 2. September 1993

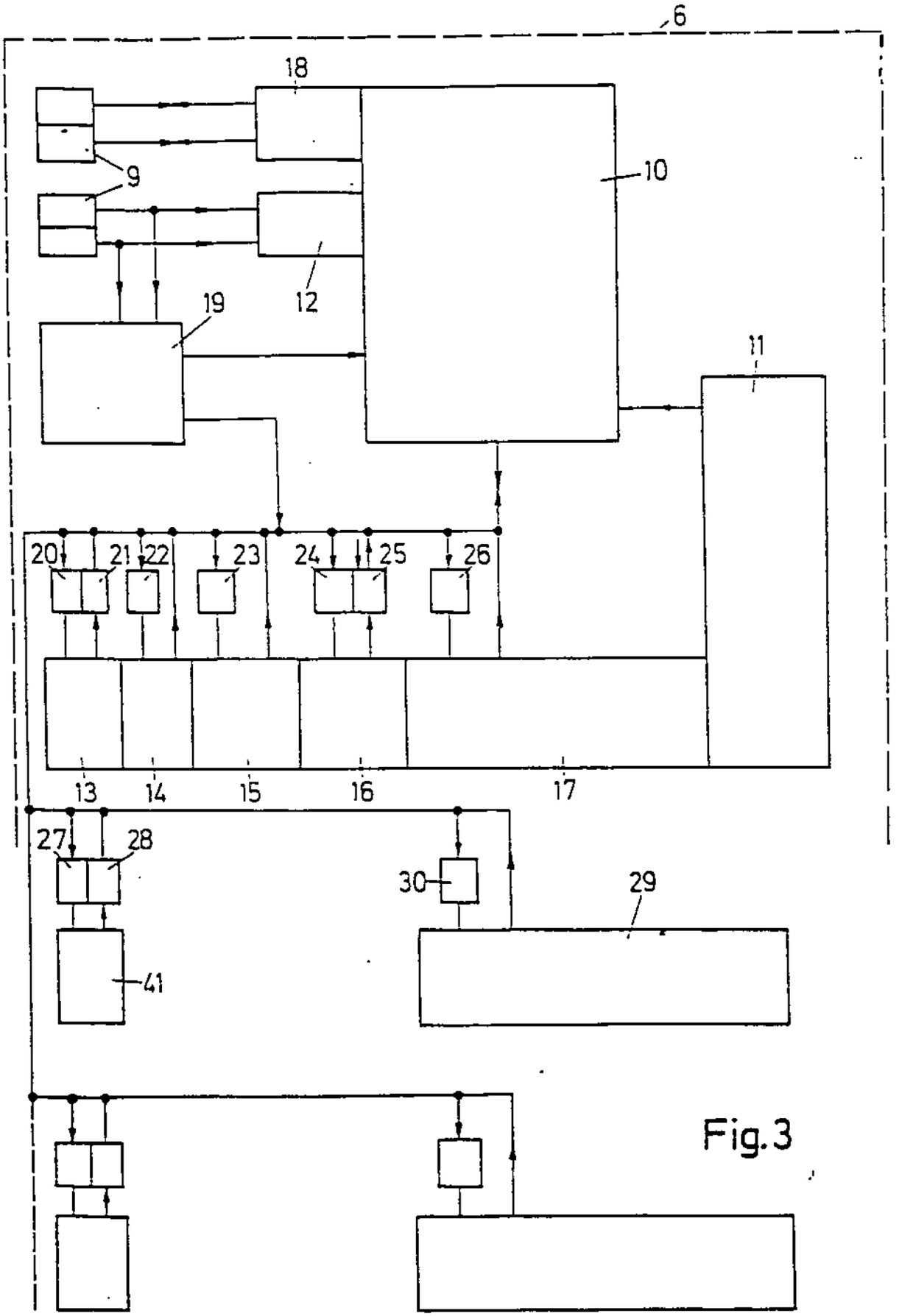

Fig.3

Nummer: DE 27 60 486 C2
Int. Cl.[5]: G 06 K 19/073
Veröffentlichungstag: 2. September 1993

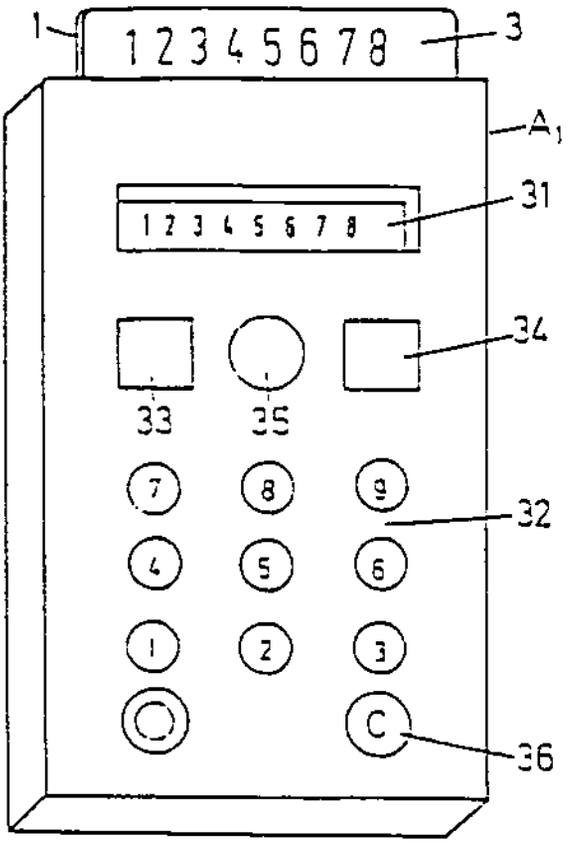

Fig.4

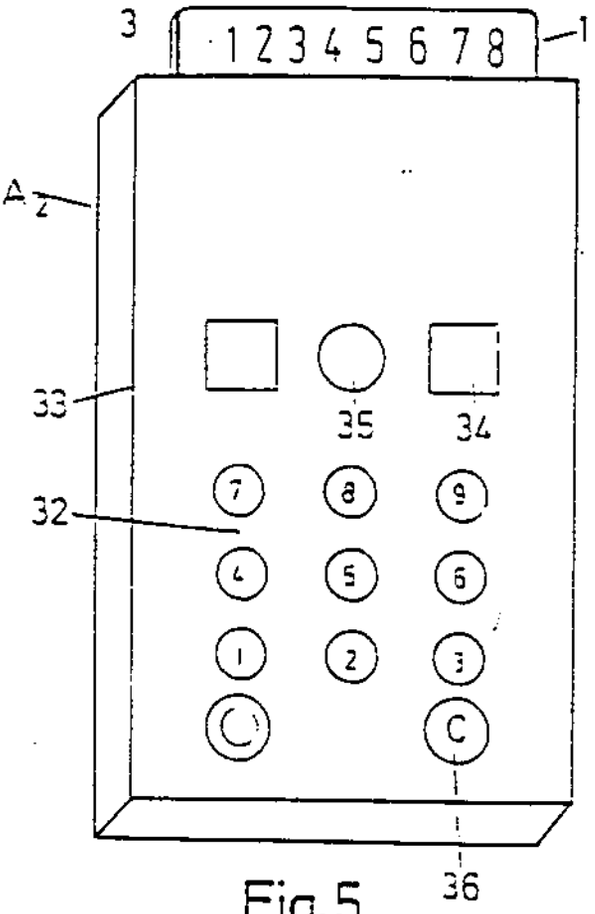

Fig.5

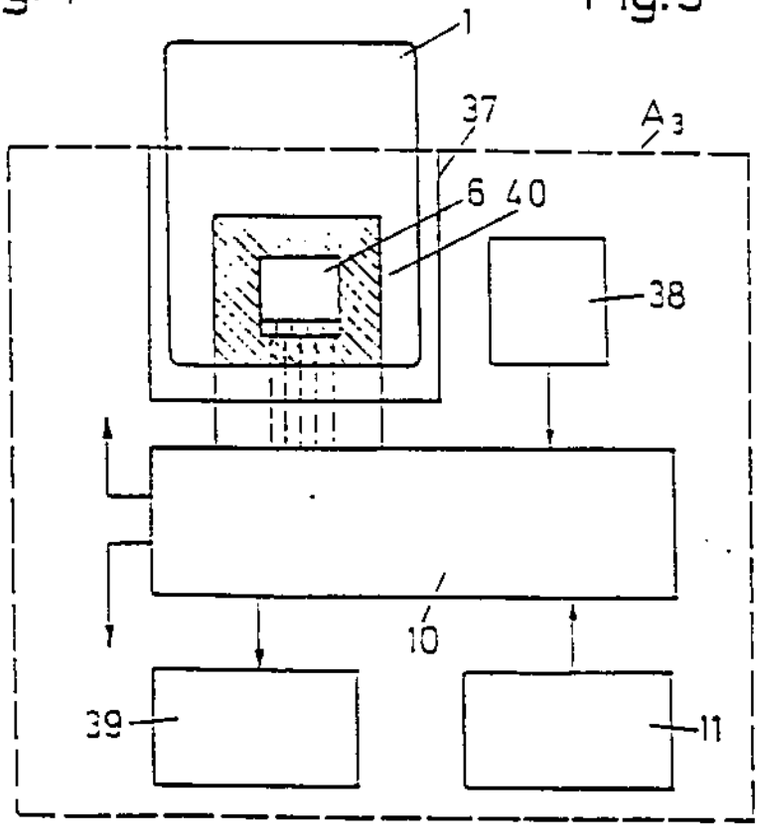

Fig.7

Nummer: DE 27 60 486 C2
Int. Cl.[5]: G 06 K 19/073
Veröffentlichungstag: 2. September 1993

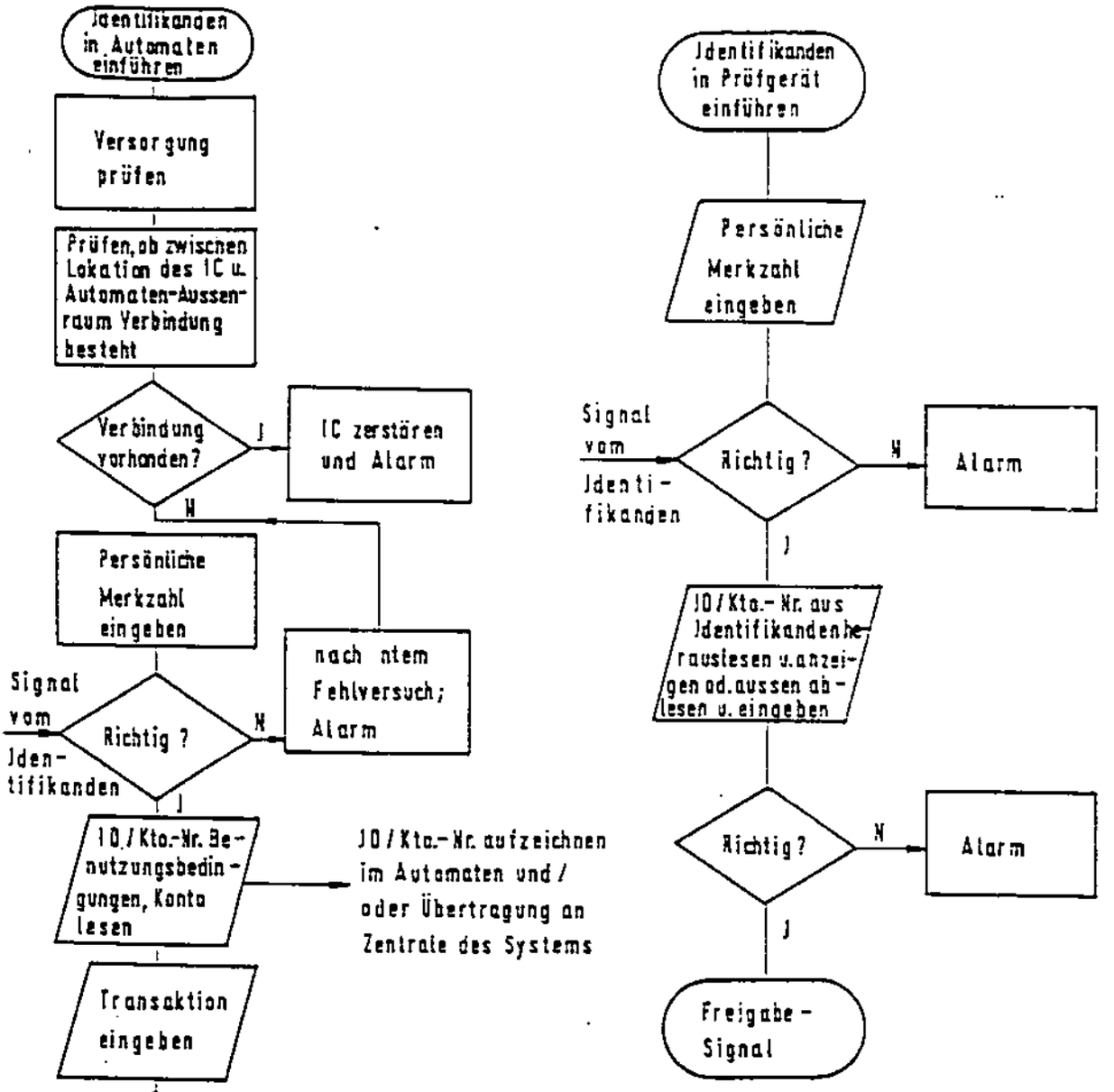

Fig. 6

Fig 8