



Europäisches Patentamt  
European Patent Office  
Office européen des brevets



(11) **EP 0 689 170 B1**

(12) **EUROPÄISCHE PATENTSCHRIFT**

(45) Veröffentlichungstag und Bekanntmachung des Hinweises auf die Patenterteilung:  
**14.12.2005 Patentblatt 2005/50**

(51) Int Cl.7: **G07B 17/02**

(21) Anmeldenummer: **95109864.9**

(22) Anmeldetag: **23.06.1995**

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

Method for adapting the datafile between an electronic franking machine and a data center

Procédé d'adaption du fichier de données entre une machine à affranchir et un centre de données

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

(30) Priorität: **24.06.1994 DE 4422263**

(43) Veröffentlichungstag der Anmeldung:  
**27.12.1995 Patentblatt 1995/52**

(60) Teilanmeldung:  
**99100885.5 / 0 915 435**

(73) Patentinhaber: **Francotyp-Postalia GmbH**  
**16547 Birkenwerder (DE)**

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

(74) Vertreter:  
**Schaumburg, Thoenes, Thurn, Landskron**  
**Patentanwälte**  
**Postfach 86 07 48**  
**81634 München (DE)**

(56) Entgegenhaltungen:  
**EP-A- 0 376 573**                      **EP-A- 0 442 761**  
**EP-A- 0 550 226**                      **GB-A- 2 080 203**  
**GB-A- 2 188 870**                      **US-A- 4 097 923**

**EP 0 689 170 B1**

Anmerkung: Innerhalb von neun Monaten nach der Bekanntmachung des Hinweises auf die Erteilung des europäischen Patents kann jedermann beim Europäischen Patentamt gegen das erteilte europäische Patent Einspruch einlegen. Der Einspruch ist schriftlich einzureichen und zu begründen. Er gilt erst als eingelegt, wenn die Einspruchsgebühr entrichtet worden ist. (Art. 99(1) Europäisches Patentübereinkommen).

## Beschreibung

**[0001]** 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.

**[0002]** 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 der 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.

**[0003]** 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.

**[0004]** Ein in der EP-A-0 376 573 beschriebenes Nachladeverfahren umfaßt einen "Resetting Mode" und einen "Unlock Mode". Im Resetting Mode wird dem Datenzentrum von der Frankiermaschine ein Nachladewunsch übermittelt. Das Datenzentrum sperrt hierauf die Frankiermaschine für den weiteren Betrieb, fragt die Registerstände ab und prüft die übermittelten Daten anhand der im Datenzentrum für den jeweiligen Benutzer und die betreffende Frankiermaschine gespeicherten Daten. Der Datenaustausch erfolgt in gesicherter Form. Fällt die Prüfung positiv aus, übermittelt das Datenzentrum an die Frankiermaschine den Nachladebetrag. An dieser Stelle hat der Benutzer die Möglichkeit, den Nachladevorgang zu unterbrechen, indem er den Nachladebetrag annimmt oder nicht. Nimmt er den Gutha-

benbetrag nicht an, kehrt das Programm zu dem Start der Wiederaufladeprozedur zurück, das heißt der Benutzer befindet sich also wieder am Anfang des gesamten Nachladevorgangs. Nimmt er den Nachladebetrag an, wird dieser zu dem Guthaben im Guthabenregister hinzuaddiert. Nach dem Aufladen des Guthabenregisters kann der Benutzer die Frankiermaschine noch nicht benutzen. Er muß in einem zweiten Verfahrensschnitt die Maschine entsperren lassen, wozu der Benutzer eine eigene Anfrage an das Datenzentrum richten muß.

**[0005]** 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 Kombinationswertes 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 Kombinationswertes 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.

**[0006]** 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.

**[0007]** Diese Aufgabe wird erfindungsgemäß durch die im Anspruch 1 angegebenen Merkmale gelöst.

**[0008]** 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 einer-

seits 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 Änderung 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 werden muß. Dieser Identifikations-schritt kann dabei dem eigentlichen Wertänderungsverfahren vorschaltet werden, indem z.B. der Wertänderungsmodus erst nach dem Identifizierungsschritt eingeleitet werden kann. Er kann aber auch in das Wertänderungsverfahren eingebaut werden.

**[0009]** Die erste Transaktion kann beispielsweise so ablaufen, wie es in Anspruch 3 beschrieben ist. Das Verfahren kann nach der ersten Transaktion beendet und die Frankiermaschine in den Frankiermodus überführt werden. Das Verfahren kann aber auch fortgesetzt werden, wie es in Anspruch 4 beschrieben ist. 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.

**[0010]** Die Sicherheit gegen Manipulationen wird durch die Geheimhaltung der verwendeten Schlüssel sichergestellt. Zur Verschlüsselung kann jedes bekannte Verschlüsselungsverfahren verwendet werden, beispielsweise das DES-Verfahren. Um die Sicherheit zu erhöhen, ist es zweckmäßig, wenn ein zur Ermittlung der Codezahlen verwendeter Schlüssel nach jeder abgeschlossenen Transaktion geändert wird. Dabei wird zweckmäßigerweise während jeder Transaktion die in der Frankiermaschine gebildete Codezahl mittels eines nach Abschluß der vorhergehenden Transaktion vorhandenen Schlüssels berechnet. Die im Datenzentrum gebildete 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.

**[0011]** Für den Fall, in dem eine von der Frankiermaschine an das Datenzentrum übermittelte Codezahl im Datenzentrum 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 Frankiermaschine nicht oder nicht vollständig ausgeführt wurde. Dies gibt somit die Möglichkeit, in der Frankiermaschine 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.

**[0012]** Der Datenaustausch zwischen der Frankiermaschine und dem Datenzentrum kann sowohl über Modem (im weiteren als Modem-Verfahren bezeichnet) als auch über eine fernmündliche Kommunikation zwischen dem Benutzer der Frankiermaschine und einer Bedienungsperson im Datenzentrum (im weiteren als Voice-Verfahren bezeichnet) erfolgen.

**[0013]** In jedem Falle wird die das Datenzentrum zu übermittelnde Information (Registerwerte, Portoauffnummer oder persönliche Identifizierungsnummer etc.) in der Frankiermaschine mittels einer ersten Funktion verschlüsselt. Hierbei kommt ein gebräuchliches Verschlüsselungsverfahren, vorzugsweise der Data-Encryption-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 gebildet. Die Ausführung der geheimen ersten Funktion erfordert eine als Schlüssel bezeichnete Geheimnummer und eine Programmsequenz (Verschlüsselungs-Code), welche mittels des Schlüssels eine Information verschlüsseln bzw. entschlüsseln kann. Die Ausführung der zweiten geheimen Funktion benötigt hingegen keinen Schlüssel.

**[0014]** 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.

**[0015]** 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.

**[0016]** 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.

**[0017]** Die Erfindung betrifft ferner eine elektronische Frankiermaschine gemäß Anspruch 9.

**[0018]** Die erfindungsgemäße elektronische Frankiermaschine gibt die Möglichkeit, die Änderung des Vorgabewertes und den Nachladevorgang getrennt voneinander zu behandeln mit den oben geschilderten Vorteilen.

**[0019]** 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.

**[0020]** Es 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 Modem-Verfahren ausgeführt werden soll.

**[0021]** 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 Auswahlnü 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.

**[0022]** Gemäß einer weiteren Variante sind zwei Wahl- oder Sondertasten vorgesehen, durch deren Betätigung direkt das Voice-Verfahren oder das Modem-Verfahren ausgewählt werden kann.

**[0023]** Die folgende Beschreibung erläutert in Verbindung mit den beigefügten Zeichnungen die Erfindung anhand eines Ausführungsbeispiels. 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 Mo-

dem-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.

**[0024]** In Figur 1 ist mit 10 eine Benutzerstation bezeichnet, die eine Frankiermaschine 12 und ein 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.

**[0025]** 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.

**[0026]** 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 die-

sem Falle das Telefon 16 ersetzt.

**[0027]** 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.

**[0028]** 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.

**[0029]** 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.

**[0030]** 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 Code-

zahl 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).

**[0031]** 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.

**[0032]** 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.

**[0033]** Es versteht sich, daß der Operator weitere Daten über die Frankiermaschine, insbesondere weitere Registerstände 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.

**[0034]** 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.

**[0035]** 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 Unter-

schied besteht darin, daß beim Modem-Verfahren zwischen der Frankiermaschine und dem Datenzentrum nur die Krypto-Meldungen, d.h. die verschlüsselten Meldungen und nicht die aus diesen gewonnenen verkürzten Codezahlen ausgetauscht werden.

**[0036]** Anhand der Figuren 4 bis 7 wird nun ein Verfahren zum Speichern von sicherheitsrelevanten Daten insbesondere während der Fernwertvorgabe beschrieben.

**[0037]** 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 Zählvariable "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.

**[0038]** 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.

**[0039]** 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.

**[0040]** Gemäß Figur 5 umfaßt das Initialisieren des Speichers die folgenden Schritte:

**[0041]** 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.

**[0042]** 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.

**[0043]** 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.

**[0044]** 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.

**[0045]** Ist mindestens eine der vorstehend genannten Voraussetzungen nicht erfüllt, so liegt ein fataler Fehler vor und die Frankiermaschine geht in den Service Modus.

**[0046]** Zur Konsistenzprüfung werden folgende Schritte durchgeführt, die anhand der Figur 7 erläutert werden sollen.

**[0047]** 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.

**[0048]** 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).

**[0049]** Bei einer abgewandelten Ausführungsform kann die Frankiermaschine sowohl für das Voice-Verfahren als auch für das Modem-verfahren 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), wobei die Abstimmung des Datenbestandes in zwei in sich abgeschlossenen Transaktionen zum festen Abspeichern eines gültigen Vorgabewertes bzw. zum Nachladen mit dem abgespeicherten gültigen Vorgabewert erfolgt, wobei in einer ersten Transaktion an der Frankiermaschine (12) ein Wertänderungsmodus eingestellt wird, bei welchem der gespeicherte Vorgabewert wahlweise ungeändert bestätigt und die Transaktion ohne Ausführung einer Wertänderung abgeschlossen wird oder zur Änderung eines in der Frankiermaschine gespeicherten und angezeigten Vorgabewertes unter Austausch von verschlüsselten Meldungen bzw. Kryptomeldungen zwischen der Frankiermaschine (12) und dem Datenzentrum (18) ein in die Frankiermaschine eingegebener neuer Vorgabewert an das Datenzentrum (18) übermittelt und in einem jeweiligen Vorgabewertspeicher (28, 45) der Frankiermaschine (12) und des Datenzentrums (18) gespeichert wird, und dass nach Abschluss der ersten Transaktion wahlweise ein Frankiermodus oder ein Nach-

lademodus eingestellt wird, indem in einer zweiten den Austausch von Kryptomeldungen 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 nach Anspruch 1, **dadurch gekennzeichnet, dass** aus der jeweiligen Kryptomeldung vor ihrer Übermittlung eine verkürzte Codezahl gebildet und diese übermittelt wird.

3. Verfahren nach Anspruch 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 (45) 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 2 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 2 bis 4, **dadurch gekennzeichnet, dass** ein zur Ermittlung der Codezahlen verwendeter Schlüssel nach jeder abgeschlossenen Transaktion geändert wird.

6. Verfahren nach einem der Ansprüche 2 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 Wahl Taste (58) ausgewählt wird.

9. Elektronische Frankiermaschine, umfassend eine elektronische Datenverarbeitungseinrichtung (22) mit einem Guthabenspeicher (26) zum Speichern eines Portoguthabens und einem Vorgabewertspeicher (28) zur festen Abspeicherung 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 Wertände-

rungsmodus, in welchem der im Vorgabewertspeicher (28) fest abgespeicherte und in der Datenanzeigeeinrichtung (36) angezeigte Vorgabewert wahlweise ungeändert bestätigt oder in einer in sich abgeschlossenen Transaktion nach Eingabe und Verifizierung einer Wertänderungsschlüsselzahl **durch** einen in die Frankiermaschine (12) eingegebenen geänderten Vorgabewert ersetzbar ist.

10. Frankiermaschine nach Anspruch 9, **dadurch gekennzeichnet, dass** die Datenverarbeitungseinrichtung (22) eine kryptographische Einrichtung (30) zur Erzeugung und/oder Verifizierung von Schlüsselzahlen hat.

11. Frankiermaschine nach Anspruch 10, **dadurch gekennzeichnet, dass** die kryptographische Einrichtung (30) einen Speicher (32) für mindestens einen Schlüssel (K1, K2...) hat.

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.

14. Frankiermaschine nach einem der Ansprüche 9 bis 13, **dadurch gekennzeichnet, dass** der Nachlade-modus nach Einstellen des Wertänderungsmodus durch Betätigung einer dritten Sondertaste (56) einstellbar ist.

15. Frankiermaschine nach einem der Ansprüche 9 bis 13, **dadurch gekennzeichnet, dass** der Nachlade-modus nach Einstellen des Wertänderungsmodus durch Betätigung der ersten Sondertaste (52) einstellbar ist.

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.

## Claims

1. A method for matching the data base in the data processing device (22) of an electronic postage meter machine (12), containing a credit memory (26) for a postage credit, and the debiting unit (42) of a

data centre (18), comprising a debiting memory (46) for the postage meter machine, wherein the matching of the data base takes place in two self-contained transactions for the permanent storing of a valid selected amount or, respectively, for reloading with the stored valid selected amount, wherein in a first transaction a change of value mode is set on the postage meter machine (12), in which the stored selected amount is optionally confirmed unmodified and the transaction is terminated without implementing a change of value or, for modifying a selected amount stored and displayed in the postage meter machine by exchanging encrypted messages or, respectively, cryptomessages between the postage meter machine (12) and the data centre (18) a new selected amount entered in the postage meter machine is communicated to the data centre (18) and is stored in a respective selected amount memory (28, 45) of the postage meter machine (12) and of the data centre (18), and that after termination of the first transaction optionally a franking mode or a reloading mode is set by adding in a second transaction comprising the exchange of cryptomessages between the postage meter machine (12) and the data centre (18) the selected amount stored in the respective selected amount memory (28) to the value stored in the credit memory (26) of the postage meter machine (12) and the value stored in the debiting memory (46) of the data centre.

2. The method according to claim 1, **characterized in that** an abbreviated code number is formed from each cryptomessage prior to its communication and this code number is communicated.

3. The method according to claim 2, **characterized in that** an identification number identifying the postage meter machine (12) is entered into the postage meter machine (12) and **in that** during the first transaction a first code number is formed in the postage meter machine (12) by means of a key (K1) using the identification number, the entered selected amount and an additional information, the identification number, the desired selected amount and the additional information are communicated to the data centre (18) together with the first code number, the first code number is verified in the data centre (18) and the desired selected amount is stored in the selected amount memory (45) of the data centre (18), a second code number is formed in the data centre (18) by means of a key (K2) using the identification number and the additional information and is communicated to the postage meter machine (12) and the second code number is verified in the postage meter machine (12), whereupon in the case of a successful verification of the second code number the desired selected amount is stored in the selected amount memory (28) of the postage meter ma-

chine (12).

4. The method according to one of the claims 2 to 3, **characterized in that** during the second transaction a third code number is formed in the postage meter machine (12) by means of a key (K2) using the identification number and an additional information and is communicated to the data centre, the third code number is verified in the data centre (18) and in the case of a successful verification the selected amount stored in the selected amount memory (45) of the data centre (18) is added to the value stored in the debiting memory (46) of the data centre (18), a fourth code number is formed in the data centre (18) by means of a key (K3) using the identification number and the additional information and is communicated to the postage meter machine (12), and the fourth code number is verified in the postage meter machine, whereupon after successful verification the selected amount stored in the selected amount memory (28) of the postage meter machine is added to the value stored in the credit memory (26) of the postage meter machine (12).
5. The method according to one of the claims 2 to 4, **characterized in that** a key used for the determination of the code numbers is changed after each terminated transaction.
6. The method according to one of the claims 2 to 5, **characterized in that** during each transaction the code number formed in the postage meter machine (12) is calculated by means of a key (K1) present after the termination of the preceding transaction, **in that** the code number formed in the data centre is calculated by means of the same key (K2), and **in that** the new key (K2) is stored in the data centre, is communicated to the postage meter machine as part of the code number communicated from the data centre (18) and is stored in the postage meter machine (12) after verification of this code number.
7. The method according to claim 6, **characterized in that** in the case in which a code number communicated to the data centre (18) from the postage meter machine (12) cannot be verified in the data centre (18), the verification is repeated by means of the key (K1) used prior to the last change of key, and **in that** in the case of a successful verification of the code number the last transaction is corrected with the aid of this key (K1).
8. The method according to one of the claims 3 to 7, **characterized in that** after entering the identification number the type of communication procedure between the postage meter machine and the data centre is selected by actuation of at least one selection key (58).
9. An electronic postage meter machine, comprising an electronic data processing device (22) having a credit memory (26) for storing a postage credit and a selected amount memory (28) for the permanent storing of a selected amount by which the postage credit can be modified, and a printer device (38) connected to the data processing device (22) for printing postage values, a data display device (36), an input device (34) for entering postage values to be printed and a device for setting a credit reloading mode in which, after entry and verification of a reloading code number, the selected amount stored in the selected amount memory (28) is added to the postage credit, **characterized by** means (52) for setting a change of value mode in which the selected amount permanently stored in the selected amount memory (28) and displayed in the data display device (36) is optionally confirmed unmodified or can be replaced by a modified selected amount entered into the postage meter machine (12) in a self-contained transaction after entry and verification of a change of value code number.
10. The postage meter machine according to claim 9, **characterized in that** the data processing device (22) comprises a cryptographic device for generating and/or verifying code numbers.
11. The postage meter machine according to claim 10, **characterized in that** the cryptographic device (30) comprises a memory (32) for at least one key (K1, K2...).
12. The postage meter machine according to one of the claims 9 to 11, **characterized in that** the change of value mode can be set by the entry of an identification number identifying the postage meter machine (12) and the actuation of a first special function key (52).
13. The postage meter machine according to one of the claims 9 to 12, **characterized in that** it can be switched from the change of value mode to a franking mode by the actuation of a second special function key (54).
14. The postage meter machine according to one of the claims 9 to 13, **characterized in that** the reloading mode can be set after setting of the change of value mode by the actuation of a third special function key (56).
15. The postage meter machine according to one of the claims 9 to 13, **characterized in that** the reloading mode can be set after setting the change of value mode by the actuation of the first special function key (52).

16. The postage meter machine according to one of the claims 9 to 15, **characterized by** at least one selection key (58) for selecting the communication procedure between the postage meter machine and the data centre.

5

### Revendications

1. Procédé d'adaptation du fichier de données dans le dispositif de traitement de données (22), comprenant une mémoire de crédit (26) pour un crédit de port, d'une machine à affranchir électronique (12) et dans le dispositif de calcul (42) d'une centrale de données (18), comprenant une mémoire de décompte (46) pour la machine à affranchir, selon lequel

10

- l'adaptation du fichier de données s'effectue en deux transactions fermées sur elles-mêmes, pour mémoriser fixement une valeur donnée valable ou pour recharger avec cette valeur, et dans la première transaction est réglé sur la machine à affranchir (12) un mode de modification de valeur selon lequel, au choix soit la valeur donnée enregistrée est confirmée sans modification et la transaction achevée sans que soit effectuée une modification de valeur, soit pour modifier une valeur donnée mémorisée et affichée dans la machine à affranchir, par échange de messages chiffrés ou de cryptomessages entre la machine à affranchir (12) et la centrale de données (18), une nouvelle valeur donnée entrée dans la machine à affranchir est transmise à la centrale de données (18) et enregistrée dans une mémoire de valeurs données (28, 45) correspondante de la machine à affranchir (12) et de la centrale de données (18),
- après achèvement de la première transaction, est mis au choix un mode d'affranchissement ou un mode de rechargement, tandis que dans une seconde transaction, comprenant l'échange de cryptomessages entre la machine à affranchir (12) et la centrale de données (18), la valeur donnée enregistrée dans la mémoire de valeurs données (28) correspondante est ajoutée à la valeur enregistrée dans la mémoire de crédit (26) de la machine à affranchir (12) et à la valeur enregistrée dans la mémoire de décompte (46) de la centrale de données.

20

25

30

35

40

45

50

2. Procédé selon la revendication 1, **caractérisé en ce qu'un** nombre codé raccourci est formé à partir de chaque message crypté avant la transmission de celui-ci, et ce nombre est transmis.

55

3. Procédé selon la revendication 2, **caractérisé en**

### ce que

- dans la machine à affranchir (12) est entré un nombre d'identification la caractérisant et pendant la première transaction dans cette machine, en utilisant le nombre d'identification, la valeur donnée entrée et une information additionnelle, un premier nombre codé est formé au moyen d'un code (K1),
- le nombre d'identification, la valeur donnée désirée et l'information additionnelle sont transmis avec le premier nombre codé à la centrale de données (18) dans laquelle ce nombre est vérifié tandis que la valeur donnée désirée est enregistrée dans la mémoire de valeurs données (45) de la centrale de données (18),
- en utilisant le nombre d'identification et l'information additionnelle, un deuxième nombre codé au moyen d'un code (K2) est formé dans la centrale de données (18) et transmis à la machine à affranchir (12) dans laquelle il est vérifié, et dans le cas de vérification positive de ce deuxième nombre codé, la valeur donnée désirée est enregistrée dans la mémoire de valeurs données (28) de la machine à affranchir (12).

4. Procédé selon la revendication 2 ou 3, **caractérisé en ce que**

- pendant la seconde transaction, est formé dans la machine à affranchir (12), en utilisant le nombre d'identification et une information additionnelle, un troisième nombre codé au moyen d'un code (K2), et ce nombre est transmis à la centrale de données (18) où il est vérifié et, dans le cas de vérification positive, la valeur donnée enregistrée dans la mémoire de valeurs données (45) de la centrale de données (18) est ajoutée à la valeur enregistrée dans la mémoire de décompte (46) de la centrale de données (18),
- en utilisant le nombre d'identification et l'information additionnelle, un quatrième nombre codé est formé dans la centrale de données (18) au moyen d'un code (K3) et transmis à la machine à affranchir (12) où il est vérifié et, en cas de vérification positive, la valeur donnée enregistrée dans la mémoire de valeurs données (28) de la machine à affranchir est ajoutée à la valeur enregistrée dans la mémoire de crédit (26) de la machine à affranchir (12).

5. Procédé selon une des revendications 2 à 4, **caractérisé en ce qu'un** code utilisé pour établir les nombres codés est modifié après l'achèvement de chaque transaction.

6. Procédé selon une des revendications 2 à 5, **caractérisé en ce que** pendant chaque transaction, le nombre codé formé dans la machine à affranchir (12) est calculé en utilisant un code (K1) présent après achèvement de la transaction précédente, le nombre codé formé dans la centrale de données est calculé au moyen du même code (K2), et ce nouveau code (K2) est enregistré dans la centrale de données, puis est transmis en tant que partie du nombre codé provenant de la centrale de données (18) à la machine à affranchir (12) dans laquelle il est enregistré après vérification.
7. Procédé selon la revendication 6, **caractérisé en ce que** dans le cas où un nombre codé transmis de la machine à affranchir (12) à la centrale de données (18) ne peut être vérifié dans celle-ci, la vérification par l'intermédiaire du code (K1) utilisé avant le dernier changement de code, est répétée et en cas de vérification positive de ce nombre, la dernière transaction est corrigée au moyen de ce code (K1).
8. Procédé selon une des revendications 3 à 7, **caractérisé en ce qu'**après entrée du nombre d'identification, le genre du processus de communication entre la machine à affranchir et la centrale de données est sélectionné en actionnant au moins une touche de sélection (58).
9. Machine à affranchir électronique comprenant un dispositif électronique de traitement de données (22) avec une mémoire de crédit (26) pour enregistrer un crédit de port et une mémoire de valeurs données (28) pour enregistrer fixement une valeur donnée par laquelle peut être modifié le crédit de port, un dispositif d'impression (38) relié au dispositif de traitement de données (22) pour imprimer les valeurs de port, un dispositif d'affichage de données (36), un dispositif d'entrée (34) pour entrer des valeurs de port à imprimer et un dispositif de réglage d'un mode de recharge de crédit, dans lequel, après entrée et vérification d'un numéro de code de recharge, la valeur donnée enregistrée dans la mémoire de valeurs données (28) est ajoutée au crédit de port, **caractérisée par** des moyens (52) de mettre un mode de modification de valeur, dans lequel la valeur donnée, enregistrée fixement dans la mémoire de valeurs données (28) et indiquée dans le dispositif d'affichage de données (36), est au choix confirmée sans modification ou peut, au cours d'une transaction fermée sur elle-même, être remplacée, après entrée et vérification d'un numéro de code de modification de valeur, par une valeur donnée modifiée entrée dans la machine à affranchir (12).
10. Machine à affranchir selon la revendication 9, **caractérisée en ce que** le dispositif de traitement de données (22) possède un dispositif cryptographique (30) pour établir et/ou pour vérifier des numéros de code.
11. Machine à affranchir selon la revendication 10, **caractérisée en ce que** le dispositif cryptographique (30) possède une mémoire (32) pour au moins un code (K1, K2...).
12. Machine à affranchir selon une des revendications 9 à 11, **caractérisée en ce que** le mode de modification de valeur peut être réglé en entrant un nombre d'identification caractérisant la machine à affranchir (12) et en actionnant une première touche spécifique (52).
13. Machine à affranchir selon une des revendications 9 à 12, **caractérisée en ce qu'**en actionnant une deuxième touche spécifique (54), la machine peut passer du mode de modification de valeur à un mode d'affranchissement.
14. Machine à affranchir selon une des revendications 9 à 13, **caractérisée en ce qu'**en actionnant une troisième touche spécifique (56), la machine peut passer du mode de modification de valeur à un mode de recharge.
15. Machine à affranchir selon une des revendications 9 à 13, **caractérisée en ce qu'**en actionnant la première touche spécifique (52), la machine peut passer du mode de modification de valeur à un mode de recharge.
16. Machine à affranchir selon une des revendications 9 à 15, **caractérisée en ce qu'**au moins une touche de sélection (58) est prévue pour sélectionner le processus de communication entre la machine à affranchir et la centrale de données.

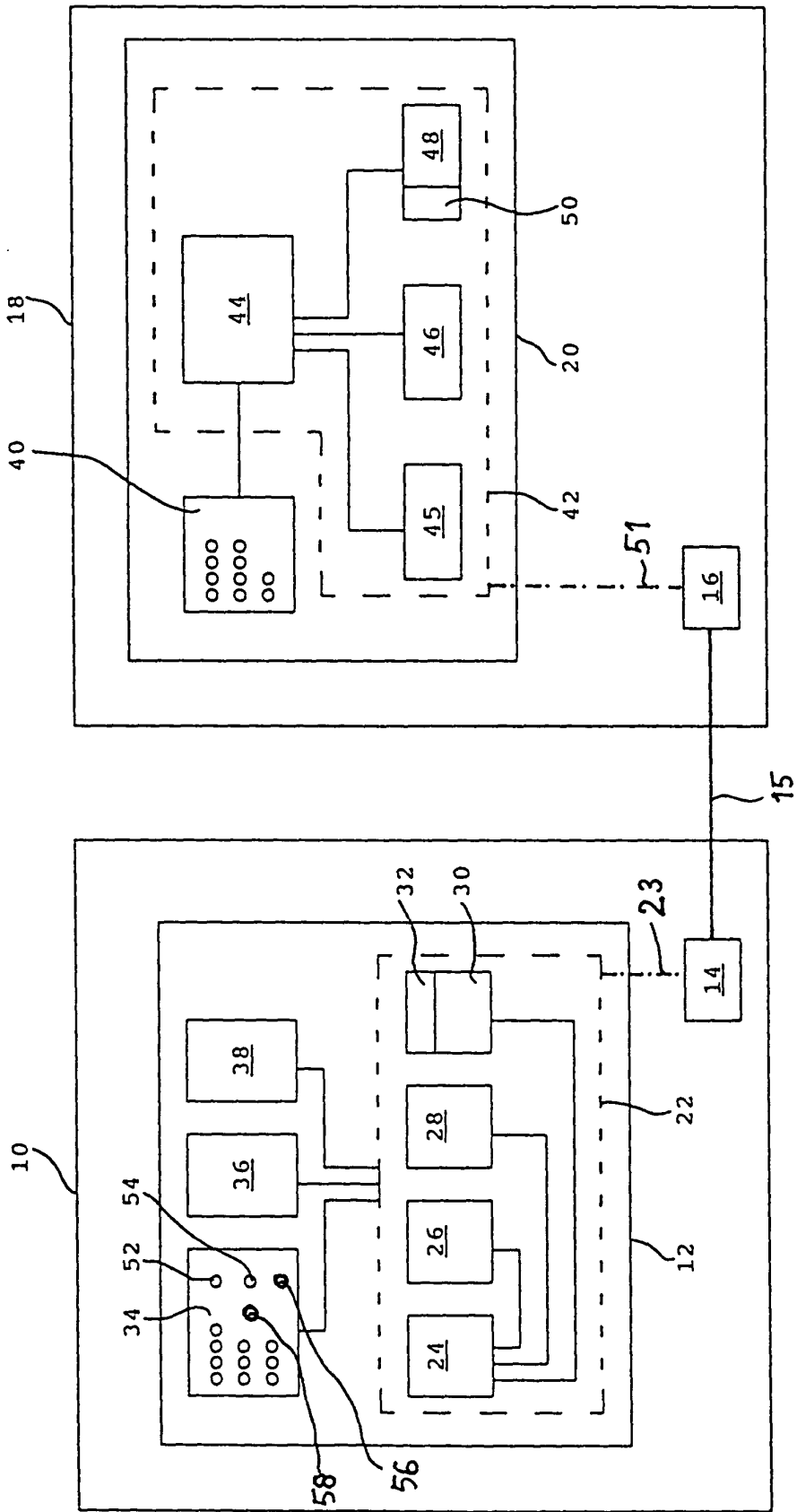


Fig. 1

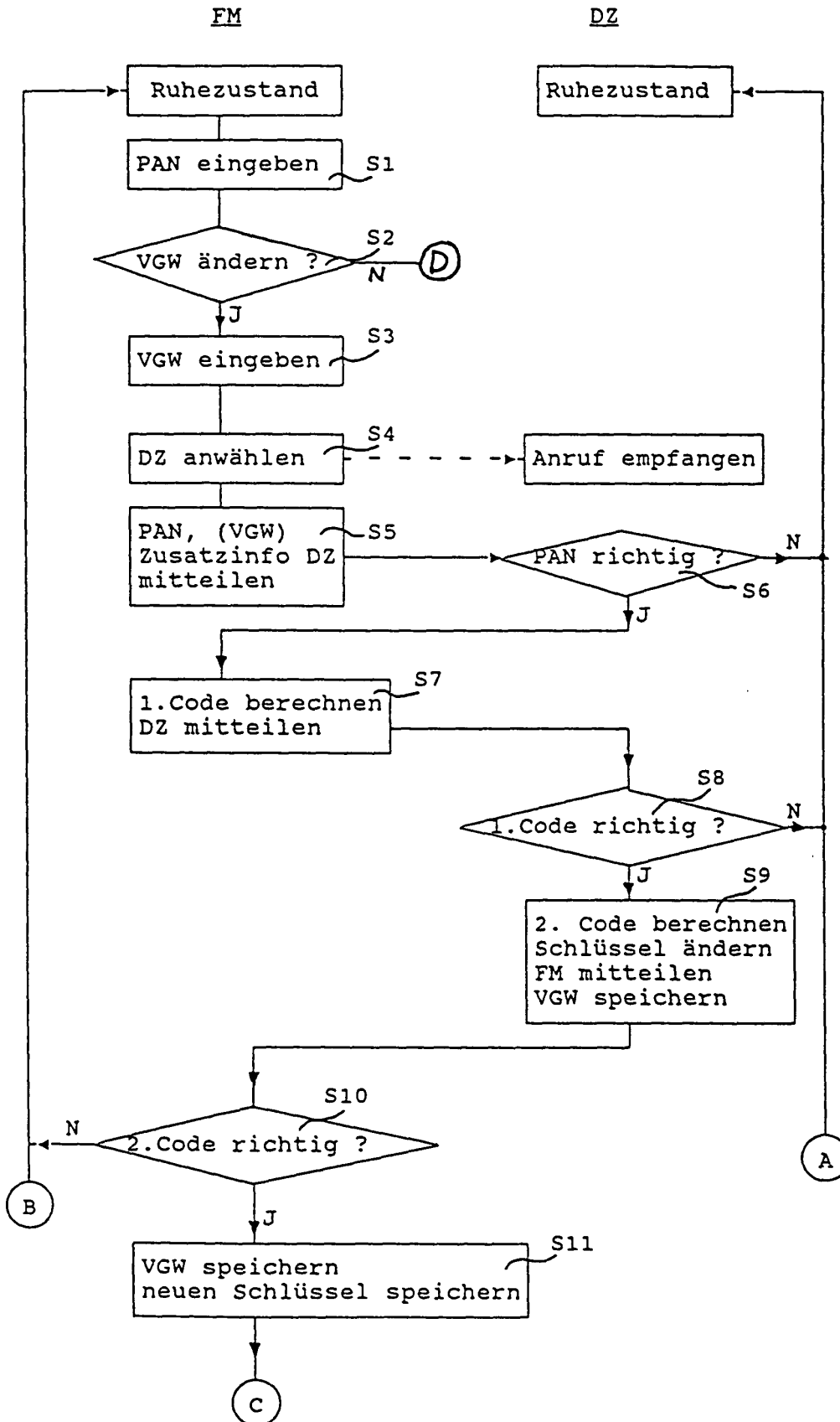


Fig. 2a

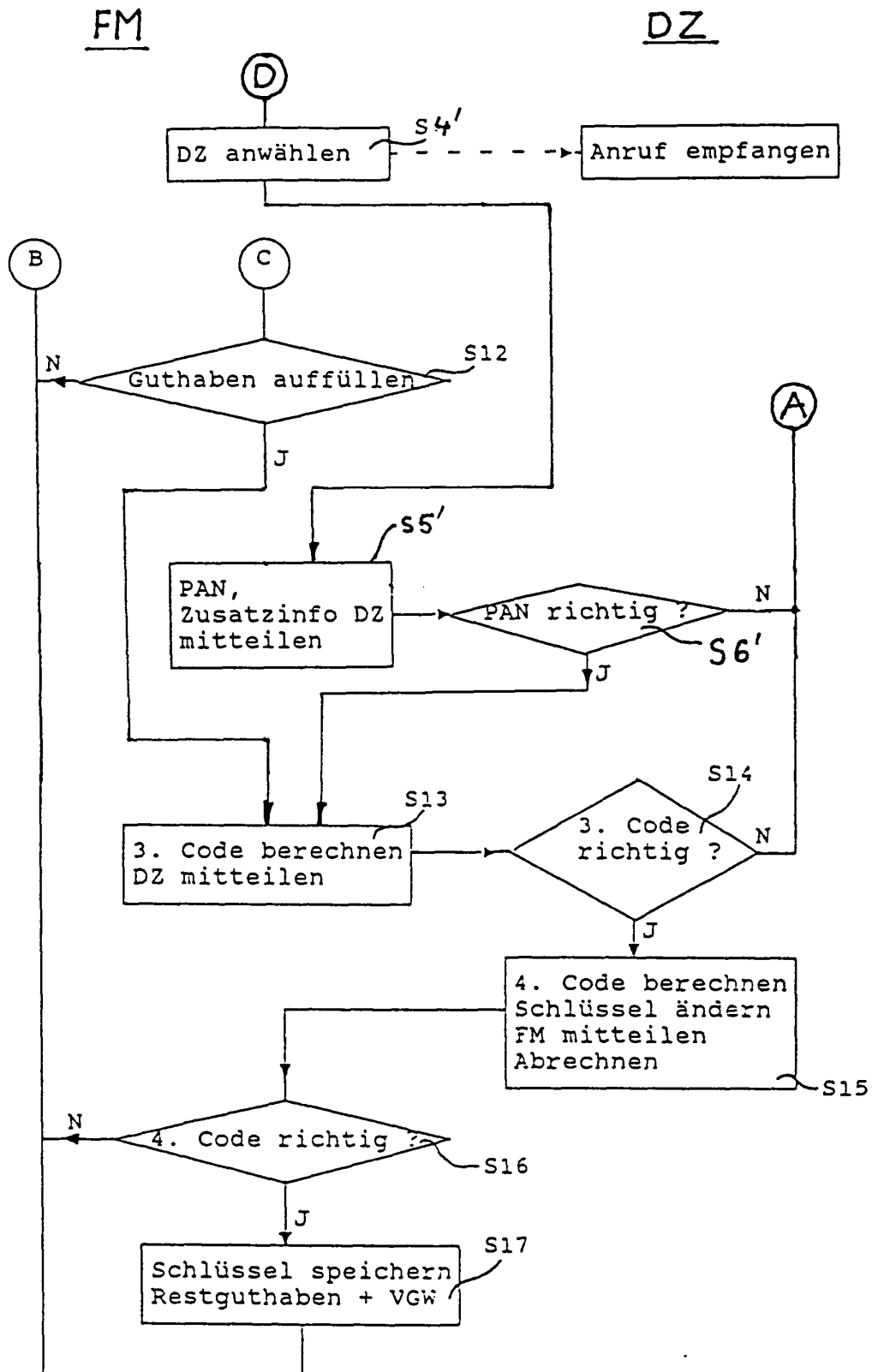


Fig. 2b

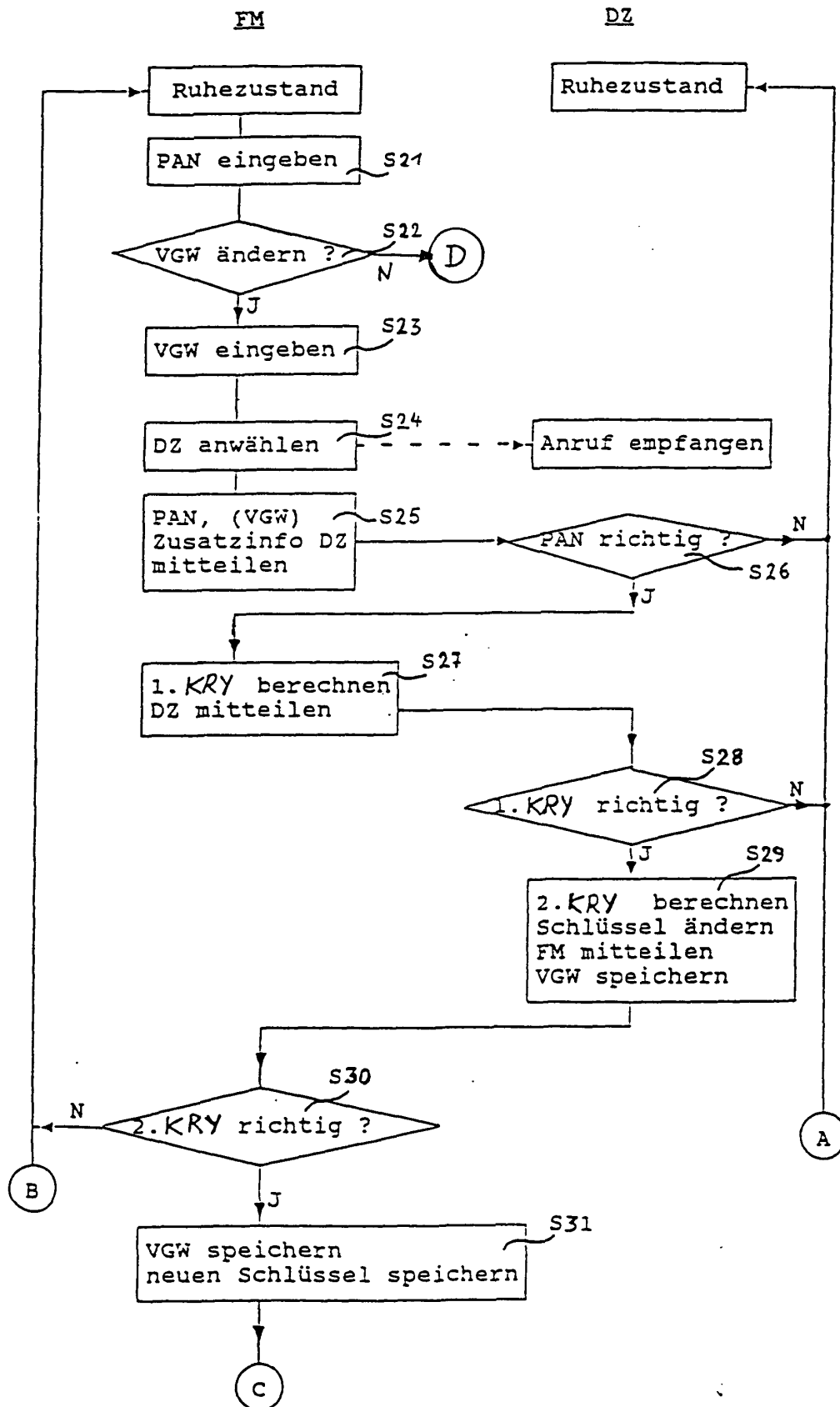


Fig. 3a

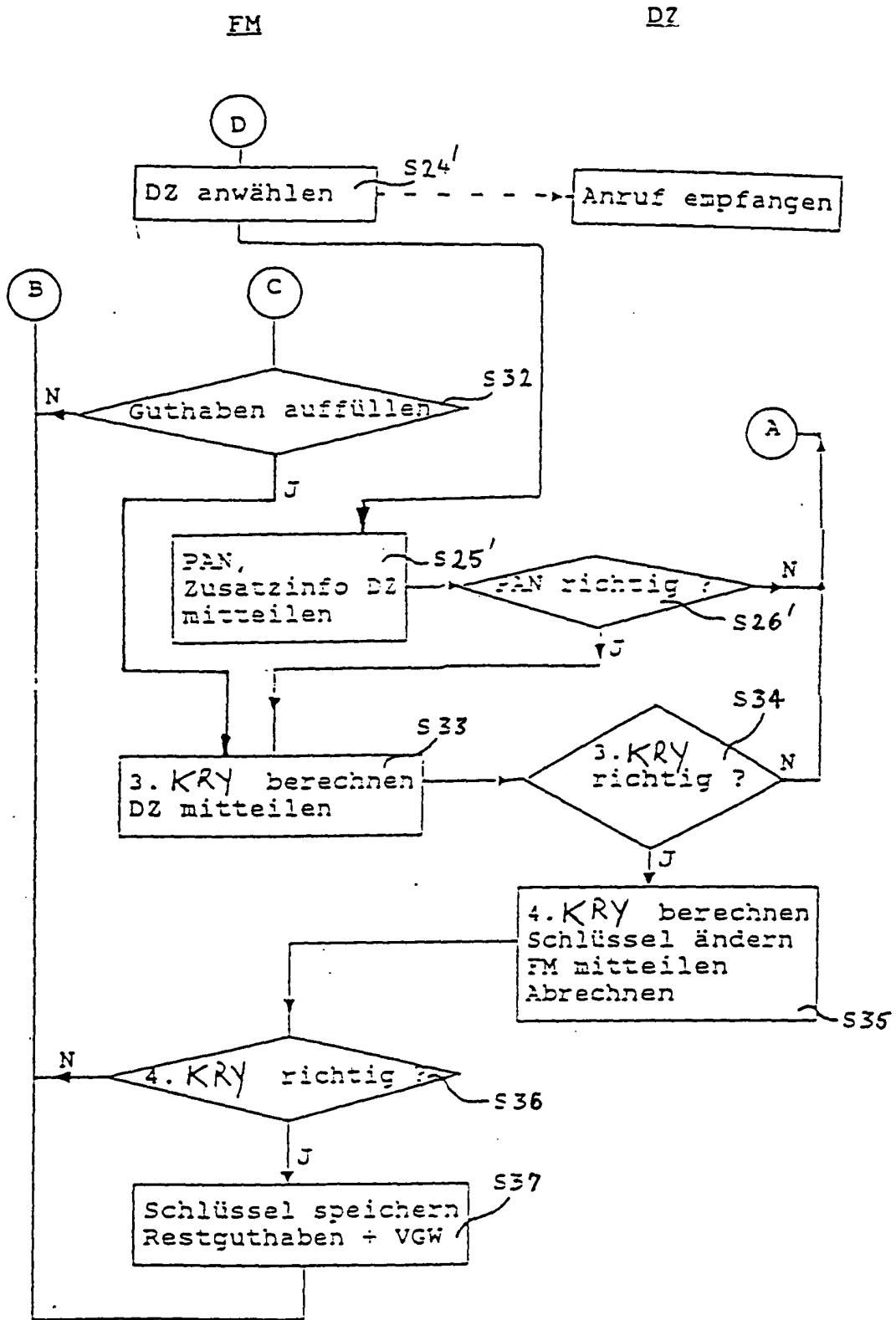


Fig. 3b

Fig.4

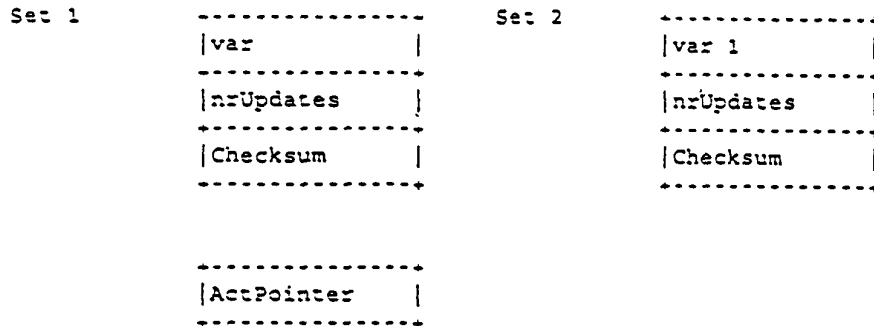


Fig.5

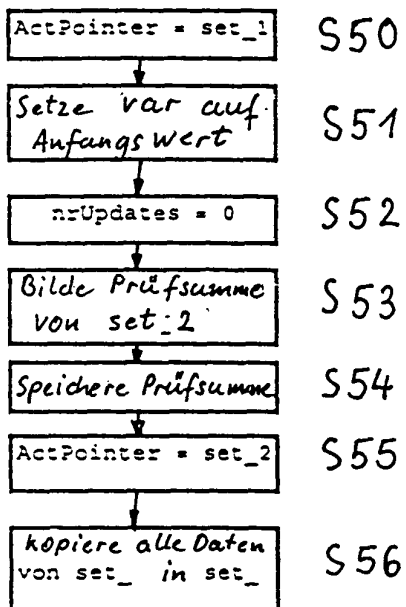


Fig.6

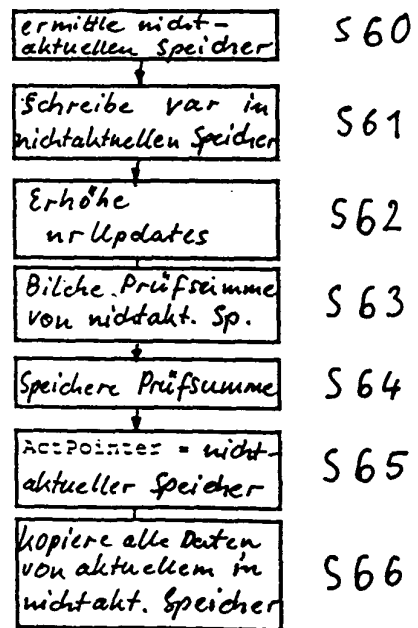


Fig 7

