(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Veröffentlichungsnummer: **0 377 763 A1**

(12) EUROPÄISCHE PATENTANMELDUNG

(21) Anmeldenummer: **89100453.3**

(51) Int. Cl.5: **G07F 7/10**

(22) Anmeldetag: **12.01.89**

(43) Veröffentlichungstag der Anmeldung:
18.07.90 Patentblatt 90/29

(84) Benannte Vertragsstaaten:
AT BE CH DE ES FR GB GR IT LI NL SE

(71) Anmelder: **SCHEIDT & BACHMANN GMBH**
Breite Strasse 132
D-4050 Mönchengladbach 2(DE)

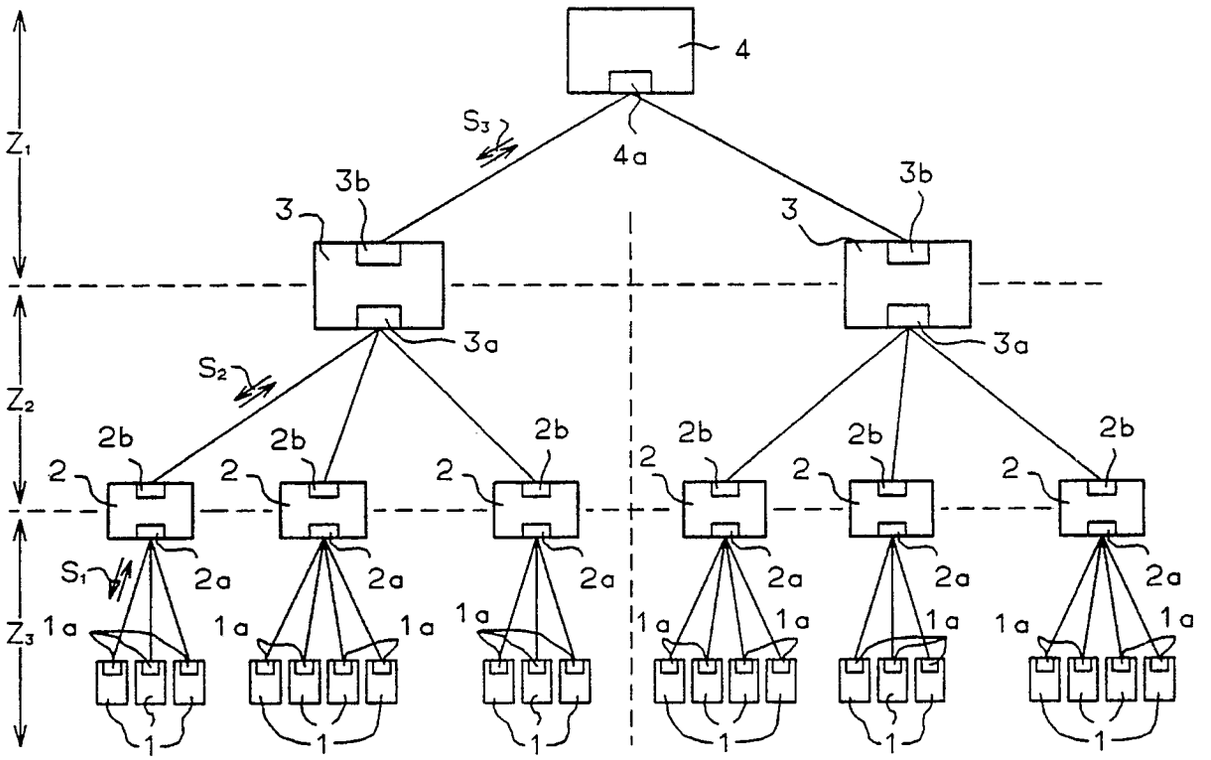
(72) Erfinder: **Miller, Gert, Dipl.-Ing.**
Schongauer Strasse 19
D-4050 Mönchengladbach 1(DE)
Erfinder: **Busch, Erwin**
Annakirchstrasse 188
D-4050 Mönchengladbach 1(DE)
Erfinder: **Brandts, Klaus**
Peter-Gens-Strasse 5
D-4052 Korschenbroich(DE)
Erfinder: **Wortelkamp, Ulrich, Dipl.-Ing.**
Köhlesfahrt 7
D-4050 Mönchengladbach 2(DE)

(74) Vertreter: **Patentanwälte Dipl.-Ing. Alex Stenger Dipl.-Ing. Wolfram Watzke Dipl.-Ing. Heinz J. Ring**
Kaiser-Friedrich-Ring 70
D-4000 Düsseldorf 11(DE)

(54) Einrichtung zur Überprüfung der Berechtigung eines Benutzers eines Gerätes zum Warenverkauf oder zur Erbringung oder Abrechnung von Dienstleistungen unter Verwendung eines maschinenlesbaren Berechtigungsausweises.

(57) Die Erfindung betrifft eine Einrichtung zur Überprüfung der Berechtigung eines Benutzers eines Gerätes (1) zum Warenverkauf oder zur Erbringung oder Abrechnung von Dienstleistungen unter Verwendung eines maschinenlesbaren Berechtigungsausweises, insbesondere einer Magnetkarte, und einer persönlichen Identifizierungsnummer (PIN). Bei derartigen Einrichtungen sind sämtliche Geräte (1) über Datenverbindungen mit einer Autorisierungsstelle (4) verbunden, wobei die Datenübertragung zwischen den Geräten (1) und der Autorisierungsstelle (4) unter Anwendung eines Verschlüsselungsverfahrens mit einem geheimen Schlüssel (S_3) erfolgt. Um die Sicherheit bei einer derartigen Überprüfung zu erhöhen und gleichzeitig die vorhandenen Datenverarbeitungen einschließlich ihrer Netze für diese Überprüfung heranzuziehen, sind die gruppenweise mit einem Gruppenrechner (2) verbundenen Geräte (1) mit einem kryptografischen Datenverarbeitungsmodul (1a) ausgestattet. Auch die Gruppenrechner (2) sind mit ihrem jeweils zugehörigen Leitrechner (3) über kryptografische Datenverarbeitungsmodule (2b,3a) verbunden. Die Schlüssel (S_1, S_2) für die kryptografischen Datenverarbeitungsmodule (1a,2a; 2b, 3a) einerseits zwischen den Geräten (1) und den Gruppenrechnern (2) und andererseits zwischen den Gruppenrechnern (2) und den Leitrechnern (3) sind unterschiedlich zueinander und unterschiedlich zu dem Schlüssel (S_3), der für das kryptografische Datenverarbeitungsmodul (4a) an der Autorisierungsstelle (4) verwendet wird.

EP 0 377 763 A1


4
4a
S3
Z1
3b
3
3a
S2
Z2
2b
2
2a
S1
Z3
1a
1

Einrichtung zur Überprüfung der Berechtigung eines Benutzers eines Gerätes zum Warenverkauf oder zur Erbringung oder Abrechnung von Dienstleistungen unter Verwendung eines maschinenlesbaren Berechtigungsausweises

Die Erfindung betrifft eine Einrichtung zur Überprüfung der Berechtigung eines Benutzers eines Gerätes zum Warenverkauf oder zur Erbringung oder Abrechnung von Dienstleistungen unter Verwendung eines maschinenlesbaren Berechtigungsausweises, insbesondere einer Magnetkarte, und einer persönlichen Identifizierungsnummer (PIN), mit einer über Datenverbindungen mit sämtlichen Geräten verbundenen Autorisierungsstelle, wobei die Datenübertragung zwischen den Geräten und der Autorisierungsstelle unter Anwendung eines Verschlüsselungsverfahrens mit geheimen Schlüsseln erfolgt.

Geräte zum Warenverkauf oder zur Erbringung von Dienstleistungen sind in unterschiedlichsten Ausführungen bekannt, beispielsweise in der Form von Zapfstellen zum Verkauf flüssiger oder gasförmiger Kraftstoffe oder als Geräte zur Ausgabe und Abrechnung von Berechtigungsausweisen für die Inanspruchnahme einer Dienstleistung, beispielsweise die Benutzung eines Transportmittels oder einer Parkfläche.

Um derartige Geräte ohne großen Personaleinsatz betreiben zu können, ist es bekannt, sie als selbstkassierende Automaten auszuführen. Hierbei ist die bezogene Ware unmittelbar nach Bezug durch Münzen oder Banknoten zu bezahlen, wogegen der Berechtigungsausweis entweder vor Inanspruchnahme der Dienstleistung, beispielsweise beim Bezug einer Fahrkarte, oder nach Erbringung der Dienstleistung, beispielsweise bei Benutzung einer Parkfläche, zu bezahlen ist. Die Mehrzahl derartiger Automaten ist mit einer Wechselgeldrückgabe ausgestattet, so daß der Benutzer die Ware oder Dienstleistung nicht nur erwerben kann, wenn er den passenden Geldbetrag bereithält.

Mit der zunehmenden Verbreitung von Kredit- und Debitkarten in Form von maschinenlesbaren Berechtigungsausweisen ergibt sich die Notwendigkeit, die Geräte zum Warenverkauf oder zur Erbringung von Dienstleistungen derart auszustatten, daß sie auch unter Verwendung eines maschinenlesbaren Berechtigungsausweises benutzt werden können. Um die Benutzung durch Unberechtigte oder mit Hilfe gefälschter Berechtigungsausweise zu unterbinden, wird jedem Besitzer eines maschinenlesbaren Berechtigungsausweises eine persönliche Identifizierungsnummer (PIN) zugeteilt, die nach einem bestimmten Algorithmus ermittelt wird und vom Berechtigten geheimgehalten werden muß. Diese persönliche Identifizierungsnummer muß mit Hilfe einer Tastatur zusätzlich eingegeben werden, wenn der maschinenlesbare Berechtigungsausweis in das jeweilige Gerät eingeführt wird. Die maschinenlesbaren Daten und die persönliche Identifizierungsnummer werden über Datenverbindungen einer mit sämtlichen Geräten verbundenen Autorisierungsstelle zugeführt, welche das jeweilige Gerät nur dann freigibt, wenn die Überprüfung der beiden Datensätze durch die Autorisierungsstelle ergeben hat, daß sämtliche Daten richtig sind.

Um zu verhindern, daß die zu einem bestimmten Berechtigungsausweis gehörende persönliche Identifizierungsnummer während des Datentransportes zwischen Gerät und Autorisierungsstelle ermittelt werden kann, erfolgt der Transport unter Anwendung eines Verschlüsselungsverfahrens mit einem geheimen Schlüssel. Zu diesem Zweck ist es bei den bekannten Geräten erforderlich, jedes einer bestimmten Autorisierungsstelle zugeordnete Gerät zum Warenverkauf oder zur Erbringung von Dienstleistungen mit einem kryptografischen Datenverarbeitungsmodul zu versehen, das die maschinengelesenen Daten des Berechtigungsausweises und die per Tastatur eingegebene persönliche Identifizierungsnummer mit Hilfe eines Verschlüsselungsverfahrens mit dem geheimen Schlüssel verschlüsselt. Die verschlüsselten Daten werden erst beim Eingang in die Autorisierungsstelle durch ein entsprechendes Modul entschlüsselt.

Da jedes der zu einer Autorisierungsstelle gehörenden Geräte mit einem kryptografischen Datenverarbeitungsmodul ausgestattet ist und diese Module wegen der Zugehörigkeit zu derselben Autorisierungsstelle identisch sind, bietet jedes Gerät die Möglichkeit zur Ausspionierung des geheimen Schlüssels. Als weiterer Nachteil kommt hinzu, daß die Geräte für die Öffentlichkeit zugänglich sind. Trotz einer aufwendigen kryptografischen Absicherung ist das bekannte Verschlüsselungssystem deshalb verhältnismäßig unsicher.

Der Erfindung liegt die Aufgabe zugrunde, die Sicherheit der bekannten Einrichtung zur Überprüfung der Berechtigung eines Benutzers eines Gerätes zum Warenverkauf oder zur Erbringung von Dienstleistungen unter Verwendung eines maschinenlesbaren Berechtigungsausweises und einer persönlichen Identifizierungsnummer ohne wesentliche Zusatzkosten erheblich zu erhöhen.

Die Lösung dieser Aufgabenstellung durch die Erfindung ist dadurch gekennzeichnet, daß die zur Verarbeitung von organisa torischen und betriebswirtschaftlichen Daten gruppenweise mit einem Gruppenrechner verbundenen Geräte zur Uberprüfung der Berechtigung eines Benutzers ebenso wie der Gruppenrechner jeweils mit einem kryptografi-

schen Datenverarbeitungsmodul ausgestattet sind, daß die Gruppenrechner ihrerseits mit einem jeweils für die organisatorische und betriebswirtschaftliche Datenverarbeitung vorhandenen, zugehörigen Leitrechner ebenfalls über kryptografische Datenverarbeitungsmodule verbunden sind und daß die Schlüssel für die kryptografischen Datenverarbeitungsmodule einerseits zwischen den Geräten und den Gruppenrechnern und andererseits zwischen den Gruppenrechnern und den Leitrechnern unterschiedlich zueinander und unterschiedlich zu dem Schlüssel sind, der für das kryptografische Datenverarbeitungsmodul an der Autorisierungsstelle verwendet wird, das ebenfalls an jedem Leitrechner angeordnet ist.

Durch die erfindungsgemäße Weiterbildung der eingangs beschriebenen, bekannten Einrichtung werden die mit dem geheimen, für die Autorisierungsstelle zuständigen Schlüssel ausgestatteten Datenverarbeitungsmodule lediglich an den Leitrechnern eingesetzt, die außerhalb des Publikumszugangs in gesicherten Räumen stehen, so daß sich für den geheimen Schlüssel eine Sicherheitszone mit erheblich gesteigerter Sicherheit ergibt. Dieser Sicherheitszone werden zwei weitere Sicherheitszonen vorgeschaltet. In der einen dieser Sicherheitszonen befinden sich die Gruppenrechner, in der anderen die für das Publikum zugänglichen Geräte. Da die für die jeweils zusammenwirkenden kryptografischen Datenverarbeitungsmodule verwendeten Schlüssel der beiden zusätzlichen Sicherheitszonen unterschiedlich sind, würde selbst das Ausspionieren des zwischen den Geräten und den Gruppenrechnern verwendeten Schlüssels keinen Durchgriff zum Leitrechner und erst recht keinen Durchgriff zur Autorisierungsstelle ermöglichen. Durch die er findungsgemäße Weiterbildung ist demzufolge die Sicherheit der Überprüfungseinrichtung ganz entscheidend vergrößert worden, wozu lediglich zusätzliche kryptografische Datenverarbeitungsmodule entsprechend der doppelten Anzahl der Gruppen- und Leitrechner erforderlich sind. Dieser Mehraufwand an kryptografischen Datenverarbeitungsmodulen wird insgesamt jedoch dadurch mehr als ausgeglichen, daß für die erfindungsgemäße Einrichtung nicht nur Gruppen- und Leitrechner Verwendung finden, die bereits für die Verarbeitung von organisatorischen und betriebswirtschaftlichen Daten der Geräte vorhanden sind, sondern daß auch deren vorhandenes Datenleitungsnetz für die Überprüfung der Berechtigung eines Benutzers herangezogen wird, so daß lediglich noch die Leitrechner mit der zugehörigen Autorisierungsstelle verbunden werden müssen. Die durch die erfindungsgemäße Weiterbildung erheblich gesteigerte Sicherheit muß demgemäß nicht mit zusätzlichem Hardwareaufwand erkauft werden.

Eine zusätzliche Steigerung der Sicherheit läßt sich gemäß einem weiteren Merkmal der Erfindung dadurch erzielen, daß die Schlüssel für die kryptografischen Datenverarbeitungsmodule der jeweils an einen Leitrechner angeschlossenen Gruppenrechner zueinander und/oder zu denen eines anderen, derselben Autorisierungsstelle zugeordneten Leitrechners unterschiedlich ausgebildet sind. Erfindungsgemäß können auch die Schlüssel für die kryptografischen Datenverarbeitungsmodule der jeweils an einen Gruppenrechner angeschlossenen Geräte zueinander unterschiedlich ausgebildet werden.

Bei einer bevorzugten Ausführungsform der Erfindung sind die kryptografischen Datenverarbeitungsmodule an den Gruppenrechnern als Sicherheitsmodul ausgebildet, das ausschließlich mit dem bestimmten Gruppenrechner funktionsfähig ist. Derartige Sicherheitsmodule sind gegen Ausspionieren der ge speicherten Daten und Programme geschützt. Damit ein derartiges Sicherheitsmodul nur für den einen bestimmten Gruppenrechner verwendbar ist und Manipulationen oder Vertauschen von Modulen ausgeschlossen sind, wird erfindungsgemäß bei der Erstinbetriebnahme dem Sicherheitsmodul ein kryptografisches Kennzeichen eingegeben, das ausschließlich für diesen bestimmten Gruppenrechner vergeben ist.

Auf der Zeichnung ist ein Ausführungsbeispiel der erfindungsgemäßen Einrichtung anhand eines Blockschaltbildes dargestellt.

Das Blockschaltbild zeigt eine Anzahl von Geräten 1, die jeweils zu Gruppen zusammengefaßt sind. Bei diesen Geräten 1 handelt es sich entweder um Geräte zum Warenverkauf, beispielsweise um Zapfstellen für flüssige und/oder gasförmige Kraftstoffe, oder um Geräte zur Erbringung von Dienstleistungen, beispielsweise um Automaten zur Abrechnung von Parkgebühren. Die jeweils zu einer Tankstelle oder einem Parkhaus gehörenden Geräte 1 sind gruppenweise jeweils mit einem Gruppenrechner 2 verbunden, der die organisatorischen und betriebswirtschaftlichen Daten der zugehörigen Geräte verarbeitet. Mehrere dieser Gruppenrechner 2 sind ihrerseits einem Leitrechner 3 zugeordnet, der ebenfalls für die Verarbeitung der organisatorischen und betriebswirtschaftlichen Daten herangezogen wird. Ein derartiger Leitrechner 3 steht beispielsweise in der Zentrale einer Ölgesellschaft. Die beiden auf der Zeichnung dargestellten Leitrechner 3 können somit beispielsweise die in der Zentrale angeordneten Rechner zweier Ölgesellschaften sein, die über eine Mehrzahl von zwischengeschalteten Gruppenrechnern 2 mit sämtlichen Tankstellen der Gesellschaft verbunden sind. Ein derartiges Datenverarbeitungsnetz ist üblicherweise für die Verarbeitung organisatorischer und betriebswirtschaftlicher Daten vorhanden.

Bei der auf der Zeichnung schematisch darge-

stellten Einrichtung ist jedes Gerät 1 sowohl mit einer Tastatur als auch mit einem Magnetkartenleser versehen. Mit Hilfe dieses Magnetkartenlesers ist es möglich, die Daten maschinenlesbarer Berechtigungsausweise, vorzugsweise von Eurocheque-Karten zu erfassen. Die Tastatur dient dazu, die dem Inhaber des jeweiligen Berechtigungsausweises zugeteilte persönliche Identifizierungsnummer (PIN-Code) in das Gerät 1 einzugeben.

Da eine Inbetriebnahme des jeweiligen Gerätes 1 nur dann erfolgen soll, wenn zuvor die Berechtigung des Benutzers anhand der maschinenlesbaren Daten seines Berechtigungsausweises und der von ihm eingegebenen persönlichen Identifizierungsnummer überprüft worden ist, erfolgt vor der Benutzungsfreigabe eine Überprüfung durch eine übergeordnete Autorisierungsstelle 4. Wie die Zeichnung zeigt, kann diese Autorisierungsstelle 4 mehreren selbständigen Betrieben zugeordnet sein und demzufolge mit einer Mehrzahl von Leitrechnern 3 zusammenarbeiten.

Da verhindert werden muß, daß die vom jeweiligen Berechtigten über die Tastatur eingegebene persönliche Identifizierungsnummer im Zusammenhang mit den maschinenlesbaren Daten seines Berechtigungsausweises, beispielsweise seiner Eurocheque-Karte, unbefugt abgefragt wird, ist jedes Gerät 1 mit einem kryptografischen Datenverarbeitungsmodul 1a ausgestattet, in dem die maschinell gelesenen und von Hand eingegebenen Daten mit einem bestimmten Schlüssel S_1 verschlüsselt werden, bevor sie über die auf der Zeichnung dargestellten Datenverbindungen an den jeweiligen Gruppenrechner 2 weitergegeben werden. Dieser Gruppenrechner 2 besitzt seinerseits ein kryptografisches Datenverarbeitungsmodul 2a, das die von den Geräten 1 gelieferten Daten zur Überprüfung der Berechtigung mit dem Schlüssel S_1 entschlüsselt, bevor diese Daten verarbeitet bzw. weitergegeben werden.

Auch die Weitergabe der für die Überprüfung der Berechtigung erforderlichen Daten vom Gruppenrechner 2 an den Leitrechner 3 erfolgt nach entsprechender Verschlüsselung. Zu diesem Zweck ist der Ausgang jedes Gruppenrechners 2 und der Eingang jedes Leitrechners 3 wiederum jeweils mit einem kryptografischen Datenverarbeitungsmodul 2b bzw. 3a versehen, die unter Verwendung eines Schlüssels S_2 arbeiten. Auch der Transport der Daten zwischen Gruppenrechner 2 und Leitrechner 3 ist demzufolge gegen unbefugte Abfrage geschützt.

Am Ausgang jedes Leitrechners 3 ist schließlich wiederum ein kryptografisches Datenverarbeitungsmodul 3b angeordnet, das mit dem kryptografischen Datenverarbeitungsmodul 4a der Autorisierungsstelle 4 zusammenarbeitet, und zwar unter Benutzung des geheimen Schlüssels S_3, der originär von der Autorisierungsstelle 4 zur Erstellung der persönlichen Identifizierungsnummer verwendet worden ist. Der unter Verwendung dieses geheimen Schlüssels S_3 erfolgende Datentransport findet somit in einer Sicherheitszone Z_1 statt, die bereits deshalb eine erhöhte Sicherheit aufweist, weil sowohl die Autorisierungsstelle 4 als auch die Leitrechner 3 in besonders abgesicherten Räumen stehen und dem Publikum nicht zugänglich sind. Durch die voranstehend erwähnte Vorschaltung zweier weiterer Verschlüsselungsverfahren werden dieser Sicherheitszone Z_1 zwei weitere Sicherheitszonen Z_2 und Z_3 vorgeschaltet, die ebenfalls in der Zeichnung eingetragen sind. Die Sicherheitszone Z_2 hat hierbei eine höhere Sicherheit als die Sicherheitszone Z_3, weil sich auch die Gruppenrechner 2 in besonders abgesicherten Räumen befinden, wogegen die Geräte 1 dem Publikum zugänglich und damit besonderen Manipulationsmöglichkeiten ausgesetzt sind.

Wie aus den voranstehenden Erläuterungen ersichtlich ist, läßt sich die Sicherheit der Überprüfung der Berechtigung eines Benutzers im Hinblick auf den hierbei zu verwendenden geheimen Schlüssel S_3 unter Einsatz der bereits für die Verarbeitung organisatorischer und betriebswirtschaftlicher Daten vorhandenen Datenverarbeitung (Gruppenrechner 2 und Leitrechner 3 einschließlich des zugehörigen Leitungsnetzes) dadurch wesentlich steigern, daß nicht nur die Geräte 1 und die Autorisierungsstelle 4, sondern auch die Gruppenrechner 2 und Leitrechner 3 mit entsprechenden kryptografischen Datenverarbeitungsmodulen versehen werden, so daß die Berechtigungsüberprüfung unter Einsatz der vorhandenen Datenverarbeitungen bei gleichzeitiger Schaffung zweier zusätzlicher Sicherheitszonen Z_2 und Z_3 erfolgen kann. Mit der erfindungsgemäßen Einrichtung ist es demzufolge möglich, beispielsweise auch Eurocheque-Karten anstelle oder zusätzlich zu den bekannten Kreditkarten zur Abrechnung der bezogenen Ware oder erbrachten Dienstleistungen heranzuziehen.

Die Sicherheit der Einrichtung gegen unerlaubtes Ausspionieren insbesondere der geheimen persönlichen Identifizierungsnummern kann noch dadurch erhöht werden, daß der Schlüssel S_2 für die kryptografischen Datenverarbeitungsmodule 2b und 3a der jeweils einem Leitrechner 3 zugeordneten Gruppenrechner 2 zueinander und/oder zu den Schlüsseln S_2 eines anderen Leitrechners 3 unterschiedlich ausgebildet werden. Beim Ausführungsbeispiel gemäß der Zeichnung kann demzufolge nicht nur ein unterschiedlicher Schlüssel S_2 für den linken und für den rechten Leitrechner 3 verwendet werden, sondern auch unterschiedliche Schlüssel S_2 zwischen dem jeweiligen Leitrechner 3 und den ihm zugeordneten Gruppenrechnern 2.

Schließlich ist es ebenfalls möglich, die Schlüssel S_1 für die kryptografischen Datenverarbeitungsmodule 1a und 2a der jeweils an einen Gruppenrechner 2 angeschlossenen Geräte 1 zueinander unterschiedlich auszubilden. Hiermit würde erreicht, daß ein an einem bestimmten Gerät 1 ausspionierter Schlüssel S_1 nicht bei der Benutzung oder Manipulation an Geräten 1 verwendet werden kann, die mit einem anderen Gruppenrechner 2 zusammenarbeiten.

Die kryptografischen Datenverarbeitungsmodule 2a bzw. 2b an den Gruppenrechnern 2 werden vorzugsweise als Sicherheitsmodul ausgebildet, das ausschließlich mit dem bestimmten Gruppenrechner 2 funktionsfähig ist. Dies kann beispielsweise dadurch bewirkt werden, daß bei der Erstinbetriebnahme dem Sicherheitsmodul ein kryptografisches Kennzeichen eingegeben wird, das ausschließlich für einen bestimmten Gruppenrechner 2 vergeben wird.

Bezugszeichenliste:

1 Gerät
1a kryptografisches Datenverarbeitungsmodul
2 Gruppenrechner
2a kryptografisches Datenverarbeitungsmodul
2b kryptografisches Datenverarbeitungsmodul
3 Leitrechner
3a kryptografisches Datenverarbeitungsmodul
3b kryptografisches Datenverarbeitungsmodul
4 Autorisierungsstelle
4a kryptografisches Datenverarbeitungsmodul
S_1 Schlüssel
S_2 Schlüssel
S_3 Schlüssel
Z_1 Sicherheitszone
Z_2 Sicherheitszone
Z_3 Sicherheitszone

Ansprüche

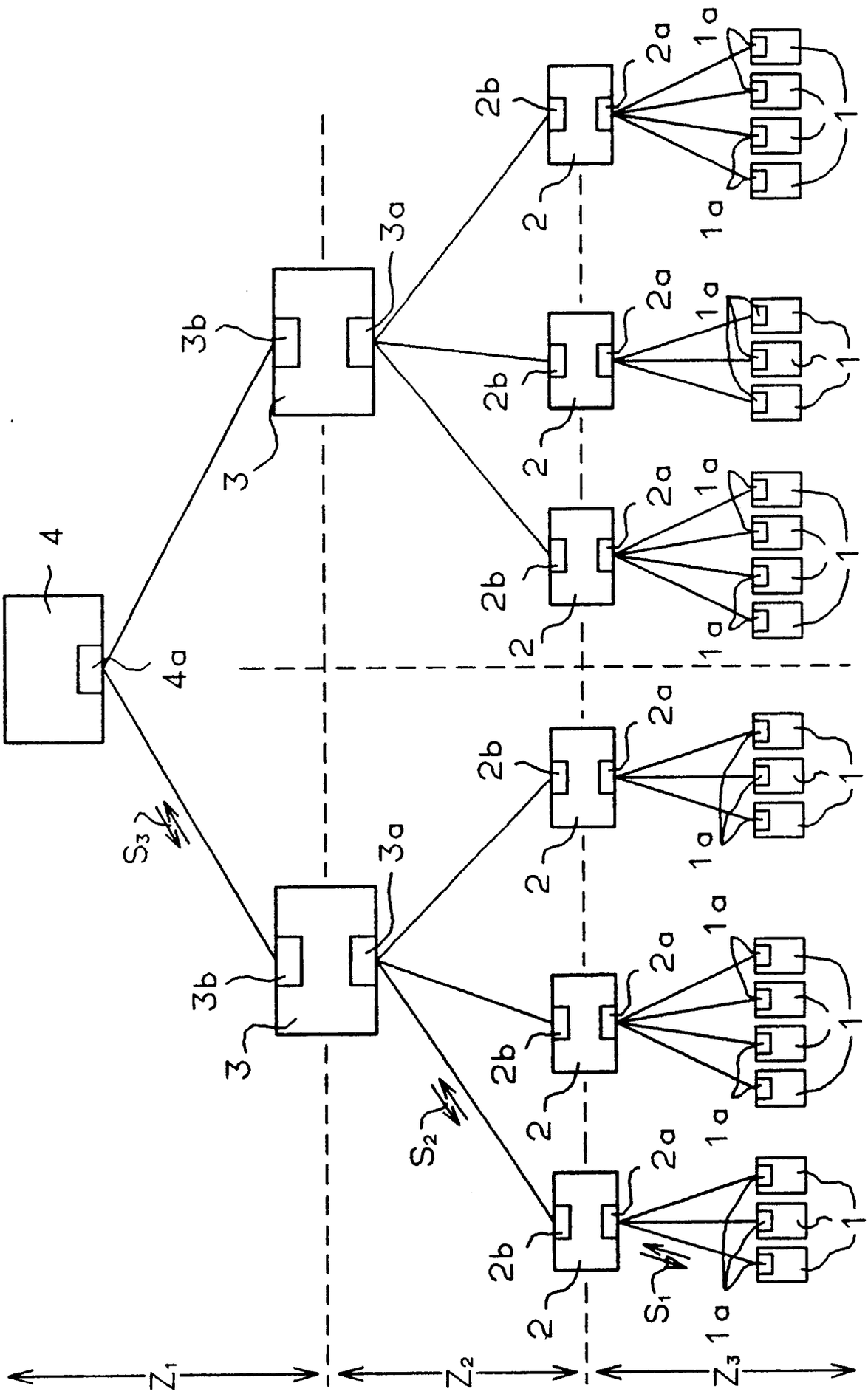
1. Einrichtung zur Überprüfung der Berechtigung eines Benutzers eines Gerätes (1) zum Warenverkauf oder zur Erbringung oder Abrechnung von Dienstleistungen unter Verwendung eines maschinenlesbaren Berechtigungsausweises, insbesondere einer Magnetkarte, und einer persönlichen Identifizierungsnummer (PIN), mit einer über Datenverbindungen mit sämtlichen Geräten (1) verbundenen Autorisierungsstelle (4), wobei die Datenübertragung zwischen den Geräten (1) und der Autorisierungsstelle (4) unter Anwendung eines Verschlüsselungsverfahrens mit einem geheimen Schlüssel (S_3) erfolgt,
dadurch gekennzeichnet,
daß die zur Verarbeitung von organisatorischen und betriebswirtschaftlichen Daten gruppenweise mit einem Gruppenrechner (2) verbundenen Geräte (1) zur Überprüfung der Berechtigung eines Benutzers ebenso wie der Gruppenrechner (2) jeweils mit einem kryptografischen Datenverarbeitungsmodul (1a,2a) ausgestattet sind, daß die Gruppenrechner (2) ihrerseits mit einem jeweils für die organisatorische und betriebswirtschaftliche Datenverarbeitung vorhandenen zugehörigen Leitrechner (3) ebenfalls über kryptografische Datenverarbeitungsmodule (2b,3a) verbunden sind und daß die Schlüssel (S_1, S_2) für die kryptografischen Datenverarbeitungsmodule (1a,2a; 2b,3a) einerseits zwischen den Geräten (1) und den Gruppenrechnern (2) und andererseits zwischen den Gruppenrechnern (2) und den Leitrechnern (3) unterschiedlich zueinander und unterschiedlich zu dem Schlüssel (S_3) sind, der für das kryptografische Datenverarbeitungsmodul (4a) an der Autorisierungsstelle (4) verwendet wird, das ebenfalls an jedem Leitrechner (3) (Modul 3b) angeordnet ist.

2. Einrichtung nach Anspruch 1, dadurch gekennzeichnet, daß die Schlüssel (S_2) für die kryptografischen Datenverarbeitungsmodule (2b) der jeweils an einen Leitrechner (3) angeschlossenen Gruppenrechner (2) zueinander und/oder zu denen eines anderen, derselben Autorisierungsstelle (4) zugeordneten Leitrechners (3) unterschiedlich ausgebildet sind.

3. Einrichtung nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die Schlüssel (S_1) für die kryptografischen Datenverarbeitungsmodule (1a) der jeweils an einen Gruppenrechner (2) angeschlossenen Geräte (1) zueinander unterschiedlich ausgebildet sind.

4. Einrichtung nach mindestens einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß die kryptografischen Datenverarbeitungsmodule (2a,2b) an den Gruppenrechnern (2) als Sicherheitsmodul ausgebildet sind, das ausschließlich mit dem bestimmten Gruppenrechner (2) funktionsfähig ist.

5. Einrichtung nach Anspruch 4, dadurch gekennzeichnet, daß bei der Erstinbetriebnahme dem Sicherheitsmodul ein kryptografisches Kennzeichen eingegeben wird, das ausschließlich für diesen Gruppenrechner (2) vergeben ist.


4
4a
3
3a
3b
2
2a
2b
1
1a
S1
S2
S3
Z1
Z2
Z3

Europäisches Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung

EP 89 10 0453

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (Int. Cl.5)
X	EP-A-0 068 805 (VISA U.S.A.) * Zusammenfassung; Abbildungen 1-8; Seite 6, Zeile 10 - Seite 9, Zeile 17; Patentanspruch 1 *	1-4	G 07 F 7/10
A	---	5	
A	WO-A-8 102 655 (M. SENDROW) * Zusammenfassung; Seite 5, Zeile 20 - Seite 7, Zeile 29; Abbildung 1; Patentansprüche *	1-5	
A	---		
A	FR-A-2 608 338 (ELECTRONIQUE SERGE DASSAULT) * Zusammenfassung; Abbildungen; Patentansprüche *	1,3-5	
A	---		
A	US-A-4 408 203 (C.M. CAMPBELL)		
A	---		
A	EP-A-0 186 981 (IBM)		

RECHERCHIERTE SACHGEBIETE (Int. Cl.5)

G 07 F
G 06 F
H 04 L

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
DEN HAAG	14-09-1989	DAVID J.Y.H.

KATEGORIE DER GENANNTEN DOKUMENTE

X : von besonderer Bedeutung allein betrachtet
Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie
A : technologischer Hintergrund
O : nichtschriftliche Offenbarung
P : Zwischenliteratur

T : der Erfindung zugrunde liegende Theorien oder Grundsätze
E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist
D : in der Anmeldung angeführtes Dokument
L : aus andern Grunden angeführtes Dokument

& : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument

EPO FORM 1503 03.82 (P0403)