





EUROPÄISCHE PATENTANMELDUNG

 **Anmeldenummer : 95109864.9**

 **Int. Cl.⁶ : G07B 17/02**

 **Anmeldetag : 23.06.95**

 **Priorität : 24.06.94 DE 4422263**

 **Veröffentlichungstag der Anmeldung :
27.12.95 Patentblatt 95/52**

 **Benannte Vertragsstaaten :
AT BE CH DE DK ES FR GB GR IE IT LI LU MC
NL PT SE**

 **Anmelder : Francotyp-Postalia GmbH
Triftweg 21-26
D-16547 Birkenwerder (DE)**

 **Erfinder : Wagner, Andreas
Ritterstrasse 42
D-10969 Berlin (DE)**

 **Vertreter : Schaumburg, Thoenes & Thurn
Postfach 86 07 48
D-81634 München (DE)**

 **Verfahren zum Abstimmen des Datenbestandes zwischen einer elektronischen Frankiermaschine und einem Datenzentrum**

 Das Abstimmen des Datenbestandes in der einen Guthabenspeicher (26) für ein Portoguthaben umfassenden Datenverarbeitungseinrichtung (22) einer elektronischen Frankiermaschine (12) und der einen Abrechnungsspeicher (46) für die Frankiermaschine umfassenden Abrechnungseinrichtung (42) eines Datenzentrums (18), erfolgt in der Weise, daß an der Frankiermaschine (12) ein Wertänderungsmodus eingestellt wird, daß in einer ersten den Austausch von Codezahlen umfassenden Transaktion zwischen der Frankiermaschine (12) und dem Datenzentrum (18) ein in die Frankiermaschine (12) eingegebener Vorgabewert an das Datenzentrum (18) übermittelt und in einem jeweiligen Vorgabewertspeicher (28 ; 45) der Frankiermaschine (12) und des Datenzentrums (18) gespeichert wird, daß ein Nachlademodus eingestellt wird und daß in einer zweiten den Austausch von Codezahlen zwischen der Frankiermaschine (12) und dem Datenzentrum (18) umfassenden Transaktion der im jeweiligen Vorgabewertspeicher (28) gespeicherte Vorgabewert zu dem im Guthabenspeicher (26) der Frankiermaschine (12) und dem im Abrechnungsspeicher (46) des Datenzentrums gespeicherten Wert addiert wird.

Die Erfindung betrifft ein Verfahren zum Abstimmen des Datenbestandes in der einen Guthabenspeicher für ein Portoguthaben umfassenden Datenverarbeitungseinrichtung einer elektronischen Frankiermaschine und der einen Abrechnungsspeicher für die Frankiermaschine umfassenden Abrechnungseinheit eines Datenzentrums sowie eine zur Durchführung des vorstehend genannten Verfahrens geeignete Frankiermaschine.

Früher mußten Frankiermaschinen nach Verbrauch des in der Frankiermaschine gespeicherten Portoguthabens zum Postamt gebracht werden, wo ein Postbeamter den Guthabenspeicher gegen Entrichtung der entsprechenden Gebühren wieder auffüllen konnte. Um dem Benutzer der Frankiermaschine diesen Gang zum Postamt zu ersparen, ist es ferner seit langem bekannt, über eine sogenannte Fernwertvorgabe durch Datenaustausch zwischen einer die Frankiermaschine umfassenden Benutzerstation und einem Datenzentrum das Guthaben in der Frankiermaschine wieder aufzuladen. Dabei muß sichergestellt sein, daß der in der Frankiermaschine nachgeladene Betrag auch im Datenzentrum erfaßt wird, so daß er dem Benutzer der Frankiermaschine berechnet werden kann. Es muß zuverlässig verhindert werden, daß der Benutzer das Portoguthaben in seiner Frankiermaschine unbemerkt vom Datenzentrum auffüllt oder daß der in die Frankiermaschine eingegebene Nachladebetrag von dem dem Datenzentrum übermittelten Betrag verschieden ist.

Aus der US-A-3 792 446 ist ein Fernwertvorgabeverfahren bekannt, bei dem der Datenaustausch zwischen der Benutzerstation und dem Datenzentrum die Übermittlung einer Schlüsselzahl von dem Datenzentrum an die Benutzerstation beinhaltet. Mit dieser Schlüsselzahl kann der Benutzer ein Schloß an der Frankiermaschine für einen einmaligen Nachladevorgang mit einem fest vorgegebenen Nachladebetrag entsperren. Da der Nachladebetrag oder Vorgabebetrag fest vorgegeben ist und nicht geändert werden kann, genügt es für eine Abrechnung, im Datenzentrum die Anzahl der Nachladevorgänge zu erfassen.

Aus den verschiedensten Gründen kann es für den Benutzer der Frankiermaschine vorteilhaft sein, wenn er die Höhe des Nachladebetrages zumindest in gewissen Grenzen von Fall zu Fall selber bestimmen kann. Hierzu wurde in der DE-C-28 20 658 bereits ein Fernwertvorgabeverfahren mit einem variablen Nachladebetrag vorgeschlagen. Die Übereinstimmung des in der Frankiermaschine zu dem Restguthaben hinzuaddierten Nachladebetrags mit dem im Datenzentrum abgerechneten Nachladebetrag wird dabei dadurch sichergestellt, daß der frei wählbare Nachladebetrag in die in der Frankiermaschine und dem Datenzentrum unabhängig voneinander ablaufende Berechnung von Kombinationskennwerten eingeht. Eine Verifizierung des von dem Datenzentrum an die Frankiermaschine übermittelten und den variablen Guthabenwert beinhaltenden Kombinationskennwertes in der Frankiermaschine ist nur dann möglich, wenn sowohl die Frankiermaschine als auch das Datenzentrum mit demselben Nachladebetrag gerechnet haben. Dieser Nachladebetrag wird bei erfolgreicher Verifizierung des übermittelten Kombinationswerts in der Frankiermaschine selbsttätig zu dem Restguthaben im Guthabenspeicher der Frankiermaschine addiert, ohne daß ein weiterer Eingriff in die Nachladeprozedur seitens des Benutzers möglich ist.

Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren der eingangs genannten Art anzugeben, mit dem auf eine für den Benutzer bequeme und noch sicherere Weise eine Abstimmung von Daten zwischen einer Frankiermaschine und einem ihr zugeordneten Datenzentrum erfolgen kann, die das Nachladen der Frankiermaschine auf bequeme Weise ermöglicht.

Diese Aufgabe wird erfindungsgemäß dadurch gelöst, daß an der Frankiermaschine ein Wertänderungsmodus eingestellt wird, daß in einer ersten den Austausch von Codezahlen umfassenden Transaktion zwischen der Frankiermaschine und dem Datenzentrum ein in die Frankiermaschine eingegebener Vorgabewert an das Datenzentrum übermittelt und in einem jeweiligen Vorgabewertspeicher der Frankiermaschine und des Datenzentrums gespeichert wird, daß ein Nachlademodus eingestellt wird und daß in einer zweiten den Austausch von Codezahlen zwischen der Frankiermaschine und dem Datenzentrum umfassenden Transaktion der im jeweiligen Vorgabewertspeicher gespeicherte Vorgabewert zu dem im Guthabenspeicher der Frankiermaschine und dem im Abrechnungsspeicher des Datenzentrums gespeicherten Wert addiert wird.

Die erfindungsgemäße Aufteilung des Verfahrens zum Abstimmen der Abrechnungsdaten in der Frankiermaschine und dem Datenzentrum in zwei in sich abgeschlossene Transaktionen hat eine Reihe von Vorteilen. Zum ersten kann die erste Transaktion entfallen, wenn der Vorgabewert nicht geändert werden soll. In diesem Falle wird das Portoguthaben mit dem im Vorgabewertspeicher gespeicherten Wert wieder aufgefüllt. Dies ergibt ein vereinfachtes Verfahren für den Fall, daß der Benutzer den Vorgabewert gar nicht ändern will. Wünscht der Benutzer jedoch eine Änderung des Vorgabewertes, so kann dieser Wert getrennt von dem Nachladevorgang geändert werden. Dies bietet einerseits die Möglichkeit, zunächst die Änderung des Vorgabewertes abzuschließen und zu überprüfen. Dies erhöht die Sicherheit, daß das Portoguthaben auch tatsächlich mit dem gewünschten Nachladebetrag aufgefüllt wird. Zum anderen besteht die Möglichkeit, eine Benutzerhierarchie für das Ändern des Vorgabewertes und das Nachladen aufzubauen. Beispielsweise kann vorgesehen sein, daß die Angestellten in der Poststelle eines Unternehmens zwar das Fernwertvorgabeverfahren mit einem bestimmten Vorgabebetrag durchführen dürfen, daß dieser Vorgabebetrag aber nur von bestimmten Personen im Unternehmen geändert werden darf. Dies kann z.B. dadurch sichergestellt werden, daß sich die zur Ände-

5 rung des Vorgabewertes berechnete Person durch eine nur ihr bekannte Identitätsnummer oder ein geeignetes
 Paßwort ausweisen muß, das für die Änderung des Vorgabewertes in die Frankiermaschine eingegeben wer-
 den muß. Dieser Identifikationsschritt kann dabei dem eigentlichen Wertänderungsverfahren vorgeschaltet
 werden, indem z.B. der Wertänderungsmodus erst nach dem Identifizierungsschritt eingeleitet werden kann.
 Er kann aber auch in das Wertänderungsverfahren eingebaut werden.

Die erste Transaktion kann beispielsweise so ablaufen, daß eine die Frankiermaschine kennzeichnende
 Identitätsnummer in die Frankiermaschine eingegeben wird und daß während der ersten Transaktion in der
 Frankiermaschine unter Verwendung der Identitätsnummer, des eingegebenen Vorgabewertes und einer Zu-
 10 satzinformation mittels eines Schlüssels eine erste Codezahl gebildet wird, die Identitätsnummer, der ge-
 wünschte Vorgabewert und die Zusatzinformation zusammen mit der ersten Codezahl an das Datenzentrum
 übermittelt werden, die erste Codezahl im Datenzentrum verifiziert und der gewünschte Vorgabewert im Vor-
 gabespeicher des Datenzentrums gespeichert wird, im Datenzentrum unter Verwendung der Identitätsnum-
 mer und der Zusatzinformation mittels eines Schlüssels eine zweite Codezahl gebildet und an die Frankier-
 15 maschine übermittelt wird und die zweite Codezahl in der Frankiermaschine verifiziert wird, worauf bei erfolg-
 reicher Verifizierung der zweiten Codezahl der gewünschte Vorgabewert in dem Vorgabewertspeicher der
 Frankiermaschine gespeichert wird. Das Verfahren kann nach der ersten Transaktion beendet und die Fran-
 kiermaschine in den Frankiermodus überführt werden. Das Verfahren kann aber auch fortgesetzt werden, wo-
 bei während der zweiten Transaktion in der Frankiermaschine unter Verwendung der Identitätsnummer und
 einer Zusatzinformation mittels eines Schlüssels eine dritte Codezahl gebildet und an das Datenzentrum über-
 20 mittelt wird, die dritte Codezahl im Datenzentrum verifiziert und bei erfolgreicher Verifizierung der im Voga-
 bewertspeicher des Datenzentrums gespeicherte Vorgabewert zu dem im Abrechnungsspeicher des Daten-
 zentrums gespeicherten Wert addiert wird, im Datenzentrum unter Verwendung der Identitätsnummer und der
 Zusatzinformation mittels eines Schlüssels eine vierte Codezahl gebildet und an die Frankiermaschine über-
 mittelt wird, und die vierte Codezahl in der Frankiermaschine verifiziert wird, worauf nach erfolgreicher Veri-
 25 fizierung der in dem Vorgabewertspeicher der Frankiermaschine gespeicherte Vorgabewert zu dem im Gut-
 habenspeicher der Frankiermaschine gespeicherten Wert addiert wird. Die zweite Transaktion beinhaltet also
 das eigentliche Nachladeverfahren, das mit einem in der Frankiermaschine fest abgespeicherten Vorgabewert
 erfolgt. Diese zweite Transaktion kann auch jederzeit für sich ohne Änderung des Vorgabewertes ausgeführt
 werden.

Die Sicherheit gegen Manipulationen wird durch die Geheimhaltung der verwendeten Schlüssel sicher-
 gestellt. Zur Verschlüsselung kann jedes bekannte Verschlüsselungsverfahren verwendet werden, beispiels-
 30 weise das DES-Verfahren. Um die Sicherheit zu erhöhen, ist es zweckmäßig, wenn ein zur Ermittlung der Co-
 dezahlen verwendeter Schlüssel nach jeder abgeschlossenen Transaktion geändert wird. Dabei wird zweck-
 mäßigerweise während jeder Transaktion die in der Frankiermaschine gebildete Codezahl mittels eines nach
 Abschluß der vorhergehenden Transaktion vorhandenen Schlüssels berechnet. Die im Datenzentrum gebil-
 35 dete Codezahl wird mittels des gleichen Schlüssels berechnet. Der neue Schlüssel wird der Frankiermaschine
 als Teil der vom Datenzentrum übermittelten Codezahl mitgeteilt und nach Verifizierung dieser Codezahlen
 in der Frankiermaschine für die nächste Transaktion gespeichert. Gleichzeitig wird der neue Schlüssel auch
 im Datenzentrum für die nächste Transaktion gespeichert.

Für den Fall, in dem eine von der Frankiermaschine an das Datenzentrum übermittelte Codezahl im Da-
 40 tenzentrum nicht verifiziert werden kann, hat das Datenzentrum die Möglichkeit, die Verifizierung mittels des
 vor der letzten Schlüsseländerung verwendeten Schlüssels zu wiederholen. Kann die Codezahl mit diesem
 Schlüssel verifiziert werden, ist dies ein Zeichen dafür, daß die vorhergehende Transaktion in der Frankier-
 maschine nicht oder nicht vollständig ausgeführt wurde. Dies gibt somit die Möglichkeit, in der Frankiermaschi-
 45 ne nicht oder nicht vollständig abgeschlossene Transaktionen, die dazu führen, daß die Datenbestände in der
 Frankiermaschine und dem Datenzentrum nicht mehr kongruent sind, zu stornieren, zu wiederholen oder zu
 korrigieren.

Der Datenaustausch zwischen der Frankiermaschine und dem Datenzentrum kann sowohl über Modem
 (im weiteren als ModemVerfahren bezeichnet) als auch über eine fernmündliche Kommunikation zwischen
 50 dem Benutzer der Frankiermaschine und einer Bedienungsperson im Datenzentrum (im weiteren als Voice-
 Verfahren bezeichnet) erfolgen.

In jedem Falle wird die das Datenzentrum zu übermittelnde Information (Registerwerte, Portoauffrurnum-
 mer oder persönliche Identifizierungsnummer etc.) in der Frankiermaschine mittels einer ersten Funktion ver-
 schlüsselt. Hierbei kommt ein gebräuchliches Verschlüsselungsverfahren, vorzugsweise der Data-Encryption-
 55 Standard (DES) zum Einsatz. Nach der Bildung einer verschlüsselten Meldung oder Kryptomeldung mittels
 des DES-Algorithmus wird beim Voice-Verfahren mittels einer zweiten geheimen Funktion eine Code-Zahl ge-
 bildet. Die Ausführung der geheimen ersten Funktion erfordert eine als Schlüssel bezeichnete Geheimnummer
 und eine Programmsequenz (Verschlüsselungs-Code), welche mittels des Schlüssels eine Information ver-

schlüsseln bzw. entschlüsseln kann. Die Ausführung der zweiten geheimen Funktion benötigt hingegen keinen Schlüssel.

Der Datenaustausch erfolgt nun beim Voice-Verfahren mittels der Code-Zahlen in der bereits oben erläuterten Weise. Durch die Bildung der Code-Zahlen ist es möglich, die Anzahl der zu übermittelnden Ziffern im Vergleich zur zunächst gebildeten Krypto-Meldung zu reduzieren. Dies ist zweckmäßig, um die Übermittlung der Informationen zwischen dem Benutzer der Frankiermaschine und der Bedienungsperson im Datenzentrum zu vereinfachen.

Im Gegensatz dazu erfolgt der Datenaustausch beim Modem-Verfahren mittels der Krypto-Meldungen analog zu der oben beschriebenen Verfahrensweise. Da der Datenaustausch beim Modem-Verfahren automatisch erfolgt, können im Vergleich zum Voice-Verfahren wesentlich längere verschlüsselte Meldungen fehlerfrei ausgetauscht werden. Die Bildung von Code-Zahlen kann daher beim Modem-Verfahren unterbleiben.

Dennoch sind beide Verfahren bezüglich des gemeinsamen Datenzentrums kompatibel. Dies ist insbesondere dann wesentlich, wenn die Bedienungsperson im Datenzentrum durch eine automatische Einrichtung ersetzt wird.

Die Erfindung betrifft ferner eine elektronische Frankiermaschine zur Durchführung des vorstehend beschriebenen Verfahrens, umfassend eine elektronische Datenverarbeitungseinrichtung mit einem Guthabenspeicher zum Speichern eines Portoguthabens und einem Vorgabewertspeicher zur Speicherung eines Vorgabewertes, um den das Portoguthaben verändert werden kann, und mit der Datenverarbeitungseinrichtung verbunden eine Druckeinrichtung zum Drucken von Portowerten, eine Datenanzeigeeinrichtung, eine Eingabeeinrichtung zur Eingabe von auszudruckenden Portowerten und eine Einrichtung zum Einstellen eines Guthabennachlademodus, in dem nach Eingabe und Verifizierung einer Nachlade-Schlüsselzahl der im Vorgabewertspeicher gespeicherte Vorgabewert zu dem Portoguthaben addiert wird. Eine Frankiermaschine dieser Art umfaßt erfindungsgemäß ferner eine Einrichtung zur Einstellung eines Wertänderungsmodus, in dem nach Eingabe und Verifizierung einer Wertänderungsschlüsselzahl der Vorgabewert im Vorgabewertspeicher durch einen in die Frankiermaschine eingegebenen geänderten Vorgabewert ersetzbar ist.

Die erfindungsgemäße elektronische Frankiermaschine gibt die Möglichkeit, die Änderung des Vorgabewertes und den Nachladevorgang getrennt voneinander zu behandeln mit den oben geschilderten Vorteilen.

Der Wertänderungsmodus kann beispielsweise durch Eingabe einer die Frankiermaschine kennzeichnenden Identitätsnummer und die Betätigung einer ersten Sondertaste einstellbar sein. Für die Umstellung der Frankiermaschine aus dem Wertänderungsmodus in den Frankiermodus kann eine zweite Sondertaste vorgesehen sein. Ein sich nach Abschluß der Wertänderung oder ohne Wertänderung, d.h. ohne Ausführung der ersten Transaktion unmittelbar an die Einstellung des Wertänderungsmodus anschließender Nachladevorgang wird vorzugsweise durch nochmalige Betätigung der ersten Sondertasten eingeleitet.

Erfindungsgemäß kann die Möglichkeit vorgesehen sein, durch Betätigung mindestens einer an der Frankiermaschine vorgesehenen Wahl Taste nach Eingabe der Identitäts- oder Portoauffruffnummer die Art des Kommunikationsverfahrens zwischen der Frankiermaschine und der Datenzentrale auszuwählen, d.h. die Wahl zu treffen, ob der Wertänderungs- und/oder Nachladevorgang im Voice-Verfahren oder im Modern-Verfahren ausgeführt werden soll.

Hierzu sind zwei Alternativen denkbar. Gemäß einer ersten Variante wird nach der Eingabe der Portoauffruffnummer oder Identitätsnummer eine Wahl- oder Sondertaste gedrückt, um in ein Auswahlmenü zu gelangen, das dem Benutzer der Frankiermaschine in dem Anzeigefeld derselben angezeigt wird. Durch Betätigen eines vorbestimmten Betätigungselementes, beispielsweise einer geeigneten numerischen Taste wechselt die Anzeige und zeigt den derzeit gültigen Vorgabewert an, der dann bestätigt oder verändert werden kann.

Gemäß einer weiteren Variante sind zwei Wahl- oder Sondertasten vorgesehen, durch deren Betätigung direkt das Voice-Verfahren oder das Modem-Verfahren ausgewählt werden kann.

Die Erfindung betrifft ferner ein Verfahren zum gesicherten Speichern von veränderlichen Daten, insbesondere den Daten, die sich während einer Fernwertvorgabe ändern können.

Ein Spannungsausfall kann dazu führen, daß ein Datensatz in einem Speicher fehlerhaft gespeichert wird. Zum Betreiben einer Datenverarbeitungsanlage ist es daher bereits bekannt, einen zweiten Speicher für einen identischen Datensatz und einen Zustandspeicher für eine Zustandskennung vorzusehen, wobei letztere anzeigt, ob der Datensatz aus dem ersten oder dem zweiten Speicher ausgelesen werden soll, wenn die Spannung wiederkehrt.

Fehler in der Zustandskennung können durch redundantes Abspeichern der Zustandskennung unwirksam gemacht werden. Die häufigste Zustandskennung bei einer Majoritätsprüfung muß aber nicht immer die richtige Zustandskennung sein. Es ist lediglich am wahrscheinlichsten, daß die häufigste Zustandskennung auch die richtige ist. Auch eine zusätzliche Plausibilitätsprüfung überprüft nur die Zugehörigkeit zu einem gültigen Wertebereich, liefert aber keine eindeutige Aussage, ob die Zustandskennung richtig ist oder nicht. Mit dem vorstehend beschriebenen Verfahren wird also ein Fehler nicht erkannt, der am häufigsten gespeichert ist und

dabei im gültigen Wertebereich liegt.

Es ist eine weitere Aufgabe der Erfindung, die Sicherheit beim redundanten Abspeichern mit einfachen Mitteln zu erhöhen und ggf. auftretende Fehler zu beseitigen.

Zur Lösung dieser Aufgabe wird vorgeschlagen, daß mittels eines Zeigers ein erster Datensatz als aktueller unveränderlicher Datensatz bestimmt wird, dessen Daten für eine Abfrage zur Verfügung stehen, daß bei einer Änderung von Daten diese Änderung in dem nicht aktuellen zweiten Datensatz erfolgt, daß anschließend mittels des Zeigers der zweite Datensatz zum aktuellen Datensatz bestimmt wird und daß die Daten aus dem aktuellen zweiten Datensatz in den nicht aktuellen ersten Datensatz kopiert werden.

Diese vorstehend beschriebenen Verfahrensschritte werden sowohl beim Initialisieren des Speichers, d.h. beim Einspeichern der Anfangsdaten als auch im laufenden Betrieb ausgeführt. Der aktuelle Datensatz ist stets unveränderlich. Seine Daten sind auch bei einem Spannungsausfall nicht gefährdet, da ein Spannungsausfall in der Regel nur zu Fehlern in laufenden Schreibvorgängen führen kann. Das erfindungsgemäße Verfahren arbeitet unabhängig von der Detektion eines Spannungsausfalles während des Speichervorganges. Ein wesentlicher Schritt des erfindungsgemäßen Verfahrens liegt darin, die Konsistenz der gespeicherten Daten sowie die Gleichheit der in den beiden Datensätzen gespeicherten Daten zu überprüfen und ggf. wieder herzustellen, wie dies weiter unten noch genauer beschrieben wird.

Weitere Merkmale und Vorteile der Erfindung ergeben sich aus den weiteren Unteransprüchen und der folgenden Beschreibung, welche in Verbindung mit den beigefügten Zeichnungen die Erfindung anhand eines Ausführungsbeispiels erläutert. Es zeigen:

- Fig. 1 eine schematische Darstellung einer Frankiermaschine und eines Datenzentrums,
- Fig. 2a und 2b eine schematische Darstellung eines Fernwertvorgabeverfahrens mit Änderung eines Vorgabewertes für das Voice-Verfahren,
- Fig. 3a und 3b eine schematische Darstellung eines Fernwertvorgabeverfahrens mit Änderung eines Vorgabewertes im Modem-Verfahren,
- Fig. 4 die Aufteilung eines Speichers für die gesicherte Speicherung von Daten in Form zweier Datensätze,
- Fig. 5 ein Flußdiagramm zur Erläuterung der Initialisierung der Daten in den beiden Datensätzen,
- Fig. 6 ein Flußdiagramm zur Erläuterung der Speicherung von Daten im laufenden Betrieb und
- Fig. 7 ein Flußdiagramm zur Erläuterung der Prüfung und Korrektur von Daten in den beiden Datensätzen.

In Figur 1 ist mit 10 eine Benutzerstation bezeichnet, die eine Frankiermaschine 12 und eine Telefon 14 umfaßt. Dieses Telefon oder Kommunikationsendgerät, wie z.B. ein Modem, steht über eine Telefonleitung 15 in Verbindung mit einem Telefon oder Kommunikationsendgerät 16 in einem Datenzentrum 18, das ferner eine Abrechnungseinrichtung 20 enthält.

Die Frankiermaschine 12 umfaßt eine allgemein mit 22 bezeichnete Datenverarbeitungseinrichtung mit einer CPU 24, einem Guthabenspeicher 26, einem Vorgabewertspeicher 28 und einer kryptografischen Einrichtung 30, die einen Schlüsselspeicher 32 beinhaltet. Die Datenverarbeitungseinrichtung 22 umfaßt selbstverständlich noch weitere Teile, Speicher und Register, die hier jedoch nicht dargestellt sind, da sie für die Beschreibung des erfindungsgemäßen Verfahrens nicht benötigt werden. In einer vorteilhaften Variante können statt der separaten Einrichtung 30 Software-Mittel bzw. Programmspeichermittel der CPU 24 in Verbindung mit dem nicht flüchtigen Schlüsselspeicher 32 eingesetzt werden, um die Verschlüsselung auszuführen. Im Falle eines automatischen Datenaustausches (Modem-Verfahren) ist die Datenverarbeitungseinrichtung 22 über eine Leitung 23 mit dem Kommunikationsendgerät Modem 14 verbunden, welches dann das Telefon 14 ersetzt. Mit der Datenverarbeitungseinrichtung 22 verbunden ist ferner eine Eingabeeinrichtung 34, beispielsweise eine Tastatur, eine Anzeigeeinrichtung 36 und eine Druckeinrichtung 38.

Die Abrechnungseinrichtung 20 im Datenzentrum 18 umfaßt eine Eingabeeinrichtung 40 sowie eine Datenverarbeitungseinrichtung 42 mit einer CPU 44, einem Vorgabewertspeicher 45, einem Abrechnungsspeicher 46 und einer kryptografischen Einrichtung 48 mit einem Schlüsselspeicher 50. Auch hier kann die Verschlüsselung statt in der Einrichtung 48 in Verbindung mit der CPU 44 und dem nicht flüchtigen Schlüsselspeicher mittels Software erfolgen. Für das Modem-Verfahren ist die Datenverarbeitungseinrichtung 42 über eine Leitung 51 mit dem Modem verbunden, welches in diesem Falle das Telefon 16 ersetzt.

Beim Voice-Verfahren erfolgt der Datenaustausch zwischen der Benutzerstation 10 und dem Datenzentrum 18 über die Telefone 14 und 16 und zwar vorzugsweise durch fernmündlichen Austausch zwischen dem Benutzer der Frankiermaschine 12 und einem Operator im Datenzentrum 18. Die mit dem Ablauf des Fernwertvorgabeverfahrens in der Frankiermaschine und dem Datenzentrum verbundenen wesentlichen Vorgänge sollen nun anhand der Figuren 2a und 2b erläutert werden, die links die Vorgänge in der Benutzerstation oder Frankiermaschine (FM) und rechts die Vorgänge im Datenzentrum (DZ) zeigen.

Das in Figur 2 dargestellte Wertänderungs- und Fernwertvorgabeverfahren beginnt dadurch, daß man in die Eingabeeinrichtung 34 der Frankiermaschine 12 eine Identitätsnummer (PAN) eingibt (S1), die durch eine Sondertaste 52 (Fig. 1) bestätigt wird. In der Anzeige erscheint der im Vorgabewertspeicher 28 gespeicherte Vorgabewert. Für den Fall, daß dieser Wert geändert werden soll, verzweigt das Programm der Datenverarbeitungseinrichtung die der Transaktion "Wertänderung" entsprechenden Routine (S2). Anschließend wird der gewünschte Vorgabewert mittels der Eingabeeinrichtung 34 in die Datenverarbeitungseinrichtung eingegeben und durch Betätigung der Sondertaste 52 bestätigt.

Der Benutzer ruft nun den Operator im Datenzentrum 18 an (S4) und teilt ihm die Identitätsnummer (PAN) mit. Der Operator gibt die Identitätsnummer in die Eingabeeinrichtung 40 der Abrechnungseinrichtung 20 ein, um den Anrufer und die Frankiermaschine 12 der Benutzerstation 10 zu identifizieren. Die Prüfung der Identitätsnummer ist bei S6 dargestellt. Ist die Überprüfung negativ, wird das Verfahren abgebrochen und gegebenenfalls wiederholt. Läßt sich die Frankiermaschine dagegen identifizieren, wird das Verfahren fortgesetzt. Dabei werden dem Operator der Vorgabewunsch des Benutzers sowie gegebenenfalls weitere Informationen über die Frankiermaschine, insbesondere Werte in den Abrechnungsregistern mitgeteilt.

In der Frankiermaschine wird zur Fortsetzung des Verfahrens aus der Identitätsnummer, dem Vorgabewunsch und einer Zusatzinformation, beispielsweise einem weiteren Registerwert mittels eines Schlüssels K1 eine erste Codezahl berechnet (S7), die in der Anzeigeeinrichtung 36 der Frankiermaschine 12 angezeigt und von dem Benutzer dem Operator im Datenzentrum 18 übermittelt wird. Bei Schritt S8 wird diese Codezahl in dem Datenzentrum 18 überprüft mit Hilfe des im Datenzentrum gespeicherten Schlüssels K1. Bei negativem Prüfungsergebnis wird die Prüfung mit dem bei der vorhergehenden Transaktion verwendeten Schlüssel wiederholt. Gelingt die Verifizierung jetzt, bedeutet das, daß die vorhergehende Transaktion in der Frankiermaschine nicht oder nicht vollständig und korrekt ausgeführt wurde. Die vorhergehende Transaktion wird daher storniert und das Verfahren fortgesetzt. Kann die Codezahl auch mit dem vorhergehenden Schlüssel nicht verifiziert werden, wird das Verfahren abgebrochen. Läßt sich dagegen die erste Codezahl erfolgreich verifizieren, wird der Vorgabewert im Speicher 45 des Datenzentrums gespeichert und die Datenverarbeitungseinrichtung 42 im Datenzentrum 18 berechnet eine zweite Codezahl aus der Identitätsnummer, der Zusatzinformation und dem Schlüssel K1. Ferner wird ein zweiter Schlüssel K2 (S9) berechnet. Diese zweite Codezahl, in die der neue Schlüssel K2 integriert ist, wird dem Benutzer mitgeteilt, der sie in die Eingabeeinrichtung 34 der Frankiermaschine eingibt. Die kryptographische Vorrichtung 30 in der Frankiermaschine verifiziert die zweite Codezahl, extrahiert aus der übermittelten zweiten Codezahl den Schlüssel K2 und speichert ihn an Stelle des Schlüssels K1. Bei negativem Ergebnis wird das Verfahren abgebrochen, bei positivem Ergebnis wird der eingegebene Vorgabewunsch im Vorgabewertspeicher 28 gespeichert, wobei der frühere Vorgabewert gelöscht wird (S11).

Damit ist die erste Transaktion beendet und der Vorgabewert geändert. Der Benutzer hat nun die Möglichkeit, das Verfahren zu beenden und durch Betätigung einer weiteren Sondertaste 54 die Frankiermaschine 12 in den Frankiermodus zurückzustellen oder durch nochmalige Betätigung der ersten Sondertaste 52 den Nachladevorgang einzuleiten (S12). Geschieht letzteres, wird in der Frankiermaschine unter Verwendung der Identitätsnummer und der Zusatzinformation mittels des abgespeicherten Schlüssels K2 eine dritte Codezahl berechnet, die dem Datenzentrum mitgeteilt wird (S13). Im Datenzentrum wird die dritte Codezahl verifiziert (S14). Bei negativem Ergebnis wird das Verfahren abgebrochen, bei positivem Ergebnis berechnet das Datenzentrum aus der Identitätsnummer, der Zusatzinformation und dem Schlüssel K2 eine vierte Codezahl (S15), die der Frankiermaschine zusammen mit einem neuen Schlüssel K3 übermittelt wird. In der Frankiermaschine wird wie bei der ersten Transaktion die vierte Codezahl verifiziert (S16) und der neue Schlüssel K3 aus der vierten Codezahl extrahiert und gespeichert, wie dies bei der ersten Transaktion mit dem Schlüssel K2 erfolgte. Im Datenzentrum werden jeweils der alte und der neue Schlüssel gespeichert. Bei negativem Ergebnis wird das Verfahren abgebrochen. Bei positivem Ergebnis wird der im Vorgabewertspeicher 28 der Frankiermaschine gespeicherte Wert zum Restguthaben im Guthabenspeicher 26 der Frankiermaschine und der im Vorgabewertspeicher 45 der Abrechnungseinrichtung 20 gespeicherte Wert zu dem Restguthaben im Abrechnungsspeicher 46 des Datenzentrums 18 addiert (S17). Damit ist auch die zweite Transaktion, das heißt die Fernwertvorgabe mit geändertem Vorgabewert abgeschlossen. Die Frankiermaschine kehrt selbsttätig in den Frankiermodus zurück.

Wenn eine Änderung des Vorgabewertes nicht gewünscht ist, wird durch Betätigung der Sondertaste 52 oder auch einer wahlweise vorgesehenen dritten Sondertaste der im Vorgabewertspeicher 28 gespeicherte Vorgabewert bestätigt und das Verfahren geht von Schritt S2 unmittelbar zu Schritt 4' in Fig. 2b. Der Benutzer ruft das Datenzentrum an und teilt dem Operator die Identitätsnummer (PAN) und gegebenenfalls weitere Informationen mit (S5'). Ist die Identitätsnummer richtig (S6'), läuft das Fernwertvorgabeverfahren dann entsprechend der vorstehenden Beschreibung von Schritt S13 bis Schritt S17 durch.

Es versteht sich, daß der Operator weitere Daten über die Frankiermaschine, insbesondere weitere Re-

gisterstände abfragen kann, um die Korrektheit aller Abrechnungsdaten in der Frankiermaschine und dem Datenzentrum zu überprüfen. Es ist auch möglich, weitere Informationen und weitere Teilschlüssel in die Berechnung der Codezahl einzubeziehen, wenn dies zur Erhöhung der Sicherheit sinnvoll erscheint. Wenn im Datenzentrum im Schritt S14 eine von der Frankiermaschine übermittelte Codezahl überprüft wird, und das Ergebnis negativ ist, wird stets mit dem in der Frankiermaschine bei der unmittelbar vorhergegangenen Transaktion verwendeten Schlüssel die Prüfung nochmals wiederholt. Damit wird ein Fall erfaßt werden, in dem eine Transaktion in der Frankiermaschine nicht korrekt abgeschlossen wurde, ohne daß das Datenzentrum hiervon Kenntnis erhalten hat. In diesem Falle würde der vom Datenzentrum übermittelte neue Schlüssel in der Frankiermaschine nicht abgespeichert und die Frankiermaschine verschlüsselt daher mit dem alten Schlüssel. Dies gibt die Möglichkeit, die letzte Transaktion zu annullieren oder zu korrigieren und damit Schaden für den Benutzer oder das Datenzentrum zu vermeiden.

Das Flußdiagramm gemäß den Figuren 3a und 3b zeigt das Wertänderungs- und Nachladeverfahren für den Fall, daß die Kommunikation zwischen der Frankiermaschine und dem Datenzentrum automatisch über Modem erfolgt. Da die Schritte des Verfahrens im wesentlichen die gleichen sind wie bei dem Verfahren gemäß den Figuren 2a und 2b sind die einzelnen Schritte auch mit den gleichen Bezugsziffern vermehrt um die Zahl 20 versehen.

Wie bei dem anhand der Figuren 2a und 2b beschriebenen Verfahren gibt der Benutzer der Frankiermaschine nach dem Einschalten derselben die Portoauffruffnummer oder Identitätsnummer PAN ein und bestätigt diese Eingabe durch die Betätigung der Sondertaste 52. Es wird nun der abgespeicherte Vorgabewert angezeigt. Entweder bestätigt der Benutzer diesen Wert durch die Betätigung der Sondertaste 52 oder er überschreibt ihn durch einen neuen Vorgabewert, der ebenfalls durch die Betätigung der Sondertaste 52 bestätigt wird. Alle weiteren Schritte laufen nun automatisch ohne Zutun des Benutzers der Frankiermaschine zwischen der Frankiermaschine und dem Datenzentrum ab und zwar in der gleichen Weise, wie dies bei dem anhand der Figuren 2a und 2b beschriebenen Voice-Verfahren erläutert wurde. Der einzige Unterschied besteht darin, daß beim Modem-Verfahren zwischen der Frankiermaschine und dem Datenzentrum nur die Kryptomeldungen, d.h. die verschlüsselten Meldungen und nicht die aus diesen gewonnenen verkürzten Codezahlen ausgetauscht werden.

Anhand der Figuren 4 bis 7 wird nun ein Verfahren zum Speichern von sicherheitsrelevanten Daten insbesondere während der Fernwertvorgabe beschrieben.

Figur 4 zeigt in schematischer Weise die Aufteilung des Speicherplatzes in einem nicht flüchtigen Speicher, beispielsweise einem NVRAM, das in der Frankiermaschine und ggf. auch im Datenzentrum vorhanden ist. Der Speicher muß Platz zum Speichern zweier Datensätze, nämlich Satz 1 und Satz 2 sowie zum Speichern eines Zeigers haben. Jeder Datensatz umfaßt einen variablen Satz "var", der aus beliebig vielen Byte bestehen kann. Ferner umfaßt jeder Datensatz eine Zählervariable "nr Updates, welche die Anzahl von Änderungen des Datensatzes angibt, d.h. bei jeder Änderung oder Erneuerung der Daten eines Satzes um 1 erhöht wird. Schließlich gehört zu einem Datensatz noch eine Prüfsumme "Checksum", die unter Einbeziehung mindestens eines Teils von variablen Daten des Datensatzes ermittelt wird.

Der Zeiger "Act Pointer" kann nur zwei zulässige Werte haben, die angeben, welcher der beiden Datensätze gerade als der aktuelle Datensatz betrachtet wird. Dabei werden nicht die Werte 0 und 1 abgespeichert, da bei diesen Werten kein Bitfehler erkannt werden kann. Vielmehr werden die Werte $0 \times A5$ bzw. $0 \times 5A$ verwendet, wobei $0 \times$ andeutet, daß die Werte hexadezimal notiert sind. Bei dieser in binärer Darstellung symmetrisch aufgebauten Zahl können Bitfehler aus der Zahl selbst heraus erkannt werden.

Das gesamte Verfahren unterteilt sich in drei Schritte:

1. Initialisierung des Speichers für das Speicherverfahren;
2. Abspeichern von Variablen im laufenden Betrieb und
3. Überprüfung der Variablen auf Konsistenz und ggf. Korrektur.

Gemäß Figur 5 umfaßt das Initialisieren des Speichers die folgenden Schritte:

Zunächst wird der Zeiger auf Satz 1 gesetzt (Schritt S50). Das bedeutet, daß der Satz 1 als aktueller Speicher betrachtet wird, dessen Daten unveränderlich sind. Dann werden im Schritt S51 die Variablen des Datensatzes 2 auf ihre Anfangswerte gesetzt. Der Zählwert nr Updates in Datensatz 2 erhält den Wert 0 (S52). Anschließend wird die Prüfsumme unter Verwendung mindestens eines Teiles der variablen Werte des Datensatzes 2 erzeugt und an den hierfür vorgesehenen Platz des Datensatzes 2 abgespeichert (S53, S54). Nun wird der Zeiger auf den zweiten Datensatz gesetzt, d.h. der zweite Datensatz wird zum aktuellen Datensatz bestimmt (S55), auf dessen Daten nun als zuverlässige und unveränderliche Daten zurückgegriffen werden kann. Abschließend wird in Schritt S56 der gesamte Inhalt des Datensatzes 2 in den Datensatz 1 kopiert, so daß beide Datensätze identische Daten enthalten.

Im laufenden Betrieb erfolgt eine Änderung von Daten nur im nicht aktuellen Datensatz. Gemäß Figur 6 wird im laufenden Betrieb zunächst festgestellt, welcher Datensatz der nicht aktuelle Datensatz ist (S60). In

Schritt S61 werden sich ändernde Daten in den nicht aktuellen Datensatz eingeschrieben. Da sich in Schritt S61 die Daten des Datensatzes geändert haben, wird der Zählwert nr updates in Schritt S62 um 1 erhöht. Anschließend wird die Prüfsumme aus Daten des nicht aktuellen Speichers neu gebildet (S63) und im nicht aktuellen Datensatz gespeichert (S64). Nun wird der Zeiger auf den Datensatz gerichtet, in dem soeben die Daten geändert wurden, so daß dieser Satz nun der aktuelle Datensatz ist (S65). Abschließend werden die gesamten Daten des nunmehr aktuellen Datensatzes in den anderen, nicht aktuellen Datensatz kopiert (S66). Beide Datensätze enthalten wiederum die identischen Daten.

Beim Einschalten der Frankiermaschine und vor dem Aufrufen der Fernwertvorgabe muß überprüft werden, ob eine vorangegangene Transaktion beispielsweise durch ein Spannungsabfall unterbrochen wurde und daher Operationen erforderlich sind, um Inkonsistenzen in den abgespeicherten Daten zu beheben.

Für die Prüfung werden folgende Grundvoraussetzungen gemacht:

1. Der Zeiger Act Pointer muß einen zulässigen Wert haben. Wie bereits oben erläutert wurde, sind nur zwei Werte erlaubt, wobei solche Werte gewählt werden, in denen aus dem Wert selbst heraus Bitfehler erkannt werden können.

2. Der aktuelle durch den Zeiger bezeichnete Satz muß eine gültige Prüfsumme haben.

Ist mindestens eine der vorstehend genannten Voraussetzungen nicht erfüllt, so liegt ein fataler Fehler vor und die Frankiermaschine geht in den Service Modus.

Zur Konsistenzprüfung werden folgende Schritte durchgeführt, die anhand der Figur 7 erläutert werden sollen.

Zunächst wird in Schritt S70 geprüft, ob der Wert des Zeigers zulässig ist. In Schritt S71 wird geprüft, ob die Prüfsumme des aktuellen durch den Zeiger bezeichneten Datensatzes gültig ist. Ist einer der beiden Schritte nicht erfüllt, so schaltet die Frankiermaschine, wie oben bereits erwähnt, in den Service Modus.

Haben die Prüfungen in den Schritten S70 und S71 dagegen zu einem positiven Ergebnis geführt, wird in Schritt S72 die Gültigkeit der Prüfsumme des nicht aktuellen Speichers überprüft. Fällt diese Prüfung negativ aus, d.h. ist die Prüfsumme nicht gültig, so ist davon auszugehen, daß die Datenspeicherung oder die Datenspiegelung unterbrochen wurden. Zur Korrektur dieses Fehlers wird die Spiegelung wiederholt, d.h. alle Daten des aktuellen Datensatzes werden in den nicht aktuellen Datensatz kopiert (S73). Hat sich die Prüfsumme dagegen als gültig erwiesen, wird in S74 geprüft, ob die Prüfsummen der beiden Datensätze und damit auch ihre Daten gleich sind. Ist dies der Fall, ist die Prüfung beendet. Sind dagegen beide Prüfsummen zwar gültig, aber ungleich, so ist der Datensicherungsvorgang vor der Spiegelung unterbrochen worden. In diesem Falle wird der Datensatz, dessen Zählwert nr Updates größer ist als der Zählwert des anderen, als aktueller Satz gewählt. Seine Daten werden in den anderen Datensatz kopiert (S75).

Bei einer abgewandelten Ausführungsform kann die Frankiermaschine sowohl für das Voice-Verfahren als auch für das Modemverfahren eingerichtet sein. Mittels einer Wahl taste 58 (Fig. 1) an der Frankiermaschine kann der Benutzer die Art des Kommunikationsverfahrens mit dem Datenzentrum wählen.

Patentansprüche

1. Verfahren zum Abstimmen des Datenbestandes in der einen Guthabenspeicher (26) für ein Portoguthaben umfassenden Datenverarbeitungseinrichtung (22) einer elektronischen Frankiermaschine (12) und der einen Abrechnungsspeicher (46) für die Frankiermaschine umfassenden Abrechnungseinrichtung (42) eines Datenzentrums (18), dadurch **gekennzeichnet**, daß
 - a) an der Frankiermaschine (12) ein Wertänderungsmodus eingestellt wird,
 - b) daß in einer ersten den Austausch von Codezahlen umfassenden Transaktion zwischen der Frankiermaschine (12) und dem Datenzentrum (18) ein in die Frankiermaschine (12) eingegebener Vorgabewert an das Datenzentrum (18) übermittelt und in einem jeweiligen Vorgabewertspeicher (28; 45) der Frankiermaschine (12) und des Datenzentrums (18) gespeichert wird,
 - c) daß ein Nachlademodus eingestellt wird und
 - d) daß in einer zweiten den Austausch von Codezahlen zwischen der Frankiermaschine (12) und dem Datenzentrum (18) umfassenden Transaktion der im jeweiligen Vorgabewertspeicher (28) gespeicherte Vorgabewert zu dem im Guthabenspeicher (26) der Frankiermaschine (12) und dem im Abrechnungsspeicher (46) des Datenzentrums gespeicherten Wert addiert wird.
2. Verfahren zum Abstimmen des Datenbestandes in der einen Guthabenspeicher (26) für ein Portoguthaben umfassenden Datenverarbeitungseinrichtung (22) einer elektronischen Frankiermaschine (12) und der einen Abrechnungsspeicher (46) für die Frankiermaschine umfassenden Abrechnungseinrichtung (42) eines Datenzentrums (18), dadurch **gekennzeichnet**, daß

- a) an der Frankiermaschine (12) ein Wertänderungsmodus eingestellt wird,
 b) daß in einer ersten den Austausch von verschlüsselten Meldungen (Krypto-Meldungen) umfassenden Transaktion zwischen der Frankiermaschine (12) und dem Datenzentrum (18) ein in die Frankiermaschine (12) eingegebener Vorgabewert an das Datenzentrum (18) übermittelt und in einem jeweiligen Vorgabewertspeicher (28; 45) der Frankiermaschine (12) und des Datenzentrums (18) gespeichert wird,
 c) daß ein Nachlademodus eingestellt wird und
 d) daß in einer zweiten den Austausch von Krypto-Meldungen zwischen der Frankiermaschine (12) und dem Datenzentrum (18) umfassenden Transaktion der im jeweiligen Vorgabewertspeicher (28) gespeicherte Vorgabewert zu dem im Guthabenspeicher (26) der Frankiermaschine (12) und dem im Abrechnungsspeicher (46) des Datenzentrums gespeicherten Wert addiert wird.
3. Verfahren nach Anspruch 1 oder 2, dadurch **gekennzeichnet**, daß eine die Frankiermaschine (12) kennzeichnende Identitätsnummer in die Frankiermaschine (12) eingegeben wird und daß während der ersten Transaktion in der Frankiermaschine (12) unter Verwendung der Identitätsnummer, des eingegebenen Vorgabewertes und einer Zusatzinformation mittels eines Schlüssels (K1) eine erste Codezahl gebildet wird, die Identitätsnummer, der gewünschte Vorgabewert und die Zusatzinformation zusammen mit der ersten Codezahl an das Datenzentrum (18) übermittelt werden, die erste Codezahl im Datenzentrum (18) verifiziert und der gewünschte Vorgabewert im Vorgabewertspeicher des Datenzentrums (18) gespeichert wird, im Datenzentrum (18) unter Verwendung der Identitätsnummer und der Zusatzinformation mittels eines Schlüssels (K2) eine zweite Codezahl gebildet und an die Frankiermaschine (12) übermittelt wird und die zweite Codezahl in der Frankiermaschine (12) verifiziert wird, worauf bei erfolgreicher Verifizierung der zweiten Codezahl der gewünschte Vorgabewert in dem Vorgabewertspeicher (28) der Frankiermaschine (12) gespeichert wird.
4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch **gekennzeichnet**, daß während der zweiten Transaktion in der Frankiermaschine (12) unter Verwendung der Identitätsnummer und einer Zusatzinformation mittels eines Schlüssels (K2) eine dritte Codezahl gebildet und an das Datenzentrum übermittelt wird, die dritte Codezahl im Datenzentrum (18) verifiziert wird und bei erfolgreicher Verifizierung der im Vorgabewertspeicher (45) des Datenzentrums (18) gespeicherte Vorgabewert zu dem im Abrechnungsspeicher (46) des Datenzentrums (18) gespeicherten Wert addiert wird, im Datenzentrum (18) unter Verwendung der Identitätsnummer und der Zusatzinformation mittels eines Schlüssels (K3) eine vierte Codezahl gebildet und an die Frankiermaschine (12) übermittelt wird, und die vierte Codezahl in der Frankiermaschine verifiziert wird, worauf nach erfolgreicher Verifizierung der in dem Vorgabewertspeicher (28) der Frankiermaschine gespeicherte Vorgabewert zu dem im Guthabenspeicher (26) der Frankiermaschine (12) gespeicherten Wert addiert wird.
5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch **gekennzeichnet**, daß ein zur Ermittlung der Codezahlen verwendeter Schlüssel nach jeder abgeschlossenen Transaktion geändert wird.
6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch **gekennzeichnet**, daß während jeder Transaktion die in der Frankiermaschine (12) gebildete Codezahl mittels eines nach Abschluß der vorhergehenden Transaktion vorhandenen Schlüssels (K1) berechnet wird, daß die im Datenzentrum gebildete Codezahl mittels des gleichen Schlüssels (K2) berechnet wird, und daß der neue Schlüssel (K2) im Datenzentrum gespeichert, der Frankiermaschine als Teil der vom Datenzentrum (18) übermittelten Codezahl mitgeteilt und nach Verifizierung dieser Codezahl in der Frankiermaschine (12) gespeichert wird.
7. Verfahren nach Anspruch 6, dadurch **gekennzeichnet**, daß in dem Fall, in dem eine von der Frankiermaschine (12) an das Datenzentrum (18) übermittelte Codezahl im Datenzentrum (18) nicht verifiziert werden kann, die Verifizierung mittels des vor der letzten Schlüsseländerung verwendeten Schlüssels (K1) wiederholt wird, und daß bei erfolgreicher Verifizierung der Codezahl mit diesem Schlüssel (K1) die letzte Transaktion korrigiert wird.
8. Verfahren nach einem der Ansprüche 3 bis 7, dadurch **gekennzeichnet**, daß nach Eingabe der Identitätsnummer die Art des Kommunikationsverfahrens zwischen der Frankiermaschine und der Datenzentrale durch die Betätigung mindestens einer Wahltaaste (58) ausgewählt wird.
9. Elektronische Frankiermaschine, umfassend eine elektronische Datenverarbeitungseinrichtung (22) mit einem Guthabenspeicher (26) zum Speichern eines Portoguthabens und einem Vorgabewertspeicher

- (28) zur Speicherung eines Vorgabewertes, um den das Portoguthaben verändert werden kann, und mit der Datenverarbeitungseinrichtung (22) verbunden eine Druckeinrichtung (38) zum Drucken von Portowerten, eine Datenanzeigeeinrichtung (36), eine Eingabeeinrichtung (34) zur Eingabe von auszudruckenden Portowerten und eine Einrichtung zum Einstellen eines Guthabennachlademodus, in dem nach Eingabe und Verifizierung einer Nachladeschlüsselzahl der im Vorgabewertspeicher (28) gespeicherte Vorgabewert zu dem Portoguthaben addiert wird, **gekennzeichnet** durch Mittel (52) zur Einstellung eines Wertänderungsmodus, in dem nach Eingabe und Verifizierung einer Wertänderungsschlüsselzahl der Vorgabewert im Vorgabewertspeicher (28) durch einen in die Frankiermaschine (12) eingegebenen geänderten Vorgabewert ersetzbar ist.
- 10 **10.** Frankiermaschine nach Anspruch 9, dadurch **gekennzeichnet**, daß die Datenverarbeitungseinrichtung (22) eine kryptographische Einrichtung (30) zur Erzeugung und/oder Verifizierung von Schlüsselzahlen hat.
- 15 **11.** Frankiermaschine nach Anspruch 10, dadurch **gekennzeichnet**, daß die kryptographische Einrichtung (30) einen Speicher (32) für mindestens einen Schlüssel (K1, K2...) hat.
- 20 **12.** Frankiermaschine nach einem der Ansprüche 9 bis 11, dadurch **gekennzeichnet**, daß der Wertänderungsmodus durch Eingabe einer die Frankiermaschine (12) kennzeichnenden Identitätsnummer und die Betätigung einer ersten Sondertaste (52) einstellbar ist.
- 13.** Frankiermaschine nach einem der Ansprüche 9 bis 12, dadurch **gekennzeichnet**, daß sie durch Betätigung einer zweiten Sondertaste (54) aus dem Wertänderungsmodus in einen Frankiermodus umstellbar ist.
- 25 **14.** Frankiermaschine nach einem der Ansprüche 9 bis 13, dadurch **gekennzeichnet**, daß der Nachlademodus nach Einstellen des Wertänderungsmodus durch Betätigung einer dritten Sondertaste (56) einstellbar ist.
- 30 **15.** Frankiermaschine nach einem der Ansprüche 9 bis 13, dadurch **gekennzeichnet**, daß der Nachlademodus nach Einstellen des Wertänderungsmodus durch Betätigung der ersten Sondertaste (52) einstellbar ist.
- 35 **16.** Frankiermaschine nach einem der Ansprüche 9 bis 15, **gekennzeichnet** durch mindestens eine Wahl taste (58) zur Auswahl des Kommunikationsverfahrens zwischen der Frankiermaschine und dem Datenzentrum.
- 40 **17.** Datenzentrum (18) umfassend eine Kommunikationseinrichtung (16) zum Datenaustausch mit mindestens einer Benutzerstation (10), die mindestens eine Frankiermaschine (12) hat, und eine Datenverarbeitungseinrichtung (20) mit einer Dateneingabeeinheit (40), einer Recheneinheit (44) und einem Abrechnungsspeicher für jede Frankiermaschine (46), in dem die in der Frankiermaschine (12) geladenen Guthabenbeträge über einen vorgegebenen Zeitraum aufsummiert werden, **gekennzeichnet** durch einen Vorgabewertspeicher (45) für jede Frankiermaschine (12) zur Speicherung eines der Frankiermaschine (12) zugeordneten Vorgabewertes (VGW), um den ein in der Frankiermaschine (12) gespeicherter Guthabenwert geändert werden soll, wobei die Datenverarbeitungseinrichtung (20) so programmierbar ist, daß sie entsprechend ersten von der Benutzerstation (10) über die Kommunikationseinrichtung (16) erhaltenen Daten den Vorgabewert im Vorgabewertspeicher (45) ändert und daß sie entsprechend zweiten von der Benutzerstation (10) über die Kommunikationseinrichtung (16) erhaltenen Daten den im Vorgabewertspeicher (45) gespeicherten Wert zu dem im Abrechnungsspeicher (46) gespeicherten Wert addiert.
- 45 **18.** Datenzentrum nach Anspruch 17, dadurch **gekennzeichnet**, daß die Kommunikationseinrichtung ein Modem umfaßt, das mit einem Modem der Benutzerstation (10) verbindbar ist.
- 50 **19.** Datenzentrum nach Anspruch 17, dadurch **gekennzeichnet**, daß die Kommunikationseinrichtung einen Fernsprechapparat (16) umfaßt, der mit einem Fernsprechapparat (14) der Benutzerstation (10) verbindbar ist.
- 55 **20.** Datenzentrum nach einem der Ansprüche 17 bis 19, dadurch **gekennzeichnet**, daß es eine kryptograp-

hische Einrichtung (48) zur Erzeugung und/oder Verifizierung von Schlüsselzahlen hat.

21. Datenzentrum nach Anspruch 20, dadurch **gekennzeichnet**, daß die kryptographische Einrichtung eine Einheit (50) zur Erzeugung und Speicherung von Schlüsseln hat.

5

22. Verfahren zum gesicherten Speichern von veränderlichen Daten durch Erzeugen und Speichern zweier übereinstimmender Datensätze, dadurch **gekennzeichnet**, daß mittels eines Zeigers ein erster Datensatz als aktueller unveränderlicher Datensatz bestimmt wird, dessen Daten für eine Abfrage zur Verfügung stehen, daß bei einer Änderung von Daten diese Änderung in dem nicht aktuellen zweiten Datensatz erfolgt, daß anschließend mittels des Zeigers der zweite Datensatz zum aktuellen Datensatz bestimmt wird und daß die Daten aus dem aktuellen zweiten Datensatz in den nicht aktuellen ersten Datensatz kopiert werden.

10

23. Verfahren nach Anspruch 22, dadurch **gekennzeichnet**, daß eine Variable der veränderlichen Daten jedes Datensatzes ein für die Anzahl der vorgenommenen Änderungen repräsentativer Zählwert ist.

15

24. Verfahren nach Anspruch 22 oder 23, dadurch **gekennzeichnet**, daß eine Variable der veränderlichen Daten jedes Datensatzes eine aus mindestens einem Teil der veränderlichen Daten errechnete Prüfsumme ist.

20

25. Verfahren nach einem der Ansprüche 22 bis 24, dadurch **gekennzeichnet**, daß der Wert des Zeigers auf Konsistenz und ausgewählte Daten der Datensätze auf Konsistenz und Gleichheit geprüft und gegebenenfalls korrigiert werden.

25

30

35

40

45

50

55

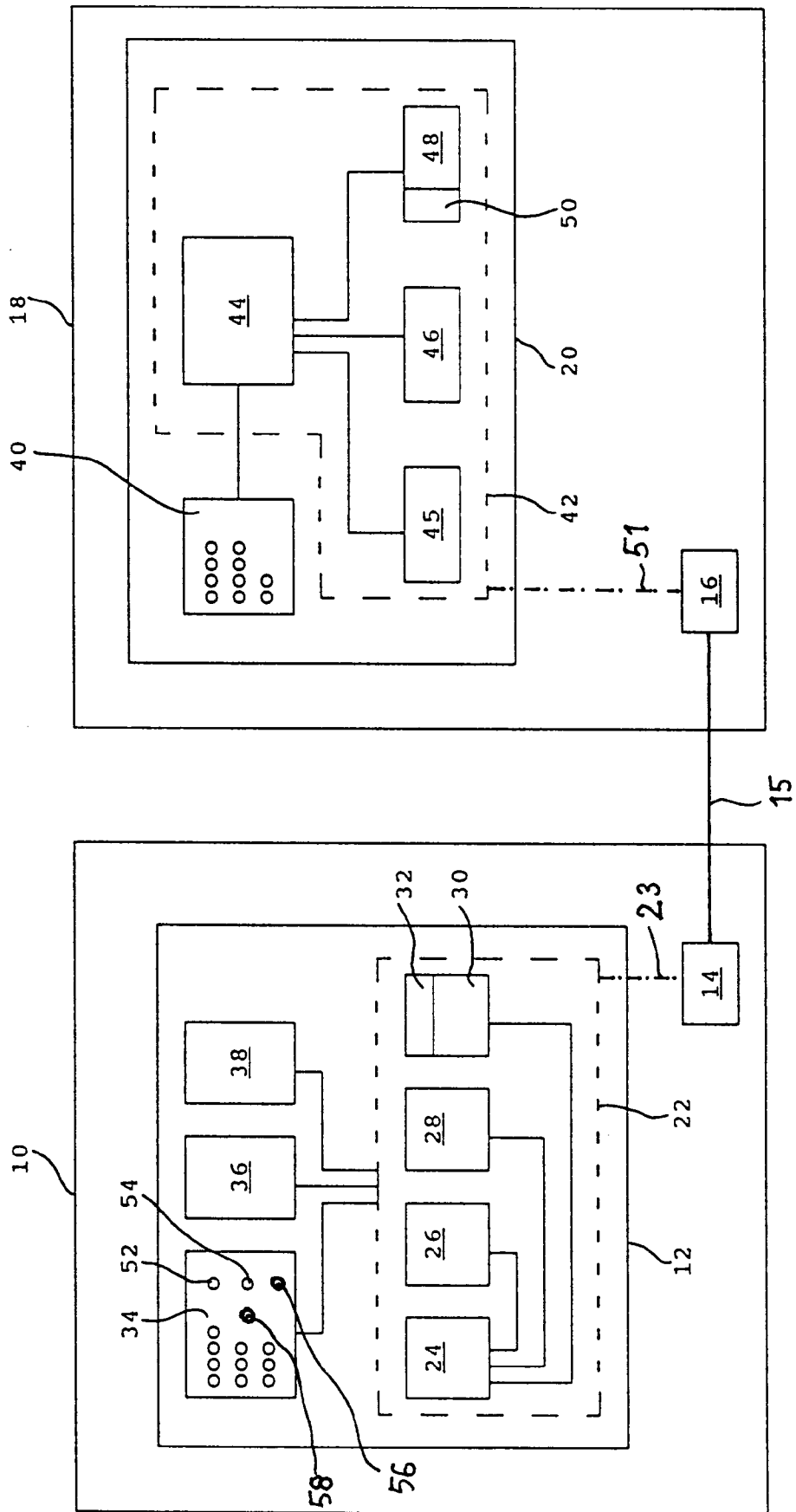


Fig. 1

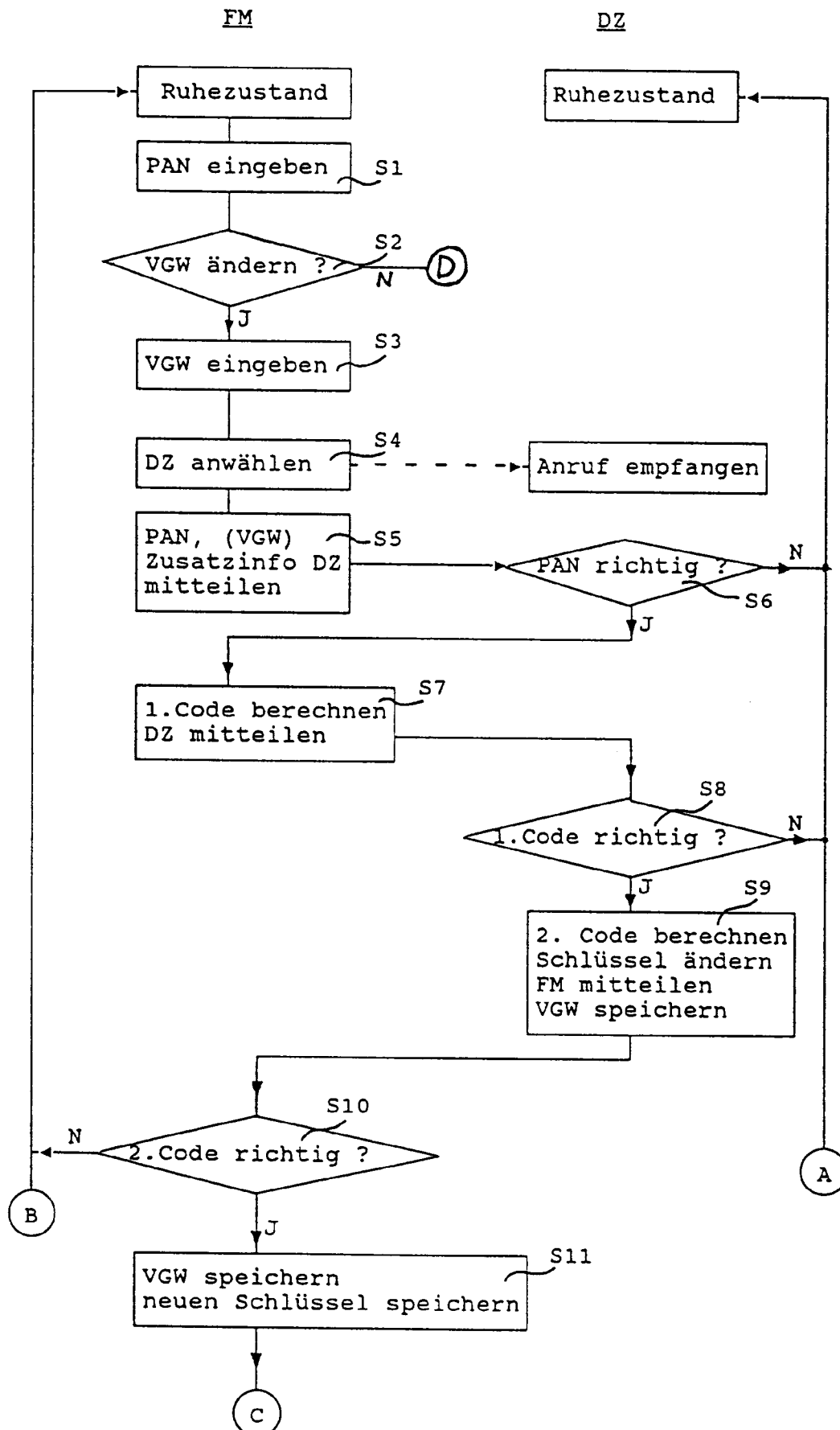


Fig. 2a

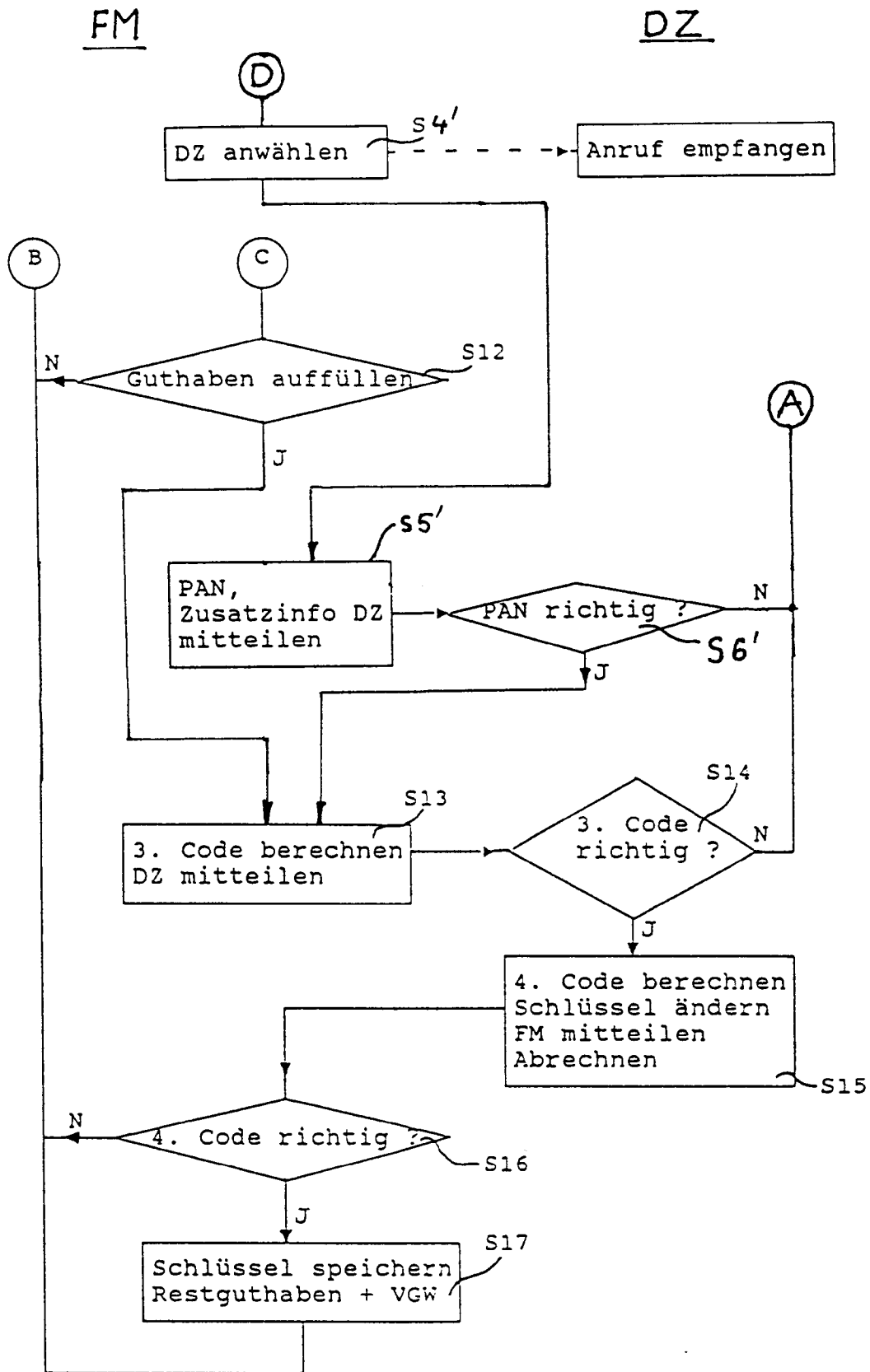


Fig. 2b

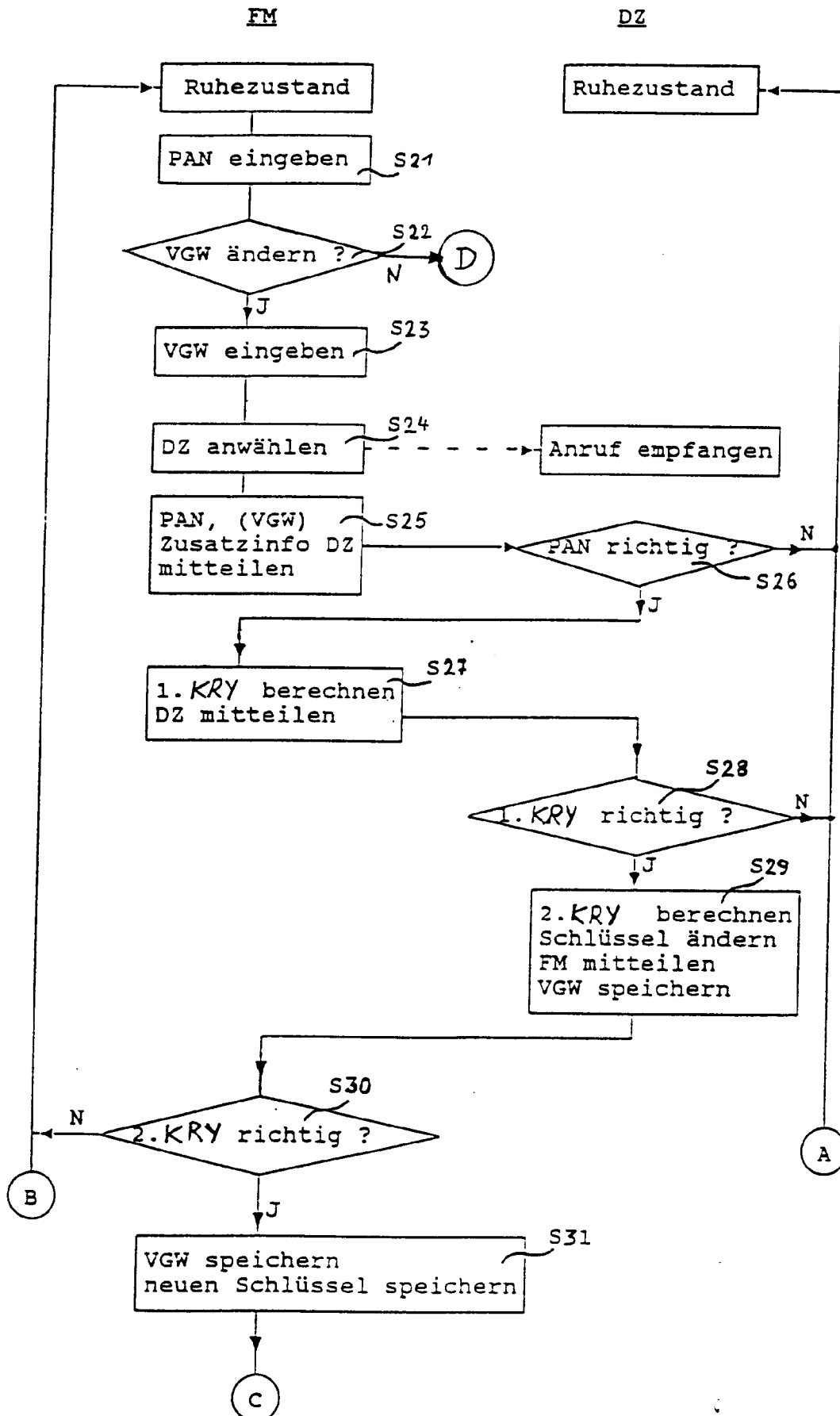


Fig. 3a

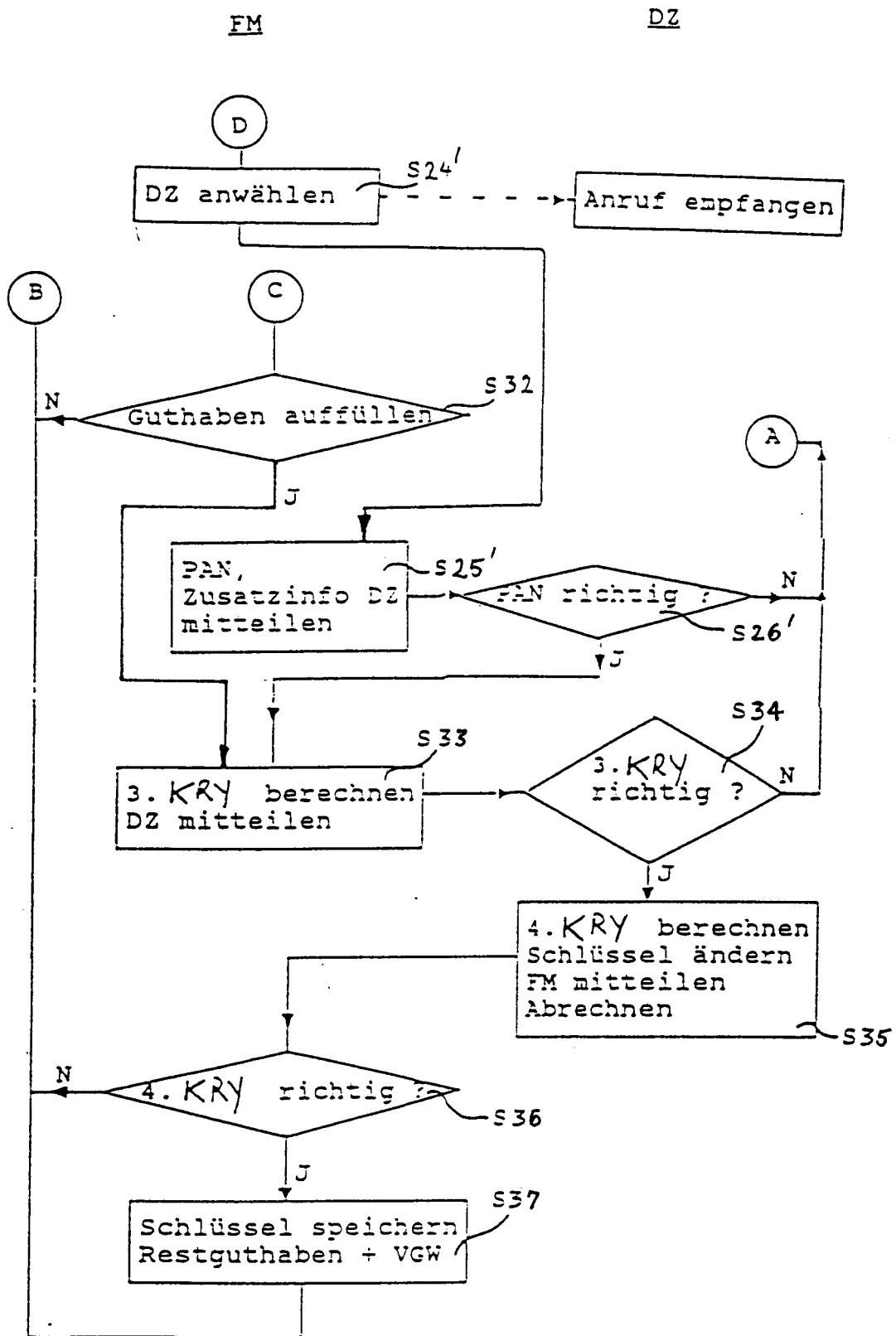


Fig. 3b

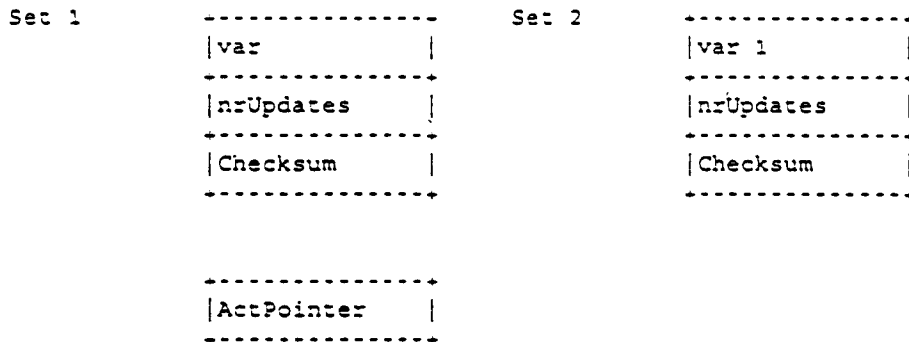
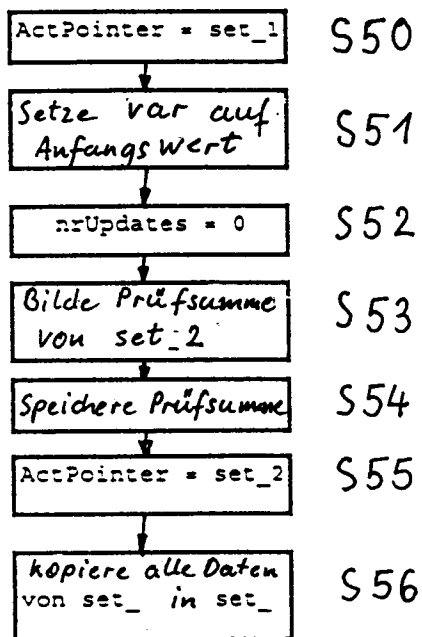
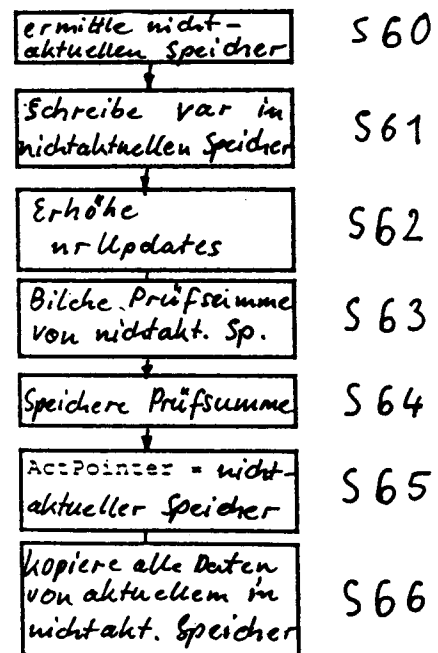
Fig. 4Fig. 5Fig. 6

Fig 7